PNNL-27574

Pacific Northwest
NATIONAL LABORATORY

Universal Utility Data Exchange (UUDEX) Initial Interview Results

Cybersecurity of Energy Delivery Systems (CEDS) Research and Development

May 2018

SR Mix
MJ Rice
S Sridhar

U.S. DEPARTMENT OF ENERGY

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

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
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <http://www.ntis.gov/about/form.aspx>
Online ordering: http://www.ntis.gov


This document was printed on recycled paper.
(8/2010)

PNNL-27574

Universal Utility Data Exchange (UUDEX) Initial Interview Results

Cybersecurity of Energy Delivery Systems (CEDS) Research and Development

SR Mix
MJ Rice
S Sridhar

May 2018

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

Pacific Northwest National Laboratory
Richland, Washington 99352

Summary

This report summarizes the results of the information received from the interviews of industry stakeholders concerning utility data communications. Information from these interviews will be used to inform the functional design for UUDEX.

Acronyms and Abbreviations

CIM	Common Information Model
COS	Coordinated Outage System
DER	distributed energy resource
DOE	U.S. Department of Energy
EMS	energy management system
FERC	Federal Energy Regulatory Commission
ICCP	Inter-control Center Communications Protocol
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
IT	information technology
NERC	North-American Electric Reliability Corporation
NPCC	Northeast Power Coordinating Council
NSI	Net Scheduled Interchange
OASIS	Open Access Same-time Information System
PMU	phasor measurement unit
RC	regional coordinator
RCIS	Reliability Coordinator Information System
RMT	reliability messaging tool
RTU	remote terminal unit
SAFNR	Situation Awareness for NERC, FERC, and the Regions
SCADA	supervisory control and data acquisition
SERC	SERC Reliability Corporation
UUDEX	Universal Utility Data Exchange
WECC	Western Electricity Coordinating Council

Contents

Figures

1.0 Introduction

The purpose of the Universal Utility Data Exchange (UUDEX) project is to develop a flexible utility communications protocol that can dynamically accommodate new data elements and new users (partners) while remaining secure.

Utilities have been exchanging information with each other using standards-based protocols for more than 20 years. These standards have been extended and augmented for security, but those changes have not altered the initial underlying architecture and protocol base. Additionally, several different tools have been developed during that time, each with their own syntax, configuration process, and management structure. As a result, the current toolset is inflexible, difficult to configure, and includes security as an optional add-on that is not used extensively in the United States.

The UUDEX project proposes to replace existing control center data exchange protocols, data formats, and exchange processes with a modern architecture. The architecture will take advantage of current methods of data transport and configuration to create a flexible, dynamic, and scalable platform. The platform will subsume and ultimately replace not only existing data exchanges at the control center level, but also the Reliability Coordinator Information System (RCIS), synchrophasor data transport (e.g., NASPInet), incident reporting (DOE OE-417), threat and response data (including firewall rule updates and vulnerability and patch notifications), distributed energy resource (DER) data, and power system model exchanges. It will be designed with information security as a core component that can evolve to address changing security technologies and threats. The UUDEX platform will rapidly respond to changing data exchange needs, allow for the addition of new data exchange partners on a permanent or temporary basis, and can be easily extended to the oil and natural gas energy subsector.

The objectives of the project include the following:

- Develop a secure and flexible data exchange approach to replace all communications between control centers, from control center to national-level industry data sharing and analysis centers (e.g., Electricity Information Sharing and Analysis Center [E-ISAC] and Bulk Power System Awareness [BPSA]), and from control center to federal agencies (e.g., the Department of Homeland Security [DHS], the U.S. Department of Energy [DOE], and the Federal Energy Regulatory Commission [FERC]). Hence, the data exchange is intended to support both horizontal and vertical information sharing.
- Use modern, model-driven data exchange protocols that have security designed in at the beginning and implemented by default.
- Enable dynamic and flexible communications for energy delivery systems including cybersecurity information; operational information; supervisory control and data acquisition (SCADA) data; DER data; phasor measurement unit (PMU) data; and model information.
- Develop a cybersecure communications tool suite that is transport agnostic and allows exchange of multiple data types with dynamically configured partners.
- Conduct a lab demonstration of data exchange with dynamic addition of data and partners.

UUDEX will use a Unified Modeling Language (UML)-based modeling approach for semantic modeling and profiles for interface specifications to develop a self-describing communications protocol. This protocol can be dynamically extended with new data elements or new communication recipients with minimal configuration overhead or resources. This approach will enable data and recipients to be dynamically modified with minimal impact on existing communications streams.

Figure 1 shows the proposed architecture for UUDEX, showing how UUDEX will be used to send and receive data between a utility control center and various organizations.

