EPRI ELECTRIC POWER RESEARCH INSTITUTE

IntelliGrid Newsletter

An EPRI Progress Report **September 2011**

About the Newsletter

The IntelliGrid program conducts research and development in the area of communications, data integration and cyber security to support smart grid applications in the transmission, distribution and consumer domains. The program provides results that can meet the near-term needs of our members and makes contributions that will advance the industry towards an interoperable, integrated smart grid.

This newsletter provides results from on-going and recently completed projects, status reports on current projects, plans for future projects and information on relevant industry activities.

Save the date

IntelliGrid Advisors Meeting, February 13-15 in Huntington Beach, California. The meeting will include demonstrations of IntelliGrid projects, utility presentations on implementation of IntelliGrid results and more.

SECURITY FOR POWER SYSTEM COMMUNICATIONS, INFORMATION & CONTROL

Lemnos Interoperable Security Demonstration and Evaluation

The manner in which the energy sector is designing and operating control systems is undergoing some of the most significant changes in history due to the evolution of technology and the increasing exposure to external networks and systems. These changes make cyber security a more important issue than ever before. A key requirement in helping utilities and vendors meet these challenges is interoperability.

In theory, interoperability is possible with many of the cyber security solutions available to utilities today. For example, consider IPsec, a widely-used Internet Protocol to define Virtual Private Networks, or “tunnels”, to communicate securely through untrusted public and private networks. The IPsec protocol suite has a significant number of configuration options and encryption parameters to choose from, which must be agreed upon and adopted by both parties establishing the tunnel. The exercise in getting software or devices from different vendors to interoperate is labor intensive and requires a significant amount of security expertise by the end user. Scale this effort to a significant number of devices operating over a large geographical area and the challenge may lead utilities to pursue solutions from a single vendor. These single vendor solutions may inadvertently lock utilities into proprietary solutions. The United States Department of Energy (DOE) sponsored Lemnos project is addressing this need by developing Interoperable Configuration Profiles for various cyber security related functions. These Profiles are being transitioned to the CyberSec Interop Task Force under the OpenSG subcommittee of the UCA International Users Group for long term stewardship.

This project is demonstrating the outputs of the Lemnos Interoperable Security project, the IPsec, SSH, and LDAP Interoperable Configuration Profiles within the EPRI Smart Grid Substation Lab in a multi-vendor configuration.

The following milestones have been accomplished to date in 2011:

- **Vendor Testing.** The original scope of this EPRI project focused only on the IPsec Interoperable Configuration Profile developed by the Lemnos project. The scope of the EPRI project was expanded to cover testing of SSH, LDAP and Syslog Interoperable Configuration Profiles as well. During the development of the Interoperable Configuration Profiles (ICP) in the Lemnos project, testing is mainly limited to the SEL-3620 Ethernet Security Gateway and the Sandia National Labs OPSAID reference design. In order to vet the ICPs further, interoperability testing with several vendors systems is necessary. On June 1 and 2, 2011, representatives from EPRI, EnerNex, Sandia National Labs, SEL, n-dimension, Encore Networks, Cisco met at the EPRI Smart Grid Substation Labs in Knoxville, TN and conducted testing mainly centered on IPSec and SSH connections between the various vendor combinations.

