PNNL-26621

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965

Defending the Electric Grid from IoT

May 2017

JD Taft, PhD

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)

Defending the Electric Grid from IoT

Draft Version 0.2

JD Taft, PhD[1]

May 2017

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

Pacific Northwest National Laboratory
Richland, Washington 99352

[1] Chief Architect for Electric Grid Transformation, Pacific Northwest National Laboratory

Contents

Figures

Tables

1.0 Part I: The Problem

The traditional cyber security problem for electric utilities and the grid involves the compromise of grid devices and utility systems via any of a number of communication ports or information transfer mechanisms. The problem therefore involved the prevention, detection, isolation, and mitigation of attacks along these paths. *The problem has changed*. This is not just recognition of smart devices as security vulnerabilities – that has been widely discussed for some time now. The issue here is that the grid cyber security problem has changed *structurally*. It is necessary to understand this insight in order to think about how to protect the electric grid in this emerging environment.

The emergence of a wide array of devices that have internal computing capability, combined with inexpensive and ubiquitous communication connectivity has gone well beyond cell phones and webcams to include many devices that comprise significant loads on the electric grid and/or can interact electrically with the grid in non-trivial ways. Since the communications connectivity for these devices is largely via the internet, many new possibilities for access via bad actors have become available. In cyber security parlance, the threat surface had greatly expanded. In general, the networking of "smart devices" is called Internet of things (IoT) but in terms of the grid this is sometimes called the Grid of Things. The Grid of Things is the source of the structural difference that is the focus of this paper. Before delving into the structure issue, we outline three new scenarios for electric grid cyber vulnerability.

1.1 Some Newer Scenarios

1.1.1 Bad Day in the Life of the Grid #1

A bad actor creates a highly addictive game application for smart phones (think cross between Candy Crush and Angry Birds). It is downloaded millions of times. However, it also contains hidden code that can break into the phone's IoT remote control apps to manipulate home and business electrical devices. Because the IoT app is authorized to control those Grid of Things devices, securing the devices makes no difference. Upon a signal, or at a pre-set time, the malicious game app uses the IoT apps to bounce loads and other devices in a synchronized manner. This causes not just sudden apparent load shifts but voltage fluctuations that cause smart inverters to pull off the grid en mass. The resultant volatility trips protective systems.

1.1.2 Bad Day in the Life of the Grid #2

Aggregators of Demand Response (DR) and managers of buildings and Distributed Energy Resources (DER) control various Grid of Things devices mostly via internet communications. These Energy Services Organizations (ESOs) have servers that may be located in a different state from the controlled devices, maybe not even in the country. Bad actors may invade the ESO from the outside or from the inside to perform grid attacks like the one described above.

1.1.3 Bad Day in the Life of the Grid #3

A bad actor recruits millions of IoT devices (none of which need be Grid of Things devices). It then uses the commandeered IoT army to perform denial of service attacks against ESOs, system operator dispatch communications, or grid sensing and measurement systems that use telecommunications service provider networks. Attacks may be against network services, such as happened in the recent attack on DNS

provider Dyn.[1] Such attacks can be indirect, going after essential services or other non-utility/non-Grid of Things assets in order to affect utility operations.

Traditional views of cyber-attack focus on some form of invasion or compromise of utility information systems. Consequently, many grid cyber defenses focus on dealing with unauthorized data flowing in utility communication networks and in utility software systems.

> Note that in these scenarios, no unauthorized data transits any utility communication network.

Another issue is that while it may take considerable skill to *create* some of the code that carries out cyber attacks, it does not require much skill to *use* such code and these tools often become available on the internet.[2]

1.2 Connectivity is at the Root of All Cyber Evil but It Is Worse for Electric Grids

Traditional network security theory teaches that any connectivity (meaning information connectivity) represents a potential cyber vulnerability. This includes intermittent connectivity such as through a USB thumb drive (think Stuxnet[3]) as well as through continually connected networks. It is **not** a matter of using any particular protocol suite; any connectivity may be exploited, not just connectivity using routable protocols, for example.

The situation for modern electric grids is complex, as illustrated in Figure 1 below.

