INL/EXT-20-60267
Rev 0

INTEGRATED ENERGY SYSTEMS

GAP ANALYSIS

OCTOBER | 2020

Gloria J. Martinez

Nagasri Valli Gali

IES
Integrated Energy Systems

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/EXT-20-60267
Rev 0

INTEGRATED ENERGY SYSTEMS

GAP ANALYSIS

Gloria J. Martinez

Nagasri **Valli** Gali

OCTOBER 2020

Idaho National Laboratory
Integrated Energy Systems
Idaho Falls, Idaho 83415

http://www.ies.gov

Prepared for the
U.S. Department of Energy
Office of Nuclear Science
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Page intentionally left blank

ABSTRACT

This analysis compares how the existing critical infrastructure continues to be vulnerable and with smart grid technologies being implemented exposes IES, power systems, the grid, and renewable energy in new ways. Continued work in cybersecurity will thwart efforts against adversaries having an opportunity to penetrate these systems.

ACKNOWLEDGEMENTS

This paper was prepared by Idaho National Laboratory for the Office of Department of Energy (DOE) Nuclear Energy (NE). A great deal of gratitude goes to Cristian Rabiti and Shannon M. Bragg-Sitton, from Integrated Energy Systems for their support and dedication. The authors wish to recognize our colleagues Michael B. McGregor, Critical Infrastructure Cyber Protection and Defense, Kendall M. Bean, Graduate Master Intern, Bri Rolston, Critical Infrastructure Analysis, and Robert Beason Cyber Resilience Manager, for providing expertise and insight throughout this project. Thank you to the Cyber Resilience and Infrastructure Security departments for supporting the efforts of this project.

Page intentionally left blank

CONTENTS

FIGURES

TABLES

Page intentionally left blank

ACRONYMS

AC	Alternating Current
AVG	Anti-Virus Guard
BEMS	Building Energy Management System
BES	Bulk Energy System
CAN	Controller Area Network
CISA	Cybersecurity and Infrastructure Security Agency
DC	Direct Current
DCS	Distributed Control System
DOE	Department of Energy
DoS	Denial of Service
EV	Electric Vehicle
EVSE	Electric Vehicle Supply Equipment
FERC	Federal Energy Regulatory Commission
HTTP	Hypertext Transfer Protocol
I&C	Instrumentation and Control
ICS	Industrial Control System
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IDS	Intrusion Detection
IES	Integrated Energy System
INL	Idaho National Laboratory
IPS	Intrusion Prevention
IT	Information Technology
MW	Megawatt
NEI	Nuclear Energy Institute
NERC	North American Electric Reliability Corporation
NERC CIP	North American Electric Reliability Corporation Critical Infrastructure Protection
NFC	Near-Field Communication
NIST	National Institute of Standards and Technology
NPP	Nuclear Power Plant
OCPP	Open Charge Point Protocol
OSI	Open Systems Interconnection
OT	Operational Technology
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Manager
SOC	Security Operations Center

Page intentionally left blank

INTEGRATED ENERGY SYSTEMS

1. Integrated Energy Systems

Many states, utilities, and public commissions set standards to reduce carbon emissions. They follow laws on building codes and engineering standards, but the laws on cybersecurity standards are still catching up when it comes to securing digital equipment. This analysis supports the idea that all Integrated Energy Systems (IES) have things in common i.e., if the IES is modernized then it uses digital equipment with software and firmware controlling the equipment and it has interconnected networks and communication capabilities. IES networks, digital equipment, and communication systems are installed and configured but must be adequately monitored to verify the security continues to protect the infrastructure required by regulation or needed in daily operations. In turn, this makes these systems susceptible to cyber threats based on vulnerabilities within these systems. Standardizing equipment is one thing, installing the equipment is another, but securing this equipment is vital!

With current and future trends of moving the existing grid infrastructure to IES and smart grid capabilities with digital and network functions, the stakes of having cyber vulnerabilities significantly increases. Current nuclear power plants (NPP), bulk energy system (BES), and the grid still have analog systems built from the 1970s or earlier; most, if not all are implementing upgrades to the facilities and are functioning in a digital and networked space that has access to internets and intranets. Having vulnerabilities allows for cyber-attacks to come in from anywhere in the world at any given time. In addition to a team of armed forces protecting the infrastructure, what is also required is a savvy cybersecurity computer team with the necessary advanced technological tools to protect the digital equipment and networks installed at every facility.

With one goal to standardize digital and networked technologies used in IES, the potential exists for adversaries to gain access to an IES or other facilities that are connected to each other with the hopes to disrupt the power source and associated infrastructure whether for fun or malicious intent. This undesired event has the potential to happen at any unprotected facility and cause harm to the facility, its equipment, and to the customers that rely on the energy it provides. Due to the costs of implementing and maintaining a cybersecurity program, these facilities are incurring huge dramatic costs. The protection of digital assets is in the forefront since vulnerabilities exist and threats are prevalent. If the threats can attack a system, the attack can cost money, time, fines, lawsuits, and the respect from stakeholders.

IES markets have research and development projects that target technologies and markets for three reasons: reduce fossil fuel use and air pollutant emissions; IES to improve the electric grids power quality, efficiency, reliability; a return on investment; and to enhance energy security (LeMar, 2002). LeMar's report is almost 20 years old, but the foundation for these same ideas continue to challenge the industry. Industry must overcome obstacles and strive for better technological advances to secure the digital and networked technologies used in IES including all other energy systems.

Research has been conducted on cybersecurity technologies for over 20 years and improvements have been made, but threats evolve, and the same issues are true today that we need to protect the assets. Technology does progress, and it makes technology a highly viable target because of its capability to be networked, digital, and communicate with all IES, NPP, BES, and the grid. IES technologies span to nuclear power, bulk electric energy, the grid, solar power, wind power, renewable energy, and smart grids.

What is an Integrated Energy System? Per INL's Integrated Energy Systems: 2020 Roadmap,

"IES are cooperatively-controlled systems that dynamically apportion thermal and/or electrical energy to provide responsive generation to the power grid. They are comprised of multiple subsystems, which may or may not be geographically co-located, including a nuclear heat generation source, a turbine that converts thermal energy to electricity, at least one renewable energy source, and one or more industrial process that utilize heat and/or power from the energy sources to produce a commodity-scale product."

Figure 1. IES by ies.inl.gov.

2. Gap Analysis

A gap analysis was conducted to determine potential gaps in cybersecurity performance within the IES and associated power systems infrastructure to determine if cybersecurity requirements are being met and if not, what gap(s) need(s) to be addressed? Take for instance, if unique cybersecurity situations arise and impacts to the network and communication occur because of a breach, then the data going across the network is unreliable. This leads to the confidentiality, availability, and integrity of data that could potentially be unreliable and compromised. Which in turn leads to implications and possible work stoppages effecting operations, engineering, maintenance, and system administrators. Communication of the networks and the digital technology relies on best cybersecurity practices. The protection of these systems must be practical, cost effective, configured properly, and maintained not to impede or hinder operations. Wars, nation states, and terrorists use cybersecurity to defeat their enemy especially to the systems that are not cyber secure or cyber resilient. How better than to disrupt a nation's infrastructure, instill fear, and disgrace the reputation of a company if an opportunity lends itself to shut down operations and cause electric grid failures to its customers. The possibilities for an adversary to maliciously disrupt networking capabilities and data flow increases as each digital asset is installed along the IES disrupting nuclear power plants, bulk energy systems, and the grid from communicating. Adding digital technology increases the potential for the adversary to create chaos and wreak havoc to all these power systems. If not immediately discovered and dealt with, bad things happen and for many it is too late. Providing identified gaps based on research and industry observations, key points for research are listed below. Given the identified path forward and needs to effectively operate IES the following considerations and questions arise with respect to cybersecurity:

1. There is the potential for major IES impacts to interconnected energy systems and the grid that does not have the sufficient means to protect communications links from unauthorized modifications, accidental disruptions, or deliberate interruptions and it goes unnoticed, what can happen?

