SANDIA REPORT
SAND2017-13113
Unlimited Release
Printed August 2017

Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators

Cedric Carter, Christine Lai, Nicholas Jacobs, Shamina Hossain-McKenzie, Patricia Cordeiro, Ifeoma Onunkwo, Jay Johnson

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

DRAFT FOR PUBLIC COMMENT
SEND COMMENTS TO JAY JOHNSON (jjohns2@sandia.gov) BY DEC 31, 2017.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology and Engineering Solutions of Sandia, LLC.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone:	(865) 576-8401
Facsimile:	(865) 576-5728
E-Mail:	reports@osti.gov
Online ordering:	http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone:	(800) 553-6847
Facsimile:	(703) 605-6900
E-Mail:	orders@ntis.gov
Online order:	http://www.ntis.gov/search

SAND2017-13113
Printed November 2017
Unlimited Release

Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators

Cedric Carter
Christine Lai
Nicholas Jacobs
Shamina Hossain-McKenzie
Cyber Resilience R&D

Patricia Cordeiro
Mission Analytics Solutions

Ifeoma Onunkwo
Computer Systems Security Analysis R&D

Jay Johnson
Renewable and Distributed Systems Integration

Sandia National Laboratories
P. O. Box 5800
Albuquerque, New Mexico 87185

Abstract

This report provides an introduction to cyber security for distributed energy resources (DER)—such as photovoltaic (PV) inverters and energy storage systems (ESS). This material is motivated by the need to assist DER vendors, aggregators, grid operators, and broader PV industry with cyber security resilience and describe the state-of-the-art for securing DER communications. The report outlines basic principles of cyber security, encryption, communication protocols, DER cyber security recommendations and requirements, and device-, aggregator-, and utility-level security best practices to ensure data confidentiality, integrity, and availability. Example cyber security attacks, including eavesdropping, masquerading, man-in-the-middle, replay attacks, and denial-of-service are also described. A survey of communication protocols and cyber security recommendations used by the DER and power system industry are included to elucidate the cyber security standards landscape. Lastly, a roadmap is presented to harden end-to-end communications for DER with research and industry engagement.

TABLE OF CONTENTS

NOMENCLATURE

AAA	Availability, Authorization, and Accounting
AC	Alternating Current
ACL	Access Control List
AES	Advanced Encryption Standard
ANSI	American National Standard Institute
BITW	Bump-in-the-Wire
BPS	Bulk Power System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
CA	Certificate Authority
CBC	Cipher Block Chaining
CIA	Confidentiality, Integrity, and Availability
CIGRE	International Council on Large Electric Systems
CIP	Critical Infrastructure Protection
CPU	Central Processing Unit
CPUC	California Public Utilities Commission
CRC	Cyclic Redundancy Checking
CSIP	Common Smart Inverter Profile
DC	Direct Current
DCS	Distributed Control System
DDoS	Distributed Denial of Service
DER	Distributed Energy Resource(s)
DERMS	Distributed Energy Resource Management System
DES	Data Encryption Standard
DHS	Department of Homeland Security
DNP3	Distributed Network Protocol
DOE	Department of Energy
DoS	Denial of Service
DR	Demand Response
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
EAP	Extensible Authentication Protocol
ECC	Elliptic Curve Cryptography
ECC	Error Correcting Code
EO	Executive Order
EPRI	Electric Power Research Institute
EPS	Electric Power System
EPU	Electric Power Utility
ERO	Electric Reliability Organization
ESS	Energy Storage System
EXI	Efficient XML Interchange
FEMS	Facility Energy Management System
FERC	Federal Energy Regulatory Commission
FIPS	Federal Information Processing Standard

GCM	Galois/Counter Mode
GDOI	Group Domain of Interpretation
GOOSE	Generic Object Oriented Substation Event
HAN	Home Area Network
HTTPS	Hypertext Transfer Protocol Security
ICS-CERT	Industrial Control System Cyber Emergency Response Team
ICT	Information and Communication Technologies
IDS	Intrusion Detection System
IED	Intelligent Electronic Device
IoT	Internet of Things
IOU	Investor-Owned Utility
IPS	Intrusion Prevention System
IPS	Internet Protocol Suite
IPSec	Internet Protocol Security
ISO	International Organization for Standardization
LICs	Logical Interface Categories
MESA	Modular Energy Storage Architecture
MMS	Manufacturing Message Specification
NAT	Network Address Translation
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NSM	Network and System Management
OE	Office of Electric Delivery and Energy Reliability
OSGP	Open Smart Grid Protocol
OSI	Open System Interconnection
PCC	Point of Common Coupling
PCS	Power Conditioning System
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PPD	Presidential Policy Directive
PUC	Public Utilities Commission
PV	Photovoltaic
RAID	Redundant Array of Independent Disks
RBAC	Role-Based Access Control
REP	Retail Energy Providers
RFC	Request for Comments
Risk	Financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems
RMP	Risk Management Process
Root-CA	Root Certificate Authority
RTCP	Real-time Transport Control Protocol
SCADA	Supervisory Control and Data Acquisition
SIWG	Smart Inverter Working Group
SNL	Sandia National Laboratories
SRTP	Secure Real-time Transport Protocol

SSL	Secure Socket Layer
Threat	Possibility of a malicious attempt to damage or disrupt a computer network or system
TLS	Transport Layer Security
UDP	User Datagram Protocol
VEN	Virtual End Node
VPN	Virtual Private Network
VTN	Virtual Top Node
Vulnerability	A weakness which allows an attacker to reduce a system's information assurance
WEP	Wired Equivalent Privacy
XML	Extensible Markup Language

1. OVERVIEW

Cyber security for DER devices is essential for secure, reliable, and resilient operation of the power system. With the increasing prevalence of DER devices, common-mode vulnerabilities run the risk of simultaneously disconnecting massive quantities of generation, which could lead to localized power disruptions or bulk system collapse. This report covers cyber security for DER devices, protocols, and requirements. We examine the current cyber security requirements and present our recommendations for ensuring data confidentiality, integrity, and availability to aid DER vendor, aggregator, and grid operators.

The need to address cyber security has become more critical in the last year due to new interconnection and interoperability standards that will mandate a combination of DER functionality that will allow remote users to change the behaviors of thousands of devices. Interoperability requirements in the forthcoming revision to the U.S. interconnection standard IEEE Std. 1547 presents an emerging, fundamental challenge in securing power systems.[1] Specifically, since distributed energy resource (DER) communications run over public and poorly-secured private networks, the addition of DER devices significantly increases the electrical grid attack surface. While DER devices typically have small active and reactive capacities and individually have little impact on the bulk or local power systems, in aggregate they are increasingly a large portion of the generation. Control of these aggregations can influence grid reliability.

In January 2017, the second installment of the Quadrennial Energy Review (QER 1.2) focused on the electricity system and found it was a strategic imperative to protect and enhance the cyber defenses of the U.S. through modernization and transformation.[2] Historically, DER devices were programmed statically and not designed to provide any grid-support services. However, with the increasing penetration of DER and energy storage systems, there is growing need to provide grid-support capabilities. In fact, the forthcoming revision to IEEE Std. 1547 includes a range of DER grid-support functions. Interoperability capabilities are common for most inverters deployed in the U.S. now. These devices communicate over Ethernet, Wi-Fi, Bluetooth, and serial connections using a variety of proprietary and standardized protocols (e.g., SunSpec Modbus). Enphase Energy made headlines worldwide when it remotely updated 800,000 inverters (154 MW of capacity) on the Hawaiian Islands of O'ahu, Hawai'i, Moloka'i, and Lana'i in 2015.[3,4] While many praised the achievement as a breakthrough for reducing the costs of firmware upgrades, others warned of the cyber security implications. If one company could remotely update the settings of 100s of megawatts of power equipment, anyone with access to that control network would be able to make malicious changes to those devices as well. Certain settings could damage equipment, cause distribution overvoltages, or initiate a blackout if the

[1] *IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems*, IEEE Std. 1547-2003, 2003.

[2] Quadrennial Energy Review (QER), "Transforming the Nation's Electricity System," Jan. 6, 2017.

[3] P. Fairley. (2015). *800,000 Microinverters Remotely Retrofitted on Oahu—in One Day* [Online]. Available: https://spectrum.ieee.org/energywise/green-tech/solar/in-one-day-800000-microinverters-remotely-retrofitted-on-oahu

[4] A. Konkar. (2015). *'Something Astounding Just Happened': Enphase's Grid- Stabilizing Collaboration with Hawaiian Electric* [Online]. Available: https://enphase.com/en-us/blog/'something-astounding-just-happened'-enphase's-grid-stabilizing-collaboration-hawaiian-electric

contingency reserve was not sufficient. For example, on the island of O’ahu, there will be an estimated 400 MW of installed PV capacity in 2017 but only 180 MW of contingency reserves.[5] Therefore, disconnecting or curtailing a significant portion of the solar generation on a sunny day could cause a blackout.

1.1. Report Structure

The following sections provide an encompassing primer of cyber security for DER. Section 2 discusses the basic tenets of cyber security including confidentiality (encryption), integrity, availability, authentication, authorization, and non-repudiation. Common types of cyber security attacks are provided in Section 3, e.g., eavesdropping, masquerading, man-in-the-middle, replay attacks, Trojan horses, denial-of-service, etc. Section 4 presents the current U.S. requirements for DER communications. Section 5 conducts a review of cyber security recommendations, guidelines, and reports by:

- Department of Energy (DOE)
- Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (DHS ICS-CERT)
- Electric Power Research Institute (EPRI)
- Federal Information Processing Standard (FIPS)
- Institute of Electrical and Electronics Engineers (IEEE)
- International Council on Large Electric Systems (CIGRE)
- International Electrotechnical Committee (IEC) and International Organization for Standardization (ISO)
- Internet Engineering Task Force (IETF)
- National Institute of Standards and Technology (NIST)
- North American Electric Reliability Corporation (NERC) and Federal Energy Regulatory Commission (FERC)

Section 6 covers cyber security recommendations for DER interoperability standards, cyber security requirements, and risk management procedures for DER vendors, aggregators, and grid operators. Finally, Appendix A provides further details on the different protocols, standards, and models discussed.

[5] GE Energy Consulting, “Oahu Distributed PV Grid Stability Study, Part 1: System Frequency Response to Generator Contingency Events,” Hawai‘i Natural Energy Institute, Mar. 3, 2016.

2. CYBER SECURITY PRINCIPALS

DER systems are cyber-physical systems that combine operational power equipment with cyber controls to achieve the generation objective. In addition to information-based attacks, they also need to protect against control network attacks, inadvertent errors, and equipment failures that have a direct physical impact. All information within these systems should address the following goals in an effort to protect, preserve, and promote data transactions to authorized systems and users[6]:

- Confidentiality
- Integrity
- Availability

In the realm of cyber security, these three principle attributes are known as the CIA triad. Confidentiality refers to the protection of information, so that only the sender and the intended receiver will be privy to the information. Integrity ensures the information is protected from unintended modifications or alterations. Availability guarantees information is available to all the intended users. Although many operational systems are built with high availability in mind, the importance of confidentiality is often overlooked. For example, loss of confidentiality over a network can lead to degradation of integrity and availability, as a malicious attacker may use their unauthorized access to alter parameters or trip power generation in an energy system. The confidentiality, integrity, and availability of systems are managed under the AAA framework, which refers to the following three aspects of access control, policy enforcement, and auditing[7]:

- Authentication
- Authorization
- Accounting

The CIA triad and AAA framework are detailed in the following subsections, providing an overview of cyber security principals.

