NextGrid: Utility of the Future Study
WG 3: Reliability, Resiliency and Cyber Security Working Group Meeting No. 2
April 27, 2018

Working Group Leaders:
Manimaran Govindarasu
Dominic Saebeler

MEETING SUMMARY

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

Agenda Item I: Meeting # 1Recap, Introduction to Topic Matrices, other Updates

Manimaran Govindarasu, Dominic Saebeler and Wei Chen Lin -(see presentation slide deck.)

- Agenda review: 1st will recap and provide an overview of the first meeting. Followed by 40 minutes of presentations from ComEd, WSU, and PJM. Subsequently the WGL, Manimaran will provide an overview of a priority list. Then the meeting will open for discussion.
- Meeting No. 1 Overview:
    - Overview of WG 3 focus is on reliability, resiliency, security.
    - In order to really understand reliability, resiliency and security, topics are further broken down into technology, process, people, regulation, and compliance.
        - The WG will discussion each area.
    - WG 3 meeting no. 2 will focus on technology.
    - Another category – education may be added because it is a theme throughout all subcategories that we must continue to educate everyone throughout process.
    - Ameren, ComEd, MISO, PJM were invited to give presentations and share their thoughts on priorities.
- Meeting No. 2 focus is on the technology aspect
    - The Technology discussion will consider 9 topics. (see matrix of priority topics)
        - Challenges of technology for achieving reliability, resiliency, security of modern grid
        - Opportunities that we have
        - Potential solutions
        - Key action items to address challenges

The list of priority topics for technology include:

1. Harmonizing the pace of IT and OT deployment cycles; bridging the gap between legacy infrastructure (slow/long) and new technologies (fast/short)
    a. Seeking input on opportunities, solutions, potential action items
2. Assessing the dynamic threat landscape: Expanding the attack surface with cyber technology deployments and IoT integration

   a. Seeking input on opportunities, solutions, potential action items
3. Integration of DERs and microgrids, managing increased complexity of: "smart" inverters, ADMS, system architecture.
   a. Seeking input on opportunities- designing a better system for integration, solutions, and potential action items.
4. Addressing security of emerging technologies as they integrate with the grid (including third-party infrastructure and solutions.
   a. Seeking input on opportunities- address both security of device itself and overall grid security, solutions, and potential action items.
5. Ensuring security of external interactions: customers, third-parties, vendors, peer utilities, ISO/RTO to address impact on utility operations and overall grid.
   a. Seeking input on opportunities- segmentation, standardization, interoperability, solutions, and potential action items
6. Improving grid's ability to tolerate natural extreme events (both frequently occurring events, such as storms and floods, as well as rare but high impact events, such as earthquakes and geomagnetic storms).
   a. Seeking input on opportunities, solutions, potential action items
7. Enhancing grid's ability to detect, isolate/contain, and recover from targeted physical and cyber-attacks.
   a. Seeking input on opportunities, solutions, potential action items
8. Architecting communications networks to meet the evolving reliability, resiliency, and security requirements of the future grid.
   a. Seeking input on opportunities, solutions, potential action items
9. Integrating intermittent energy sources while maintaining reliability and resiliency
   a. Seeking input on opportunities, solutions, potential action items

   - A lot of things need to be defined and filled in.
   - Additional topics include:
     - Responding to consumer-driven marketplace
     - Proactive
     - Ransomware or malware
   - Going forward, smart grid and modern definition – We are looking at the cyber-physical system -- not just physical.
     - See diagram from NIST – 7 domains. Related to physical infrastructure. But others related to cyber. Much more complex cyber-physical system.

Agenda Item II: Technology Presentations

I. <u>Adam Hahn, Washington State University</u>

- Challenge 1: Harmonize IT and OT deployment
  - Significant challenge on grid. How long do technologies last? – look at chart.
  - Offer platforms – ten years on average. But what if ICS has longer lifespan? Cryptographic protocols are a little longer lasting technology. More conceptual. Cryptographic algorithms