2. There is a need to maximize the efficiency of IES components to be co-controlled and aware of the electrical grid demand in real-time (ex. operators are reliant on near real-time data).

3. Are automated controls capable of responding to a system within the IES and take over at the time of a demand or supply event to prevent or mitigate severe cascading blackouts with minimal or no operator intervention?

The above considerations can be translated in cyber risk terms as follows:

1. The integration of digital communication in IES increases attack vector and attack surface exposure.

2. Ownership of IES resources exponentially increases as complexity of administering and combining networked and digital communications.

3. Regulations and regulatory authorities (U.S. NRC, NERC, FERC, NEI, and NIST) are applied differently across stakeholders.

4. Cybersecurity equipment is not standardized along IES digital pathways.

What is at stake:

1. Megawatts (Mw) that powers homes, businesses, and industry

2. Threat to infrastructure

3. Fear to those who rely on electricity

4. Economic impacts

The basis for this analysis is to provide recommendations and build a testbed that affords all IES infrastructure the opportunity to test their procedures, methods, equipment, etc. free from impeding operations. Doing business as usual helps the adversary because if infrastructure and cybersecurity do not evolve the adversary will. If nothing changes, nothing improves!

3. Power Generation Systems

Power generating systems come in a variety of types, e.g., hydroelectric plants, solar facilities, nuclear power plants, natural gas plants, coal-fired plants, and wind facilities. All these generation systems do this to drive a turbine which drives a generator to produce electricity. Sounds simple but there is a lot of physics and equipment behind this process. The engineered systems used at these facilities include a supervisory control and data acquisition (SCADA), a distributed control system (DCS), or an instrumentation control system (ICS). This analysis regarding the equipment as it relates to cybersecurity only refers to digitally based equipment because engineering systems use a combination of analog, mechanical and digital equipment. These engineered systems (the SCADA, DCS, or ICS) consist of local control loops, sensors, turbine controls wireless cranes, smart transmitters, recorders, governors, regulators, relays, programmable logic controllers (PLC), computers, switches, etc. that are digital and

rely on software. For a facility to operate, these IES, NPP, BES, and grid facilities are required to have numerous safety features built in, e.g., multiple trains, backup equipment, and redundancies. These facilities incur hefty costs for the safety features, but it is required by regulation and these measures prevent the facilities from a trip, a transient, or a shutdown. Cybersecurity is concerned with the digital equipment because of the nature of cyber-attacks and cybersecurity features must be afforded similar precautions and then implemented. U.S. NRC (Nuclear Regulatory Commission) and NERC (North American Electric Reliability Corporation) are two primary regulators for NPPs and BES, respectively.

The U.S. electric grid exists with older legacy equipment mixed with highly connected and networked digital assets. Equipment is installed locally onsite or geographically dispersed in remote areas. The equipment is found in the control room, intake structures, relay rooms, turbines, transformers, generators, switchyards, etc. Older legacy analog and mechanical equipment was not originally designed for digital connectivity, so equipment has been upgraded, retrofitted, or completely replaced. When the equipment goes through a design change, the newer standards are evolving to include cybersecurity measures but wasn't always the case in the past. This newer equipment operates by digital means and it has software, firmware, or connectivity features that engineers must consider when installing the equipment. Digital equipment is complex and must be setup; for example, establishing configurations settings, installing patches, changing factory passwords, configuring protocols, setting pin numbers, establishing group policies, etc. If these are not thoroughly configured and tested prior to install, it leaves the equipment vulnerable and exploits might exist. Due to equipment having a potential for vulnerabilities and can be exploited, these facilities run the risk of equipment malfunction or failure, physical equipment damage, power disruptions, or blackouts.

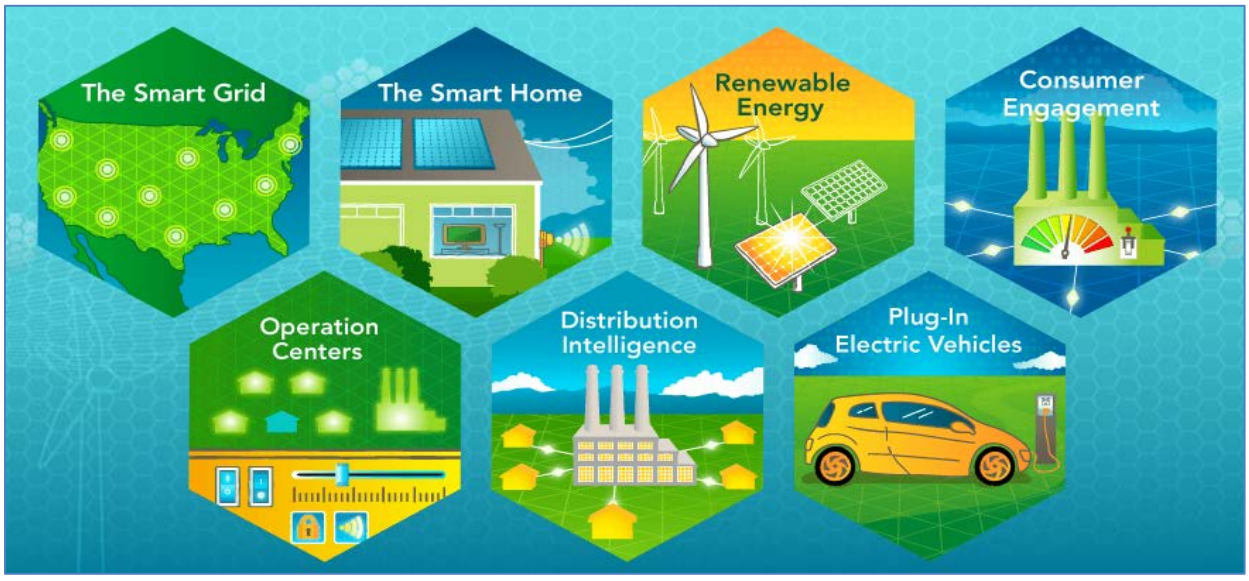

Figure 2. smartgrid.gov by US DOE.

3.1 Generation

Power generation facilities produce electricity for the consumption of customers. Electricity is generated in many forms and includes making electricity from the following sources:

Coal – widely common, inexpensive, most polluted fuel, and produces greenhouse gases.

Natural gas – widely common, replacing coal facilities, inexpensive, fewer pollutants, and most constructed before the 1980s.

Nuclear power – uses energized uranium ions to produce steam to turn a turbine to generate electricity.

Geothermal – uses thermal energy from the earth, cost effective, reliable, sustainable, and a renewable energy source.

Petroleum and Oil – operates for short periods during high peak capacities, no regular use due to high price of petroleum and air pollution restrictions.

Solar – collection of sunlight, sunlight not constant, and a renewable energy source.

Wind – turns propeller blades to generate electricity, low price energy source, and a renewable energy source.

Hydroelectric/power – relies on the flow of water, costs relatively low, and a renewable energy source hydropower; types include hydropower stations, Impoundment (dams), diversions, and pumped storage.