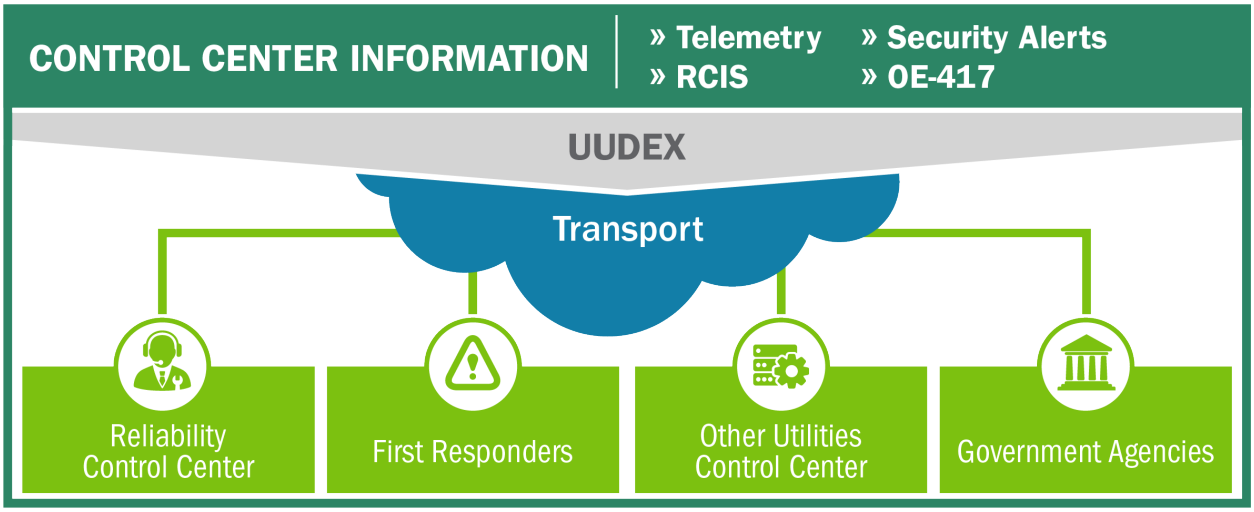

Figure 1. UUDEX Architecture

This report documents the initial findings of industry interviews to gather existing communications streams used between utilities (e.g., Inter-control Center Communications Protocol [ICCP], Reliability Coordinator Information System [RCIS], synchrophasor, and power system model exchange).

A total of five organizations were interviewed. Interviews were conducted by telephone during the period of April 13, 2018 through May 4, 2018. One organization provided responses from a group of respondents; all others provided responses from a single individual within their organization. Most respondents had a transmission operations background. Much of the information provided was specific to a particular organization, and generalized responses were difficult to derive from the data.

Not all questions were applicable to all organizations interviewed, and in certain cases, responses were not provided.

Information from the interviews will be used during the development of the functional specification for UUDEX.

2.0 Summary of Initial Findings

The data exchanged can be sorted into three categories—data exchanged for real-time monitoring and control, data exchanged for regular reporting on a periodic basis, and event-triggered reporting.

Entities still depend on primitive, awkward, inefficient, cumbersome, and insecure methodologies for data exchange. Further, many proprietary protocols and systems are still used for data exchange.

Periodic and event-triggered reporting is unstructured, free-form textual data in most cases. Event reports are written by humans and therefore are non-uniform with varying grammar, language, and structure.

Outdated mechanisms like FTP (an inherently insecure protocol using plain-text usernames and passwords) are used to exchange information critical to real-time operation. These mechanisms rely on parsing text/CSV/XML files received via FTP.

Many critical messages are exchanged via phone calls between entities, especially during emergency scenarios. The information is rarely presented in a proper structured form using computer systems. This makes repeating information difficult and could potentially lead to spreading of inaccurate information. Similarly, some elements of emergency communications need to be highly nuanced in a way that is difficult to achieve with pre-defined standards and machine-to-machine communications. A balance must be found that removes that need for human operators to spend time exchanging technical information that machines can easily express and use, while not constraining those operators to try to express highly contextualized information using finite and limited structures.

Multiple parties cited a desire to enable direct communications with partner organizations rather than having the data go through some central broker or authority. They cited concerns about exchanges having a single point of failure caused by chokepoints. This could be solved with support for peer-to-peer network topologies and for hub-and-spoke topologies for exchanges that rely on a central authority.

The interviewed organizations indicated wide variation including the use of different protocols and data formats for the same information, employment of different data sources and authorities, and different decisions whether to use certain data. Their input suggests that any solution will need to be flexible and configurable to account for the highly individualized needs of participants.

Incident reporting (whether operating incidents, or cyber security incidents) was identified by all participants as necessary communications, however, it is largely accomplished through telephone calls, web forms, or manual creation of text files.

Participants also identified the ability to restrict access of information to relevant and authorized entities as a critical security and privacy need.

Appendix A contains a more detailed set consolidated of interview responses, along with the interview questions.

Appendix A

Consolidated Interview Responses

A.1 Section 1 – Questions about Your Organization

1. Is your organization registered with NERC?

   Four out of five responders belong to an organization registered with NERC.

2. If applicable, please select each NERC Regions in which your organization belongs.

   The responders belong to the following NERC regions: Western Electricity Coordinating Council (WECC), Northeast Power Coordinating Council (NPCC), ReliabilityFirst (RF), Midwest Reliability Organization (MRO), and SERC Reliability Corporation (SERC).

3. If your organization is registered with NERC, please select each NERC Functional Model designation your organization is registered for.

   Responses included: N/A, reliability coordinator, generator operator, generator owner, transmission operator, transmission owner, balancing authority, planning coordinator, transmission planner, transmission service provider, purchasing-selling entity, and distribution provider.

4. Is your organization registered in the North American Energy Standards Board Electric Industry Registry?

   Both yes and no were received as responses. The registration roles included reliability coordinator and purchasing and selling entity.

5. Is your organization a participant in an electricity market?

   All three responses—yes (just one), yes (more than one) and no—were received. The markets include NYISO, PJM, NPCC, and RF.

6. Is your organization (or someone employed at your organization) registered as a member of the E-ISAC?

   All NERC registered entities indicated YES.

A.2 Section 2 – Questions about Information Exchanged

7. What are the organizations your control center communicates (including non-computer communications) with? Please provide names and/or types.

