NextGrid: Utility of the Future Study
Reliability, Resiliency, and Cyber Security Working Group Meeting No. 1
April 11, 2018

Working Group Leaders:

Manimaran Govindarasu

Dominic Saebeler

NextGrid Senior Study Consultant: Annette Beitel

MEETING SUMMARY

[Note: descriptions of comments and discussion are condensed summaries and paraphrases]

Agenda Item I: NextGrid background, Purpose, Process (Chairman Sheahan, U of I, Senior Consultants

Chairman Sheahan - Outlined overall purpose and goals of the study, roles of project participants, and process for working group members and public involvement. (See Letter from Chairman Sheahan on NextGrid website)

Agenda Item II: Participant Introductions: Working Group Members introduced themselves, organization and title.

Agenda Item III: WG 3 overview, strawman topic areas

Manimaran Govindarasu ,Dominic Saebeler and Wei Chen Lin -outlined Work Group 3: "Reliability, Resiliency and Cyber Security topics to study. (See presentation slide deck.)

Agenda Item V: Presentations on Current Challenges and Opportunities

I. Presentation and Comments: Overview Presentations from Am IL, ComEd, PJM (contributions from MISO)

WG leaders asked for Ameren IL, ComEd, PJM and MISO to work together to identify challenges and opportunities. Not company-specific, even though differences between all companies and was a collaborative effort. (See presentation slide deck)

Group looked at:

- reliability and resilience
  - Associated Challenges and opportunities
- cyber and physical security
  - Associated Challenges and opportunities

Current state – Central generating plant provides electricity in a one-way radial feed down to customers (Slide from EPRI- good representation)

Future State – Significantly expanded DER; customers are installing solar, batteries. Changing from one-way radial system to bi-directional networked system. More customer opportunities, but providing complexity in how we will operate and how we will plan for the grid in the future.

Reliability and Resilience challenges: (Opening Comments)

- Distribution system is large.
- Ongoing investments are necessary to continue modernizing grid. No longer one-way power flows. Last few years; reliability has increased and customer expect increased reliability.
- FEJA will spawn more DR, and will make grid more complicated and more two-way power flows.
- New technology needs new employees with new skill sets.
- While renewable generation offers benefits, it is cleaner, it creates challenges that must be addressed like shared responsibility for resiliency.

Reliability and Resiliency Opportunities: (Opening Comments)

- To address core challenges posed by high penetration of renewables. Looking at distribution energy resources system so utilities can reliability and safely operate the system.
- Remote monitoring of substations so potential problems can be identified.
- Requirements/opportunities for employees to gain new skillsets. New technology is increasing need for new employee skillsets.
- Customers have higher expectations. Microgrids will give us additional resources to recover from attacks and physical events.
- Leveraging relationships is important to share information and get information to strengthen our programs.

Physical and Cyber Security Challenges: (Opening Comments)

- From a physical and cybersecurity challenges – new vulnerabilities.
- Increase in IOT creates a new tax on pathways to critical infrastructure, closer to devices, need secure communications between organizations and internally need message authentication.
- Ransomware and other disruptive malware will be an increasing challenge.
    - Ransom Nation-state attackers and
    - Financial motivation (ransom)
- Sophistication of the atmosphere is a challenge- technology detective methods move from lock key now and move to adversary techniques and tactics.
- Antiquated infrastructures will continue to be a problem.
- People: Talent and skill gap. Need to attract right talent to secure and defend infrastructure.
- Security clearances – takes 18 months. Need to reduce.
- Need to identify data privacy framework to be able to harness privacy analytic purposes. Need to be able to secure private data but also harness benefits of big data analysis.
- Regulatory constraints for adoption of Emerging Technologies

Process: (Opening Comments)

- Securing supply change- vetting service providers.
- Operationalizing intelligence -look at tactics and techniques of adversary.
- Find ways to exercise GridX and risk management programs, capabilities and vulnerabilities – pretend attack is going on. What does company do in response (like fire drill)?
- Need to integrate operational skill sets with cyber security skill sets to better detect anomaly.
- Risk-based framework – when we are having conversations we have a common language so we can talk about risk. By coming together with common language, easier to share best practices.
- Regulation and compliance, data privacy – will continue to be an issue as more data is collected for analytical use.
- See a gap in regulation compliance with technology used to protect the network.

People: (Opening Comments)

- People and process is relationships. Managing relationships with peers, PUCs, government entities. Great way to share information, get information, to try to strengthen programs.
- Need to foster a cyber culture
- Educating people. Colleges starting to offer information security. Start with high school – STEM programs.
- NERC drafting teams – Adopting standards proactively as soon as they get released. Share with others how adoption went. Talk to regulators also – they want to see how it is going. Long run need to work together to improve reliability of grid.