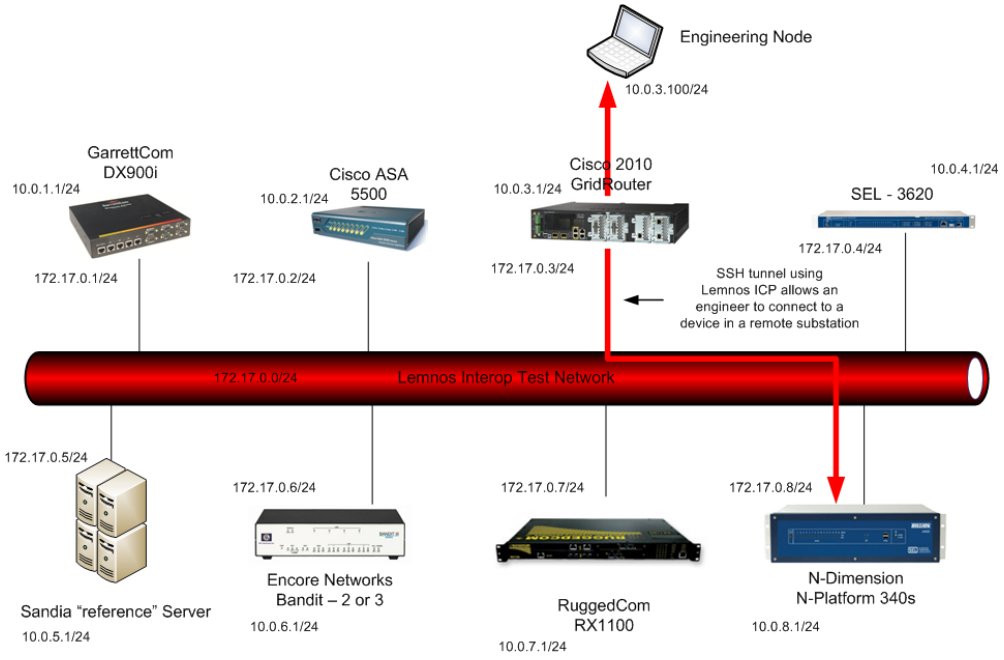

Figure 1 - Typical SSH Test

- **Interoperability Demonstration**. EPRI conducted follow up interoperability testing in an open industry event at the EPRI Smart Grid Substation Lab in Knoxville, TN on August 11th 2011. This testing demonstrated all 4 security protocols (IPsec, SSH, LDAP, Syslog) and focused on outreach to communicate the benefits of the work to the industry stakeholders. There were over 40 attendees at the event including DoE technical staff, utilities, vendors, national labs, commercial labs, integrators and individual subject matter experts.

Interoperable Configuration Profiles are developed to describe a specific instantiation of a particular security related protocol. The hypothesis of the DOE Lemnos work is that if a vendor independently implements a security function based on an Interoperable Configuration Profile and tests it against the reference implementation developed and maintained by Sandia National Laboratories, that product should interoperate with any other product which has done the same. This process alone is not sufficient however to ensure the effectiveness of the Interoperable Configuration Profiles and therefore additional testing must be conducted and corresponding conformity goals must be developed. Once adopted, the Interoperable Configuration Profiles will make it easier to procure and implement secure systems, reducing the cost of integration, facilitating competition among the vendor community to reduce prices, and minimizing the cost of configuring and maintaining devices supporting cyber security functions over their lifetime. This EPRI project is providing valuable feedback to the DOE Lemnos team as well as to OpenSG on the effectiveness and usability of the Interoperable Configuration Profiles.

For more information on this project, please contact Erfan Ibrahim (eibrahim@epri.com) or (925) 785-5967.

DNP3 Security Interoperability Testing

The Distributed Network Protocol (DNP3) is the most widely used utility communications protocol in North America. Ensuring that DNP3 communications are secure is an important goal for the power industry. EPRI is working to facilitate conformance and interoperability testing between DNP3 suppliers who implement the specification. Also, the applicable DNP3, IEC and IEEE standards must be updated.

Previous EPRI projects have enabled the completion of version 3 of the DNP3 Secure Authentication specification and a draft framework (test approach and list of approximately two hundred possible tests) for conformance testing of this specification. Work remains to complete the conformance test procedures and to add procedures for interoperability testing between devices. Once these procedures are complete, testing of actual DNP3 devices can take place.

Before the test procedures can be completed, however the specifications must be updated. There are several reasons for these updates:

- Since version 3 of the DNP3 Secure Authentication specification was released in early 2010, suppliers have encountered several technical concerns while implementing the protocol..

- The specification has come under the review of the Cyber-Security Working Group (CSWG) of the NIST Smart Grid Interoperability Panel, and they have discovered vulnerabilities that must be mitigated before the specification can be approved.