2.1. Confidentiality

Confidentiality refers to the protection of information against unauthorized access or disclosure. Confidentiality is often the core focus of information security, in which the primary goal is to protect the secrecy of sensitive data. Although confidentiality is usually deprioritized in operational systems, loss of confidentiality can often give an attacker the information needed to execute a successful attack on system integrity and availability. Moreover, the sensitive nature of user data, including customer usage statistics and personally identifiable information (PII) is often overlooked.

To protect information confidentiality, access controls and encryption are employed. Encryption ensures that only you and the intended recipient, using a special key, can read the message. The sender uses encryption to convert intelligible information (known as plaintext) using an encryption key and encryption algorithm into unintelligible information (known as ciphertext). The receiver uses a decryption key with a decryption algorithm to convert the unintelligible information back to the original intelligible information. This process is illustrated in Figure 1.

[6] Federal Information Processing Standards Publication, “Standards for Security Categorization of Federal Information and Information Systems”, Feb. 2004.

[7] K. Hoeper and L. Chen, “Recommendation for EAP Methods Used in Wireless Network Access Authentication,” NIST Special Publication 800-120, National Institute of Standards and Technology, 2010.

This art of securing communication is also known as cryptography. Today, encrypted communications are found everywhere on the internet, and are being used by most major communication protocols to secure information. Encryption is generally grouped into symmetric or asymmetric key encryption.

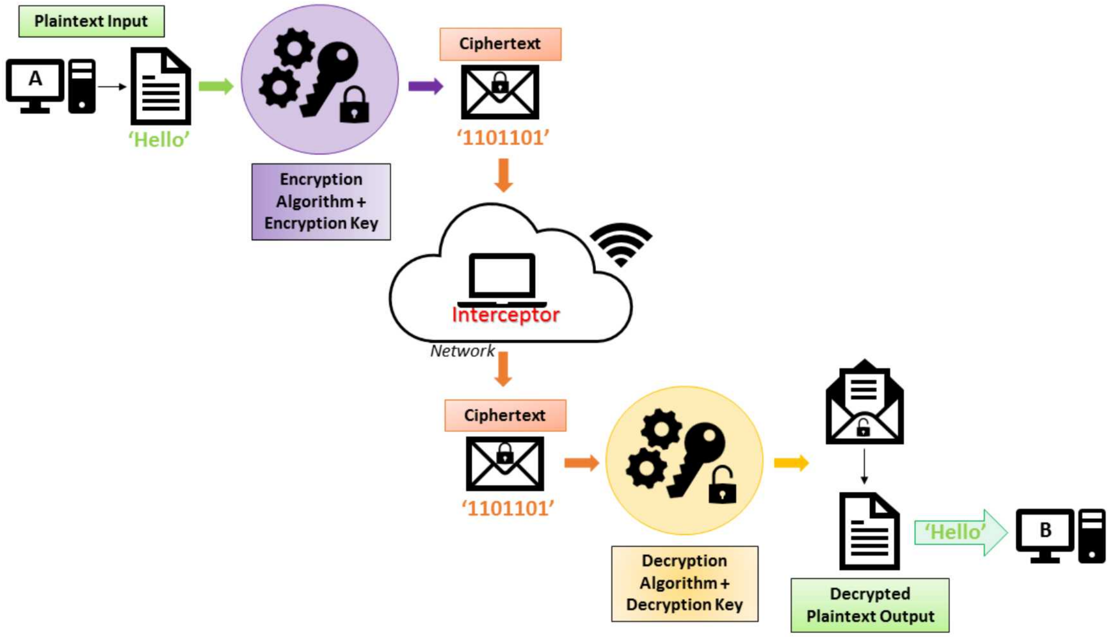
Plaintext Input
A
'Hello'
Encryption Algorithm + Encryption Key
Ciphertext
'1101101'
Interceptor
Network
Ciphertext
'1101101'
Decryption Algorithm + Decryption Key
Decrypted Plaintext Output
'Hello'
B

Figure 1: Basic model of encryption process as a plaintext input is sent through the network from computer A to computer B; interceptor(s) would only have access to the encrypted ciphertext.

2.1.1. Symmetric Key Encryption

Symmetric key encryption takes its name from the use of a single key that is shared by two known communicating parties or entities, and is often used for bulk encryption of data. Symmetric encryption algorithms are mathematically more efficient than asymmetric encryption algorithms, and thus suitable for large amounts of data.

Stream ciphers and block ciphers represent the two major categories of symmetric key encryption algorithms. Stream ciphers encrypt individual bytes or characters in a data stream, whereas block ciphers encrypt the data in larger chunks. The first block cipher that came into wide usage was 3DES, an extension of the Data Encryption Standard (DES) that was first approved in 1995.[8] As of 2017, the Advanced Encryption Standard (AES) is the only symmetric encryption algorithm accepted by most federal standards, and the block ciphers typically use Galois/Counter Mode (GCM) to maximize performance.[9,10]

[8] *The ESP Triple DES Transform*, RFC 1851, 1995.

[9] *Specification for the Advanced Encryption Standard (AES)*, Federal Information Processing Standards Publication 197, 2001.

[10] *Recommendation for Block Cipher Models of Operation: Galois/Counter Mode (GCM) and GMAC*, NIST Special Publication 800-38D, 2007.

Symmetric key encryption is also known as private-key cryptography. The symmetric key encryption has five components:

1. **Plaintext** is the information or message that the sender wants to transmit.
2. **Encryption algorithm**, also called a cipher, is the algorithm used for information encryption that is generally known to all.
3. **Secret key** is a protected key that should only be known to the communicating parties.
4. **Ciphertext** is encrypted data that is a product of combining the encryption algorithm, the key, and plaintext.
5. **Decryption algorithm** is an algorithm that is used for decrypting information.

Based on the input data, there are two types of symmetric ciphers:

1. Stream cipher: a symmetric cipher that encrypts one bit at a time. For example, the RC4 algorithm was a popular cipher that outputs a pseudorandom stream of bits,[11] and was employed in Wired Equivalent Privacy (WEP), a security algorithm used to protect 802.11 wireless networks. However, several critical vulnerabilities were discovered in 2015 and its use is now prohibited in recent versions of the Transport Layer Security (TLS) and Secure Socket Layer (SSL) protocols. Newer variants of RC4 address some of these flaws, but alternative stream ciphers such as Salsa20 have also emerged to replace RC4.[12]
2. Block cipher: a symmetric cipher that breaks plaintext message into equal-size blocks and encrypts each block as a unit. As introduced above, AES is a block cipher that uses a fixed length block size of 128 bits with varying key sizes of 128, 192, or 256 bits. A block cipher can have many operating modes of encryption, some of which require a non-secret random or pseudo-random initialization vector to encrypt the first block of data or message. This initialization vector should be unique for each message or session, so that the resulting ciphertext is unique. A common example of this is Cipher Block Chaining (CBC), which uses a chaining mechanism that makes the output of the current block of data dependent on both the plaintext of the current block and the ciphertext from the previous block of data.

2.1.2. Asymmetric Key Encryption

Asymmetric encryption employs the use of public and private keys for encryption and decryption. The public and private keys are typically generated as a pair. When a sender wishes to send information to an intended recipient, the sender takes that information, and together with the recipient's public key and an encryption algorithm, encrypts the message. The receiver will now use the associated decryption algorithm with the private key to decrypt the information. Two prevalent asymmetric key encryption algorithms are RSA (named after the originators—Rivest, Shamir, and Adelson), which makes use of modular arithmetic to encrypt and decrypt information, and elliptic curve cryptography (ECC) making use of elliptic curve point multiplication.[13,14] However, because performing asymmetric encryption on bulk data is

[11] W. Stallings, "The RC4 Stream Encryption Algorithm," Cryptography and Network Security, 2005.

[12] D.J. Bernstein, "Salsa20 specification," Department of Mathematics, Statistics, and Computer Science, The University of Illinois at Chicago, 2005.

[13] R.L. Rivest, A. Shamir, and L. Adleman,"A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM 21.2, 1978, 120-126.

computationally expensive, communicating entities typically use asymmetric key cryptography for establishing a secure communication channel to exchange the symmetric key that will be used for encrypting information.

2.1.3. Key Exchange

Before encryption is applied, two endpoints communicating in a session must first exchange their keys through secure means. In one-way communications, the public encryption key of the recipient is shared with all sending entities, with the private decryption key being known only to the receiver. However, when bulk two-way communications are performed, it is more efficient for both parties to arrive at the same shared secret key over a public communications channel. In modern cryptographic suites, this is usually achieved through the Diffie-Hellman key exchange protocol. As shown in Figure 2 below, the two parties start with a shared piece of information that is exchanged over a public channel. Each party then mixes this shared information with their own secret, and exchanges the result. Finally, they combine their secret with the exchanged result to arrive at a shared secret. The process leverages mathematical properties (such as large prime number moduli or elliptic curves) to ensure that an eavesdropping party cannot feasibly guess the final secret using the exchanged information.

[14] V. Kapoor, S. Abraham, and R. Singh. “Elliptic curve cryptography,” Ubiquity 2008, May 2008.

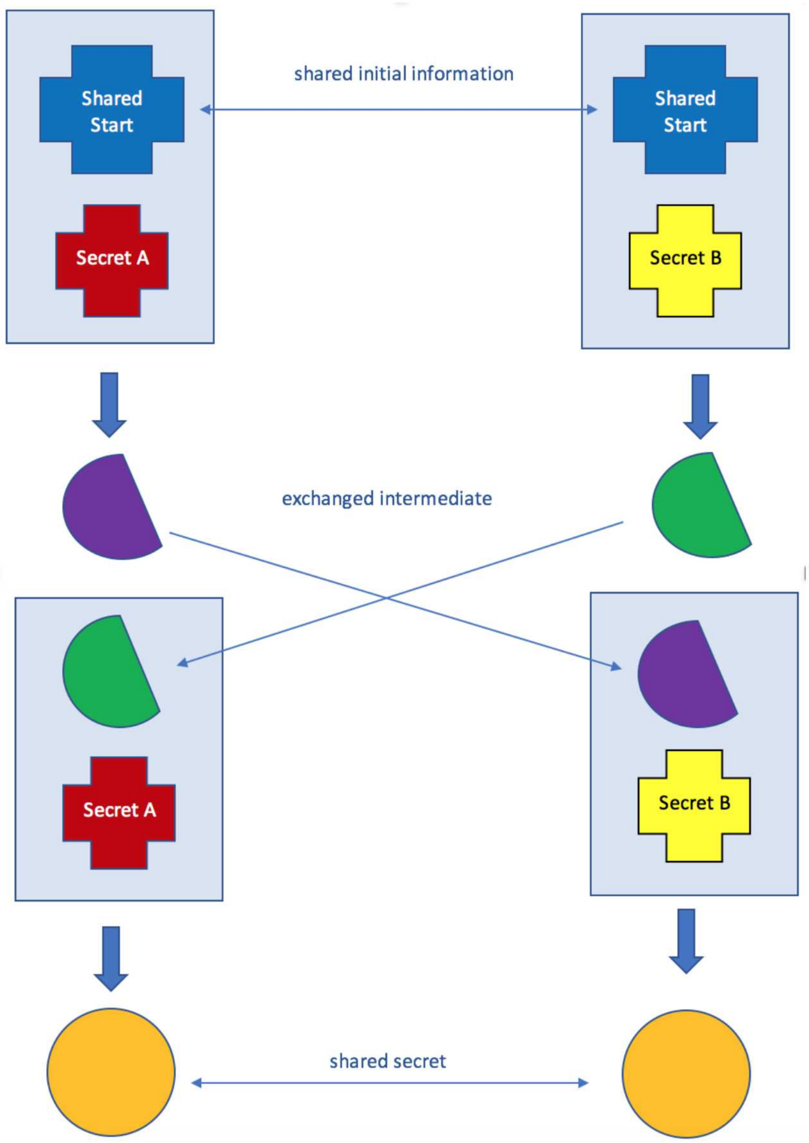

Figure 2: Diffie-Hellman key exchange protocol.