Agenda Item VI: Discussion on key topics to refine focus, feedback on strawman project plan. Request volunteers to present in subsequent meetings.

I. Participant Comments: Technology

- On technology side, grid is changing. Currently distribution is designed in blocks. We have additional threats with smart devices, we need to think about how to deal with attacks on houses. We need to challenge vendors to be thinking about challenges that will come through household devices.
- Recently legislation in Senate to "dumb down" grid and not allow Smart devices to manage risk from them.
- One of ***challenges around cyber*** is that we don't model cyber as we do physical. Analogies I would give. Should we be doing electronic payload inspection and state boarder as we do with trackers/trailers? Should data have to go through inspection before it crosses boarder?
- Another example – WWII "ghost army" tool- enabling honeypots, modeling systems, and having a fake infrastructure to learn tactics and tools that the adversary is using. Need to learn tactics and tools that our adversaries are designing. Should there be legal ways to test the tools so that testers cannot be prosecuted with entrapment. What are we allowed to do?
- What tools do we need to protect information state by state?
- Importance of starting with the future that IL has committed. FEJA is at the core of that. We can start to think about critical weak links. Then we can discuss the weak links. Inverters will be "weak link" - converter that is connecting to solar panel. We need to see the new surface of vulnerability from FEJA DER and determine how to address.
- Do we allow customers to determine level of cyber security protection or do we mandate this?
- Momentary losses of power lead to loss of life (hospitals). We are on fast track of digitization; are we thinking sufficiently about how DER can impact reliability.
- Communication for sharing information when attacks take place. When one entity can sense and attack can this be communicated to all entities that are part of the consortium?
- When companies rely on other companies to do things for them, that extends the threat surface.
- Regulations tend to focus on owner/operator. That is end of the line. We need to regulate vendors who make and sell the products. Regulations are heavier on consumer. We need to regulate on the manufacturer side.
- Do we have mechanism to proactively fund protection as attack surface areas grow? As ratepayers, do we appreciate value we get? Just like you pay for insurance, you need to protection from cyber security risks.
- What is acceptable level of risk? You can spend a lot of money. What is prudent amount so that cost is considered? If utility comes to regulators and asks for cost recovery, regulators need to consider prudency of request. You can spend a lot of money on cybersecurity. We don't have answer to how much risk tolerance we have.
- Open Issue: Finding appropriate risk level of risk tolerance (balancing cost and benefit)
- Need to have definition of what is cyber secure from utility/regulatory perspective. Vendors need to invest to address these concerns and incorporate into products. Question, if we invest in this technology, will utilities value the investment. Did we just do overkill? We are helping to define middle ground. What do we need to accomplish first and foremost?

- On bulk power system very clear, and distribution system less clear. Bulk power system requirements very clear, clear processes and procedures. For distribution, there are many security protocols (what type of encryption – lots of choices). More difficult for distribution – lots more touch points that are starting to be enabled. Also, many more options to address.
- Chairman – Any consumer device that is connected to grid (even indirectly) needs to be considered. What if all refrigerators turned on at the same time?
- Need better cyber secure interface so they can't attack into network.
- For attack space, need well-defined metrics to establish baseline. Extremely important. What is baseline security? Need to know. Must have methodology and tools that can help vendors develop products to establish baseline security in their products.
- Smart Grid telecom networks with introduction of DERs. Quite a bit of latency with DER. The more we add to these networks, the more we create risk. Do we see them getting quicker and more resilient? We need more discussions.
- There is an assumption that backbone will handle all the traffic. As traffic increases, may be swamping backbone quickly.

II. Participant Comments – People

- How do we find partnership between utility companies and customers? We can only secure our grid with everyone's participation/contribution.
- It's an entire grid system question- how do we foster policy to foster collaboration between stakeholders?
- IT/OT convergence. IT people just doing normal business. OT engineers doing normal OT. Need to integrate two different workforces.
- Training – red team/blue team exercises. If you look at what UNIX administrators do when you have an attack, she knew what operating system looks like. Need to really understand what types of training do we really need? We need to define skills and experience needed clearly.
- Industry and workforce education needed, but we also need average consumer education. With all new technology, everyone can have a NEST or similar product that interacts with the grid.
- Agree, we do workforce development . . .set direction with bold ideas. Require all residents of state to have cyber driver's license. Thinking about the number of people. How many do police, fire fighters, etc. We need to have active cyberdefense. Some elements of defense may not be civilian role. When you look at response of law enforcement and firefighters, we have certain critical assets that are cyber-guarded. We need to be much more efficient to detect and respond with public safety mentality.
- How do we use AI and machine learning? How do we supplement human capital that is really being stretched in this area?
- Need to communicate vision that is inspiring, particularly to young people. Imagine getting letter from internship from Apple or utility. What would you accept? Where does money come from to do that?
- How hard is it for DHS to recruit? That is tough. Need to look at Office of Personnel Management. Lots of different pieces.