are even longer. Definite problem with software programs and cryptographic protocols to use in long term technology.
    - Processes and procurement language and legislation. Heard a great idea from Australia – if stop supporting something, make it open source.
- Challenge 2: Dynamic threat landscape
    - What we are seeing -- DER becoming critical security concern because there is a new attack surface with DER. If we see heavy consumer adoption and ownership of PEVs, people own at their homes, and they are not security experts. How can utilities connect to DER devices and control them? Volt Var control for example.
    - Also, these devices are consumer friendly and connected to the internet of things. The device talks to some vendor cloud or system. Could be a single system connected to 100k devices, and an attack to those devices could cause a problem. But don't know what is connected.
    - Solar city. Panels in people's houses. Will have systems connected to large number of devices.
    - Will be connected to home wifi networks and have vulnerable routers and systems that they depend on for communication. Chance for attackers to compromise DER devices and cause impact on grid.
    - One opportunity is to come up with additional methodologies to assess risk. If we look at information, figure out what vendors or PPAs are being used commonly in the area, and use it to build graph models showing connectivity and how much DER critical systems can control. Key nodes in there that can connect and act as large number of DER devices.
    - Physical side- Opportunity to model what would happen if someone took out a large cluster and attack all DER devices on a critical node, what is impact on system?
    - Another challenge – emerging technology interacting with grid. Smart phone, email and apps. Security of iPhone is impressive – great secure processes and biometrics and pure elements – great best practice features. If you look at devices for IoT on the grid, they are increasingly important, but security devices they advertise (password and encryption) -- not state of the art security. Opportunities to add better security features.
    - What we are doing – use tech in armed processor, trusted secure environment. Phones use it all the time for secure pay features and biometrics. If you get malware on the phone, it can't tamper with secure components. Secure component may have cryptographic model with its own key and signing. Develop architecture for smart inverter. Trusted environment can read from hardware, and sign, and pass to rich environment. So by doing this, have to assume that IoT devices have compromised rich environment, malware in it, or out of date. But trusted environment should be trusted, small, and secure from all that stuff. If you get trusted rich environment, pass on signed message, even if it is compromised so attacker finds it harder.
- Challenge 3: Expanding attack surface
    - How do we manage the growing attack surface? If attack from one of these devices, could propagate to control center. Need mechanisms to ensure that won't happen
    - Attack surface reduction techniques – combo of approaches people have been using, and emerging tech not used as often. From non-tech approach, NERC CIP – benefit of non-routable communications. Rather than Ethernet, use serial.

- Get rid of digital communication when you don't need it. Ensuring systems have less noise and nimble technologies. Understand operation and activities better.
- A lot of emerging tech – software side. Interconnection of system and temporal aspects. Software – modern operating systems prevent malicious data, randomization, make difficult to compromise systems. Implemented in most software we use every day. But in industry, don't use these.
- Furthermore, system side. Virtualization and containers. Could provide dynamic things like ensuring rebooting systems.
- Network side, diodes. Granular ability to control and monitor flows. Diodes provide one-way flow and authorize flows based on that tech. Both tech and non-tech approaches.
- See what is connected to what. Look at platform and see what its connected to, and what risk is based on that. This is a tool to understand it.
- Important tools, but caveat is that we have a lot of technologies, but need to verify they work. Don't install tool and magically have security. To install something correctly, must know a lot about environment. Firewalls, authentication, information flow of system. Sophisticated network and IDS. Hard to validate and know it is working well.

II. Jonathan Moken, PJM

- General context – "resiliency" increasingly being discussed in industry. However, we do not have an increased understanding of the term.
- PJM's working definition of resilience = "the ability to withstand or quickly recover from events that pose operational risks."
- From PJM perspective, to understand the term resiliency- looking at -- prepare, operate, recovery. Only when combine this definition with FERC's proposed definition = "the ability to withstand and reduce the magnitude and/or duration of disruptive events, which included the capability to anticipate, absorb, adapt to, and/or rapidly recover from such an event," - does it have a positive effect on resiliency.
- Risk assessment model is still illusive to PJM and all companies – need to measure, quantify and better understand if resilient. Good place to start is to understand context of risk and environment you are working on.
- Resilience scale risk. Not routine stuff baked into reliability standards in industry. Not binary issue of whether electricity is available or how long unavailable. It's the many shades of gray that create an event – geographic footprint, duration, etc.
  - Good example right now – raised awareness -- physical threats to substations and CI.
- Potential risks- Targeted attacks have a much higher risk level than discriminatory attacks in nature, such as a storm. Storm won't hit most critical infrastructure simultaneously—will have warning.
- 2012 Superstorm Sandy- not weather event itself, but example to not learn the wrong lesson. Response and recovery was good from utility perspective – high restoration levels during short time. Failures that were near to occurring did not occur because of interdependent system. Natural gas generation, communication resources, maintain visibility in system. Water pumping system narrowly avoided issue with patchwork generation, but close to having bigger problems. Resiliency is about avoiding tipping points of interconnected systems. Other systems we need to restore on our own must be available to us.