Both of these sets of changes must be migrated back into the IEC 62351-5 and IEC 60870-5-7 specifications that the DNP3 work was based on. This must take place before the release of those specifications can proceed.

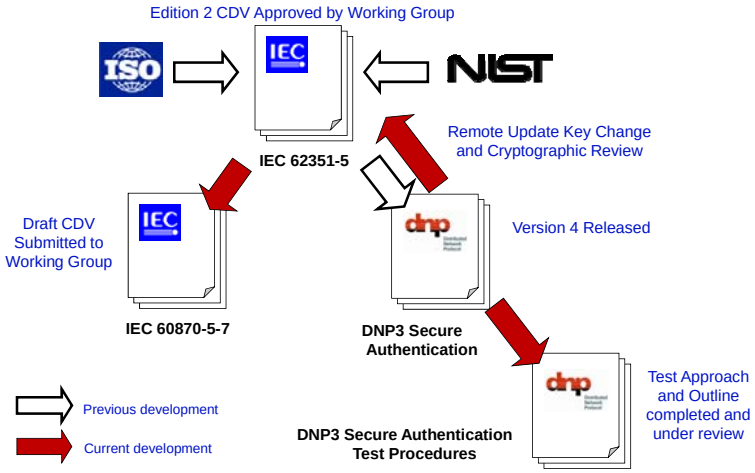

Figure 2 – Current Status of Secure Authentication Specifications

The following milestones have been achieved in 2011:

- Common Certificate Format. The IEC working group in charge of data communications security was about to submit for balloting a draft of IEC 62351 Part 8 on Role-Based Access Control. This specification contains a proposed X.509 standard-based cryptographic certificate format to be used by all utility protocols managed by the IEC, such as IEC 60870-6 (ICCP), IEC 61850, and IEC 60870-5 and would be a major aid to interoperability. EPRI contractors facilitated meetings between the IEC security working group (TC57 WG15) and

the DNP Technical Committee to ensure DNP3 could use the same standard certificate format. This format was resolved in teleconferences ending March 7, 2011.

- Backward Compatibility Report. With the release of version 4, some implementers who had already deployed version 2 became concerned that they could not deploy mixed networks including both version 2 and version 4 equipment. After considerable discussion in the DNP Technical Committee, the committee decided to produce a report on the differences between the two versions, and recommended guidelines for addressing these differences in mixed networks.

- Vulnerability Report and Solution. As a part of the work done by this project to release new drafts of the IEC 62351-5 and 60870-5-7 specifications, members of the IEC security working group identified some security vulnerabilities in the DNP3 Secure Authentication version 4 specifications. These members are also members of the NIST Smart Grid Interoperability Panel (SGIP) cyber-security working group (CSWG) and therefore noted that DNP3 Secure Authentication would not pass an SGIP review if these vulnerabilities were not addressed. As a part of this project, EPRI contractors produced a summary of the vulnerabilities and submitted this summary to the DNP technical committee, the IEC security working group, and the NIST CSWG. Several design meetings have been held with the CSWG and a proposed solution has been agreed upon as of June 10, 2011.

- Work on Detailed Test Procedures. While the revisions to the specifications described previously were progressing, ten of the approximately two hundred tests in the testing framework were drafted. These included the “quick check” and “initialization” tests.

When completed, this project will have accomplished the following:

- Produce DNP3, IEC 62351-5, and IEC 60870-5-7 specifications that resolve the security vulnerabilities that have been identified by the IEC and SGIP working groups.

- Incorporate the DNP3 changes into the IEEE 1815 standardization process that will produce the next edition in 2012.

- Finish the first draft of the Secure Authentication Test Procedures based on the revised specifications.

For more information on this project, please contact Erfan Ibrahim (eibrahim@epri.com) or (925) 785-5967.