2.2. Integrity

Data integrity refers to the assurance that the data that is stored, transferred, accessed, or otherwise used by a system maintains its accuracy and consistency over the course of its lifecycle. This includes the prevention of data corruption and data loss that may result from unintentional means or malicious actors. Ensuring integrity entails securing both the physical hardware and logical systems that manage data. Modern computing platforms and databases utilize a multitude of strategies for maintaining data integrity, including:

- Locks or mutual exclusion mechanisms to obtain access to required resources before executing a thread.
- Copy-on-write of modified resources to provide snapshots of a logical volume.
- Filesystems that integrate error detection and correction (e.g. ECC) and cyclic redundancy checking (CRC) of internal data and metadata.

- Hardware redundant array of independent disks (Hardware RAID) configurations to provide redundancy and recovery of corrupted data.
- Checksums or hash functions to verify that the correct data has been copied or transferred.

Checksums are used for error detection and most often take the form of a word that is produced by first breaking the data into bit segments of a fixed size, then either computing the exclusive or (XOR) of the segments or taking the modular sum of the segments. However, checksums do not provide sufficient protection against files that have been corrupted, particularly if the change was made by a malicious actor seeking to obscure their actions. For security, cryptographic hash functions are employed that exhibit the following properties:

- Deterministic. Any given data input will always result in the same hash value, or digest.
- One-way. The original data cannot be reversed from the hash value without computing all possible values, which should be infeasible with current computing power.
- Sensitive. A small change to the data, even a flip of a single bit, produces a significant change in the hash value.
- Collision resistant. It should be extremely difficult to find two different inputs that produce the same hash value.
- Efficient. The hash function should operate quickly on data inputs of varying sizes.

The 128-bit Message Digest 5 (MD5) has been the most commonly employed hash function since its inception in 1992, but its security is considered to be severely compromised and is now considered obsolete. The 160-bit Secure Hash Algorithm 1 (SHA-1) is designated by NIST as a current U.S. Federal Information Processing Standard, but is no longer considered to be secure against well-funded organizations with vast computing resources for generating a collision. SHA-1 has been deprecated by most major software and technology organizations in 2017, to be replaced by SHA-2 or SHA-3, which include a collection of variants named after the length of their hash values, including SHA-256, SHA-384, and SHA-512. Although many DER systems may still employ SHA-1, it is recommended that data integrity checks be performed using SHA-2/SHA-3 to prevent computational attacks that will arise in the near future.

2.3. Availability

Availability of data refers to ensuring that authorized personnel are able to access data at all times of need, especially during emergencies or disasters. Denying access to information has become a very common attack vector in computational systems. In addition, denying access of data could be as a result of a natural disaster, equipment failure, or human error. Denial of Service (DoS) or Distributed DoS (DDoS) attacks are common attacks used to disrupt websites and web services. The primary aim of a DDoS attack is to deny access for authorized users. As a result, unavailability of data creates costly downtime to troubleshoot the availability of access to authorized users. Availability of the interactions from request and replies can range from milliseconds to hours or days. Unlike the other cyber security requirements, availability generally relies on engineering design, configuration management, redundancy, functional analysis, communication network design, and engineering practices.

2.4. Authentication and Authorization

Authentication is the process of verifying a user, client, server, or other entity's credentials to prove that they are who they say they are. The confidentiality of user account credentials, passwords, biometrics profiles, and certificates is paramount, as they represent the various means through which authentication may be performed. Encryption without authentication does little to preserve confidentiality, as there is no guarantee that the secret keys have been shared with genuine entities. Conversely, authentication without encryption provides little protection against threats that bypass authentication mechanisms through eavesdropping attacks. Enforcing both authentication and encryption mechanisms enables defense in depth—multiple layers of protection that need to be bypassed before a system is fully compromised.

Entities that have been authenticated in a system must be authorized to perform actions on the system. This is typically done through an access control policy. A mandatory access control policy represents the strictest form of access control, whereby the access level of a user determines the types of resources the user is able to access. A discretionary access control policy allows individual users to assign access levels to resources they own, and is widely implemented in Unix-based filesystems. A Role-Based Access Control (RBAC) policy assigns resources to user groups based on their functional roles, and has been implemented in Windows filesystems and networks.[15] Authorization should be granted to each user under the principle of least privilege, which restricts user privileges to the minimum level required to perform their tasks.

2.5. Accountability and Non-Repudiation

To provide accountability, the security related actions performed on any digital asset, including access control changes and logins, should be recorded in a log. Furthermore, policies should be in place to ensure non-repudiation, or assurance of the origins of data in authenticated transactions such as e-mail, web traffic, or contracts.

2.5.1. Public Key Infrastructure (PKI)

The standard method for providing non-repudiation is Public Key Infrastructure (PKI), which employs the use of digital certificates registered to a Certificate Authority (CA), as defined by the X.509 standard.[16] As shown in Figure 4, the CA serves as a trusted third party that verifies the authenticity of each sender and digitally signs the sender's public key with the CA's private key to produce a certificate. The sender uses a hash function to produce a message digest which they sign with their private key. The recipient then verifies the sender's identity through the CA before using the sender's public key to recover the message digest from the signature and verify that it matches the hash value of the received message. The standard process for generating, signing, and verifying the keys is governed by the Digital Signature Algorithm (DSA)[17], which employs SHA-2 hash functions to produce a message digest. Care must be taken to ensure that a system is not vulnerable to forgery. Prior to accepting a certificate, the following checks should be performed:

[15] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," Computer, vol. 29, no. 2, pp. 38-47, Feb. 1996.

[16] *Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks*, International Telecommunications Union (ITU-T) X.509, Oct. 2016.

[17] *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186, 1993.

- The certificate is not self-signed, i.e., signed by the same party whose identity is being verified.
- The certificate has been signed by a trusted third party whose root certificate you have in your possession.
- The certificate is current and has not been revoked by the CA.
- The certificate is signed using a secure hash algorithm, such as SHA-256.

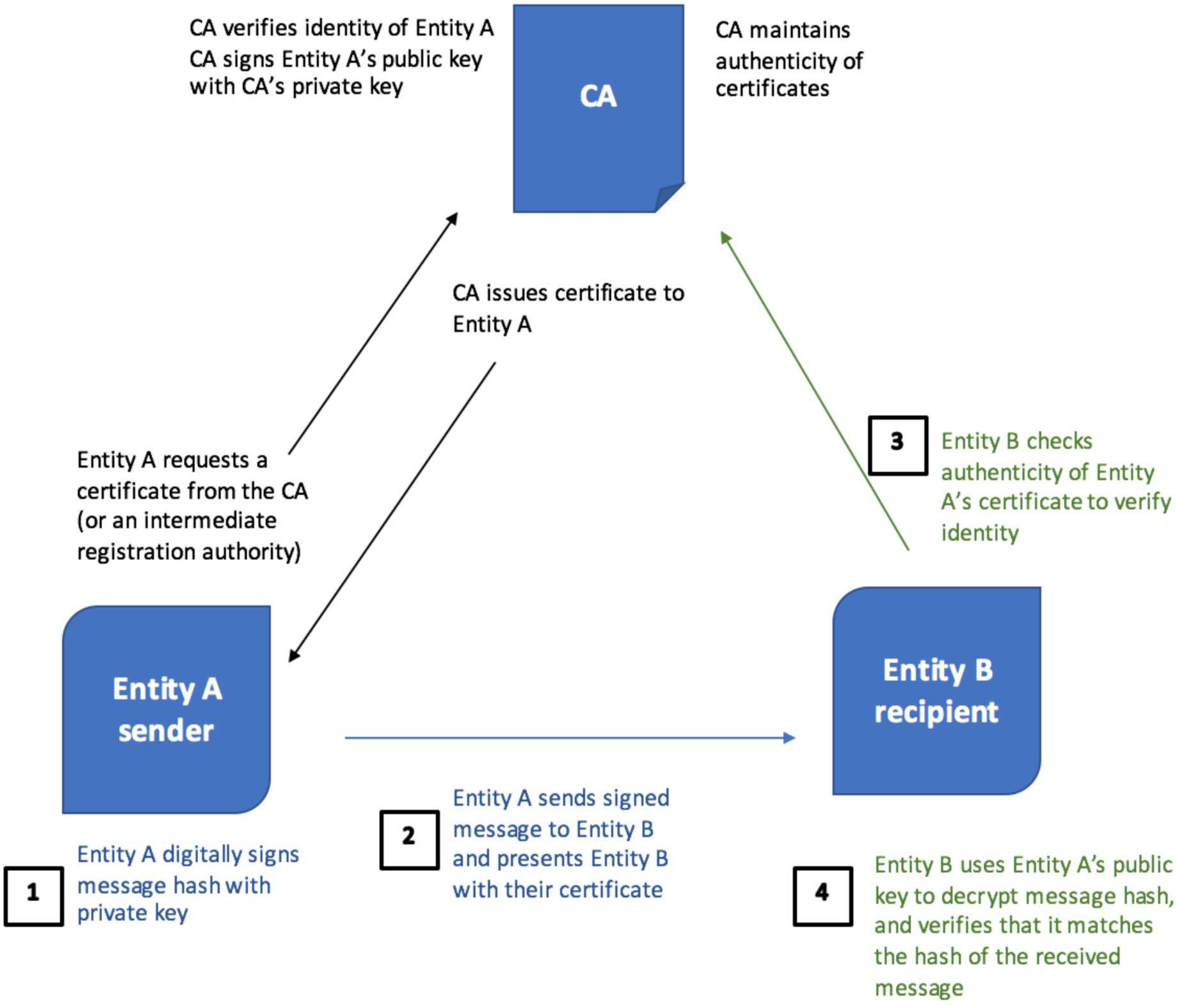
CA verifies identity of Entity A
CA signs Entity A's public key with CA's private key
CA
CA maintains authenticity of certificates
CA issues certificate to Entity A
Entity A requests a certificate from the CA (or an intermediate registration authority)
3
Entity B checks authenticity of Entity A's certificate to verify identity
Entity A sender
Entity B recipient
2
Entity A sends signed message to Entity B and presents Entity B with their certificate
1
Entity A digitally signs message hash with private key
4
Entity B uses Entity A's public key to decrypt message hash, and verifies that it matches the hash of the received message

Figure 3: Public key infrastructure as applied towards non-repudiation and integrity via digital signatures.