- Geomagnetic storm – can't stop it. But 100% chance it'll happen. Geographic footprint of impact – interconnection. Exceeds geographic scope of what we've seen. Impacted area – challenges core assumption of accessing electricity from unaffected areas.
- Manmade or natural events – NE blackout. System operation visibility. Not much damage to infrastructure – it was question of how well we can see system. Bad data, old data, making poor decisions – cascading outage. Operational issues.
- Ukraine power grid – has potential effects on grid. Loss of control for operating work station. Worked their way to permissions and access to open breakers – OT impacts. Not worst-case scenario – if you corrupt data, convince people that something is happening that wasn't happening to them. More profound impacts on system. Compromising protocols. Cause significant system damage – wasn't widespread infrastructure damage to extent it wasn't recoverable. If physical damage is so widespread that we can't restore, that's problem
- How to mitigate this stuff. This is how PJM approaches it
    - 6 focus areas contributing to resilience. It is not a one and done silver bullet. Several things need to be done in coordination. If just about infrastructure, could focus on one thing. Security is integration of physical and cyber security – can't have one without the other
    - Examples – prepare, operate, recover. Things we can do to prepare for these events. Better restoration drills, coordinate with partners, looking at things like infrastructure improvements, generation resources secure in adverse operating conditions.
    - On operations side, can look at things like tertiary communications recognizing that data links could be severed, or something not available to us in Blue Sky. Communication redundancy – need to identify critical data needed for acceptable system operation.
    - Recovery side – flexible solutions and recognizing that setting targets is important part of achieving resiliency. Acceptable timelines and goals. Taking CI into account.
    - Decisions must be made with different litmus test – need holistic approach.

III. <u>Carol Bartucci, ComEd</u>

- We all want reliability, resiliency, security for our grid and customers. They are all intertwined. Can't have security without reliability and resiliency. All three are in mind as we build out the system.
- Current state – described in 3 towers –
    - 1.) what is it - data we are collecting, what data comes from – smart meters, DA devices, substation equipment.
    - 2.) how does it get where its' going – communication network.
        - With intense security, there are no openings to outside world to let hacker in.
    - 3.) data in the system. Where does it go, how is it used?
- Communications has become a critical system. Network enables data flow and gives us visibility to the status of the grid. It will only get more critical over time.
- This is a high-level picture of what the network looks like- 3 tiers:
    - 1.) fiber backbone – backbone of the network. Always runs through the fiber - significant bandwidth and high speed.
    - 2.) medium bandwidth networks.
    - 3.) field area networks