EPRI’s Involvement in IEEE 802 Standards Development

The May issue of the IntelliGrid newsletter contained an article on IEEE 802.16 standards development related to the Smart Grid and the Field Area Network. This issue continues the discussion with IEEE 802.15.4 and 802.11.

The IEEE 802.15.4 standard is the basis for ZigBee, which is used in home automation, Smart Meters, and HAN devices. The IEEE 802.15.4 standard specifies only the lower layers (MAC and PHY) in the stack. The remaining functionality is specified by the ZigBee Alliance, which is a commercial trade organization and not an open standards development organization like the IEEE.

In a divergence from the 802.15 charter for the Personal Area Network, the 802.15.4g amendment defines new physical layers (PHYs) specifically for smart metering. These PHYs are intended to

operate outdoors over neighborhood-scale ranges. The standard is called Smart Utility Network (SUN), and the scope is to support “large, geographically diverse networks with minimal infrastructure, with potentially millions of fixed endpoints.” The 802.15.4g Task Group has representatives from utilities and meter vendors, among others. The 802.15.4g standard is in the final phase of the standards development process – it was submitted for Sponsor Ballot at the July 2011 meeting. It contains three different PHY options. Two represent “legacy” AMI systems that are already in the field. The third uses the modern OFDM modulation to provide a growth path. To address concerns about interoperability and interference between the PHYs in the 802.15.4g standard (and legacy advanced metering infrastructure (AMI) systems), the task group has introduced coexistence mechanisms. These include a mandatory common signaling mode (CSM) and a coexistence beacon that is periodically transmitted using the CSM.

EPRI has participated in the development of 802.15.4e, which specifies a diverse set of enhancements to the 802.15.4 MAC layer. Some of the new functions are not relevant to smart grid applications, but some are needed to support 802.15.4g. Other communication standards’ MAC layers provide performance measurements and metrics to support network management functions. EPRI identified the lack of MAC layer performance metrics in 802.15.4, and developed a proposal that was adopted in 802.15.4e. These metrics will be useful in 802.15.4g AMI applications as well as standard 802.15.4 (e.g. ZigBee) applications in the HAN. The 802.15.4e standard is on the same timetable for adoption as 802.15.4g. Both are on similar schedules for final approval – possibly by the end of 2011, but probably early 2012 (depending on the number of Sponsor Recirculation Ballots that are required).

The 802.11 standard has achieved a tremendous level of market success, and Wi-Fi is now ubiquitous in devices from notebook computers and phones to TVs and cameras. The 802.11 industry has been focused on these markets, and has not developed a significant market presence in Smart Grid applications to date. That is beginning to change with the 802.11ah amendment that will extend 802.11 to Sub-1GHz frequency bands. Many AMI systems are currently deployed in the 915MHz ISM band, and that band is one that is supported by 802.15.4g. The advent of 802.11ah devices in the same band would enable 802.11 to address the AMI market. This standard could become relevant to utilities in other applications above and beyond AMI, however. The combination of 802.11ah with the 802.11s mesh network standard will enable meshed Field Area Networks. These can cover wide areas and provide broadband services to support distribution automation, distributed resources integration, and other smart distribution applications. Although the 802.11ah standard development is just beginning and the data rates are not specified, it is virtually certain that the standard will provide significantly higher rates than 802.15.4g.

The involvement of EPRI in the standards development process provides a dual benefit. First, there is the direct visibility and exposure to the process and the people involved. The true pace and schedule is apparent from the inside, and the participants are very open about facts that would be considered confidential in other forums. Second, we have the ability to influence the requirements and direction of the standards to the benefit of our members.

For more information on this project, please contact Tim Godfrey at tgodfrey@epri.com or (650) 855-8584.

CIM – MultiSpeak® Harmonization

Multiple standards that cover the same information domain present a problem for the vendor community when developing products to serve the industry. The classic challenge becomes one of determining which standards to support or how best to support one or both standards. Harmonization involves performing a mapping from one standard to another. Harmonization is used when the two standards communities are well entrenched in their respective products and customers. Where flexibility exists or the standards are not yet fully developed, a unification approach is possible.