U.S. utility-scale electricity generation by source, amount, and share of total in 2019[1]

Energy source	Billion kWh	Share of total
Total - all sources	4,118	
Fossil fuels (total)	2,580	62.7%
Natural Gas	1,582	38.4%
Coal	966	23.5%
Petroleum (total)	19	0.5%
Petroleum liquids	12	0.3%
Petroelum coke	7	0.2%
Other gases	14	0.3%
Nuclear	809	19.7%
Renewables (total)	720	17.5%
Hydropower	274	6.6%
Wind	300	7.3%
Biomass (total)	58	1.4%
Wood	40	1.0%
Landfill gas	10	0.2%
Municipal solid waste (biogenic)	6	0.1%
Other biomass waste	2	0.1%
Solar	72	1.8%
Photovoltaic	69	1.7%
Solar thermal	3	0.1%
Geothermal	16	0.4%
Pumped storage hydropower[3]	-5	-0.1%
Other sources[3]	13	0.3%

Figure 3. EIA U.S. utility generation by source.

3.2 Transmission

Transmission of electricity from a power generation facility to a distribution facility requires the bulk movement of electrical energy. This is moved along the interconnected overhead power transmission lines throughout the country that starts from the switchyard of the generation station out to distribution substations. Federal Energy Regulatory Commission (FERC) is the primary regulator of electric power transmission. FERC works to ensure cybersecurity is included as new technology is built into the transmission networks including the smart grid networks.

Risk from loss of transformers is due to the lack of alternate delivery paths or lack of access to spare transformers in many transmission utilities. Power surges can occur due to a lack of transmission capacity and lead to cascading failures throughout the grid along with long-lasting power outages. While the loss of a transformer is rare, recovery without a spare can take months. Spare transformers ease this burden, yet most utilities do not own or have access to spare transformers capable of replacing one damaged by a cyber event. Modern substations use several communications to manage local functions using Ethernet-based networks. Controllers and other devices used in substation automation are sources of ICS vulnerabilities.

Substations are an entry point to networks along the grid. An attacker with the necessary skills can disrupt local functions and impact data communications also using an Ethernet-based networks and causing load instability. Substation networks without intrusion detection capabilities allows an attacker to manipulate multiple substations, over time, and without discovery. In these networks, the risk of an adversary coordinated cyber-attack can be powerful to disrupt a portion of the grid. ICS experts also note that if an adversary can physically access a substation there is virtually no limit to the potential damage that it can cause; for example, malware can be directly introduced to local computers and protective relays to be manipulated or digital controllers destroyed. To protect from threats, substations need to harden these facilities with cyber-related technology and secure equipment through physical security means.

3.3 Distribution

Distribution systems play a role in transferring electrical power from an alternating current (AC) or direct current (DC) to its customers. Distribution systems use equipment such as transformers, circuit breakers, and protective devices. Upgraded equipment has network capability and the capacity for software or firmware installed. For the distribution system to maintain an electric power supply within specifications and to reach its customers, it is required to have proper voltage, availability of power on demand, and reliability of the power. By not properly controlling the voltage of the distribution system where the voltages are varied leads to damage of the load which in turn causes revenue costs and the possibility of ruining equipment. Electric power is not stored so the distribution system must be capable of supplying demand loads to all its customers.

Substations at the distribution level are not bound by cybersecurity standards and are more likely to be lacking in basic cybersecurity practices and physical security protections just like its transmission counterparts. A cyber-attack on a distribution substation can involve manipulating breakers to interrupt power or compromising SCADA operations to cause load instability. The distribution substations are not bound by the same regulatory standards because they exist outside of the bulk energy systems and this leaves the substations vulnerable. Grid connections such as step-down transformers between the transmission and distribution systems do not have the same regulatory standards and this also presents with cyber vulnerabilities.

4. Renewable Energy

Renewable generation differs from bulk energy systems in that bulk energy consists of one or two generators and renewable generation consists of many small renewable generators that has a direct connection to the grid (Gevorgian, n.d.). Renewable energy comes from natural resources and consists of wind, solar, hydro, and geothermal power. As these systems are moving to distributed generation and distributed control systems, the digital and networked communications are more advanced and offer better methods to boost reliability and efficiency. This is more complex than the previous centrally controlled electric grid that offered only a one-way delivery of electrical power (Murali, n.d.). Individual energy generation technologies like solar photovoltaics, wind turbines, fuel cells, and microturbines are integrated using networks of devices, data sciences, software integration, and machine learning

technology (Gevorgian, n.d.). Digital devices like smart inverters hardware and firmware, inverter control algorithms, interaction of multiple inverters is highly prone to cyber risks.

Solar panels use micro inverters that convert DC power to AC power. These micro inverters connect to every solar panel and connect wirelessly to a controller which connects to the internet. It has monitoring systems to provide real-time solar panel monitoring (Treacy, 2018). Devices like the smart inverter includes hardware and firmware, inverter control algorithms, internet faced inverters which are prone to exploits and require proper password and network protections. This could allow remote access which leads to an adversary controlling the inverters, altering the flow of electricity causing an overload the system, and instability in grid causing power outages.

It is important to note that some inverters are produced by foreign or foreign-owned companies such as the Chinese company Huawei. This technology has been identified as a cyber risk because there are no universal standards assuring the integrity of inverters regardless of where they are manufactured. (Devine, 2018). Purchasing technology that is labeled as a cyber risk and testing these devices prior to install would help in implementing policies and standards in hopes to greatly reduce vulnerabilities in devices.

Without proper firewall and security protocols, adversaries can target a central server in a remote location and steal energy from multiple sites. Ransomware and denial-of-service attacks are significantly under-reported in the renewable energy industry. Cyber risk insurance increases one way to mitigate the potential exposure (Hurin, n.d.).

5. Electric Vehicles

Most of this analysis evolves around power systems and associated architecture. IES is much more than power, it also includes electric vehicles and charging stations. Take for instance, hybrid vehicles, their use in recent years continues to gain popularity. So popular that the number of electric vehicles can grow from 3 million to 120 million over the next ten years (Gottumukkala, et al., 2019). Electric vehicle supply equipment (EVSE), also known as electric vehicle charging stations are for charging electric vehicles computers that connect directly to the Internet. The EVSE serves important control functions such as authorization of electric vehicle payment and connection to the local power grid (Gottumukkala, et al., 2019). Like a lot of industrial equipment, charging stations were built with safety, rather than security in mind. Electric vehicle charging stations are an unattended, unmonitored and in remote spots (Starks, 2019). This is a two-way interactive technology between users, the smart grid, and wireless networks. It disregards aspects of cybersecurity and becomes a mess when it fails to control the electric vehicle charging station technology (Ahmed & Dow, 2016). Schneider Electric issued patches for three security flaws in its charging stations, the most serious of which involved hardcoded credentials like default passwords or embedded security keys (Lyngaas, 2019).

Networks enable an infected EV to communicate with its charging station, to a network of vehicles, and the electric grid at large. The Near-Field Communication (NFC) card used to handle billing when drivers charge their EVs. These ID cards are vulnerable when used to charge vehicles because of billing and personal information associated with that account. Many charging stations use a Hypertext Transfer Protocol (HTTP) which does not encrypt data or communications. This could lead to relay attack or man-in-the-middle attack where the attack takes advantage of open Wi-Fi. This vulnerability could lead to an adversary rewiring charging requests and gaining root access to the station. Direct physical access to a universal serial bus (USB) port on charging stations can also be used for malicious intent and directly affect driver privacy.

The Open Charge Point Protocol (OCPP) which regulates communications between billing management systems on one end and the electric charging point on the other end. The charging point sends a request identifying you to the billing system; billing management approves the request and lets the charging point

know; then the station lets you start charging. The amount of electricity is calculated and sent back to the billing management system so that it can bill you at the end of the month (Ryabova, 2018). Through a simple flash drive, logs and data can be copied to the drive, giving attackers not only the data on the OCPP server itself, but also confidential information users of the charging point allowing attackers to copy their ID numbers or even track their location (Oded, n.d.).