        - In field area, 10k devices that we connect wirelessly to – grows quickly. 4 million meters – going up to 4.2 meters – growing attack surface and no question that is happening. More devices on the grid to get data out of them. Cannot stress enough to build security across the whole network. Security runs through everything we do. Every time we add new devices to it, have to test everything and make secure.
- Variety of technologies – standards driven. We are moving toward having less of a variety of network components, standardizing network infrastructure. Itron – current wireless network to attach to end components. 1800 miles of fiber. 100 firewalls. 3k access points. Carrier based private LTE. A few other technologies. We drain network to the right – drain into higher bandwidth or higher speed – 3 drains to 2 or 1. Gain speed and bandwidth.
- What are these networks made up of?
    - Speed with each
    - Called out some of technology we are using and what we want to standardize
    - Fiber – DWDM – high bandwidth to get more usage out of fiber infrastructure.
    - Medium tier –4g LTE.
    - SSN network, Itron.
- Future communication needs
    - Where are we going, what do we need, how to make resilient and secure.
    - Communication needs to be much more complex – more devices, more security to build in. Speed and bandwidth. Intra-device communication – think there is a place for this. Think end devices will speak to each other. How do you maintain something like that? Configuration management must go on with that. How are you going to secure it?
- Smart meter network – pinging the meters. Now it is a common term. Ping and reach out to meter to understand status. Helpful in outage situations. Restoration of the grid has become dependent on new tech – make it efficient to understand outages. Next slide talks about what our future communication might look like. Combo of strong fiber background and wireless tech for grid edge devices
    - 5G, LTE play – looking at these things.
- Cybersecurity at Exelon
    - Cyber and physical security controls – based on NIST framework. Left to the right. Having intelligence, identify where problem, protections in place, also detect if something does happen and respond and recover. We want to not just protect with one layer, but multiple layers.
- Evolution of cyber threat actors
    - Not meant to portray anything specific to Exelon. Just illustrative.
    - Required actor knowledge – used to need a lot of knowledge. Now knowledge required has dropped. Severity and attack sophistication has increased. Significant and evolving threats. Number of attacks increased, skill and knowledge decreased
    - Easier, and many more groups
- Overview of strategies
    - NIST
    - Projects and efforts have reduced risk
    - Plans continue to evolve and mature

  - Continue to prepare for hazards through training and exercises.
- Electric subsector counsel:
  - Coordinating counsels
  - Specific to electricity subsector – principle liaison to federal government and electric industry.
  - Strategic infrastructure group. All of these different groups – electric, financial, communications. Brings in all CI groups to work through response and how to work together when something does happen.
  - Always assume it will happen, make sure protected if does happen. Response team. Coordination across government and agencies.

Agenda item III: Technology Discussion

CHALLENGE ONE

- **Working Group Leader (WGL)** – Number one challenge – harmonize IT and OT – legacy is slow and has long deployment cycle. IT tech 3-4 years things change. More sophisticated attacks.
  - How do we find solutions?
- There is a disconnect between ability to write off cost of investment of cybersecurity and useful lifespan of the technology. Policy point of view – how that impacts gap of deployment – slow OT.
  - WGL– Cross linkage in in policy discussion
- Need tactical solutions and opportunities. When talk about legacy infrastructure devices on system today, many are cyber obsolete in a way, only so much you can do to bring up to cyber standards today. There needs to be some focus around things like implementing bump in the wire solutions- look at several providers, provide third box, cyber security device to go in front of legacy devices – interfacing to control systems in back office
  - Second opportunity and challenge for utilities – even if upgrade them, need firmware software upgrades. Challenges to how to do that to thousands of devices in the field, especially if don't have communications system to do remotely. As more threats occur, third party bump in wire, policies and procedures and need to invest in those in order to do. It takes investment, new tool sets, new communication systems to do remotely.
  - WGL- are long term solutions? Technology perspective aside from bump in wire solutions?
  - Retrofitting legacy devices with new platforms – secure boots, hardware and software security advancements. Options to go and do, but need investments for utilities to swap out and bring up to standards of today and future.

CHALLENGE TWO

- Challenge 2 – Priority Matrix. Expanding attack surface with smart grid deployment and IT integration. Grid security for cyber expansion.
  - WGL- question. As this is evolving and expanding attack surface is growing due to new technologies. Are benefits from integration of new tech outpacing additional work and threat of security? Are they even? Is benefit same as risk? Doing it to hope we change dynamic? Cost of overhead more of a challenge?

- Academic answer, rather than real world opinions. Will change as become interconnected. Can go from no to yes very quickly. Ransomware and IoT attacks – weren't threats to grid at first, quickly relevant threats.
- WGL– early stage and later stage of threat, depends on what part of continuum you are looking at.
- WGL- can segmentation type of technologies – equipped to deal with this type of enormous growth of IoT devices. Washington State University Presentation on communication devices. Is there new architect of solutions out there that could be promoted aside from network segmentation?
- NIST framework for risk assessment. First step of any risk assessment process is to assess components you are working with. But you can no longer do that. Don't know what is out there, and what is connected to what, thus can't assess components.