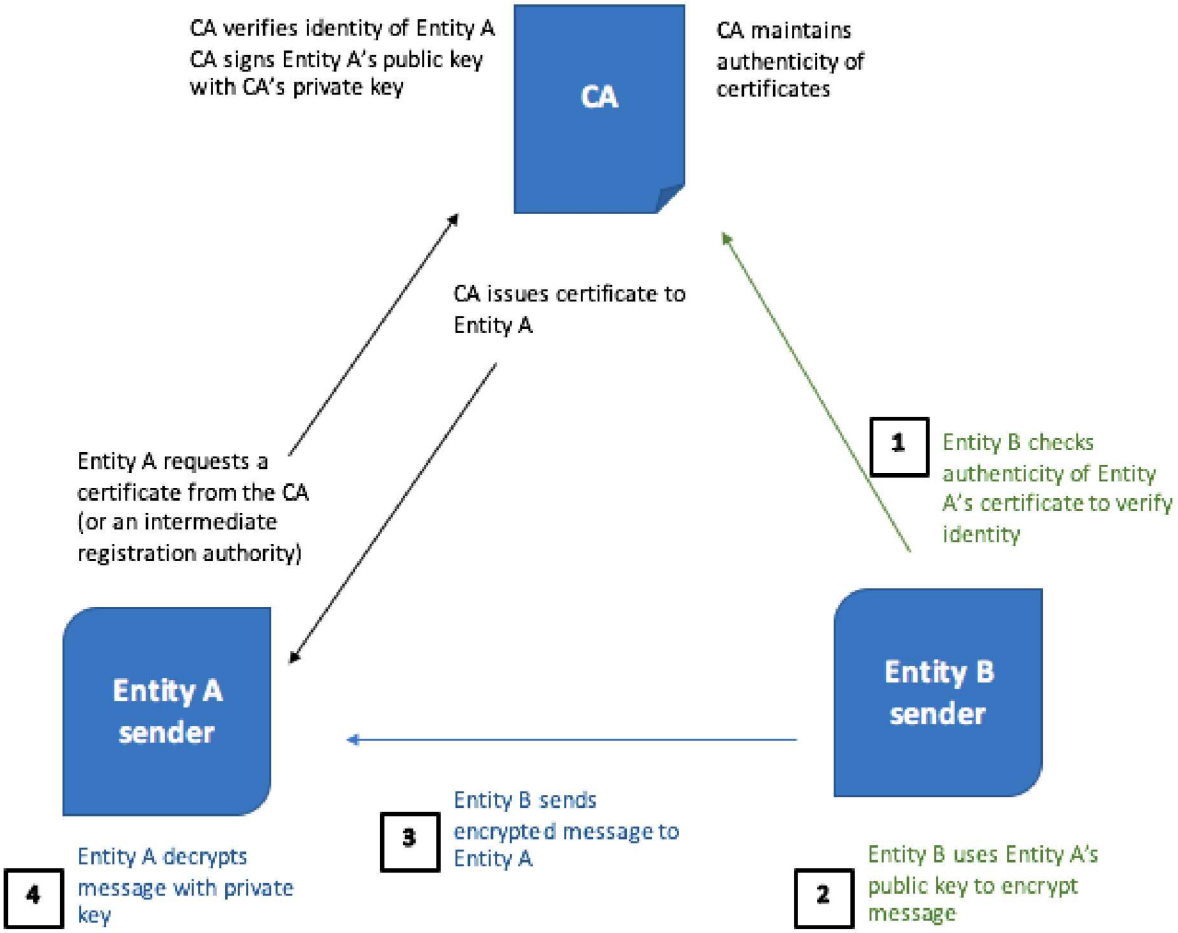
CA verifies identity of Entity A
CA signs Entity A's public key with CA's private key
CA
CA maintains authenticity of certificates
CA issues certificate to Entity A
Entity A requests a certificate from the CA (or an intermediate registration authority)
1
Entity B checks authenticity of Entity A's certificate to verify identity
Entity A sender
Entity B sender
3
Entity B sends encrypted message to Entity A
4
Entity A decrypts message with private key
2
Entity B uses Entity A's public key to encrypt message

Figure 4: Public key infrastructure as applied towards confidentiality via asymmetric encryption. In this case, Entity B sends the message and Entity A is the receiver.

As illustrated here, PKI has the added benefit of providing integrity through the message digest. PKI may also be used for establishing a secure channel for symmetric encryption or for conducting asymmetric encryption using the recipient's keys. In the asymmetric encryption example shown in Figure 4 above, if Entity B were to verify Entity A's identity through the authenticity of their certificate, Entity B could then encrypt their entire message using Entity A's public key. Entity B would then send the ciphertext message to Entity A, and Entity A would decrypt the message to plaintext using their private key. This method of asymmetric encryption can be used to securely pass a symmetric key to another user for establishing a secure channel for symmetric encryption using the securely passed symmetric key.

3. CYBER SECURITY ATTACKS

When facets of the CIA triad are not properly protected, or understood, a DER system can suffer from a range of cyber vulnerabilities. These vulnerabilities can be exploited by an adversary via cyber attacks; various attack vectors and attack types are possible and common types are described next. Specific examples of industrial control system (ICS) threats are also provided.

3.1. Types of Cyber Attacks

A cyber attack is an orchestrated attempt by an adversary or insider to sell, share, steal, damage, or destroy information from a computer network or system.[18] Table 1 includes a list of common attack vectors and Table 2 includes a list of common cyber attack categories.[19] A visual summary of requirements, threats, and attacks is shown in Figure 5, as well as their relationships to different cyber security principles.

Table 1: Attack vectors.

Attack Vector	Description
Lack of security controls	Security controls do not exist or are never "turned on."
Indiscretions by personnel	Employees write down their username and passwords and place them in their desk drawer or in plain sight.
Weak passwords	Employees use short alpha-only passwords or use their dog's name and/or their birthday as their password. Multifactor authentication is not employed.
Social engineering	An attacker uses personal information or subterfuge to learn a user's password, such as pretending to be from a bank or leaning over someone's shoulder as they type their password.
Misconfiguration of controls	Employees turn off security measures, do not change default passwords, or everyone uses the same password to access all substation equipment. Or a software application is assumed to be in a secure environment, so its actions are not authenticated.
Implementation errors	The system is implemented improperly and has features that may be exploited for unintentional uses or errors that may be triggered intentionally.
Integrity violation	Data is modified without adequate validation, such that the modified data causes equipment to malfunction or allows access to unauthorized users or applications.
Software updates and patches	The software is updated without adequate testing or validation such that worms, viruses, and Trojan Horses are allowed into otherwise secure systems. Alternatively, security patches needed to fix vulnerabilities are not applied.
Lack of trust	Different organizations have different security requirements and use different cyber security standards.
Insider	A malicious threat to an organization that comes from people within the organization, who have inside information concerning the organization's security practices, data, and computer systems.
Supply Chain	A malicious threat to an organization that comes from the manufacturers of a device component, system, or infrastructure. Attacks usually tamper with the delivered product by installing rootkits and/or hardware-based eavesdropping programs.

[18] R. Kissel, "Glossary of key information security terms," NIST Interagency Reports, vol.7298, no.3, 2013.

[19] J. Henry, R. Ramirez, F. Cleveland, A. Lee, B. Seal, T. Tansy, B. Fox, A. Pochiraju., "Cyber Security Requirements and Recommendations for CSI RD&D Solicitation #4 Distributed Energy Resource Communications," Oct. 2015.

Table 2: Common types of cyber attacks.

Types of Attacks	Description
Eavesdropping	A hacker "listens" to confidential or private data as it is transmitted, thus stealing the information. This is typically used to access intellectual property, market and financial data, personnel data, and other sensitive information.
Masquerade	A hacker uses someone else's credentials to pretend to be an authorized user and steal information, take unauthorized actions, and possibly "plant" malware.
Man-in-the-Middle	A gateway, data server, communications channel, or other non-end equipment is compromised, so the data that is supposed to flow through this middle node is read or modified before it is sent on its way.
Resource exhaustion or Denial of Service	Equipment is inadvertently (or deliberately) overloaded and cannot therefore perform its functions. Or a certificate expires and prevents access to equipment. This denial-of-service can seriously impact a power system operator trying to control the power system.
Replay	A command being sent from one system to another is copied by an attacker. This command is then used at some other time to further the attacker's purpose, such as tripping a breaker or limiting generation output.
Trojan horse or supply chain	The attacker adds malware to a system, possibly as part of an innocent-appearing enhancement or application, and possibly during the supply chain (e.g., during component manufacturing or system integration or shipping or installation). This malware does nothing until some circumstance locally or remotely triggers it to cause an unauthorized action.
Wireless	The attacker takes advantage of devices that have wireless capabilities and is able to add, modify, and/or delete data wirelessly from a remote location, bypassing any physical security protocols that have been put in place.
Air Gap	Attacker infects machines that are not connected to the internet through malicious updates on flash drives, DVDs, or other media.

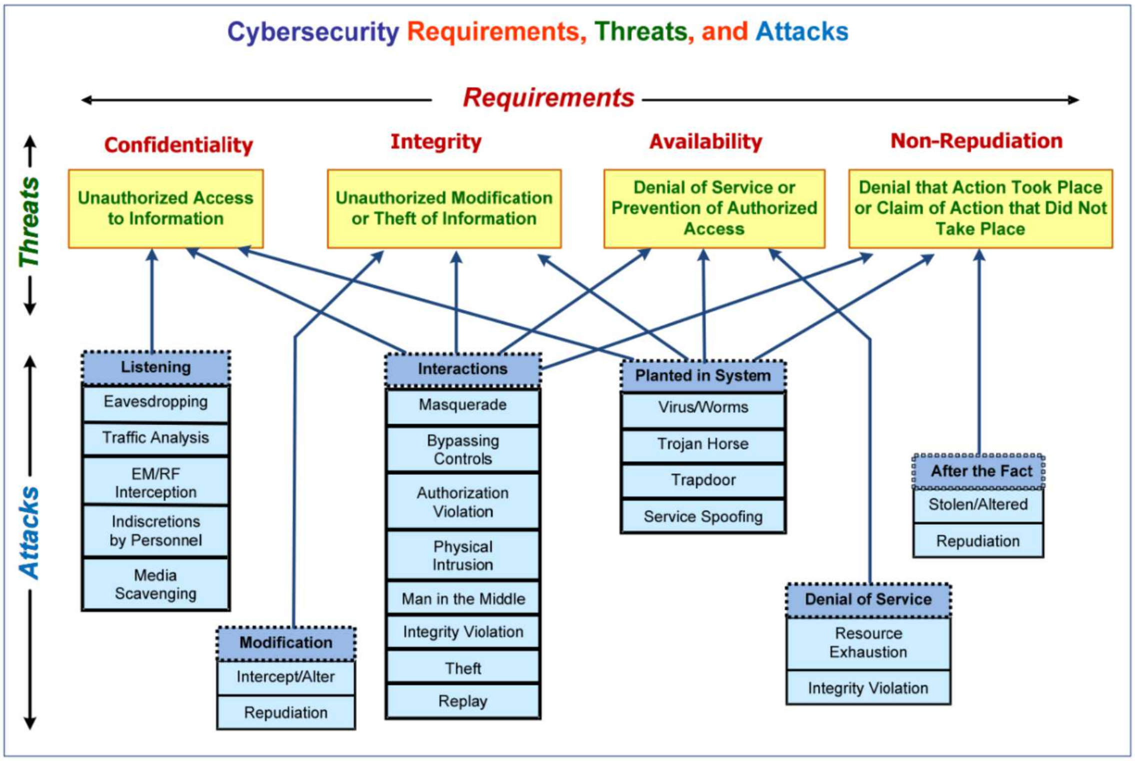

Figure 5: Visual of cyber security requirements, threats, and attacks.[20]

[20] F. Cleveland, "Draft Distributed Energy Resources (DER) Cybersecurity Recommendations for DER System Stakeholders," 28 April, 2013.