When electric vehicles refuel, components controller area network (CAN), telematics, infotainment, cellular communications, etc., are connected physically and electronically with electric vehicle supply equipment (EVSE), which in many cases is also connected to the Power Grid and may be connected to a facilities Building Energy Management System (BEMS) and these are all connected to the Internet. EVSEs are composed of embedded systems with electric components and one or more microcontrollers that handle control of the charging circuits as well as communication with all external systems. For cyber security purposes the microcontrollers and network communications are the most interesting parts.

There two different entry points that could compromise the security of the EVSE: network-based entry points and physical access points, such as through the charging port or by tampering with the devices' hardware. Network-based attacks compromise the security of network endpoints i.e. controller servers and station operation interfaces because of poor authentication or lack of encryption has the potential to affect all the charging stations connected to the end note. Poor network connection will lead to spoofing attacks, man-in-the-middle attack, denial-of-service, SQL-injection attack, and malware attack (Gottumukkala, et al., 2019).

Physical access to an EVSE could probe the charging station board to eavesdrop on inter-component communications. Physical & side-channel attacks involve getting access to the chip-level components to manipulate and interfere with the system internals. Side-channel attacks that involves reverse engineering a chip by observing timing information, power consumption and electromagnetic leaks. Interception-based attacks involves eavesdropping on sensitive data to compromise user's privacy and confidentiality through access and monitor the ports of the physical hardware. Modification attacks compromises software integrity by exploiting detected vulnerabilities like using buffer overflow to overwrite stack memory, thereby transferring control to malicious program (Gottumukkala, et al., 2019).

EV/EVSE compromise can synchronize their attack to affect large portions of the grid simultaneously. Attacker could manipulate large fleets of EVSEs and could cause distribution and transmission impacts (Johnson, 2019). IES using the feature of distributed generation and distributed control systems (DCS) based on advanced communications (Murali, n.d.). Individual energy generation technologies like solar photovoltaics, wind turbines, fuel cells, and microturbines are integrated using networks of devices, Data sciences and software integration and machine learning technology. IT and OT devices like smart inverters hardware and firmware, inverter control algorithms, interaction of multiple inverters is highly prone to cyber risks.

A renewable generation consists of hundreds of small renewable energy generators with power that interface with the grid when compare with a power plant consists of one or two large synchronous generators (Gevorgian, n.d.)

6. Security Levels

Equipment that is designated as digital is defined as equipment with software, firmware, microcontrollers, digital processors, computers – any devices that are programmable and have embedded applications. Program features include setpoints, controllers, timers, relays, etc. Most digital equipment installed in the facilities fall under the purview of the operations and engineering departments. Engineering equipment is referred to at Operational Technology (OT) and must be separated from the Information Technology (IT) equipment. IT is referred to as the business side of the network and the OT is the engineering side of the

network. These two networks should never communicate with one another. Major reasons include the business network is the internal corporate that allows its users to go out to the Internet; whereas, the engineering network is used to monitor or control systems within the plant and should never go out to the Internet. Even within the IT and OT networks they are separated into different levels e.g. Level 0 is public domain, Level 1 and 2 are designated for IT and Level 3 and 4 are designated for OT and is shown in various models (Levels 1-5 are described in references such as Purdue model, RG 5.71, and IAEA publication NSS No. 17).

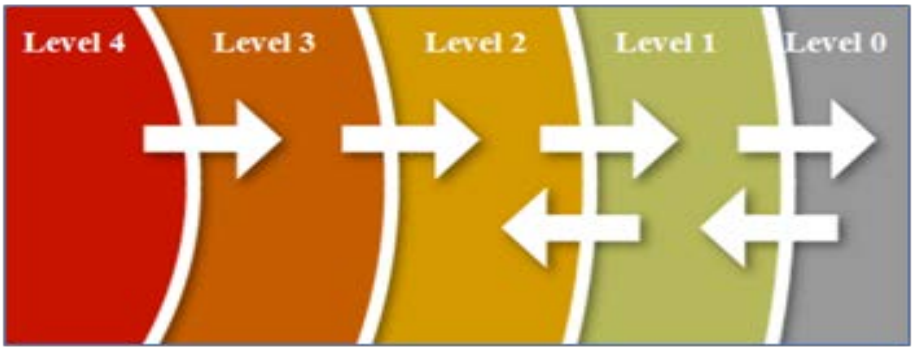

Figure 4. RG 5.71 Security Levels.

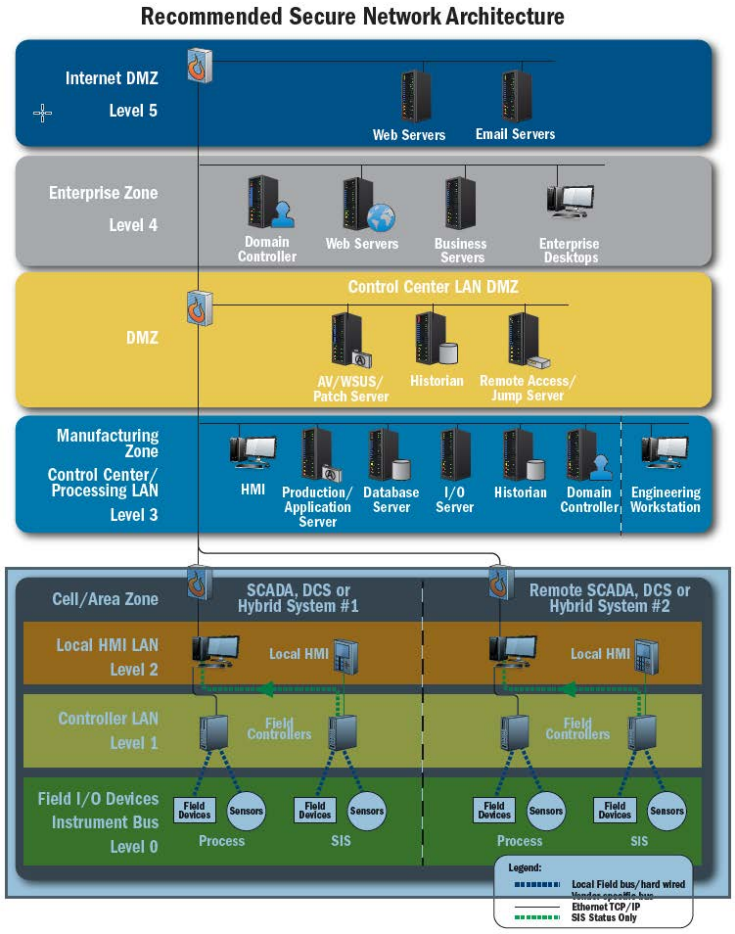

Figure 5. Purdue Security Model.

7. Industrial Control Systems

IES, power plants, and the grid use a variety of industrial equipment designs and configurations. This stems from the type of plant and architecture in the control room and throughout the facility. The control systems used in throughout the plants consist of any of the following configurations such as an Industrial Control System (ICS), a Supervisory Control and Data Acquisition (SCADA), a Distributed Control System (DCS), and Programmable Logic Controllers (PLC). ICS is a configuration combination of designs that include SCADA, DCS, and PLCs which monitor daily operations. SCADA systems are large design architectures used in facilities that extend over many geographical miles of a facility. SCADA systems are centralized systems used to monitor and control assets that are dispersed locally and to field devices. Field devices control operations of opening and closing valves and breakers, collects data from sensors, and monitors conditions. These systems play a critical role maintaining efficiency by collecting the data in the field and sends commands to control those processes. SCADA systems use remote terminals to send data back to a control room for monitoring. These systems have numerous analog and digital equipment returning data to their respective systems. They are designed and configured to very distinct specifications and operate on a 24/7 basis. Operators rely on the information of these systems to make decisions that impact the operation of the facility.