   The organizations questioned about real-time operations included reliability coordinators, ISOs, neighboring utilities, balancing authorities, transmission operators, scheduling vendors, and other regional entities. These message exchanges typically happened through direct communication using ICCP/DNP, uploads to platforms provided by commercial service vendors providing operations support services and hosted by regional entities, FTP connections, telephone conversations, and email exchanges.

   The organizations questioned about periodic reporting, event reporting, and situational awareness included FBI, NERC, FERC, DHS, NPCC, PUCs, FEMA, fire department, and law enforcement. These message exchanges typically happened through phone calls, email alerts, web form-based uploads, and website-based data dissemination. Sometimes, platforms hosted by these organizations

facilitate wide-area situational in the event of a large-scale disturbance or system-wide problem. Communications included incident reporting and information receipt.

8. With reference to the above, please provide answers to the following questions.

   a. What knowledge does your organization wish to obtain from the information exchange, that is, what is the end goal of the exchange?

      - Supplement tools with data to support functions such as state estimation, contingency analysis, and voltage and transient stability analysis.
      - Notifying neighboring utilities, regional entities, state and federal agencies that an event or an emergency has occurred. Similarly, gain knowledge of event occurrences outside of their jurisdiction.
      - Interact with neighboring utilities to convey changes to status, meter validation, and sudden changes to system; situational awareness; and power transfers.
      - Awareness of gross longer-term trends of things happening in the industry that could influence future trends from a monitoring perspective (e.g., organizational changes, new legislation, and media reports).
      - After-the-fact analysis of events by looking at data from different sources to identify problems.
      - Real-time observation of system behaviors to monitor grid stability, occurrence of significant disturbances.

   b. How is the information structured when it is sent or received (e.g., XML, CSV, free text)?

      - Outage information is reported to a region-wide repository provided by a commercial vendor via web forms or XML messages produced by outage management systems.
      - ICCP to communicate analog, status, generator basepoints, measurements for state estimation, and other functions.
      - DNP for plan control messages from control center to remote terminal unit (RTU) and measurements from substation to control center.
      - FTP to exchange generator schedules, day-ahead operating schedules, and interchange schedules in CSV/XML or free text.
      - Email exchanges for alerts pointing to operations-oriented situational awareness reports and daily reports to NERC/EISAC/FERC.
      - Web forms for outage reporting (scheduled and unplanned).
      - Direct uploads to commercial platforms maintained by different entities to exchange updates to feeder ratings (spreadsheets) and topology changes (spreadsheets), MW and MVARs from large generators, and in large transmission lines (ICCP).
      - Telephones for communicating emergency communications and communicating with transmission operators.

   c. What mechanism, method, or tool does your organization use to send or receive the information (e.g., the specific network protocol, phone conversation, fax, email, website form)?

      Refer above.

9. For each of these exchanges, we are interested in aspects of your organization's current practices that work especially well or which are especially challenging. Examples of challenges include being time consuming, requiring excessive preparation, complexity of the user interface or required inputs, incompatibility with would-be recipients or senders, number of different recipients via different methods of transmittal, or other factors. Please elaborate.

   – One organization noted that data exchange using ICCP is good for status and analog signals only. But, establishing interoperability between different vendors requires significant tweaks to settings to get it to work. In addition, it was noted that ICCP is not ideal for rest of the message types.

   – One organization lacks access to a phasor gateway, hence no real-time access to PMU data streams through PUB-SUB technology. It was remarked that all users get all PMU data without any security. They prefer this transaction to be a negotiation-like ICCP setup to determine what is used and useful on a participant-to-participant basis.

   – One organization exchanges net scheduled interchange data via FTP. As the vendor is not allowed into the SCADA network, on receiving the data via FTP, the organization has to move it into the SCADA network every minute. The information is then immediately consumed into an area control error calculation.

   – One organization remarked that the reports received daily are not the same every time and are produced by humans. Style and grammar differences exist based on the particular analyst; thus, making it a significant hurdle for automation. Similarly, the information (reports on significant disturbances in the grid, indicators of grid stability, reports of significant load loss) is derived from multiple sources and hence leads to issues of data aggregation and challenges in mapping data to the correct points.

   – One organization would like to see a common process that different entities would subscribe to disseminate changes to models and ratings. This would reduce the challenges associated with updating their model with changes external to their system.

10. What information would be useful to exchange but cannot now?

    Responses included the following:

    – Model exchange using a common data format like Common Information Model (CIM).

    – Access to PMU data in real time from regional entities and other key PMUs.

    – One common protocols for all functional requirements with one security procedure.

    – Improved monitoring from IP connected substations.

    – The need for access to external models at the right granularity.

11. Is there information that is available, but, difficult or impractical to use? Why? (For example, it is too time consuming to convert the received information into a format we can use. We do not trust the information to be sufficiently reliable. Information is not reliably timely.)

    One organization wanted to see supplemental data like weather and information on fires to be overlaid over the electrical network for display at the control center. The diversity in data formats and associated software constraints and mismatches makes this difficult.

    Access to PMU data also seems to be restrictive. Sometimes, organizations lack access to PMU streams from neighboring entities in real time. Access is only restricted to bulk downloads from regional entities in this case.

In some instances, critical operational information such as day-ahead plans and the master generation schedule info are contained with flat files that need to be parsed. The responder expressed the desire for a more efficient approach.