3.2. Known ICS Cyber Security Incidents

Industrial control systems in the past have been able to mostly avoid being targeted by cyber attacks, because historically these systems have either been disconnected from the internet or of low value to any adversary attempting to achieve financial gain. However, as these systems become more connected, "smart," and internet-accessible, the number of attacks aimed at them has grown, with several achieving a high degree of success at penetrating critical infrastructure targets. One of the most well-known examples is Stuxnet, which was the first case of malware being designed to specifically target ICS hardware and operations. There were several features of Stuxnet that made it noteworthy, including its extensive use of zero-days (four in total), its sophisticated construction, and how it was used to cause destruction of physical equipment by manipulating the programmable logic controllers (PLCs) that were controlling their operation.[21] Another instance of a cyber attack against ICS was Dragonfly/Havex, which appeared around 2011 and performed an extensive information gathering campaign on the ICS equipment of many defense, aviation, and energy firms across both the U.S. and Europe. It is believed that if Dragonfly had used the access they obtained in compromising these systems to sabotage instead of collect information, they could have caused damage to the energy supply of the countries it targeted.[22] On December 23, 2015, another campaign that utilized the BlackEnergy trojan did just that. By targeting the SCADA systems of the Ukrainian Kyivoblenergo, a regional electricity distribution company, BlackEnergy successfully created outages that impacted 230,000 people and left them without power for 1 to 6 hours.[23] Nearly a year later on December 17, 2016, another attack occurred in Ukraine, this time on a single transmission-level substation. This attack was performed by a malware platform called CrashOverride, and represents another significant development in the capabilities displayed by adversaries. CrashOverride was able to leverage pieces of prior malware, including Havex and BlackEnergy, as it was constructed as a modular framework to provide sophisticated attack capabilities and scales effectively by allowing the inclusion of modules for different ICS environments.[24]

[21] N. Falliere, L. O. Murchu, and E. Chien, "W32.Stuxnet dossier," Symantic Security Response, Tech. Rep., Oct. 2010.

[22] Symantic Security Response. (2014, Jun. 30). *Dragonfly: Western Energy Companies Under Sabotage Threat* [Online]. Available: https://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat

[23] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid," SANS Industrial Control Systems, 2016.

[24] "CRASHOVERRIDE, Analysis of the threat to electric grid operations," Dragos INC, 2017.

4. COMMUNICATION PROTOCOLS

ICS cyber security is closely tied to the communication technology being employed in the control network. Each communication protocol comes with different security features, and it is essential that these security strengths and weaknesses are analyzed in current and future systems to assess and respond to the associated level of risk.

4.1. OSI Stack

The Open System Interconnection (OSI) model defines a networking framework to implement protocols in seven layers.[25] It divides network communication into seven layers. Layers 1-3 are considered the lower or media layers, and are mostly concerned with packaging and moving data from physical bit signals to the network level. Layers 4-7, the upper layers, are usually implemented at the host level. Each layer is able to receive and pass data onto the next layer. When a user executes a function at the application layer, control and information is passed from one layer to the next, starting from the application layer and ending at the physical layer, then back up the hierarchy as shown in Figure 6 below. The communications protocols discussed in this report reside at the upper layers of the OSI stack. The lower level connections are well defined for a range of applications and will not be directly addressed here. For more information about protocol stacks, please refer to International Telecommunication Union, Telecommunication Standardization Sector (ITU-T) Recommendation X.200, *Basic Reference Model: The Basic Model* and X.800, *Security Architecture for Open Systems Interconnection for CCITT applications*. [26,27]

[25] H. Zimmermann, "OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection," IEEE Transactions on Communications, vol. 28, no. 4, pp. 425-432, Apr. 1980.

[26] *Data Network and Open System Communications, Open Systems Interconnection–Model and Notations, Information Technology–Open Systems Interconnection–Basic Reference Model: The Basic Model*, International Telecommunications Union (ITU-T) X.200, July. 1994.

[27] *Security architecture for Open Systems Interconnection for CCITT applications*, International Telecommunications Union (ITU-T) X.800, Mar. 1991.

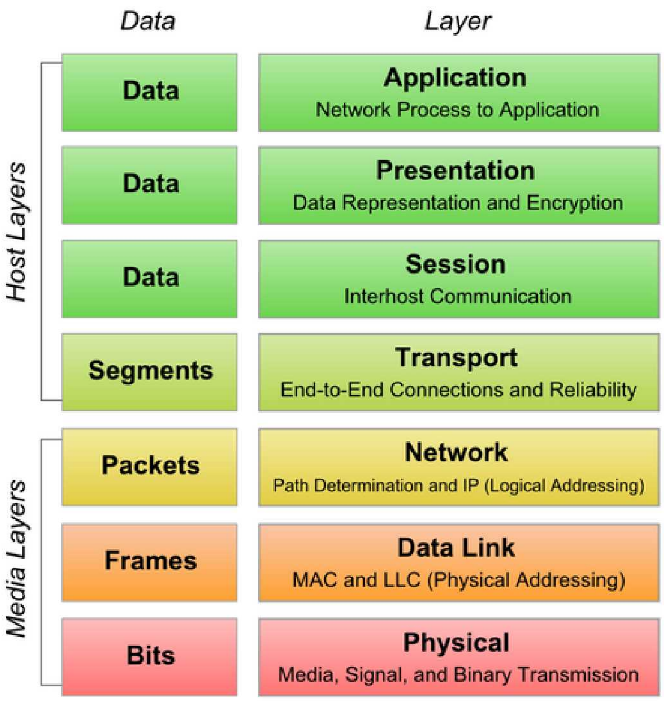
Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Interhost Communication
Segments
Transport
End-to-End Connections and Reliability
Packets
Network
Path Determination and IP (Logical Addressing)
Frames
Data Link
MAC and LLC (Physical Addressing)
Bits
Physical
Media, Signal, and Binary Transmission

Figure 6: OSI model, seven layer protocol stack.[28]

4.2. DER Communication Requirements

While there is a wide range of communication protocols for power systems equipment, only a few standardized protocols exist for DER equipment. At this time, IEEE 1815, IEC 61850, Modbus, and IEEE 2030.5 are defined to communicate with DER equipment and were considered for inclusion in IEEE 1547.[29,30,31,32,33] Each of the protocols defines the exchange of information with entities, but does not define the encoding of measurement and control data points, operating modes, grid function parameters, and device information. These values and their organization are defined in data or information models for each parameter, as shown in Table 3.

It should be noted that although the DER industry is primarily focused on Modbus, IEEE 2030.5, IEEE 1815, and IEC 61850, other protocols have been suggested by different organizations. These protocols are incorporated through the use of different wrapper functions (e.g., IEC Common Information Model) or suggest novel protocols (e.g., OpenFMB).[34,35] A list of communication protocols is included in Appendix A as well as in a GMLC report.[36]

[28] Tech-FAQ, *The OSI Model – What It Is; Why It Matters; Why It Doesn't Matter*. Available: http://www.tech-faq.com/osi-model.html

[29] *IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3*), IEEE Std.1815-2012 (Revision of IEEE Std. 1815-2010), 2012.

[30] *IEC/IEEE International Standard - Communication networks and systems for power utility automation*, IEC/IEEE 61850, 2016.

[31] O. Hersent, D. Boswarthick and O. Elloumi, "ModBus," in *The Internet of Things: Key Applications and Protocols*, Ed. 1, Wiley Telecom, 2012.

[32] *IEEE Adoption of Smart Energy Profile 2.0 Application Protocol Standard*, IEEE Std. 2030.5, 2013.

[33] *IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems*, IEEE Std. 1547-2003, 2003.

Table 3: DER communication and interoperability requirements.

Communication Protocol	Data or Information Model	Security Requirements
IEEE 1815	DNP3 Application Note AN2013-001[37]	In IEEE 1815
IEC 61850	IEC 61850-90-7 and IEC 61850-7-420	In IEC 62351 Series[38]
Modbus	SunSpec Modbus Models[39]	None
IEEE 2030.5	Common Smart Inverter Profile (CSIP)[40]	In IEEE 2030.5, expanded in CSIP

Currently, there are limited DER communication requirements in the U.S. At this time, the California Public Utilities Commission (CPUC) is reviewing an update to Electric Rule 21 which requires DER devices to include communications. The IEEE 1547 full revision will also mandate communications for DER devices.

4.2.1. California Rule 21

The Smart Inverter Working Group (SIWG) created a series of recommendations for the California Public Utilities Commission (CPUC) to update the Electric Rule 21 interconnection requirements for DER devices.[41] These recommendations were structured into three phases:

- Phase 1: added multiple autonomous DER grid-support functions.
- Phase 2: added DER communication requirements.
- Phase 3: (forthcoming) adds grid-support functions requiring communications.

In late 2016, the SIWG Phase 2 recommendations began the review process and communications between utilities and large DER (>1 MW), Facility DER Energy Management Systems (FDEMS), Retail Energy Providers (REP), aggregators, and fleet operators were prescribed for the Investor-Owned Utilities (IOUs) in California, as shown in Figure 7. Each of the IOUs has created Interconnection Handbooks which reference the California IEEE 2030.5 Implementation Guide as the communication protocol and information model for these communications.[42]

[34] A. McMorran, “An introduction to IEC 61970-301 & 61968-11: The common information model,” University of Strathclyde, 2007.

[35] (2017). *OpenFMB™* [Online]. Available: http://www.sgip.org/openfmb/

[36] D. Narang, et al., “GMLC Gap Analysis for DER Interconnection and Interoperability Standards and Test Procedures: An Assessment of Gaps in Standards and Test Procedures for Interconnection and Interoperability of Devices Connected to the Electric Distribution Grid,” 2017 (forthcoming).

[37] “DNP3 Profile for Advanced Photovoltaic Generation and Storage,” DNP Application Note AN2013-001, 2013.

[38] F. Cleveland, “IEC 62351 Security Standards for the Power System Information System,” IEC TC57 WG15, 2012.

[39] SunSpec® Alliance Interoperability Specification, Information Model Specification, Document 12041, Version 1.9, 2015.

[40] California Smart Inverter Implementation Working Group, “IEEE 2030.5 Common California IOU Rule 21 Implementation Guide for Smart Inverters,” Common Smart Inverter Profile V1.0, Aug. 31, 2016.

[41] California Public Utilities Commission. (2017). Rule 21 Interconnection [Online]. Available: http://www.cpuc.ca.gov/Rule21/

[42] California Smart Inverter Implementation Working Group, “IEEE 2030.5 Common California IOU Rule 21 Implementation Guide for Smart Inverters,” Common Smart Inverter Profile V1.0, Aug. 31, 2016.