CHALLENGE THREE

- Challenge 3 – integration of DERs and microgrids. Managing complexity of smart PEVs and smart distribution management system. How do we manage the grid resiliency, security, reliability? How do we make sure those are secure? How many DERs do you need to compromise to have notice of a load loss?
  - Large deployment of DERs and microgrid.
  - Approved through recent legislative sessions - -microgrid in Bronzeville area.
  - This is opportunity to take a look at diff roles of utilities – NERC functional model. Where devices being connected? Depending on locale. Multispeak – interfaces of ADMS.
  - NY, CA – provide you some point of view of challenges, recommendations to address DERs.
  - Looking at architecture. In some ways, looking at how we are going to operate ahead of system architecture or what existing system can handle. Working in conjunction with vendors, understand type of information we need to get from DERs, microgrids, etc. to have visibility to make sure getting all information to ensure we are reliably and safely operating system.

CHALLENGE FOUR

- Challenge 4 – third party infrastructure – equipment and resources into these environments and how we address those challenges. As technology emerges, challenges emerge. HR, vendors
  - WGL – putting devices in on the edge, are we making sure that those devices are secure in and of themselves, and not a gateway for security of overall grid?
  - WGL– relying on third parties. Utilities may have own communication infrastructure, or rely on third party.
  - Really wide area of topic. This could benefit from subparts. Research done to create interoperability test tools for cybersecurity. Research into best practices for vendors when creating these products so more secure when get released. Vendor could assess themselves on entire life cycle process. How to improve over time. Look for some certifications.
  - Look for areas of consensus. We may all have jumped to more tech discussions, one thing we can all appreciate that this is complex. Carol's presentation around

coordination at Exelon level underscores interrelated complexity around these issues. Comment – utilities are responsible for building the physical and cybersecurity capacity of the grid. We have a regulated responsibility to secure our systems. Not just systems, but training employees, mechanisms to mitigate risks. Not just tech themselves, but new vulnerabilities that need to be mitigated. Moving away from one-way flow of data to decentralized, bi-directional model. Enabling interaction of devices, not just hooking up to grid.

- Bring up as we are building or planning for these new devices and our networks and edge keeps expanding. Utility may or may not have insight or control. Architecture needs to take into account – parts of network connected to grid that we cannot trust. Proceed from assumption that there are going to be areas of our networks – some are compromised or can be compromised. Give them solid requirements for what can and cannot be connected to our networks from the grid. Not from device or manufacturer perspective, but what those devices need to be able to do – be updated, specific security configuration, and it will be a multi-layered approach. Need to assume that these devices are compromised or can be, and we don't trust them.
- Capability to perform automated disconnects, comes with security concerns. Weaponizes customer service. Daily shut off limit, less than 1% of devices. Limits outages that could be created. Simple control.
- Don't have a lot of standards for interconnection, aside from physical interconnection requirements. Think of cyber standards as well. Governance questions as well from ICC or appropriate entity. Policy discussion
- Using new tech, can backfire if no limits.

CHALLENGE FIVE

- Challenge 5 – sharing information, data, peer to peer interaction of utilities, RTO interactions. Customer interactions on the system. Looking at energy data. Some kind of overlap, but good to lay them out. External interaction of different flavors –
  - Identifying what those external reactions are. E-tagging, etc. One of problems with putting secure ICCP in place, lack of defined certificate authority.
  - WGL- what about data sharing? Agreement in place, and how do we make sure this is followed?
  - Ongoing discussions – what is level of detail and how do you do info sharing? Private industry has a lot of interesting solutions – cross strike, etc. how those external interactions play. At GridX – practice on how you work information sharing and best practices to make sure right people that you interact with. Call whenever you need – trusted way to discuss.

CHALLENGE SIX

- Challenge 6 – extreme events. Naturally occurring. Snow storms, floods, high impact low frequency events – earthquakes, geomagnetic. Regularly and irregularly occurring. From resiliency and restoration perspective. Many studies on this.