One responder remarked that ICCP data is inherently unreliable as it is coming from unknown sources and sent through other systems that may not be reliable (down for patching, etc.). They needed to build custom stale data detection tools while working with ICCP. Critical control applications depend on ICCP data and this problem was identified as a concern.

Daily reports from the different regions and RC with basic information about area loads, reserves, outages are all in different formats. Manual processing is therefore required to coordinate the daily report.

12. Does your organization share information with federal regulators (e.g., FERC)? If so, with which organizations, how often, what kind, and what mechanisms, protocols, or formats?

    Sometimes, NERC and FERC have access to data uploaded by regional entities into data exchange platforms such as Situation Awareness for NERC, FERC, and the Regions (SAFNR) and OASIS. Some organizations provide daily reporting to their regional entities like the WECC. The report typically captures information such as major outages, forecasted peak loads, and major anticipated events. Organizations also use the OE 471 as a formal reporting process to report events and major occurrences. Other federal organizations that data is exchanged with includes DOE EIA, DOE Emergency Operations Center, E-ISAC, and PUCs. The other types of data exchanged include scheduling information (XML files), and situation reports (phone call or email).

13. Does your organization share information with other federal agencies (e.g., FEMA)? If so, with which organizations, how often, what kind, and what mechanisms, protocols, or formats?

    Organizations typically communicated with the ISAC. In cases of events and emergencies, DHS (NCCIC) and FBI are notified of the occurrence. During extreme events like hurricanes, FEMA is notified. The information is typically exchanged from the corporate office rather than the control centers. One organization identified the need to create a STIX/TAXI-based system to communicate cyberthreat information to the E-ISAC.

14. Does your organization share information with local or state regulators (e.g., utility commissions)? If so, with which organizations, how often, what kind, and what mechanisms, protocols, or formats?

    Ad hoc communication via phone or email only. Usually in response to an event or compliance-related reporting.

15. Does your organization share information with other local or state agencies (e.g., emergency response agencies)? If so, with which organizations, how often, what kind, and what mechanisms, protocols, or formats?

    Information rarely goes directly from the control center. Typically, organizations have an emergency operations department that performs the necessary communication. In emergencies, such as ice storms and physical security breaches, the telephone is used to convey the incident to incident responders.

16. Is the Inter-Control Center Communications Protocol (ICCP) used for information exchange? If yes, which blocks? How often?

The following is a summary of the different blocks used to exchange analog and status information. Blocks 1, 2, 4, and 8. Analog data was typically polled once in 10 seconds. Status information was conveyed whenever a change occurred. In cases where plant control was communicated through ICCP, the data was exchanged every four seconds. Sometimes, ICCP was also used to convey frequency and Area Control Error information. One particular organization uses all blocks of ICCP except 4.

17. What other telemetry is exchanged and how? With which organizations, how often, what kind, and what mechanisms, protocols, or formats?

    The responses include the following:

    – PMU data using C37.118 and other private networks.
    – Monitoring demand response and DER using through ICCP.
    – Data from RTUs using DNP-3.
    – Telemetry to ISO using ICCP.
    – Sometimes organizations directly pulled data from repositories hosted by regional entities.
    – FNET data from the University of Tennessee.

18. What control commands are exchanged and how? With which organizations, how often, what kind, and what mechanisms, protocols, or formats?

    Sometimes, only monitoring signals are received from external organizations. In cases where control commands are exchanged, it is primarily for plant and generator control. In these cases, ICCP is used to communicate the basepoints to the organization. Once the basepoints are received, the organization then uses DNP to transmit the commands to the relevant generators in the form of raise-lower pulses. Proprietary SCADA systems are also used for the last leg.

19. What scheduling information is exchanged and how? With which organizations, how often, what kind, and what mechanisms, protocols, or formats?

    One organization uses a commercial software vendor to exchange scheduling information with the RC. The RC in turn manually reviews and approves the schedule. Another organization conveys planned outages to the ISO. Based on this information and similar information coming from other entities, the ISO performs interchange scheduling for transmission operation planning. Another organization periodically exchanges net scheduled interchange with the scheduling vendor. The exchange is implemented using FTP and the file is parsed to capture the NSI. This data is then directly used in automatic generation control operation in real time. Other organizations exchange hourly scheduling data with neighbors via ICCP. Finally, hourly generation schedules are also received from the balancing authority.

20. Does your organization perform e-Tagging? If so, with which organizations, how often, what kind, and what mechanisms, protocols, or formats?

    Not all organizations perform this task. In one particular case, the organization verifies meter data and line overloads with the ISO over telephone calls. In another case, the information on line loading is exchanged with a scheduling vendor for operations planning. Finally, one organization performs this task in its capacity as a transmission system planner and operator.

21. How is real-time outage data reported (both automatic and planned or maintenance outages)? With which organizations, how often, what kind, and what mechanisms, protocols, or formats?

    It was noted that the outage reporting system varied from RC to RC. One organization uses an outage reporting system provided by a commercial vendor. All stakeholders in the region either use API provided by their outage management system to generate the requisite XML message to report the outage or use web-based forms. Some organizations that do not directly consume outage-related information try to triangulate outages using other data (FNET, data from commercial vendor software, and information from the RC) in their possession. Public data from the ISO/RTO website is also used sometimes to validate outages. In one particular organization's case, long-term (six months and above) planned outages are communicated via web portals. The information is then used to run studies to make sure that the outage is feasible. Information on forced outages is exchanged with an internal event analysis group using private, internal networks for study.