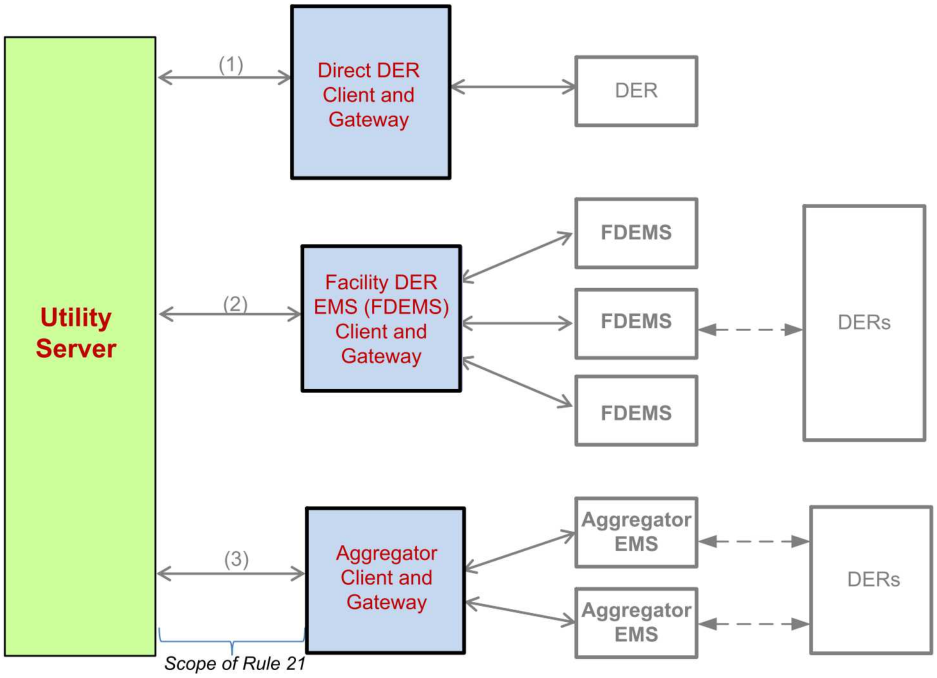
Utility Server
(1)
(2)
(3)
Direct DER Client and Gateway
Facility DER EMS (FDEMS) Client and Gateway
Aggregator Client and Gateway
DER
FDEMS
FDEMS
FDEMS
DERs
Aggregator EMS
Aggregator EMS
DERs
Scope of Rule 21

Figure 7: Scope of communication requirements in California Rule 21, based on CSIP.[43]

4.2.2. IEEE 1547

IEEE 1547 is a standard for the interconnection of DER to the Electric Power System (EPS), with the criterion for applicability being any generation with an aggregate capacity of ≤10 MVA at the point of common coupling (PCC).[44] This includes synchronous generators, induction machines, power inverters, or any other distributed resource. The intent is to provide the technical requirements and specifications needed to safely connect these distributed resources to the broader power system environment. A major, multi-year effort has been conducted to update IEEE 1547 to include grid-support functions and communications. The proposed scope of the communication requirements is shown in Figure 8 and includes the connections to individual DER devices and DER facilities. The IEEE 1547 draft includes options to communicate with the DER or DER facilities using Modbus, IEEE 2030.5, and IEEE 1815.

[43] California Smart Inverter Implementation Working Group, "IEEE 2030.5 Common California IOU Rule 21 Implementation Guide for Smart Inverters," Common Smart Inverter Profile V1.0, Aug. 31, 2016.

[44] IEEE Std. 1547-2003, *IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems*, 2003.

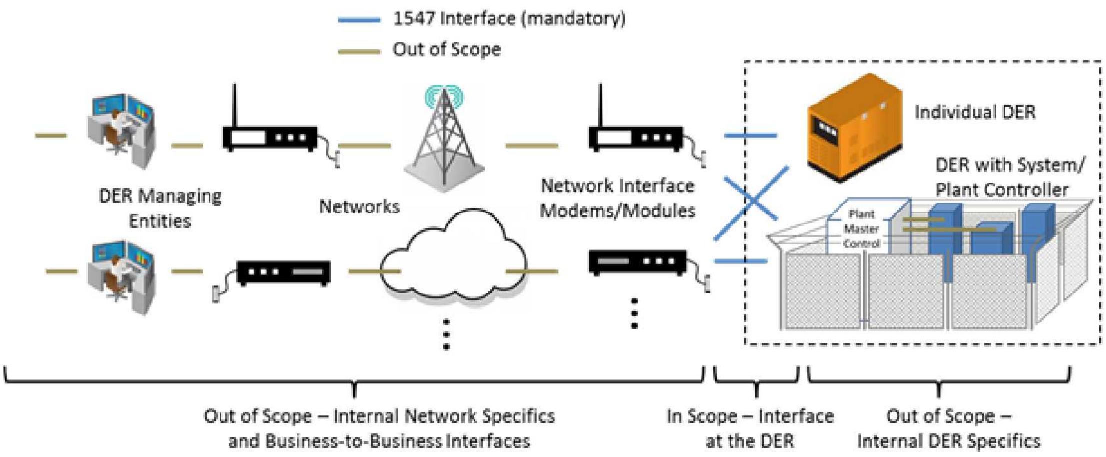
1547 Interface (mandatory)
Out of Scope
DER Managing Entities
Networks
Network Interface Modems/Modules
Individual DER
DER with System/ Plant Controller
Plant Master Control
Out of Scope – Internal Network Specifics and Business-to-Business Interfaces
In Scope – Interface at the DER
Out of Scope – Internal DER Specifics

Figure 8: Proposed scope of IEEE 1547 communication requirements.[45]

[45] IEEE P1547™ *Draft Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces*, Aug 2016.

5. KEY CYBER SECURITY GUIDELINES AND STANDARDS

In an effort to assist the solar and grid industry, we present some key cyber security guidelines, standards, and best practices in an effort to enhance security of DER devices and models. This section will first present work from several major players in developing standards for the smart grid and cyber security arenas, and then continues, in Section 6, by providing some generic recommendations for cyber security practices. Due to the vast breadth of the field of cyber security, the listed works should be considered only as a starting point, not exhaustive. This list is based on previous work for the California Solar Initiative.[46]

5.1. NIST

The National Institute of Standards and Technology (NIST) has developed multiple standards over the years to address cyber security in different applications. Standards pertinent to DER cyber security can be listed as follows:

- NISTIR 7628, Guidelines for Smart Grid Cybersecurity[47]
- NIST SP 1108, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0[48]
- NIST SP 800-82 Rev. 2, Guide to Industrial Control Systems Security[49]
- NIST Framework for Improving Critical Infrastructure Cybersecurity[50]
- NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook[51]
- NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations[52]

NISTIR 7628 is a 3 volume work on securing the smart grid that was first released in September 2010 and later updated in September 2014. NISTIR 7628 includes information on Smart Grid Cybersecurity Strategy, Architecture, and High Level Requirements, Privacy and the Smart Grid, and Supportive Analyses and References. In January 2010, NIST released the first version of NIST SP 1108 to address the Energy Independence and Security Act of 2007, which assigned NIST with the responsibility to develop a framework for attaining interoperability of smart grid devices. The resultant framework lays down an general strategy for ensuring smart grid interoperability. NIST has since updated this framework twice to address evolutions in the smart grid, to expand the breadth of content, and to address stakeholder concerns. The third version was released in September 2014.

[46] J. Henry, R. Ramirez, F. Cleveland, A. Lee, B. Seal, T. Tansy, B. Fox, A. Pochiraju., "Cyber Security Requirements and Recommendations for CSI RD&D Solicitation #4 Distributed Energy Resource Communications," Oct. 2015.

[47] V.Y. Pillitteri, and T. L. Brewer, "Guidelines for smart grid cybersecurity," NIST Interagency/Internal Report (NISTIR)-7628 Rev 1, 2014.

[48] *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0*, NIST Special Publication 1108, 2014.

[49] *Guide to Industrial Control Systems (ICS) Security*, NIST Special Publication 800-82 Revision 2, 2015.

[50] "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0," National Institute of Standards and Technology, 2014.

[51] *An Introduction to Computer Security: The NIST Handbook*, NIST SP 800-12, 1995.

[52] *Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4*, NIST SP 800-53, 2013.

NIST SP 800-82 Rev. 2 was released in May 2015 and provides instruction on important concepts and considerations for securing control systems. This includes Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS), with applicability across critical infrastructure sectors. On February 12, 2013, President Obama signed Executive Order (EO) 13636 titled "Improving Critical Infrastructure Cybersecurity".[53] This EO directed NIST to develop a cyber security framework, which was later released in February 2014 as NIST Framework for Improving Critical Infrastructure Cybersecurity. This voluntary framework was created as a general guide for how an organization may develop processes to manage cyber risk.

NIST SP 800-12 was released in October 1995 to address computer security issues in general. While this standard is older than many of the others mentioned in this report, it does cover many of the information security concepts that are still relevant to the modern smart grid, as the smart grid represents part of the Internet of Things (IoT) where massive amounts of data are generated and passed between devices and stakeholders. NIST SP 800-53 was developed as a holistic methodology and framework for the security controls required for information security and risk management, with special consideration taken for privacy considerations. Even though this standard was originally targeted at federal information systems, specifically regarding compliance with the Federal Information Processing Standard (FIPS) 200[54], it addresses privacy concerns that are crucial to many other systems including in the smart grid.

5.2. NERC / FERC

The North American Electric Reliability Corporation (NERC) is the Electric Reliability Organization (ERO) for the United States, as determined by the Federal Energy Regulatory Commission (FERC) pursuant to Section 215 of the Federal Power Act, as amended by the Energy Policy Act of 2005.[55] This means that NERC has been vested with regulatory authority by FERC to develop compulsory standards that ensure the reliability of the Bulk Power System (BPS) within the United States. As NERC standards apply to individual generators at 20+ MVA or aggregated resources at 75+ MVA connected at 100 kV or greater, NERC has historically not been interested in distributed generators, but NERC has noted that control of aggregate distributed resources would be capable of disrupting significant quantities (100s of MWs) of generation.[56] Thus, it is likely that some future NERC standards may apply to DER devices.

NERC has produced high level standards pertaining to cyber security. To address the issue of reliability in relation to cyber security, NERC issued the Critical Infrastructure Protection (CIP) Cyber Security Standards.[57] These standards, of which many are currently in their sixth version, address the issues of:

- Identifying critical cyber assets
- Developing security management controls

[53] Office of the Press Secretary, "Executive Order -- Improving Critical Infrastructure Cybersecurity", The White House, Feb. 13, 2013.

[54] *Minimum Security Requirements for Federal Information and Information Systems*, FIPS PUB 200, 2006.

[55] North American Electric Reliability Corporation. (2013). *History of NERC* [Online]. Available: http://www.nerc.com/AboutNERC/Documents/History%20AUG13.pdf

[56] North American Electric Reliability Corporation, "Distributed Energy Resources: Connection Modeling and Reliability Considerations," Distributed Energy Resources Task Force Report, Feb. 2017.

[57] North American Electric Reliability Corporation. (2016). *CIP Standards* [Online]. Available: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

- Setting requirements for personnel and training
- Establishing electronic security perimeters
- Implementing physical security
- Managing systems security
- Reporting incidents and response planning
- Developing recovery plans
- Managing configuration changes and vulnerability assessments
- Protecting information

Assets are given different levels of requirements based on their criticality and impact on BPS functions, with High, Medium, and Low impact levels defined. Note that while NERC CIP standards are the only national regulatory requirements for BPS cyber security, individual states may or may not institute their own regulations through Public Utility Commissions (PUCs). Also, certain forms of power generation may fall under other regulatory bodies, such as nuclear power being subject to the Nuclear Regulatory Commission (NRC).