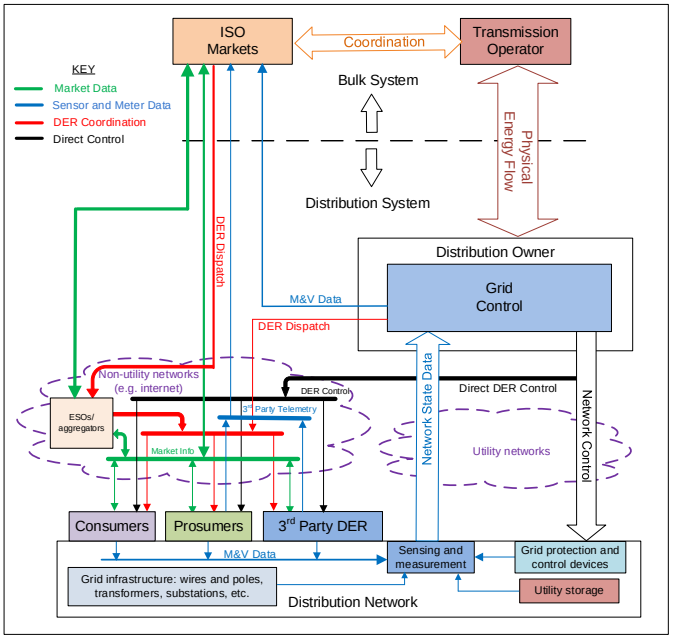

Figure 1. Some Grid Data Flows

[1] https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet
[2] https://bgr.com/2017/05/17/wannacry-computer-virus-variant/
[3] https://www.cnet.com/news/stuxnet-delivered-to-iranian-nuclear-plant-on-thumb-drive/

There are many information paths and possibly multiple non-converged communication networks in use in electric utilities. Some may be privately owned by the utility; others may be operated by telecommunication service providers and utilities may use a mix of both.

Figure 2 shows a simplified communication connectivity structure model. Note that in the diagram, the box denoted utilities denotes potentially multiple entities, such as transmission and distribution operators, generators, system operators and balancing authorities, reliability coordinators, etc. Consequently there will be communication among these entities that is not shown in the diagram for the sake of simplicity.