Unification is the blending of two disparate standards into one. Until one of these processes has been fully completed, the prevention of vendor lock-in will not be possible.

At present there are two leading standards for distribution-related software interoperability in the electric utility industry: MultiSpeak® and IEC 61968, the Common Information Model (CIM) for distribution, which is maintained by Technical Committee 57 (TC57) of the International Electrotechnical Commission (IEC). The two standards have been developed by different committees that have some overlap in membership. As a result, the two standards cover much of the same material, but in different manners. Multiple standards are important to the creation of the smart grid, and standards are generally optimized along a given direction due to the differing needs of the respective stakeholders. Both standards have a long, rich history and extensive implementations. Hence, a unification approach is not possible and so harmonization is being attempted.

When faced with how to harmonize two different standards that cover the same domain one typically looks at how to map from one class or set of attributes to the classes and attributes presented in the other standard. While having two products separated by competing standards is a problem, having a product based on a completely proprietary interface is worse. With a proprietary interface there is no hope of a future resolution, the interface will always be a custom solution, which, all things being equal, increases maintenance costs.

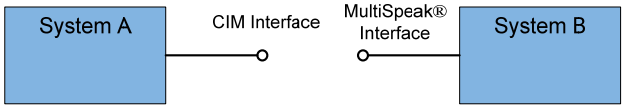

Figure 3: The classic gap in a point-to-point solution when vendors support differing standards

With the situation seen in Figure 1, the organization will typically need to buy systems that support the chosen interface (unlikely in the heterogeneous landscapes of most enterprises), or do a data transformation to support a given interface.

The project is currently about 2/3 complete. Most of the CIM profiles have been mapped to MultiSpeak and issues are being logged to be addresses by one standards community or the other. It is expected to have the project done by the end of October, 2011.

For more information on this project, please contact John Simmins at jsimmins@epri.com or (865) 218-8110.

Field Force Data Visualization

The communication of information from the operations center to the field and back has long been an issue. Whereas simple commands such as switching operations have had protocols for decades, more complex concepts have not easily been communicated. The spatial relationship between grid elements, visual data, terrain and weather (among other) concepts have not been so easy to transmit and understand.

Utilities continually struggle with justifying the investment in information technology. Inaccurate data, lack of standards, vendor “lock-in” all prevent the cost effective use of their technology investment. Data exists in disparate systems, inaccessible to the operations center and field personnel. Mobile computer power is wasted displaying out of date or irrelevant data. Data is not used because it is not available in the vendor specific software that is loaded on the mobile computing device. In short, the investment made in IT by utilities has yet to reach its full potential. To fully realize the potential promised in the investing in IT, a standards based IT architecture is needed for the visualization of data and the use of visual data in the decision making process.

Fortunately, as utilities begin to integrate systems that previously operated with little or no data interconnection, it becomes easier to link together related data. This can result in powerful diagnostic and management tools to be created that use this interconnected data to all field personnel to better understand the network and the context of any unexpected behavior. Emerging standards such as CIM and MultiSpeak® provide the back-bone of such tools.

Figure 1: Mock up of a light-weight, field force data access platform showing several different types of information in the same environment.

A key use-case could be to allow a field crew out in the field to be able to identify all relevant data for the network at the crew's current location. From this interface they could navigate through all the data for a transformer, identify its location in the GIS and a single-line, be shown the down-stream circuit on a map, trace into its asset history, maintenance history, manufacturer information and catalogue etc. Upon arriving in a street, the GIS and magnetometer (compass) built into a tablet would identify the crew's location and holding up the tablet would allow them to and see in real-time a video of the area with data on the view; on a single line diagram and on the map (see Figure 1). The crew member could query as to the state of a switch, identify premises with outages, automatically tag devices, etc. This would all be possible with properly integrated data environment and accurate GIS data.