A DCS is used to control industrial processes such as electric power generation. It too has an architecture that contains supervisory control and management of processes. It is a series of control loops where controllers, sensors, actuators, setpoints, and tolerances are monitoring and gathering data throughout the facility. A DCS is centrally located in a control room and it handles monitoring and processing of data from the field and the equipment is situated so operators can view and control any part of the process from their screens while retaining a plant overview. PLCs are digital, computer-based, software driven, solid-state devices that controls industrial equipment. PLCs are control system components and used throughout SCADA and DCS systems, they are often the primary components in control system configurations used to provide operational control of smaller processes. SCADA, DCS, and PLCs are important for three reasons: they have digital equipment, have software/firmware, and collect and process data in real-time. These systems use proprietary hardware, thought to be immune from cybersecurity attacks, which does make it more difficult for attackers to get to these systems, but not necessarily as there are numerous methods to disrupt attack vectors and attack surfaces. Often, they are isolated from other networks by air gaps and if they are connected, they are separated by a data diode or a firewall.

Table 1. Few types of equipment with digital technology found in a NPP and BES.

Manufacture	**Type of System**
Allen Bradley	Factory automation equipment that includes PLCs, Relays, I/O Modules, HMIs,
Schweitzer Engineering Laboratories	Manufacture generator and transmission protection and control systems, these are digital protective relays, it is a real-time automation controller.
GE, Siemens, Emerson	Turbine Controls and PLCs
Westinghouse 7300 system and ASIC cards	Application-specific integrated circuit (ASIC) technology offers the benefits of digital technology without many of the perceived disadvantages of software-based systems.
Westinghouse SPDS	Safety Parameter Display System / Qualified Display Parameter System SPDS / QDPS - Emergency Response Data Systems for critical and safety functions.
Rosemount	Valves, actuators, regulators, transmitters (4-24mA) and HART protocol.

Manufacture	Type of System
Yokogawa Electric	Measurement and control equipment used in DCSs consisting of production control systems, test and measurement instruments, pressure transmitters, flow meters, and fieldbus instruments.

7.1 Protocols

A communication protocol is a set of rules that allow for two or more devices communicating and transmit information. TCP/IP, Modbus, Profibus are common protocols used. The protocols allow the programmable controllers that are networked to communicate with one another. These protocols are generally connected via an RS-232 serial interface and connects to an intra or internet. An adversary could use these protocols to intercept messages and create fabricated messages between sender and receiver of these messages (Edmonds, Papa, & Shenoi, 2014).

- Modbus - A communications bus used to connect industrial devices and PLCs.
- Profibus - A fieldbus communication used by Siemens.
- Fieldbus - Used for real-time distributed control of PLCs in a DCS connects sensors, actuators, switches, valves, etc.
- Highway Addressable Remote Transducer (HART) - A hybrid analog and digital industrial protocol that communicates with 4-20mA instrumentation loops. Developed and used by Rosemount devices.

7.2 Ports

Various ports and connectors can be found on devices in a facility and the protection of these ports is important because they are an attack vector; they are also a common way a device communicates with other devices. Leaving the ports unblocked and unsecure is not a good practice, disabling unused ports must be a priority. Common ports that should be blocked or disabled are Ethernet (networking technology), USB, RS-232, RS422, and EIA-485 (these four are commonly used serial communication connections).

Connectors are just as common as ports and are often left unsecure. For example, equipment left unattended had the capacity to be vulnerable because open unused ports allows contractors and vendors to connect to a device and communicate along the network pathway, or to the software and firmware loaded in the digital device if the connect a phone or laptop without permission. All connectors should sealed or secured by a locked box until use is necessary. For example, a vendor may come into the facility to update firmware, upload current software, or patch the system via a connector or port. If a port or connector is not blocked this vendor could walk up to the device without the vendor scanning the device for malware and potentially introducing something into the system.

8. Regulators / Regulations

Regulations deal with an authoritative rule in which a facility must deal with regulation and procedure. This is a rule or order issued by an executive authority or regulatory agency of a government that has a force of law. Such rules, agencies, and laws are governed from various entities. There are many regulating entities, but a few are described here.

The U.S. Nuclear Regulatory Commission (NRC) is an independent agency of the United States government tasked with protecting public health and safety related to nuclear energy. The NRC issued a guide called the "Regulatory Guide (RG)" series which was developed to describe and make available to the public information such as methods that are acceptable to the NRC staff for implementing specific parts of the agency's regulations, techniques that the staff uses in evaluating specific problems or postulated accidents, and data that the staff needs in its review of applications for permits and licenses. This regulatory guide provides guidance to applicants and licensees on satisfying the requirements of 10CFR73.54 "Protection of digital computer and communication systems and networks." NRC has the most stringent regulation that are put upon nuclear power plants. Given that nuclear power is scary when it comes to describing these facilities pose a risk for nuclear events, the public demands stringent rules so the government imposed stringent rules and is spelled out in 10CFR73.54

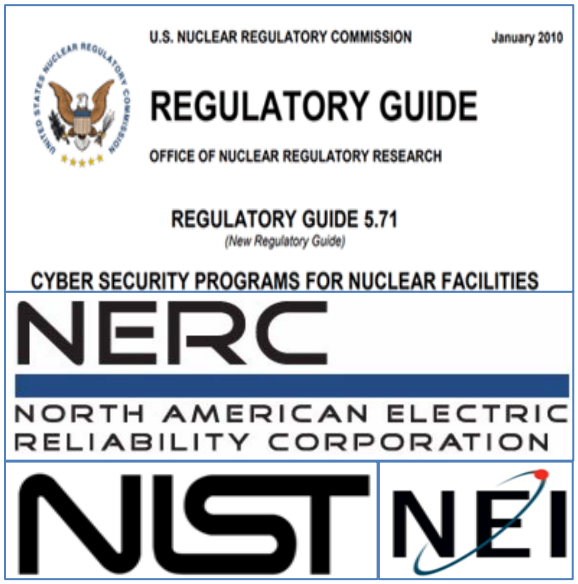

Figure 6. Regulatory Guides.

The North American Electric Reliability Corporation (NERC) is a nonprofit corporation based in Atlanta, Georgia, and formed on March 28, 2006, as the successor to the North American Electric Reliability Council. NERC oversees six regional areas in the power industry in the US, Canada, and Mexico. Responsibilities include working with stakeholders, develop standards, and monitor and enforce compliance. NERC also investigates significant power events in power systems. NERC standards, called Critical Infrastructure Protection (CIP), resembles a checklist of cybersecurity requirements. NERC CIP takes steps to address some of the ongoing concerns, however states are still taking specific actions to protect the distribution system facilities that fall outside of the scope.

The Federal Energy Regulatory Commission (FERC) The Federal Energy Regulatory Commission is the United States federal agency that regulates the transmission and wholesale sale of electricity and natural gas in interstate commerce and regulates the transportation of oil by pipeline in interstate commerce.

The Nuclear Energy Institute (NEI) is a nuclear industry trade association based in Washington, D.C. and develops policy for regulatory issues. Other than just representing the nuclear power industry it also represents nuclear medicine, uranium mining, transport of nuclear material, and nuclear fuel facilities. NEI is responsible for nuclear power cybersecurity framework that nuclear plants adopted NEI 08-09 and NEI 13-10 as a basis for the defensive strategy.

National Institute of Standards and Technology (NIST) is a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness. These entities support nuclear energy and developed the security controls used widely in throughout cybersecurity. NIST Framework is a process by which organizations may inventory their cybersecurity posture and make necessary adjustments based on findings. By IES, NPP, BES, renewable energy, and the grid following different regulation might prove how ineffective the cybersecurity practices are at the facilities. Somehow, they should be regulated in similar fashions due to how critical the infrastructure is to maintain life.