- Talks about cyber capabilities we build to defend nation against cyber. When you look at limited capacity of education system to create optimal education. Need to create collaborative environment so we can learn from each other. Must have environment where you can share information and learning. No one person will have enough technical skill. I don't think there is enough band width to develop workforce to be cyber defender. We need to learn from each other through the ecosystem.
- DOE sponsored cyberhack event. 28 universities were involved and it was really inspiring from workforce development perspective. There is now a way to scale physical models. Third year of the program. It continues to double in presentation. People should sponsor these events. This is another way to provide students with real world, hands on expertise.
- Need university to university collaboration. University of Illinois offers a summer school program, it is a good model to how do we make collaboration happen and sustain it.
- Prof. Sauer and University of Illinois runs a summer school- good way to get all stakeholders together- hands on planning exercise- similar models exist at other universities. Several models exist, elaborating them and codifying some comprehensive way- a cyber exercise of summer programs to date could be helpful and important. Making the collaboration happen is extremely important.
    - Course offered every 2 years, previous three years are available on DVDs. They are week long tutorials. Next one is next summer. It is important part of UI's research to pass on what we have discovered and pass on to industry.
    - **ACT**: Provide link to videos produced by U of I

III. <u>Participant Comments - Process</u>

- We talk a lot about security processes. We need to change business process as well. We have a ton of business process already. Needs to change business processes to embed cybersecurity.
- One of things we have done well is collaboration; looking at what future is looking like. It is important to do change management because people don't like to change.
- We have installed much more distribution automation. The big business process we put change management into our projects going forward. We have started to turn over aging workforce in field. There is less resistance among newer employees.
- We are using industry frameworks for assessing risk – NIST and DOE. We look at industry best practices and standards established by others.
- (Vendor comment): Over last two years we have done hundreds of assessments with utilities; industry has gravitated towards NIST framework as well as using NIST maturity model. This has been very positive. Generally, the industry has switched from ISO to NIST.
- Focus thinking on inset management and operating while compromised.
- National Lab: We are looking at how to transform grid and use artificial intelligence. Customers will be >>> of smart grid environment. Customers need to be trained on how to use their devices, how to connect to smart meters. When I look at apps – utility apps don't protect data in terms of privacy. This will be big trust issue. Look at aspects of how IT, OT and data sharing/privacy is handled from customer perspective.

- How do you drive cross-sector coordination (telecom and utility communication systems)? Utility in reactive mode for what is being put out there for consumer. Focus on objectives rather than "how tos." Using different encryption systems is good so if someone gets in not all are compromised.
- CEOs have to attest to financial compliance, should consider having attest to cybersecurity compliance.
- What is state of compliance now? (Co-op, muni)
- ICC does not regulate municipals and coops. Executives are asking to identify and categorize assets and following NIST approach.
- Utilities ask how to position so we can go to regulators to get rate recovery. On this side (software) how do we make business case. How do we not over-regulate but get rate recovery to get what we need to make distribution upgrades?
- Regulation of grid itself as opposed to products connected to grid. Need to consider how do you control all devices so they meet certain standard to protect the grid.
- Consumer wants choice and access. You can't regulate consumer, need to think about this.
- The grid is made up of pieces and parts, but not all parts are regulated. How do we address pieces that are not grid building blocks that are regulated?
    - PJM is audited, not official certification but auditing takes place.
- Regulations for products. What do we do about the ecosystem or IOT. Microsoft wants to get Azure/CIP certified.
- Vendors should have a responsibility to have a minimum level of CIP. Is there a way to create a minimal baseline? How do you define what secure is? Who should define that. There must be the possibility of a minimum level of security for devices that connect to grid. How do you develop regulations, standards and enforce?

Next Steps

- **ACT:** Let's think about framework to think about how much risk is acceptable. (Chairman recommendation).
- **ACT**: Provide link to videos produced by U of I
- **Suggestions**:
  - Structuring the discussion, a little bit- break down the problems we are facing, what are the solutions? How best to implements those solutions within the topics?
  - Write structure of discussion in advance- appropriate times to interject
- WGMs please send in suggestions or comments on how many speakers and content for speakers?
- **Next Meeting is April 27, 2018 from 9:00 am - 12:00 pm on WebEx.**