EPRI is developing a field force tool on an iOS (think iPad or iPhone) platform based in the Common Information Model (CIM) for messaging. The advantages of such a platform include:

- Cost – this platform is considerably cheaper than a tough-book style laptop.
- Simplicity – upgrades to iOS devices are simple and can be done in the field.
- Communication – iOS devices typically switch from Wi-Fi to cellular communications and back without issue.

The base functionality is being developed in an EPRI base project with implementations and augmentation of capability being performed in targeted supplemental project. The work has started on this project and additional participants are welcome.

A video that illustrates this concept can be found at http://www.youtube.com/watch?v=Jnnq8V92rtw

For more information on this project, please contact John Simmins at jsimmins@epri.com or (865) 218-8110.

California Utility Vision and Roadmap for the Smart Grid of Year 2020

EPRI has recently published the California Utility Vision and Roadmap for the Smart Grid of 2020 (**1022220**). This report presents a vision for the California Smart Grid of 2020 and a roadmap that defines pathways for achieving that vision. Reflecting the consensus of California's major investor-owned utilities, the vision and roadmap provide clarity and direction to support California energy

policies by defining key capabilities and needs in six broad technical areas known as domains: (1) communications infrastructure and architecture, (2) customer systems, (3) grid operations and control, (4) renewables and distributed energy resources integration, (5) grid planning and asset efficiency, and (6) workforce effectiveness.

The project team synthesized utility perspectives on the progressive development of the California Smart Grid in light of key energy policy drivers. The drivers include greenhouse gas emission reductions, renewables portfolio standards, energy efficiency, distributed resource integration, system reliability, transportation electrification, and security and consumer privacy. The project also illuminated the challenges associated with smart grid development and deployment—such as maintaining and/or increasing reliability in the face of increased grid complexity and managing technologies at different levels of maturity.

Priorities for development along the pathway to the 2020 Vision include:

1. Agreement on the architecture for the smart grid is needed.
2. The communications infrastructure and general approaches must be defined and understood so that new technologies can be developed that will connect with it.
3. Technologies for customer integration with the grid will build on the definition of the communication infrastructure. Much will depend on rate structures and other incentives for customer involvement.
4. Requirements for integrating more renewables are needed at both the transmission and distribution level. Analysis tools, forecasting, transmission infrastructure, compensation technologies, monitoring technologies, and distribution management approaches must all be developed.
5. The grid planning, operations, and control will change to support the developments described above. Real-time grid management at the transmission level will incorporate distributed energy resources, including demand response, that are part of the distribution infrastructure, requiring close coordination between advanced distribution management and the overall grid management. New models that support both planning and real-time grid management are needed and must be supported. These models will reach individual customers and associated distributed resources. Monitoring and control of the integrated grid will require management of widespread sensors integrated with the real-time system models. Technologies for reliability and security must take advantage of these real-time models and system awareness. However, system security cannot completely depend on this communication infrastructure. There is an ongoing requirement for distributed intelligence and the ability to operate local controls safely.
6. Worker and public safety must remain the top priority as new technologies and system management approaches are implemented. New training and skills must be developed as the technology base for managing and operating the system changes.

For further information on this project, please contact Don Von Dollen at dvondoll@epri.com or (650) 855-2679.

Key Dates

IntelliGrid Advisory Meeting (Boston)	***September 12, 2011***
Project Set D Webcast (161D) (60 minutes)	***October 4, 2011 (8 am pacific)***
Project Set E Webcast (161E) (60 minutes)	***October 5, 2011 (8 am pacific)***
NIST Tracking Call (161A) (60 minutes)	***October 13, 2011 (9 am pacific)***
EE/SG Public Advisory Group Meeting (Kansas City)	***October 18-19, 2011***
Project Set C (161C) (60 minutes)	***November 2, 2011 (10 am pacific)***
NIST Tracking Call (161A)(60 minutes)	***November 10, 2011 (9 am pacific)***
Smart Grid Roadmap Workshop (Phoenix)	***November 15-16, 2011***
Project Set B Webcast (161B) (60 minutes)	***December 6, 2011 (8 am pacific)***
NIST Tracking Call (161A) (60 minutes)	***December 9, 2011 (9 am pacific)***
Project Set D Webcast (161D) (60 minutes)	***December 13, 2011 (8 am pacific)***
Project Set E Webcast (161E) (60 minutes)	***December 14, 2011 (8 am pacific)***
IntelliGrid Advisory Meeting (Huntington Beach)	***February 13-16, 2012***

Please contact Ashley Eldredge for details regarding the key dates, aeldredge@epri.com.