22. Which of the following interconnections does your organization report or retrieve outage data?

    a. ☐ Eastern Interconnection

        i. Does your organization report outage information to webSDX? If yes, how often?

        ii. Does your organization retrieve outage information from webSDX? If yes, how often?

        iii. Does your organization report real-time outages via other mechanism, protocol, or format with other organizations? If yes,

            (1) Which organizations?

            (2) What is the mechanism, protocol, or format for delivery?

            (3) How often?

    b. ☐ Western Interconnection

        i. Does your organization report outage information to Peak Coordinated Outage System (COS)

        ii. Does your organization retrieve outage information from Peak COS

        iii. Does your organization report real-time outages via other mechanism, protocol, or format with other organizations?

            (1) Which organizations?

            (2) What is the mechanism, protocol, or format for delivery?

            (3) How often?

    c. ☐ ERCOT

        i. How does your organization report or retrieve in real-time outages?

            (1) Which organizations?

(2) What is the mechanism, protocol, or format for delivery?

(3) How often?

d. ☐ Quebec

i. How does your organization report or retrieve in real-time outages?

(1) Which organizations?

(2) What is the mechanism, protocol, or format for delivery?

(3) How often?

The responses to this question ranged from one to all of WECC, Eastern Interconnection, ERCOT, and Quebec. The organizations using reporting outages to the WECC use the COS to both upload and retrieve data for various purposes. The organizations reporting to the Eastern Interconnect report unscheduled outages to the ISO and neighboring utilities through a phone call, and scheduled outages through an outage scheduling system. Interaction with the Quebec interconnect is limited to only retrieving information from their website. Sometimes, FNET data from Quebec was used for daily summaries.

23. How does your organization perform after-the-fact automatic outage information reporting? With which organizations, how often, what kind, and what mechanisms, protocols, or formats?

One organization monitors and manages outages. For scheduled outages, the organization coordinates with the monitored entities to implement and execute the outage. The success of the implementation is verified through telemetry. The Coordinated Outage System is also used to exchange information on outages. Outage information is also exchanged through daily situational awareness reports. Sometimes, depending on the severity of the outage (assessed by an internal process), the outage is reported to DOE through OE-417. Phone calls and emails are also used sometimes to communicate outages to critical assets and communication infrastructure.

24. Does your organization provide transmission availability data system (TADS) data to NERC? If yes, how often?

Sometimes, the entities directly supply the information without the need for the RC. In others, the services of the NERC Reliability Risk Management Performance Analysis group are used to administer TADS. It was noted that time lag in providing the data makes it useless from the perspective of real-time operations. However, it has application from a post-event analysis perspective.

25. Does your organization provide generation availability data system data to NERC? If yes, how often?

In most responses, the organization depends on external parties like the regional entity or U.S. Army Corps of Engineers to perform this function. In one case, the organizations provided the necessary information for generators in their jurisdiction.

26. Does your organization provide demand response availability data system data to NERC? If yes, how often?

Most responders replied in the negative. Sometimes, the regional entity performed the function for the organization.

27. Does your organization exchange load forecast with other organizations? If yes, with which organizations, how often, and in what mechanisms, protocols, or formats?

    Some organizations produced the load forecast, whereas some relied on the information from another source. In one case, the organization used a dedicated portal set up by their regional entity to exchange forecast in XML format. The organization was also exploring the possibility of applying existing inter-RC data exchange portals to exchange load forecast data with RCs. Web portals were also used to upload and disseminate load forecast data. Forecast exchanged with most entities on an hourly basis. In other cases, software products from commercial vendors automatically provided the required forecast. The forecasts were all the way from hourly load forecasts to 7-day rolling forward forecasts.

28. Is weather data exchanged or received by your organization? If yes, with which organizations, how often, and in what mechanisms, protocols, or formats?

    All the organizations consume weather information from some source. The sources include dedicated third-party weather providers, open-source weather information providers and onsite meteorologists. Sometimes, the organization consumed forecast data produced by third-party vendors who in turn used weather data to generate the forecast. If weather information was directly consumed, the data was received through Simple File Transfer Protocol (SFTP) or from websites of the information providers. In one case, weather information was identified as critical to understand potential impact to transmission and generation outages. Space weather was also identified as relevant in this context.

29. What other real-time operational data exchanges occur? With which organizations, how often, and in what mechanisms, protocols, or formats?

    Most responders did not identify additional data exchanges. In one particular case, the use of ICCP for implementing reserve sharing agreements and notifying available reserves was highlighted.

30. What other reports are exchanged? To which organizations? What mechanisms, protocols, or formats are used for this purpose?

    The responses include daily reporting to regional entities, reports on voltage reduction tests and implementations, load forecast reports to scheduling vendors, and reports on shared responsibility drills, collaboration, and system testing. Event-specific reports are sent to NERC through official forms and channels. Sometimes, reports from the Electric Reliability Organization's Events Analysis program are also obtained through formal channels. These reports provide insights on cause analysis and trending information.

31. How is market data exchanged? Please provide the market-specific mechanism, protocol, or format used.

    Not all organizations exchange this type of data. In cases the data is exchanged, commercial market module vendors provide the necessary platform to exchange the relevant information. Typically, generator bids are typically sent and real-time base points received. Tie-line flows are also received to calculate power import and export. In some implementations, ICCP is used to send plant control messages and receive data for merchant function displays.

32. Are the following market data exchanged? If yes, how often and in what mechanism, protocol, or format?

    Not all organizations exchanged this type of data. Sometimes the following occurred:

    a. Bids – Manually entered via a web portal.

    b. Offers – Manually entered via a web portal.

    c. Virtuals – Responder not aware.

    d. Settlement information – Collected within market software module.

    e. TSR, CRR – Responder not aware.

    f. Any other data – None.