9. Cybersecurity

A good cybersecurity program requires management buy-in, a healthy budget, adequate time, sophisticated equipment, and a talented team. The team needs a starting point, and it is to select a framework, the set of requirements for which to build a solid cybersecurity program. Frameworks are requirements a program must have within it program. It is also a checklist to set compliance standards in the protection of assets focusing on confidentiality, integrity, and availability of resources. Requirements aid in spelling out how to protect digital assets from a threat and secure vulnerabilities in a system. But what requirements do not tell programs what to do is – for example, specifics on how many pieces of equipment to use or what brands to use. The team determines if the system needs to be air-gapped, isolated, use switches, VLAN segmentation, a firewall with deny all rules, or a data diode between security levels. In this respect requirements are vague and specifically so for the team to build a program best suited for that facility. The framework suggests building an asset inventory list, walk-down digital assets, and eventually complete an assessment on the equipment to determine if requirements are met; if not, identify gaps. For a new group to start a new cybersecurity program it can be daunting and yes, these requirements do come with a lot of overhead. Just as physical forces practice on tactics to gain an edge to defeat physical security systems, adversaries are doing the same just from a location far away in hopes to break into critical systems. They are achieved by sniffing networks, brute force attacks, man-in-the-middle attacks, ransomware attacks, and phishing email attacks among other sophisticated types of attacks. Attempts at breaking into critical systems run nonstop because the adversaries are continuously trying to figure out ways to penetrate systems.

Cybersecurity is the focus when protecting systems in the digital world. One article describes that if the electrical grid were brought down for any lengthy amount of time there would be unsurmountable damage to the American economy (Silverstein, 2020). Another article relays that the entire U.S. power grid needs to be updated yet they won't spend the money to do so (Chobrak, 2020). Both articles were authored in August of 2020 and supports the idea that the power industry needs to do more. Not enough is done because the infrastructure is fragile and ageing. The infrastructure was built years ago with analog technology and then upgraded to digital technology. It is often the case that the equipment is installed first and then the protections are added after.

With an uncertainty of cyber threats in the world and what their interest is to attack, it is anyone's guess as to the next attack might be and when. It's not like an adversary calls up and says, "hey we're going to hack your system at this day and time!" Realistically cybersecurity experts must always be prepared and on guard. Implementing a cybersecurity program takes an inordinate amount of time, planning, preparation, money, coordination, and resources. For small facilities, this is difficult to implement. Bigger facilities, it can be done, but often will wait until they are forced by regulation, fines, or after an incident.

In the last 20 years or so, new technologies brought facilities into the digital age. Digitization and upgrades brought new vulnerabilities and now cybersecurity teams must find solutions to adequately protect these systems. The cybersecurity team being referred to is different from the security staff we know has the gates, guns, and guards, also known as physical security. These cybersecurity professionals must know the digital equipment installed into the systems located throughout the facilities and how to deal with software, patching, installation, configuration, networking, etc. Cybersecurity requires years of experience, a degree, or certifications. Education and training take years, then continuous training because digital technology rapidly changes.

Cyber-attacks on IT systems focus on acquisition of business data, cyber-attacks on ICS systems focus on asset disruption. Modernization incorporates automation, digital technologies, smart grid technologies, and access points to grid networks. Lack of cybersecurity allows adversaries to compromise and exploit holes in the system. Cyber-attacks on ICS are different in nature than the majority of cybercrime. Since

Stuxnet illustrated how physical processes could be disrupted and damaged through digital means, various attack frameworks have manifested themselves. It is difficult to get an accurate picture of the number or variety of cyber-attacks on infrastructure targets, as government agencies responsible for overseeing and creating cybersecurity guidelines are dependent on the individual assets owners to report incidents. Cyber criminals targeting critical infrastructure often take previous viruses and modify them slightly to better fit the target, as illustrated by the list of major critical infrastructure cyber threats and threat actors (Hemsley & Fisher, 2018).

Many reported attacks are not directly targeting OT systems and trying to disrupt them, but are data exfiltration and reconnaissance attacks, presumably in preparation for larger scale attacks on the system. The threat actors targeting critical infrastructure are far more likely to be backed by large hacktivist group or nation state which in turn targets and attacks other types of industries.

Many cyber-attacks on IT systems are ransomware, which is why it is recommended for every business, large or small, and even individuals to have backups of their networks and data. For critical infrastructure asset owners, however, it is necessary to take additional precautions to protect their sensitive OT systems from being compromised. Most attacks that make it to an ICS network go through the respective infrastructure owner's corporate IT network (Campbell, 2015) which is why CISA (Cybersecurity and Infrastructure Security Agency) has found for the last 5 years in a row that boundary protection, or the layers of security that separate a business' enterprise and ICS networks, is routinely the least secure aspect of most asset owners' OT networks. The security efficacy of IES would rely on multiple facilities following standard business best-practices, as set out by NERC-CIP standards. Because IES inherently rely on multiple asset owners (such as with an interconnected nuclear plant, wind farm, and manufacturing plant that uses the thermal energy stored via IES technology), the risk associated with failure to follow critical infrastructure security standards is multiplied.

9.1 Cyber-Attacks

Attack vectors enable adversaries to exploit systems based on vulnerabilities within that system. The nuclear power industry spelled out the attack vectors that needed protection. 1. Physical Access, 2. Network Connectivity, 3. Wireless, 4. Portable Media, and 5. Supply Chain. This is one way to describe attack vectors whereas other facilities list them differently. This too can be tailored to fit the nature a program by considering how an adversary can penetrate the system and how the cybersecurity team protects those vectors. Attack surface is viewed as all the various opportunistic points in a system an adversary can infiltrate. When facilities complete cybersecurity assessments, usually attack vectors are looked at and evaluated. This is the beginning of trying to fix vulnerabilities and establish a baseline. With future work, attack surface needs to be evaluated and incorporated in securing the digital systems and the facilities. Cyber-attacks occur every day. This is not an all-inclusive list, but a few examples that could harm IES, NPP, and BES and what a testbed could use a scenario to evaluate systems and equipment.

DoS Attacks – attackers exploited a known vulnerability in an unpatched Cisco firewall. This caused a series of reboots over 12 hours and lead to denial-of-service (DoS) attack on U.S. wind and solar assets. Many utilities used outdated operating systems and unencrypted passwords, these two items alone left the assets vulnerable (Walton, 2019).

Physical Security Attack – inverters used between solar farms communicate via a central controller. If an adversary takes physical control of the inverter the adversary can use cyber means to shut down the facility, overcharge batteries, or cause grid instability. Cyber-attacks on a storage-backed solar farm could lead to the destruction of the storage system itself and in turn result in a fire. Taking physical control of a solar farm would enable the adversary to disrupt critical functions the same way shutting down a power system (Bellini, 2020).

Password Attack – when weak passwords are used in a system, it won't take an adversary long to break into a system. Strong passwords are a must in any system used across a network. There are numerous ways to obtain a password, but one sophisticated way is when there is a network connection, and an adversary can sniff the network. This does involve software capable of sniffing a network and a network that is unencrypted.

Phishing – technique by the adversary disguising himself to steal users' data, obtain sensitive data. It is achieved by spoofing emails or creating fake websites and sending that link to unsuspecting users.

SQL (Structured Query Language) Injection – attackers create an SQL query to disrupt a database. This controls the database and bypasses its security measures. It can circumvent authentication to a web application and retrieve, modify, add, or delete data.

Ransomware Attack – if an adversary can insert malicious software to a digital system, it would have the capability to encrypt the user's files and keep them locked until a ransom is paid for the decryption key. If this were to ever get into a facility and installed onto digital equipment it could take control, take over, and shut down operations.

Black Energy – recent incident, a trojan-based hack that exploited HMI software.

Stuxnet – most common attack reference due to the damage is caused affecting PLCs.

Table 2. Types of cybersecurity prevention methods to reduce risk.