Recently Released Deliverables

Security Industry Coordination and Collaboration Q1 Newsletter

1023162

This newsletter discusses the Electric Power Research Institute (EPRI) 161E Program effort to identify, support, and facilitate coordination and collaboration among the key institutional players in the electric sector today. Topics include the following:

- North American Electric Reliability Council's (NERC's) evolving role
- Federal Energy Regulatory Commission's (FERC's) expanding role
- DOE's collaboration efforts
- Department of Homeland Security's (DHS's) coordination efforts
- United States Computer Emergency Readiness Team (USCERT) and survivability
- Smart Grid Interoperability Panel-Cyber Security Working Group (SGIP-CSWG)

Advanced Security Acceleration Project – Smart Grid (ASAP – SG) Phase II

1022395

The Advanced Security Acceleration Project – Smart Grid (ASAP-SG) project has three primary objectives:

- Develop a Security Profile Blueprint to develop Security Profiles covering individual smart grid applications.
- Develop Security Profiles for Advanced Metering Infrastructure (AMI), Third-party Energy Data Access, and Distribution Management.
- Demonstrate a united industry interest in accelerating development, implementation, and adoption of guidance and standards for securing smart grid systems.

In order to accomplish these objectives, the ASAP-SG team will produced four major deliverables:

1. AMI Security Profile

2. Third-party Data Access (3PDA) Security Profile
3. Distribution Management Security Profile
4. Security Profile Blueprint (updated from 2008)

The four deliverables are contained in this report. These four deliverables will provide prescriptive, actionable guidance for how to build-in and implement security for smart grid functionality.

Results of OpenDSS CIM Interoperability Testing – Paris Interoperability Test, March 2011

1023218

The Electric Power Research Institute (EPRI) participated in the 2011 interoperability testing of the Common Information Model (CIM) for distribution, which was conducted at the Electricité de France facilities in Clamard, France, from March 28 through April 1, 2011. The testing covered the following parts of International Electrotechnical Commission (IEC) standard 61970, Energy Management System Application Program Interface (EMS-API), and standard 61968, Application Integration at Electric Utilities, System Interfaces for Distribution Management:

- IEC 61970-301, Common Information Model (CIM) Base, a semantic model that describes the components of a power system at an electrical level and the relationships between components, originally written with transmission systems in mind
- IEC 61968-4, Interfaces for Records and Asset Management, which describes data exchange for distribution system assets and contains equipment catalog data used in load flow models
- IEC 61968-11, Common Information Model (CIM) Extensions for Distribution, which contains diagrams and documentation for the CIM for distribution
- IEC 61968-13, CIM RDF Model Exchange Format for Distribution, called the Common Distribution Power System Model (CDPSM), which is an extension of the transmission-oriented CPSM (61970-452)

California Utility Vision and Roadmap for the Smart Grid of Year 2020

1022220

California investor-owned utilities have a vision that the California Smart Grid of 2020 will be a more capable, robust, and efficient electricity infrastructure, which will help achieve multiple energy and environmental policy goals. This report describes that vision and presents a detailed roadmap for achieving that vision. The report provides clarity and direction to support California Smart Grid initiatives and the State's energy and environmental policy goals.

The report details findings in six domains of technical expertise: Communications Infrastructure and Architecture, Customer Systems, Grid Operations and Control, Renewable and Distributed Energy Resources Integration, Grid Planning and Asset Efficiency, and Workforce Effectiveness. These domains form a structure of technical areas under which the project provides further findings on vision, baseline, technology readiness roadmaps, gaps, and recommendations.