33. What is the source system at your organization for the above data?

    Software modules provided by commercial vendors and website portals to exchange market data.

34. Does your organization exchange information with the Open Access Same-time Information System (OASIS)? If yes,

    Both yes and no were received as responses.

    a. What is the purpose?
        - As a platform to share potentially useful market information with other participants in a shared market scenario.
        - For merchant function to follow FERC order 888/889.

    b. How often?

        Depending on the organization, information was either shared continuously or on an on-demand basis.

    c. What is the mechanism, protocol, or format used for the exchange?

        The responders were unaware.

35. Does your organization exchange information with the Reliability Coordinator Information System (RCIS)? If yes,

    Both yes and no were received as responses.

    a. What information does your organization provide to RCIS?
        - Events around DC ties with neighboring RCs.
        - Information on major multi-RC events (rare).
        - System outage posting.

b. What information is your organization most interested in getting from the RCIS?
   - General announcements from other RCs.
   - Information on large unit trips.
   - Information on major transmission system interruptions.

36. Does your organization exchange information with the WECC Reliability Messaging Tool (RMT)? If yes,

    Both yes and no were received as responses.

    a. What information does your organization provide to RMT?

       One organization shares information that goes to backup control center for NERC EOP 8.

    b. What information is your organization most interested in getting from the RMT?

       Situational awareness about other utilities. The system is also used to report ICCP links that are down.

37. Does your organization submit EOP-004 or EIA-417 reports? If yes,

    Both yes and no were received as responses.

    a. To which organizations (DOE, NERC, FERC, other utilities)?

       DOE, NERC, FERC, SERC, ISO, and internal groups.

    b. What mechanism, protocol, or format is used to exchange this data?

       Website and email are used as mechanism to exchange this information.

38. Does your organization report, receive, or forward equipment mis-operation, suspicious behavior information, or analytics? If yes, to which organizations, how often, and what mechanisms, protocols, or formats?

    Most organizations replied in the positive. In one case, a dedicated disturbance exchange tool is employed. The analysis of the mis-operation is performed at the utility-level usually. However, sometimes the reliability coordinator performs the analysis. The disturbance exchange tool facilitates the data exchange required to support the analysis. Another organization responded that from a reporting perspective, any mis-operation is first filed with NPCC which is then forwarded to NERC. The OE-417 process is also employed to report mis-operation to DOE.

39. Does your organization report, receive, or forward other incident or disturbance information? If yes, to which organizations, how often, and what mechanisms, protocols, or formats?

    All organizations exchange incident or disturbance information through different methods. These include phone calls, formal incident response reports to organizations such as the ISAC, and custom reporting tools. Sometimes, organizations gather clues from Internet-based sources such as Google and Twitter see if event-specific evidence can be discovered. Open-source and free-source information are also considered.

40. Does your organization report, receive, or forward information (structured or unstructured) with the E-ISAC? If yes, how often, and what mechanisms, protocols, or formats?

    All organizations exchange information with the E-ISAC. The information exchanged mainly includes threat-related data which helps largely in maintaining situational awareness. In addition, the mechanisms used to exchange threat information include STIX/TAXII and other formal reporting (EOP-004, 417).

41. Does your organization report, receive, or forward cybersecurity information (cyber intelligence information, threats, vulnerabilities, indications of compromise, mitigation, patch availability, etc.) with other organizations? If yes, to which organizations, how often, and what mechanisms, protocols, or formats)?

    Most of the organizations receive cybersecurity information. The organizations that are involved include the US-CERT, HISN, CISCP, NCCIC, NICC, E-ISAC. The RCs, ISOs, and regions forward and disseminate information to their members. One organization uses the RMT for this purpose, where the messages are structured using standard templates defined in the manual.

42. Does your organization report, receive, or forward miscellaneous communications (text messages, free-form instructions, documents, reports) to or from RC/TOP/GOP/BA? If yes, to which organizations, how often, and what mechanisms, protocols, or formats?

    The telephone and email seems to be a popular choice for operators from different organizations to exchange information in this category. Depending on the organization, information exchanged includes, for example, topology changes, system issues, and operational guides.

43. Does your organization report, receive, or forward synchrophasor data? If yes, to which organizations, how often, and what mechanisms, protocols, or formats?

    All the organizations have access to PMU data in different capacities. One organization streams PMU traffic to the ISO, but has no real-time access to streams from neighboring utilities. When access to real-time PMU streams is available, the data is typically received at the rate of 30–60 samples per second using the C37.118 protocol. Sometimes, the organizations have access to a website where asset owners upload their PMU data. This portal is also used to make data requests to run after-the-event analysis on large disturbances.

44. Does your organization provide instructions to DER or non-DER? If yes, to which organizations, how often, and what mechanisms, protocols, or formats?

    Most organizations do not have or have a negligible number of controllable DERs in their system. However, they recognize that DERs will definitely be a part of their future operations. The vision is to use DNP3 to exchange data between the distribution control center and the DER controller, and ICCP to exchange data between the distribution control center and the transmission control center.

45. Does your organization report, receive, or forward disturbance (e.g., COMTRADE) files? If yes, to which organizations, how often, and what mechanisms, protocols, or formats?

    No regular exchange of information of this type was reported. Some organizations are able to share the information upon request. The organizations typically capture disturbance data through fault recorders or find the necessary artifacts in PMU data.