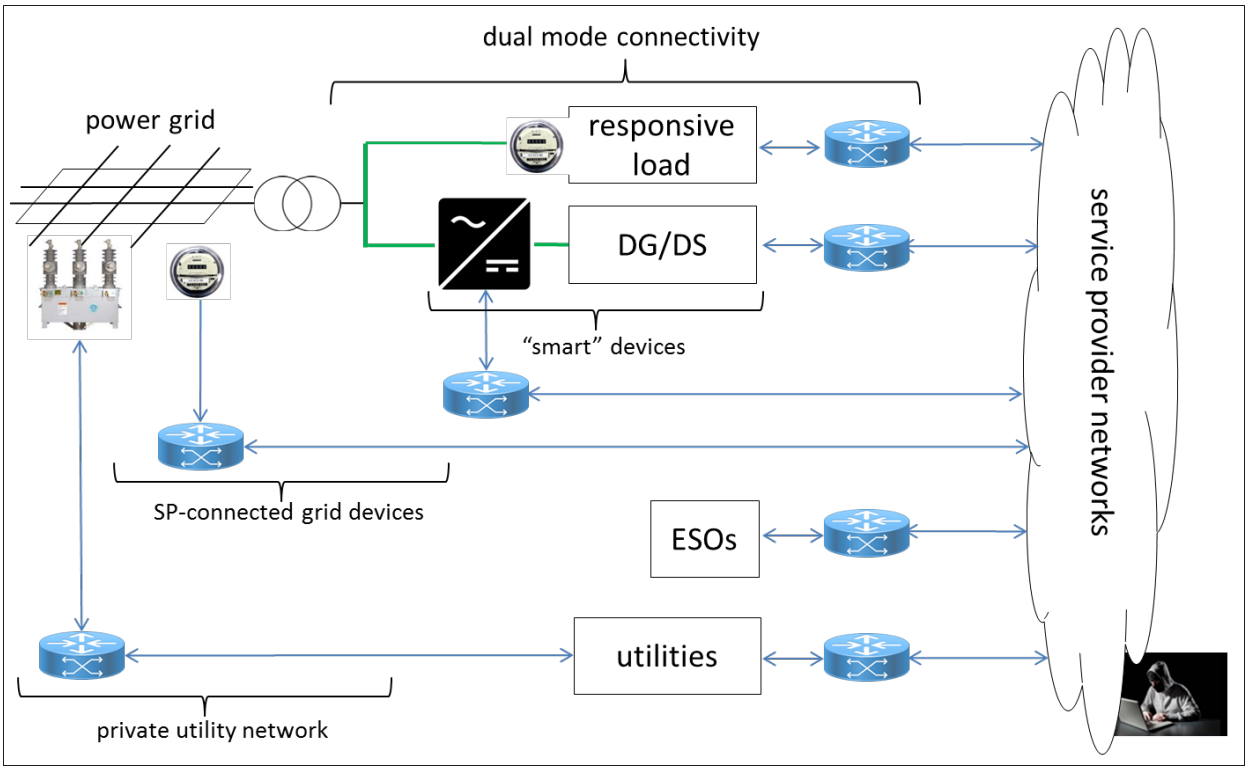

Figure 2. Simplified Utility Connectivity Structure Model

A careful examination of Figure 2 reveals an issue that does not arise in most cyber security discussions, namely that there are two forms of connectivity involved in the grid. This was not much of an issue in the 20th Century, but with the proliferation of smart grid edge devices (especially those not owned by the utility) the possibility of creating undesirable interactions arises on two fronts. The problem is with remotely controllable loads, distribution connected generation, and distribution connected storage. Due to the ubiquitous availability of cheap connectivity, such devices, now being called Internet of Things (IoT) devices (Grid of Things devices in some parlance), may be accessible via the internet and therefore by unauthorized parties. This is what leads to the Bad Day scenarios at the beginning of this paper.

The grid involves two forms of connectivity: one is the traditional information connectivity described above and the other is electrical power connectivity. This *dual connectivity* is the source of electric grid operational cyber vulnerabilities that are more complex than ordinary information system vulnerabilities.

1.2.1 IoT Creates Grid Cyber Vulnerability

It is clear from the above discussion that due to the dual connectivity issue for electric grids, IoT represents a special cyber hazard. It is not necessary to compromise any utility device or system, or invade any utility communication network to be able to compromise grid operation when IoT exists in bulk. Edge devices may be compromised directly, or IoT devices (even those that are not Grid of Things devices) may be commandeered to attack the grid directly or indirectly as described above.

Many common electrical devices can become IoT devices that interact with a grid in a detailed and perhaps real time manner. Household appliances, HVAC systems, pumps, compressors, and blowers, as well as similar equipment in commercial and industrial faculties may all act as grid devices, coordinated either directly by the utility or through ESOs. DER components such as rooftop solar PV, other distributed generation, distributed storage, and responsive (remotely controllable loads) are all elements of this scenario.

2.0 Part II: Defending the Grid

The foregoing makes it clear that the electric grid must be defended from IoT-based cyber threats and that the traditional cyber security methods, while still necessary, are not sufficient. Before considering an architectural approach, we summarize some fundamentals.

2.1 Fundamentals

2.1.1 Data Connectivity

Information connectivity represents cyber vulnerability. Standard cyber security for networks involves a good many individual measures that should be applied in a coordinated and layered manner. The Appendix at the end of this paper provides a list of 30 standard network-level security measures. Networking companies know how to apply these measures in general, but may not know how best to apply them in the electric grid.

Strong cyber security safeguards do not rely upon obscurity to work. It is unrealistic to think that communication channels or ports will remain unknown or that cyber security procedures or technologies will not be uncovered.

> Cyber security measures for the grid must work, even if bad actors know how they work.

2.1.2 Roles and Responsibilities

Prior to the development of DER, the roles and responsibilities of electric utilities were clear. In particular, the responsibilities for distribution reliability and security was the responsibility of the distribution operator. With the development of DER, especially rooftop solar PV with smart inverters, there is a suggestion that distribution feeder control could be party ceded to these devices under the control of third parties, such as ESOs, merchant DER operators, or individual prosumers. It has even been suggested that distribution utilities could forego investment in sensing and measurement capabilities and distribution level communications and just rely upon data supplied by the ESOs.

With the development of DER, some of the role of grid management may be in effect delegated to an aggregator, merchant DER provider, or even an individual prosumer. In terms of cyber security, how are the employees of the ESO vetted? Where are its servers and how are they protected? How would the ESO or aggregator or prosumer be held accountable for cyber security of the grid and what standards apply?[1] The role of the smart inverter is also an issue. Since there are no security standards for smart inverters connected to the grid, and given that they can be compromised in a variety of ways, is it proper for the smart inverter to participate in grid operations? If it is, then changes must be made in both ride-through and security standards for inverters.