Equipment	Description
Antivirus (AV)	Security software that protects a computer against malware. Common: Norton, McAfee, AVG
Data Diode	A unidirectional security gateway, allows data to travel in one direction only, placed between two network levels to control the flow of information Common: OWL Cyber Defense and Waterfall
Demilitarized Zone (DMZ)	A perimeter network that exposes the organization's external facing services to an untrusted network.
Encryption	Conceals information by altering it. Protects sent, received, and stored data.
Endpoint Detection and Response (EDR)	A centralized platform for continuously monitors endpoints and responds to incidents. Common: CrowdStrike, Check Point,
Firewalls	A network traffic-based security system that monitors incoming and outgoing traffic with predetermined security rules. Common: Cisco, Barracuda, Check Point, Fortinet, WatchGuard
Forensic Software	Software that enables you to search, identify, and prioritize potential evidence in computers. Common Tools: EnCase, Autopsy
Intrusion Prevention System (IPS)	Monitors network traffic and prevents vulnerability exploits. Common: Palo Alto and Check Point
Intrusion Detection System (IDS)	Monitors networks for malicious activity. Common: SolarWinds and Zeek
Kiosk	Scans equipment for malware, allows for laptops and USB devices to be scanned prior it connecting to equipment in the facility. Common: OPSWAT MetaDefender (regulatory compliant)

Equipment	Description
Multi-factor Authentication	Electronic authentication a computer grants to a user prior to access. Types: Something a user knows, something the user has, etc.
Patch Management	Distributing and applying updates to software and firmware installed in equipment.
Network Protocol or Packet Analyzer	Captures and analyzes signals and data traffic. Common: Wireshark, SolarWinds, Nmap, Putty
Routers	A hardware networking device that forwards data packets between computer networks. Common: Cisco and Netgear
Security Operations Center (SOC)	Build in Limited Areas, proper design is key to operating a SOC
Security Incident & Event Manager (SIEM)	A software-based solution that aggregates and analyzes network activity from different resources in your network infrastructure Common: Splunk, ArcSight, Fortinet, Rapid7
VLAN	A partitioned and isolated segmented subnetwork in a computer network at the data link OSI layer 2.
Virtual Private Network (VPN)	Encryption method used to provide secure access to remote computers. A tunneling protocol for users to pass through, an authentication method, and it keeps data secure.
Vulnerability Scanner	A vulnerability scanner, a remote security scanning tool Common: SolarWinds, Nessus, Metasploit, Nmap (port scanner), Wireshark

10. Cybersecurity Equipment Testbed IES-CsETb

Imagine how often in a facility that is operational, how much time and effort is spent on testing? Not a lot and maybe after an incident. A testbed full of the latest cyber technology and a team to conduct testing is not feasible for facilities that are setup to keep a facility running. Budgets do not allow for such expenditures and the time to create a real-time functioning testbed setup for real world scenarios based on situational circumstances rarely happens. This is rare, who has the budget and the staff to sit around doing only testing when a facility is operational 24/7? In this type of situation management would contract out testing when necessary or avoid it all together. There are few locations in the U.S. to have testing conducted but that too requires time and effort away from the facility. A testbed at INL could create real-world, real-time, worst-case cybersecurity scenarios to help facilities that do not have the proper tools or the experts to do so at their location. A testbed can be setup with equipment that a facility wants to purchase or test on existing equipment and push the equipment to limits that cannot be done locally. Initial costs for INL might be costly but working for numerous facilities will allow for getting baseline configuration and eventually dwindle costs in hopes for standardization to occur.

A functioning cybersecurity testbed allows facilities to design a real-world scenario to be run against its current configurations. By designing the configuration against that facility's baseline, the testbed can determine if the system is penetrable, can easily be defeated, or can be compromised. After the real-world scenarios are complete the following can happen:

1. Present new guidelines for equipment configuration set to cybersecurity regulation specifications.
2. Determine the attack methods adversaries are using.
3. Publish reports on key findings and resolutions.

Just as many systems in NPP have redundant systems (trains, redundancies, fail safes) this needs to be built into cybersecurity. Even if this means adding data diodes and SIEMs. Separation of IT and OT is still at 100%.

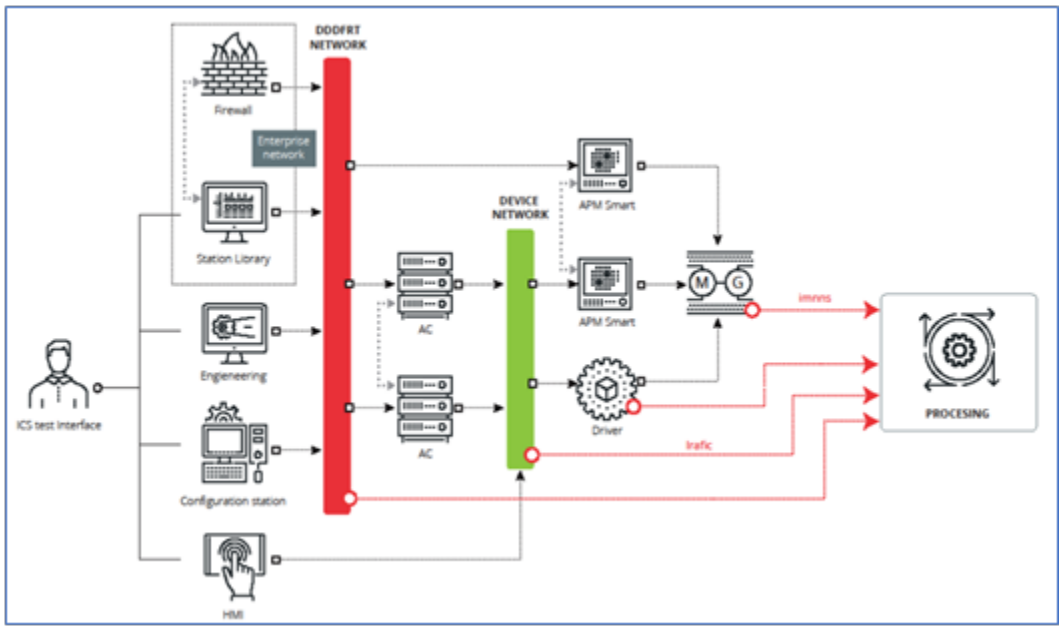

Figure 7. Example Testbed.

People are upgrading to the newer equipment. After all the equipment is installed it requires the time, effort, and dedication to operate the equipment. Configuration settings must be set, monitoring of the equipment must be ongoing. How cyber resilient are cybersecurity devices? We need a team to do tests on current configurations of these appliance that are installed at various facilities. Deployment of such equipment is costly, requires experts to use, each of the equipment has so many features it requires configuration setup. A few examples include:

- Build real-life incident response scenarios.
- Test a specific configuration and design with real-world cyber event scenarios and see what happens.
- Test digital and network equipment.
- Unique OT equipment used in the power industry, and IES.
- Test data diodes, firewalls, kiosks, switches, SIEMS, etc.
- An electric power station installed in a home but connects to the grid via their home ISP.
- Solar panels installed at homes that connect to the grid.

11. Key Findings and Recommendations

IES, power systems, and the grid, are moving to digital, networked, and smart technologies. Original grid technology was a centralized unidirectional system that sent out electricity to the customer. Today, electricity flows bidirectionally to and from the customer's location, i.e. a customer who has solar panels can sell electricity back to the electric company.

This is the age where communications and digital technology are networked and can communicate anywhere in the world. IES and power systems are incorporating smart grids. Smart grids improve performance, increase reliability, provide efficient electricity to customers. Because a customer can provide power back to the grid, the customer can make money. Regulation must be implemented to add security measures to smart meters and electric charging stations that connect to the grid.