46. Does your organization report, receive, or forward the following data? If yes, to which organizations, how often, and what mechanisms, protocols, or formats?

    Not all organizations report, receive, or share all of this data.

    a. Relay settings: Shared via ICCP or targets are set manually.

    b. Network models: The models are shared via the organization's website. The models are uploaded in CIM, a vendor-specific, and other popularly used grid simulation tool formats. In one case, the organization shares network models with the ISO, which in turn shares the data with interested parties.

    c. Planning models: An organization shares software simulation models with the planning group at the transmission operator level. Some organizations also have access to interconnect-level planning models for different regions.

47. Does your organization report, receive, or forward other information with NERC? If yes, how often, what kind, and what mechanisms, protocols, or formats?

    Some organizations provide event notifications to NERC as a part of self-reporting. In some cases, the ISO performs the event analysis and communicates with NERC. In one particular case, an organization provided ICCP data to NERC through a dedicated service.

48. Does your organization report, receive, or forward other information with the E-ISAC? If yes, how often, what kind, and what mechanisms, protocols, or formats?

    The E-ISAC portal was identified as a relevant space to report incidents and mandatory responses.

49. Does your organization report, receive, or forward information with other ISACs? If yes, which ISACs, how often, what kind, and, what mechanisms, protocols, or formats?

    Most of the responses were no. Of those that answered yes, information sharing was informal and unplanned and performed by IT.

50. Are there other information exchanges or organizations with which your organization reports, receives, or forwards data? If yes, to which organizations, how often, what kind, and what mechanisms, protocols, or formats?

    No.

A.3 Section 3 – Questions on Configuration of Information Exchange Systems

51. How often do changes to the data structures or data elements get communicated?

    Most structure changes are related to addition or deletion of new power system elements resulting from substation construction. Other changes are the result of parameter changes (static values associated with power system elements like ratings).

    One entity reported roughly "100" such changes are reported every year. Others indicated monthly or quarterly changes, schedules dictated by partner (i.e., ISO and RC) schedules for updates.

Changes include the following:

- ICCP object listings are sent out semiannually (structure or data).
- IRO-010 changes are sent on demand per Transmission Operator requirement (data).
- New equipment additions are communicated 60 days before change implementation (mostly structure, some data).
- Line rating changes should be communicated within 14 days. Corrections must be reported within seven days of discovery (data).
- Network models are updated seasonally (structure or data).

a. What sort of changes are made (e.g., new fields, additional data elements)?

   - Addition of new equipment.
   - Impedance changes.
   - Equipment rating changes.
   - Regulation levels based on demand.
   - Power factors.
   - Updates to the energy management system (EMS) model, which are accompanied by updates to the ICCP model.
   - Updates to facilities for organization footprint changes.
   - BA change between different RCs.
   - Changes to data recipient.

b. Why are the changes typically made (e.g., new information to communicate, changing communications requirements, new exchange partners)?

   Changes typically made because of model updates, which are followed by new/removed analog or status tags. Also refer above.

c. How does your organization coordinate changes with the data recipient?

   - The reliability coordinator sometimes provides the responders with a procedure to update the model.
   - Organizations also use the telephone to convey changes to the recipient.

52. How long does it take to make the change? What are the biggest bottlenecks when making the change?

    It depends on the data object that must be changed. For example, feeder rating changes take only a couple of hours. The addition of new equipment could take anywhere between a couple of hours and a week. Getting information from neighboring utilities for external models is a primary hurdle. In addition, getting approvals from the relevant personnel could also delay the process of implementing changes. Bottlenecks identified are mostly approvals and non-communication issues (e.g., engineering drawings).

53. Are there changes that would be useful to make (or make more frequently), but do not do so due to prohibitive time or cost in making the change? Please explain.

    Model development and changes to existing models was an answer most responders provided.

54. How often does your organization establish a new link and why (e.g., different application, new partner)?

    This happens very rarely. New links are established typically only when a new organization is stood up. Most respondents appear to have established appropriate communication links with all partners they deem necessary.

55. How long does it take to establish a new link? (Please do not include time necessary to physically provision the telecommunication link with a communications company).

    The process takes anywhere between a few days to a few months depending on where in the process the organization is. A major factor that influences this time range is the responsiveness of the communicating parties.

56. What coordination with the communicant is necessary before establishing this link? How is the coordination performed?

    Coordinating network settings such as firewall configurations, data routes, virtual IP addresses, and network address coordination were identified as key factors. In addition, points mapping into ICCP object IDs and the sharing of ICCP objects were also raised.

    The process starts with the negotiation of the points list between the sender and intended recipient. Once the points list is finalized, the IT department receives the points list and then proceeds to implement. Sometimes where a third-party communication provider is involved a contract is set up with them. Once the process is approved, the communications provider proceeds with the hardware installation and network configuration for communications testing.

57. Are there links your organization would like to establish, but do not due to prohibitive time or cost to establish a new link? Please explain.

    One organization identified links to PMU data as a preference citing cost as a hurdle. Another organization would like to establish communications with neighboring transmission operators to retrieve necessary data. In this case, the data from neighboring transmission operators is currently being routed through the ISO, thus introducing a single point of failure. In another case, direct links to data within substations were preferred. However, verifying that the new link is functioning in accordance with NERC CIP standards introduced additional cost. Finally, another organization remarked that they would like to establish a link with the University of Tennessee to transfer FNET data at the rate of one sample a second.

58. In addition to implementation time and dollar cost, are there other metrics your organization employs to assess cost of implementing a change? How does fragility of the system go into decision making to create new links?