2.1.3 What Does Not Work

A number of ideas have been promoted as solutions for security at the distribution grid level. In the IoT/Grid of Things environment, not all of them would be effective against the attack modes described above. Some of these ideas are listed below.

Table 1. Ineffective Security Solutions

Method	Comments
Securing IoT devices	As shown in the scenarios above, devices authorized to access Grid of Things devices can be compromised, so it would not be enough to secure the grid-connected devices and it is not practical to think all the smart phones could be secured. In fact this is in direct conflict with the desire of the makers of consumer devices to provide quick out of the box positive experiences for consumers.
Grid state estimation/situational awareness	Cyber-attacks can be carried out in less than one SCADA cycle so this will have limited effectiveness
Extending NERC CIP to Distribution	For the reasons described already, this will not accomplish much.
Dark fiber	Network isolation and air gapping are valid cyber security measures, but Transmission utility dark fiber is not uniform in type and condition and would not reach to the distribution level without massive investment in extensions.
Data diodes	Two-way or even N-way communication is needed to operate modern grids; in addition, data diodes have suffered from creeping featurism to the point where some can be compromised anyway. Access control and, network segmentation, and similar methods are all legitimate cyber security measures but are not sufficient in themselves.

2.2 Architectural Strategy for Defending the Grid

The standard and exotic information technology approaches to securing the grid against cyber threats are valuable and necessary. They are not sufficient, as seen from the discussion above. It will be necessary to use an architectural approach to protecting the grid that goes well beyond IT methods. In essence, the

[1] This in addition to issues such as what happens when an ESO that has been supplying Volt-VAr regulation services to the grid decides one day to exit the business, or the problem of multiple ESOs with interpenetrated services areas (two houses on the same service transformer, each with a smart inverter trying to do Volt-VAr regulation, but connected to and controlled by two different ESOs).

approach is to invert the EPSA-style relationship between grid resilience and grid cyber security (cyber security is a subset of resilience) and make resilience one of the key levels of defense, especially against the IoT-based threats. In addition, since the grid is composed of a network of interacting structures, it is worth considering these structures and how they might be modified to make them inherently more securable. The following is a short outline of elements an architectural cyber security strategy for electric power grids.

2.2.1 Structural Security

Structural methods involve modifying or selecting grid structures with consideration for how hard or easy they would be to secure. Some examples include:

- **Segmentation** – Ability to partition the grid as necessary to contain threat effects; this includes use of microgrids and microgrid networks, feeder level segmentation, and use of coordination schemes that can be operated in both local and system-wide modes
- **Distributed Intelligence** – Changing from completely centralized analytics and control to a hybrid of central and distributed forms, so that single point of failure attacks are not successful and to facilitate the segmentation approach above[2]
- **Communication** – Network structures that have inherent path redundancy and network segment isolation capability[3]
- **Industry Structure** – Bulk system/distribution interactions structures that avoid tier bypassing and flat fan-in from edge devices to system operators; use of layering and other mechanisms to manage or eliminate multi-tier data flows at all scales in the power delivery chain.[4]

2.2.2 Resilience as a Cyber Defense

Inverting the paradigm of cyber security as a resilience measure leads to considering grid resilience as a cyber security measure. In this light, many standard resilience measures[5] can be evaluated as cyber security elements. In some cases this sheds new light on not only value, but also roles and responsibilities, ownership, and communication and control issues.

Many standard methods for providing grid resilience, such as N-M contingency planning, System Integrity Protection Schemes (SIPS), multi-stage generation reserves, redundant communication channels, etc., are helpful in dealing with the type of threats describe in this paper. To go further, it is useful to keep in mind two key characteristics of these specific IoT-based threats:

1. No illicit data traffic has to transit any utility communication network
2. The mechanism for disrupting the grid is essentially to create extreme volatility at the distribution edge

[2] http://gridarchitecture.pnnl.gov/media/white-papers/GridArchitecture2final.pdf, see section 3.3.12.
[3] http://gridarchitecture.pnnl.gov/media/advanced/Advanced%20Networking%20Paradigms%20final.pdf
[4] http://gridarchitecture.pnnl.gov/media/advanced/Architectural%20Basis%20for%20Highly%20Distributed%20Transactive%20Power%20Grids_final.pdf
[5] J Taft, "Electric Grid Resilience and Reliability for Grid Architecture," draft May 2017.