5.3. ICS-CERT

United States Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) is an organization tasked with reducing risks across critical infrastructure sectors, including energy and the smart grid, and coordinating among federal, state, local, public and private stakeholders.[58] ICS-CERT also leads efforts to respond to control system related incidents, conducts cyber assessments, provides incident response, provides training and reference documents, and coordinates intelligence and information sharing. An example of the information sharing efforts orchestrated by ICS-CERT are the alerts released of current and past cyber incidents and threats. One such alert was released on May 16, 2017 concerning the WannaCry ransomware, and contained recommendations provided by vendors for configuring their products as well as general guidance for securing devices against the threat.[59]

ICS-CERT offers a variety of resources including web-based and in-person training courses for control system cyber security. The organization regularly publishes white papers on known threats, such as released malware, emerging technologies, and best practices related to cyber security. ICS-CERT also serves as a focal point for current information gathering, including documentation produced by other organizations. One example of a document referenced by ICS-CERT is a white paper produced by the United States Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability titled "Cybersecurity and the Smarter Grid" which details some of DOE's efforts in this arena.[60]

ICS-CERT also hosts an Industrial Control Systems Joint Working Group (ICSJWG) to provide an ongoing venue for information related to control systems cyber security issues.[61] This working group is open to the public.

[58] Industrial Control Systems Cyber Emergency Response Team. (2017). *About the Industrial Control Systems Cyber Emergency Response Team* [Online]. Available: https://ics-cert.us-cert.gov/About-Industrial-Control-Systems-Cyber-Emergency-Response-Team

[59] Industrial Control Systems Cyber Emergency Response Team. (May 17, 2017). *Alert (ICS-ALERT-17-135-01I): Indicators Associated With WannaCry Ransomware (Update I)* [Online]. Available: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-135-01I

[60] C. Hawk and A. Kaushiva, "Cybersecurity and the smarter grid," The Electricity Journal 27.8, 2014.

5.4. IEC/ISO

The International Electrotechnical Commission (IEC) and International Organization for Standardization (ISO) are international, independent organizations that provide common standards for the global community. IEC and ISO are not government bodies and as such, compliance with these standards is voluntary unless otherwise specified by national regulations. The United States is a member of both these organizations through the American National Standards Institute (ANSI), but NIST is the party responsible for coordination of standards activities for the US government.[62] Some relevant standards for DER cyber security include:

- IEC 62351: Information Security for Power System Control Operations[63,64]
- IEC/ISO 27000: Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary [65]
- IEC 62443: Series of Standards: Industrial Automation and Control Systems Security[66]

IEC 62351 is a cyber security standard for power systems that has been developed to help cover the gaps in the actual communication protocols or standards, with direct ties to other IEC standards, including IEC 60870 (related to DNP3), IEC 61850, IEC 61970, and IEC 61968.[67] This standard provides direction on the end-to-end security requirements of power systems, including security for TCP/IP communications, Manufacturing Message Specification (MMS) communications, different IEC standards, network and system management (NSM), Role-Based Access Control (RBAC), Key Management, Security Architecture, and security for XML. Note that this standard is merely layered on top of the communication protocols and standards in use in a power system, and does not replace them.

The IEC/ISO 27000 series is a family of standards devoted to information security management. IEC/ISO 27019:2013 is of special interest to the electric utility industry as it contains information security guidelines for process control and automation systems. Finally, the IEC 62443 series is a family of standards for securing industrial automation and control systems that includes general concepts, models, conformance metrics, life-cycles, use-cases, policies, procedures, system requirements, and component requirements. It is meant to build off other standard families, including the IEC/ISO 27000 standards, in order to achieve more holistic security for industrial systems.

[61] Industrial Control Systems Cyber Emergency Response Team. (2017). *Industrial Control Systems Joint Working Group* [Online]. Available: https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG

[62] C.R. DeVaux, “A Review of U.S. Participation in the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC),” NISTIR 6492, Feb. 2000.

[63] *Information Security for Power System Control Operations*, IEC 62351, 2009.

[64] F. Cleveland, “IEC TC57 WG15: IEC 62351 Security Standards for the Power System Information Infrastructure,” International Electrotechnical Commission: White Paper, 2012.

[65] *Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary*, IEC/ISO 27000, 2016.

[66] *The 62443 Series of Standards: Industrial Automation and Control Systems Security*, IEC 62443, 2016.

[67] R. Schlegel, S. Obermeier, and J. Schneider, “A security evaluation of IEC 62351,” Journal of Information Security and Applications, vol. 34, 2017.

5.5. IEEE

The Institute for Electrical and Electronics Engineering (IEEE) is an active developer and driver of standards for professionals in many fields, including cyber security. Some relevant cyber security standards include:

- IEEE 1547.3: IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems[68]
- IEEE C37.240: IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems[69]
- IEEE 1686: IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities *(*under further development*)*[70]

IEEE 1547.3 was described in detail in Section 4.2.2, and additional information is provided in Appendix A. Essentially, it provides the technical requirements and specifications needed to safely connect distributed resources to the broader power system environment. The IEEE C37.240 standard provides requirements for substation cyber security. It seeks to balance technical feasibility with economic feasibility to address the full range of risks expected to be present at a substation. IEEE 1686, currently being updated, defines the functions and features to be provided in intelligent electronic devices (IEDs) to accommodate critical infrastructure protection programs. This addresses aspects of IED control such as access, operation, configuration, firmware revision, and data retrieval.

5.6. IETF

The Internet Engineering Task Force (IETF) works to improve the internet by developing and hosting technical standards related to the use, design, and management of the internet.[71] These standards are generally then released as a Request for Comments (RFC). Many of these standards are relevant to cyber security and therefore also relevant to securing distributed resources such as DER devices and communication.

- IETF RFC 6272: Internet Protocols for the Smart Grid[72]
- IETF RFC 7744: Use Cases for Authentication and Authorization in Constrained Environments[73]
- RFC 3268: Advanced Encryption Standard (AES) Cipher suites for Transport Layer Security (TLS)[74]
- RFC 4962: Guidance for Authentication, Authorization, and Accounting (AAA) Key Management [75]
- RFC 5247: Extensible Authentication Protocol (EAP) Key Management Framework[76]

[68] *IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems*, IEEE Std. 1547-2003, 2003.

[69] *IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems*, IEEE Std. C37.240-2014, 2015.

[70] *IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities – Redline*, IEEE Std. 1686-2013 (Revision of IEEE Std. 1686-2007) – Redline, 2014.

[71] IETF. (2017). *About the IETF* [Online]. Available: https://www.ietf.org/about/

[72] *Internet Protocols for the Smart Grid*, IETF RFC 6272, 2011.

[73] *Use Cases for Authentication and Authorization in Constrained Environments*, IETF RFC 7744, 2016.

[74] *Advanced Encryption Standard (AES) Cipher suites for Transport Layer Security (TLS)*, RFC 3268, 2002.

[75] *Guidance for Authentication, Authorization, and Accounting (AAA) Key Management*, RFC 4962, 2007.

- RFC 3711: The Secure Real-Time Transport Protocol (SRTP)[77]

IETF RFC 6272 provides insight into how to best profile or leverage the Internet Protocol Suite (IPS) toward smart grid design. The document presents an overview of IPS technologies and identifies key infrastructure protocols pertinent to smart grid device integration into IP-based infrastructure. In IETF RFC 7744, representative use cases are provided that demonstrate authentication and authorization in constrained environments.

RFC 3268 proposes several new cipher suites, including the addition of AES ciphers to the symmetric ciphers supported by the TLS protocol. RFC 4962 offers guidance to designers of Authentication, Authorization, and Accounting (AAA) key management protocols, though it does not present an obligatory protocol structure. RFC 5247 defines the Extensible Authentication Protocol (EAP), an authentication framework which supports multiple authentication methods. Lastly, RFC 3711 describes the Secure Real-time Transport Protocol (SRTP), which is a secure implementation of the Real-time Transport Protocol (RTP). SRTP provides confidentiality, message authentication, and replay protection to RTP traffic and to the control traffic for RTP sent via the Real-time Transport Control Protocol (RTCP). EtherCat is an example of an open RTP used for Ethernet communication in the energy domain, specifically for wind power.[78]

5.7. CIGRE

The Council on Large Electric Systems, or CIGRE, was founded in 1921 and is an international, non-profit organization that promotes collaboration around the globe with the goal of improving electric power systems. CIGRE addresses the importance of cyber security in multiple guidelines and reports:

- CIGRE B5.38 The Impact of Implementing Cyber Security Requirements using IEC 61850[79]
- CIGRE B5/D2.46: Application and Management of Cyber Security Measures for Protection & Control Systems[80]
- CIGRE D2.31: Security architecture principles for digital systems in Electric Power Utilities EPUs[81]
- CIGRE D2/B3/C2.01: Security for information systems and intranets in electric power systems[82]

In CIGRE B5.38, a survey of standards, reports, and technical papers was performed to understand the impact of cyber security on IEC 61850 systems and also the current state of

[76] *Extensible Authentication Protocol (EAP) Key Management Framework*, RFC 5247, 2008.

[77] *The Secure Real-time Transport Protocol (SRTP)*, RFC 3711, 2004.

[78] W. Hu. *Electronics and Signal Processing: Selected Papers from the 2011 International Conference on Electric and Electronics (EEIC 2011) in Nanchang, China on June 20-22, 2011*. Nanchang, China: Springer Science & Business Media, 2011.

[79] *The Impact of Implementing Cyber Security Requirements using IEC 61850*, CIGRE B5.38, 2010.

[80] *Application and Management of Cyber Security Measures for Protection & Control Systems*, CIGRE B5/D2.46, 2013.

[81] *Security architecture principles for digital systems in Electric Power Utilities EPUs*, CIGRE D2.31, 2015.

[82] *Security for information systems and intranets in electric power systems*, CIGRE D2/B3/C2.01, 2007.

solutions developed. CIGRE B5/D2.46 seeks to address: 1) cyber security mechanisms used to protect/control access to and use of protection and control devices, systems, and applications, 2) cyber security management challenges, and 3) qualitative cyber security control of the trust placed in Electric Power Utility (EPU) personnel and support personnel. In CIGRE D2.31, general security architecture principles for digital systems in EPUs were discussed, focusing on classification methods for security zone/level definition, characterization, categorization, and modeling of threats, and remote services. Working group results and recommendations in the information and control systems security domain were given in CIGRE D2/B3/C2.01 to aid developing and implementing cyber security in an EPU.

5.8. U.S Department of Energy (DOE)

The United States Department of Energy (DOE) is a cabinet-level department of the U.S. government which performs work on both nuclear and energy related issues.. In this context, the DOE supports and contributes to various grid cyber security efforts. For instance, the DOE Office of Electricity Delivery and Energy Reliability (OE) states cyber security for critical energy infrastructure as a top priority.[83] The program supports three key areas: strengthening energy sector cyber security preparedness, coordinating cyber security incident response and recovery, and accelerating research for development and demonstration of resilient energy delivery systems. The DOE is dedicated to cyber security in the energy domain and has published two documents relevant to DER cyber security:

- DOE/DHS ES-C2M2: Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)[84]
- DOE/NIST/NERC RMP: Electricity Subsector Cybersecurity Risk Management Process Guideline[85]

The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) was developed to support a White House initiative led by the DOE and with the partnership of the United States Department of Homeland Security (DHS). DOE and DHS collaborated with private and public-sector experts to develop the ES-C2M2 model to support development and measurement of cyber security capabilities in the electric grid sector. In particular, the model sought to provide a benchmark for utilities to evaluate and compare against, share guidelines and relevant references, and enable utilities to make effective decisions for prioritizing actions and investments to improve their cyber security capabilities.