Traditional power systems are moving toward digitally enabled smart grids which will enhance

communications, improve efficiency, increase reliability, and reduce the costs of electricity services. The massiveness of the smart grid and the increased communication capabilities make it more prone to cyber attacks. Since the smart grid is classified as critical infrastructure, vulnerabilities must be identified and sufficient solutions must be implemented to reduce the risks to a secure at an acceptable level.

What was analyzed was the integration of digital communication in attack vector and attack surface exposure, ownership of resources, regulation and regulatory authorities, and cybersecurity equipment. The vulnerabilities in smart grid networks, the types of attacks and attackers, the challenges present in designing new security solutions, and the current and needed solutions. Upgrades at these facilities are happening even though it is gradual and replaced during outages. Engineers use maintenance rule, technical specifications, and design basis documents for upgrades and new designs. The past decade also brought the incorporation of cybersecurity regulations which engineers and IT groups are incorporating during the design of a project. The cybersecurity standards are being applied to the upgrades and new designs at most, but not all facilities are consistent or standardized with the implementation of security controls because of different regulations and regulatory authorities.

Why regulation and cybersecurity standards? Management should be asking what are the adversaries doing? If thoughts of adversaries causing havoc by defeating security protocols built into the automated, digital, networked, and smart grid systems; then one must push for the need of cybersecurity controls and it must be a priority. If no push for cybersecurity, adversaries win because they have the time, opportunity, and ability to exploit vulnerable systems. These adversaries will break into networks via routers and firewalls; they will do so by being anonymous, obtain passwords, install malware (e.g., keyloggers and ransomware), shutdown operations, and instill fear. One current trend is to infect a facility with ransomware. This means systems are encrypted and only unlocked if a ransom is paid. Can you see the headlines? Unnamed facility pays ransom to get their data back.

The need for IES testbed to test cybersecurity and digital functionality of various configurations, components, and designs of digital equipment would be beneficial to numerous people, organizations, and outside entities. This testbed can design configurations for systems that cannot be done to live operational equipment in the field. The facilities use similar equipment and would benefit from testing configurations in hopes to determine how to better protect and adequately protect digital assets. This testbed can be utilized by other departments, outside entities that want to test current or other configurations. Also, there are partner labs at INL and other National Laboratories that can be tapped to produce the necessary results for numerous configurations.

How much is cybersecurity worth? As seen in the nuclear industry, applying security controls to 98 nuclear power plants cost was in the millions with cyber security experts conducting thousands of assessments on all digital equipment. This method took almost a decade to achieve yet there are no real tests to determine if the cybersecurity resources in place will stop the adversary. One way to find out might be too late if the adversary gets through.

Knowing that at any given time is if a plant in not operational and shutdown for any means outside of an outage, the costs are in the millions per day. If an adversary knew the potential costs are in the millions everyday a facility is shut down and not operating. It seems to be getting easier for adversaries to figure out ways to get ransomware in the equipment and hold it hostage. This is where management needs to determine what they would do if this happens. Management just might have to pay because of other factors, reporting it to the regulator with the potential to get fined or shutdown. One last note, this was just a few items list in the beginning about what's at stake. This analysis could go on forever and include all aspects of a cybersecurity program regarding:

- The lack of cyber policies and procedures not developed nor documented.

- Asset inventory and configuration baselines.
- Cybersecurity awareness and training not developed, implemented, or maintained.
- Background checks, periodic and random checks on employees, contractors, and vendors.
- Ongoing monitoring, real-time monitoring, and continuous monitoring.
- Cloud platforms.

12. References

Ahmed, S., & Dow, F. M. (2016). Electric Vehicle and Charging station Technology as Vulnerabilities Threaten and Hackers Crash the Smart Grid. *International Journal of Innovative Science, Engineering & Technology*.

Bellini, E. (2020, April 17). *Solar inverters vs. cyberattacks*. Retrieved from pv magazine: https://www.pv-magazine.com/2020/04/17/solar-inverters-vs-cyberattacks/

Campbell, R. J. (2015). Cybersecurity Issues for Bulk Power System. *Congressional Research Service* (pp. 1-39). Washington DC: CRS Report.

Chobrak, U. (2020, August 17). *Popular Science*. Retrieved from The US has more power outages than any other developed country. Here's why.: https://www.popsci.com/story/environment/why-us-lose-power-storms/

Devine, R. (2018, November 2). *Assessing the Risk of Solar Inverters to the U.S. Electrical Grid*. Retrieved from Homeland Security Digital Library: https://www.hsdl.org/c/assessing-the-risk-of-solar-inverters-to-the-u-s-electrical-grid/

Edmonds, J., Papa, M., & Shenoi, S. (2014). Security Analysis of Multilayer SCADA Protocols: A Modbus TCP Case Study. In *Critical Infrastructure Protection* (pp. 205-221).

Gevorgian, V. (n.d.). *Renewable Energy Generation and Storage Models*. Retrieved from NREL: https://www.nrel.gov/grid/generation-storage-models.html

Gottumukkala, R., Merchant, R., Tauzin, A., Leon, K., Roche, A., & Darby, P. (2019). Cyber-Physical System Security of Vehicle Charging Stations. *IEEE*, 1-5.

Hemsley, K. E., & Fisher, R. E. (2018). *History of Industrial Control System Cyber Incidents.* Idaho Falls: Idaho National Laboratory.

Hurin, J. (n.d.). *Travelers*. Retrieved from Cyber Risks for Soar and Wind Installations: https://www.travelers.com/business-insights/industries/energy/cyber-risks-for-solar-and-wind-installations

Johnson, J. (2019). *Grid and Charging Infrastructure.* Albuquerque: Sandia National Laboratories.

LeMar, P. (2002). *Integrated Energy Systems (IES) for Buildings: A Market Assessment.* Oak Ridge: U.S. Department of Energy.

Lyngaas, S. (2019, February 25). *Government Power struggle: Government-funded researchers investigate vulnerabilities in EV charging station.* Retrieved from Cyberscoop: https://www.cyberscoop.com/ev-charging-stations-hacked-idaho-national-laboratory/

Murali, B. (n.d.). *Power Systems Operations and Controls.* Retrieved from NREL: https://www.nrel.gov/grid/power-systems-operations-controls.html

Oded, Y. (n.d.). *The Hidden Cyber Risks of Electric Vehicles*. Retrieved from Upstream: https://www.upstream.auto/blog/the-hidden-cyber-risks-of-electric-vehicles/

Ryabova, Y. (2018, January 09). *Don't be sure charging your electric car is secure enough*. Retrieved from Kaspersky Daily: https://usa.kaspersky.com/blog/electric-cars-charging-problems/14357/

Silverstein, K. (2020, August 17). *Grid Security And Cyber Defense Cannot Fall On Deaf Ears, Experts Warn*. Retrieved from Forbes: https://www.forbes.com/sites/kensilverstein/2020/08/17/grid-security-and-cyber-defense-cannot-fall-on-deaf-ears-experts-warn/#72242eae399e

Starks, T. (2019, June 11). *The dangers for electric vehicle charging stations*. Retrieved from Politico: https://www.politico.com/newsletters/morning-cybersecurity/2019/06/11/the-dangers-for-electric-vehicle-charging-stations-650477

Treacy, M. (2018, October 11). *Are Solar Panels Vulnerable to Hackers*. Retrieved from Treehugger: https://www.treehugger.com/are-solar-panels-vulnerable-hackers-4851988

Walton, R. (2019, November 4). *First cyberattack on solar, wind assets revealed widespread grid weaknesses, analysts say*. Retrieved from UtilityDive: https://www.utilitydive.com/news/first-cyber-attack-on-solar-wind-assets-revealed-widespread-grid-weaknesse/566505/