- WGL– looking at our grid, are there suggestions of some newer technologies emerging, any really focused on this area? Are there things economically and achievable?
- Solutions bucket. Grid reliability and resiliency – in terms of availability of solution today, self-healing systems. More feeder segmentation that can be done. Most feeders are segmented very limited fashion. If you segment feeders more, isolate problem areas and use self-healing to identify issue and re-route power. Automated way without human in the loop. Microgrids, DERs fold into opportunities and solutions here. Have to keep in mind cybersecurity of those as well.
- Look at three different cities.
    - New York – new set of resilient infrastructure investment guidelines for the city. Interesting way to combine and integrate with utility so everyone was aligned with growth and construction to address extreme weather. Relied on modeling materials from their partners at NREL and elsewhere. Building toward greater frequency of weather events.
    - Boston – resiliency plan that integrates work with utility.
    - Chicago – Q1 breakfast on resiliency. Consensus was that it would be helpful to do simulation exercise with catastrophe level event. Series of events to see the blind spots of cross sector collaboration.
- Very practical and important. How much do they take into account naturally occurring events? In conjunction with cyber in isolation into city planning?
- MIT Lincoln labs – studied Boston's emergency evac plan. Microgrids. What if event was dark sky event? Integrate DoD into report. 75 people died trying to get out of Houston just because evacuation not properly planned.

CHALLENGE SEVEN

- Challenge 7 – technologies to protect, isolate, contain physical and cyber-attacks. Technology building blocks and architecture. Protect and isolate. Prevention technologies. This is about detection, mitigation, containment, etc. More operational issues. Cyber and physical attacks.
    - What is communication that can handle in real time that isn't more vulnerable to cyber attacks?
    - WGL– Challenge 8 refers to communication.
    - Globally, rationale for it and didn't have Sandy to point to in Illinois. But there was robust discussion on formulation of this at commission and among stakeholders. Tornados and heat in Illinois. Could provide nice segway into policy discussions on weather conditions and securing fuel supplies for generation. For ComEd, we have a lot of info around smart grid investments. Simple hardening of system, and investments like microgrids.
    - WGL – idea of targeted physical or cyber-attack. Specific thing we should look at from action standpoint -- is response and recovery different for targeted physical or cyber attack versus a natural event that causes disruption? Are challenges markedly different?
    - To your point on recovery, from cybersecurity targeted attack we can look at what happened in Ukraine – one of differences is that it takes longer with targeted attack to actually verify and feel confident you are not just restoring service, but also that whoever is attacking you is not still there with back doors and lurking on network. From

that standpoint, a lot more computer forensics. Have to restore service, but how long does it take and how long before we are comfortable that we have eradicated that threat?
    - WGL- Unique to cyber-attacks. But follow up question – if event happens, is it easy to identify? Equipment failure, line outage, but could be triggered by cyber-attack. How do you determine response? What is the detection?
    - Involved in conversation with some of our field staff. Working through it right now to determine at what point does an operational event look like it could potentially be a cyber event? We have robust response program for cyber events, but missing at what point does a lineman troubleshooting an operational event, what triggers that it is a cyber event? Would love to hear from others. What type of technologies or process or procedural things – what point do we say this is a cyber event?
    - WGL- hard to get comfortable to share with peers for fear of alarming others. We limit what we tell others, but we want to share with our peers. How do we share intelligence with each other to help greater grid?
    - Recovery and response question. Value of those simulations with right group of people who can simulate attack we are talking about. Integrated response levels. Argonne resources to create those universally acceptable responses. Similar response escalation. If it is a cyber-attack, it is malicious. Want to leverage any existing disasters or problems. Extreme weather event is ideal time for cyber-attack.
    - When dealing with cyber or physical attack, response is different than natural event. Physical attack – typically field personnel sees something that auto triggers something is not right. They know there has been an attack. Separate path, notifications, involvement, etc. Cyber events are more challenging. You don't see it typically. One comment is that we have done internal and external entities around simulating a cyber attack. One of challenges we have is ensuring that not only folks in field understand, but also from an operator perspective in control center, things happening that are atypical to what they would see (diff from equipment failure) – equipment operates but no fault. Get a sense of something else going on. Making sure that people involved that see things happening on system every day, understand when something looks different. Ensures right triggers come up.
- Number 8 – skip. Communication architecture
- Number 9 – intermittent energy sources. Intermittency. Not cybersecurity issue, but making grid reliable could be things from load side also. EVs integrated. Broader challenges from smart grid perspective.
    - Collaborate with other working groups.
    - WGL–As we integrate these new technologies and resources, still able to keep grid reliable?

Agenda Item IV: Next Steps. Whitepaper Sample & Template, Feedback and Resources, Future Meetings

Adjourn