    Security was identified as an important metric with greater weightage than dollar cost. In addition, the accuracy the new data brings to the analysis must also be evaluated.

59. What target time would be ideal for adding a link? (Please exclude time necessary to physically provision the telecommunication link with a communications company).

    The responses varied from two weeks to a month for implementation and testing.

60. Are there organizations or locations that your organization would be more likely to establish links with if the process was easier or quicker?

    One organization expressed their wish to have direct communication with neighboring transmission operators instead of depending on the ISO to act as a conduit.

61. To what extent are the following impediments to sharing out information that might otherwise be useful to share with other organizations?

    a. Technical difficulty in establishing the logical link.

       Not identified as an impediment.

    b. Time and effort necessary to structure the data in a way that can be shared over that link.

       Yes, this was identified as an impediment. In one case, it takes four months to get model updates due to this hurdle.

    c. Concerns about disclosure of sensitive information to the intended recipient.

       Identified as a major concern and requirement.

    d. Concerns about disclosure of sensitive information to parties other than the intended recipient (either exposed during transport or exposed by the recipient).

       Yes, identified as important.

62. To what extent are the following impediments to collecting and using information that other organizations are making available?

    a. Technical difficulty in establishing the link

       The mapping exercise between the data and the model was identified as more of an impediment than establishing a new link.

    b. Time and effort necessary to take the delivered information and convert it into a format that can be used.

       Slim IT resources impacting time and effort was identified as the biggest constraint and concern.

    c. Concerns about lack of reliability of data (that would otherwise be useful if it was reliable)

       Usefulness of additional data—point of diminishing returns (e.g., modeling four busses out). Less is more.

    d. Concerns about data handling requirements of the received information (e.g., requirements for management and securing of the information are too onerous).

No responses.

63. If a private critical infrastructure only network was established, would your organization consider using it to exchange information with other critical infrastructure and government organizations?

    Responses were favorable pending approvals from their respective legal teams. Some organizations noted that they already had such a setup in their system.

64. If the communications could be made secure, would your organization consider using the public internet to establish communication links to other organizations? On a temporary basis? On a permanent basis? Only with certain types of organizations?

    Some organizations expressed their reluctance to using the internet, citing the diminishing costs of private networks and data security threats as concerns. However, other organizations were willing to test the possibility for limited cases such as the exchange of planning models. These organizations were unwilling to use the internet for ICCP or other operational data.

The following questions are about the use of CIM for the information exchange.

65. Does your organization use the CIM?

    Some organizations currently use the CIM for limited use cases. The responders identified the need to agree to a common CIM model across data exchange partners to overcome inconsistencies due to version mismatch, thus encouraging broader adoption. Model data is also being exchanged in other formats such as simulation model files. In addition, web-based technologies that support model exchange are also common. The conversion of non-CIM model exchange technologies to CIM-based was identified as expensive.

66. Are the CIM names your organization uses coordinated with communication partners?

    Most organizations were not well coordinated.

67. Are there data elements that your organization transfers that lack CIM names? Please provide examples.

    Yes.

68. Can the state estimation models for your organization's grid area (RC, RTO/ISO, BA, etc.) exchange data using the CIM?

    Most of the responses were "no." One organization identified an inbuilt capability in their EMS/DMS tool suite that enabled this feature through a model export option.

A.4 Section 4 – General Questions

69. Does your organization have experience with data modeling (CIM, UML, or otherwise)? Is that experience positive or negative? Please explain.

    The use of CIM was identified as a step in the right direction as the benefits of a more refined data model is becoming apparent. Although CIM is used by some organizations, version mismatch between communicating parties was expressed as a major hurdle in the adoption process. The

differences in schema between two different versions of CIM has forced the organizations to develop and use custom translators.

70. Does your organization have experience using XML, JSON, RDF, or other semantic descriptive data transport mechanisms, protocols, or formats? Is that experience positive or negative? Please explain.

    XML is widely used by some organizations, whereas, JSON and RDF are not currently used.

    Not sure if the response was positive or negative?

71. Does your organization have any experience with IEC 61850 data modeling? Is that experience positive or negative? Please explain.

    All organizations responded in the negative.

72. Does your organization have its own staff that performs systems integration work for data modeling or exchange?

    Both yes and no were received as responses.

73. Is your organization dependent upon third-party organizations performing systems integration work for data modeling or exchange?

    Both yes and no were received as responses. Third-party services were preferred for fast execution and as a supplemental resource.

74. Does your organization use cloud-based third-party applications for data exchange or storage?

    Some organizations do not currently use cloud technology. One organization is at an early stage in the adoption process, wherein cloud services were being used for data storage. Another organization has set up a private cloud onsite that other organizations avail for tool and data access.

75. Are cloud-based solutions preferred over onsite deployment of systems for data exchange or storage?

    In addition to cost, data integrity and communication security were identified as critical factors that will influence adoption of cloud-based solutions. Using the cloud infrastructure for non-critical applications and data was suggested as a first possible step in the adoption process. However, some responders expressed their strong preference for onsite storage and processing, citing decreasing IT infrastructure costs as a supporting argument.

76. Are there any other comments you would like to make concerning utility data communications?

    The responders would like utility communications to upgrade to a one-stop-shop solution that supported multiple business functions and applications using secure technology that provided end-to-end encryption with built-in redundancy.

Pacific Northwest
NATIONAL LABORATORY

www.pnnl.gov

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99352
1-888-375-PNNL (7665)

U.S. DEPARTMENT OF
ENERGY