Given the ability of grid energy storage to decouple volatilities, and applying the concept of using resilience as a cyber security threat defense, we can classify grid scale storage (at both bulk system and distribution levels) as cyber defenses. Storage used in this manner must have certain characteristics:

- It must be capable of bilateral operation (electric energy into storage from the grid and directly back out to the grid from storage – this implies a power electronics interface
- Maximum transfer rates into and out of storage must be high and transfers must be fast acting (low latency)
- Storage units must be secured, operated, and controlled by the utility and so cannot be operated indirectly through merchants, aggregators, ESOs, or prosumers as a service to the utility.

These three points are consistent with the view that the "combination of fast bilateral storage, flexible grid interface mechanisms, and advanced optimizing control is a general purpose grid element as fundamental as power transformers and circuit breakers, a conclusion recently arrived at by a group of more than thirty participants during a roundtable session at the CleanTech100 Summit in Washington, DC, October 6–7, 2014."[6]

Accepting the foregoing, it becomes clear that such storage should be considered as core grid infrastructure, not an optional element like AMI. The implication of this is that for such storage, it is appropriate to use the criterion of least cost/best fit for deployment, rather than benefit/cost analysis (BCA). For this class of storage, the whole question of BCA, developing storage product market mechanisms, and the resultant issue of benefit stacking is thus eliminated.

Understanding this class of storage as a cyber security and resilience mechanism transforms it into core infrastructure and changes the design, financing, acquisition, rollout, and operation of such devices significantly and positively.

3.0 Final Comments

The emergence of IoT and the consequent Grid of Things has led to new grid cyber vulnerabilities. Much of the vulnerability is due to the dual connectivity property of grid edge-connected smart devices. Exploitation of this property involves creating excessive volatility at the grid edge, leading to an understanding that grid resilience, and in particular, proper use of bulk energy storage, can provide a defense for such vulnerabilities. The general principle is to use structural approaches to strengthen the grid's ability to resist such volatility-based threats, which is also in line with more general grid resilience goals. This approach leads to a new and useful approach to application of bulk energy storage in electric power systems.

[6] https://energy.gov/sites/prod/files/2015/04/f22/QER%20Analysis%20-%20Grid%20Architecture_0.pdf, section 5.3.2.3.

Appendix A

Standard Network Security Measures

Appendix A

Standard Network Security Measures

The following is a list of standard communication network security measures. These are well-known in the communication networking industry.

Table A.1. Standard Communication Network Security Measures

Crypto: link layer, group, and application layer; GDOI, as it has been incorporated into IEC 61850-90-5 specifically for PMU network encryption	SUDI 802.1AR (secure device identity)
RBAC (RADIUS and TACACS; AAA; NAC)	Access control: VLANs, ports
Mutual authentication; EAP and media independent identity protocols	Storm detection and traffic flow control: traffic policing and port blocking
Posture assessment	ARP inspection; DHCP snooping
X.509, secure key generation and management, scalable key management (DMVPN, GETVPN for example)	Honey pots/honey nets/sinkholes
SIEM, firewalls	Unicast reverse path forwarding (IP address spoofing prevention)
IPS, including SCADA IPS signatures	Hierarchical QoS
Containment: Virtualization and Segmentation (VRF – virtual routing and forwarding, MPLS VPN and VLAN); data separation	Security policy managers
Tamper resistant device design, digitally signed firmware images, firmware/patch authentication and integrity verification	MAC layer monitoring
Digitally signed commands	Control plane protection (coarse packet classification, VRF-aware control plane policing)
Rate limiting for DOS attacks	Secure code development and code hardening (against buffer overflow, self-modification; remove unnecessary protocols)
Wire speed behavioral security enforcement	Structural/topological security
Packet tamper detection, replay resistance	Six wall physical security for devices and systems; access detection and mitigation (i.e. port shutdown)
Air gapping (physical network isolation, data diodes)	Manufacturing supply chain security management
Crypto: link layer, group, and application layer; GDOI, as it has been incorporated into IEC 61850-90-5 specifically for PMU network encryption	Data quality as tamper detection

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** *Since 1965*

U.S. DEPARTMENT OF
ENERGY

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

www.pnnl.gov