The Electricity Subsector Cybersecurity Risk Management Process Guideline (RMP) provides a risk management framework for electric subsector cyber security. DOE, NIST, and NERC worked together with industry representatives to mold RMP into a consistent and repeatable approach for managing cyber security risk. It seeks to provide organizations in the grid domain with the tools to apply effective risk management processes, tailor them to their specific organizational requirements, and/or implement a new or improved cyber security program.

[83] DOE OE (2017). *Cyber Security for Critical Energy Infrastructure* [Online]. Available: https://energy.gov/oe/activities/cybersecurity-critical-energy-infrastructure

[84] "Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), Version 1.1," U.S. Department of Energy and U.S. Department of Homeland Security, Feb. 2014.

[85] "Electricity Subsector Cybersecurity Risk Management Process Guideline," DOE/OE-0003, U.S. Department of Energy, May 2012.

5.9. Electric Power Research Institute (EPRI)

EPRI is an independent, non-profit research organization funded by the electric power industry to advance energy research both in the United States and worldwide. EPRI collaborates with both the public and private sectors to develop smart grid cyber security guidelines, industry standards, and technical specifications applicable for DER. As part of that effort, EPRI has developed a resource center which contains extensive information pertaining to the smart grid[86], including the National Electric Sector Cybersecurity Organization Resource (NESCOR), which has analyzed cyber security issues for the smart grid and seeks to strengthen the cyber security posture of the grid sector.[87] One example is a NESCOR report on Cyber Security for DER Systems[88] which examined the requirements for securing DER functions while taking into account the differences of DER communication architectures. These architectures are studied using NISTIR 7628: *Guidelines for Smart Grid Cybersecurity* (described in Section 5.1), Logical Interfaces, and Logical Interface Categories (LICs) and the associated high-level security requirements to identify the necessary cyber security requirements and gaps.

[86] EPRI. (2011). *Smart Grid Resource Center* [Online]. Available: http://smartgrid.epri.com/Index.aspx

[87] EPRI. (2011). *Smart Grid Resource Center: NESCOR* [Online]. Available: http://smartgrid.epri.com/Index.aspx

[88] F. Cleveland and A. Lee, " Cyber Security for DER Systems," National Electric Sector Cybersecurity Organization Resource (NESCOR), Electric Power Research Institute (EPRI), July 2013.

6. CYBER SECURITY RECOMMENDATIONS FOR DER NETWORKS

As DER enter the wider realm of the Internet of Things (IoT), there have been some early warning signs of the full cyber threat potential. For instance, a single-end user (Fred Bret-Mounet) gained access to a VPN tunnel established for a DC optimizer data manager, where he discovered 1000 other PV devices on the same subnet. Had he desired, he could have also remotely disconnected these devices.[89,90] A major European PV inverter manufacturer recently discovered over a dozen vulnerabilities, including those which could remotely compromise the equipment.[91] In October 2016, a large Distributed Denial-of-Service (DDoS) attack using a botnet of IoT devices affected many websites including Amazon, Twitter, and Netflix.[92] Many additional IoT and industrial control system attacks have been perpetrated in the past, some with significant detrimental impact.[93] Consequently, it is imperative to secure DER communications to provide grid reliability and resiliency.

Many DER devices communicate via unsecured serial protocols like Modbus, so there has been an effort to develop translators that integrate with DER to take encrypted protocols such as OpenADR 2.0b and IEEE 2030.5 and only unencrypt the communications within the DER.[94] As part of a California Solar Initiative grant, Sandia National Laboratories led a team to generate cyber security recommendations for PV Inverters using SunSpec Modbus removable communications modules.[95] The team presented a number of threats, vulnerabilities and high-level recommendations for residential inverter-based DER systems covering physical security, access control, integrity, confidentiality, encryption, and policy. Sandia has also conducted multiple DER cyber security assessments to understand weaknesses of the current state-of-the-art communications-enabled DER and vendor software tools.[96] The team performed network reconnaissance, then attacked the DERs using packet replay, Man-in-the-Middle (MITM), Denial-of-Service (DoS), and modified firmware uploads. The team also looked for proper maintenance of device logs and password handling procedures. The assessment discovered a number of security weaknesses within the DER devices, which were reported to the vendors to improve their cyber posture.

The DER equipment is not the only risk to the security of the DER control network. Strong cyber security practices from utilities and aggregators must also be implemented in order to secure end-to-end communications. For this reason, this section is broken into several parts that address recommendations for general cyber security and best practices, grid operators, aggregators,

[89] T. Fox-Brewster. (Aug. 1, 2016). *This Man Hacked His Own Solar Panels... And Claims 1,000 More Homes Vulnerable* [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2016/08/01/1000-solar-panels-tigo-vulnerable-hackers/#65d585844a3f

[90] F. Bret-Mounet, "All Your Solar Panels are Belong to Me," DEF CON 24, Las Vegas, Aug 4-7, 2016.

[91] (2016). *Horus Scenario: Exploiting a weak spot in the power grid* [Online]. Available: https://horusscenario.com/

[92] K. Leswing. (Oct. 21, 2016). *A massive cyberattack knocked out major websites across the internet* [Online]. Available: http://www.businessinsider.com/amazon-spotify-twitter-github-and-etsy-down-in-apparent-dns-attack-2016-10

[93] "Cyber Scoping Study Working Group," National Infrastructure Advisory Council (NIAC), Feb. 16, 2017.

[94] B. Seal, et al., "Final Report for CSI RD&D Solicitation #4 Standard Communication Interface and Certification Test Program for Smart Inverters," June 2016.

[95] J. Henry, R. Ramirez, F. Cleveland, A. Lee, B. Seal, T. Tansy, B. Fox, A. Pochiraju, "Cyber Security Requirements and Recommendations for CSI RD&D Solicitation #4 Distributed Energy Resource Communications," Oct. 2015.

[96] C. Carter, I. Onunkwo, P. Cordeiro, J. Johnson, "Cyber Security Assessments of Distributed Energy Resources," IEEE PVSC, Washington, DC, June 25-30, 2017.

specific protocols, and encryption. Lastly, we present a cyber security roadmap to work with the research and industry communities towards hardening end-to-end communications for DER.

6.1. DER Cyber Security Recommendations

General recommendations are listed below and subsequent sections detail the different categories of recommendations further. These include best practices and techniques, risk management, communication protocols, and encryption.

Assess Resources

- Time Constraints
    - Consider data rate and latency constraints for time sensitive exchanges.
    - Ensure that modifications to the information exchange mechanisms do not degrade the ability of the system to function.
- Criticality of Resources
    - Inspect criticality of resources and use limited resources wisely.
    - Based on criticality, protect components and communications accordingly.
- Updating Firmware Procedure
    - Define procedure for updating firmware and associated client software. Security considerations, such as integrity checks, must be included.
- Tampering of Firmware
    - Always check for tampering of firmware files using tools such as HMAC with MD5 or SHA hashes. Note that CRC error checking may also be used, but this is not cryptographically secure and should not be considered as such.
- Encryption
    - Use encryption where appropriate; can be performed using transport layer encryption with SSL/TLS or bump-in-the-wire, BITW.

Implement the AAA framework

- Authentication
    - Ensure that the users, devices, and applications attempting to access system resources are who they appear to be.
    - Require credentials to access the system and require them to be different for privileged access than they are for regular user access.
    - Enforce strong password policies and do not store or transfer passwords in plain text.
- Authorization
    - Ensure that the users, devices, and applications that are attempting to access system resources are authorized to access those resources.
    - Apply access control policies to system resources.
- Accounting
    - Monitor and log all host device and network traffic data.

AAA Specifics

- Keep Logs
    - Log all relevant information such as user logins, information requests, commands, measurements, etc.

    - Use analytics to filter specific requests and responses. Use this information to perform forensics and monitor system behavior.
- Monitoring
    - Monitor all traffic and resource usage on the relevant control network and log messages for future forensic study or for network analytics.
- Session Time-Out Policies
    - Enforce session time-out policies so that logins lock after a suitable period of no user activity.
- Practice Principal of Least Privilege
    - Every module (such as a process, a user, or a program, depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose.
    - If a user or resource no longer needs access to perform a legitimate task, disable their access.
- Disable Unused Ports
    - Disable all ports that are not being utilized for normal operation.

6.1.1. DER Cyber Security Techniques and Best Practices

Provided the general recommendations above, specific techniques and practices to enforce them are presented next. These particular mechanisms, devices, and methods reflect the important aspects of DER cyber security, including implementing the AAA framework.

Cryptography is a key component for ensuring confidentiality in DER systems. Several cryptography algorithms and practices were presented in Section 2, as well as their roles and impact on the CIA triad as well as AAA framework. A prominent cryptographic protocol that provides communication security is Transport Layer Security (TLS), which was derived from Secure Sockets Layer (SSL) and specifies asymmetric cryptography for authentication of key exchanges via a Public Key Infrastructure (PKI), symmetric encryption for confidentiality, and message authentication codes for message integrity.[97] As indicated by the name, TLS provides security for the transport layer. Although the most commonly implemented version is still TLS 1.0, the newest version TLS 1.2, defined in RFC 5246, should be specified for new implementations.[98] TLS includes many alternative cipher suites – these could or should be pared down to a few in specifications to ensure that implementations provide adequate security and interoperability; IEC 62351-3 provides such a specification.[99]

Internet Protocol Security (IPsec) authenticates and encrypts each IP packet as well as providing mutual authentication at the start of a session, thus providing security at the Network Layer rather than at the Transport Layer. IPsec is covered in RFCs 4101, RFC 4102, and RFC 4103 Base standards for IP Security.[100,101,102] Additional protocols include Hypertext Transfer Protocol

[97] *The Transport Layer Security (TLS) Protocol Version 1.1*, RFC 4346, 2006.

[98] *The Transport Layer Security (TLS) Protocol Version 1.2*, RFC 5246, 2008.

[99] *Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP*, IEC 62351-3 Ed 2, 2014.

[100] *Writing Protocol Models*, RFC 4101, 2005.

[101] *Registration of the text/red MIME Sub-Type*, RFC 4102, 2005.

[102] *RTP Payload for Text Conversation*, RFC 4103, 2005.

Security (HTTPS) is a combination of HTTP over TLS, and is formalized in RFC 2818.[103] Virtual Private Network (VPN) creates a "tunnel" through the Internet (or other network) in which the entire IP packet is encrypted and then encapsulated into another IP packet.[104] IPsec is often used to create the secure tunnel, although TLS and other security protocols can also be used. The Group Domain Of Interpretation (GDOI) method defined in RFC 6407 supports the distribution of a symmetric group key to all pre-configured or otherwise enrolled entities, typically devices.[105] Lastly, two other pertinent documents for cryptography standards are FIPS 186, Digital Signature Standard (DSS) and RFC 3447, Public-Key Cryptography Standards (PKCS) #1; RSA Cryptography Specifications, Version 2.1.[106,107] FIPS 186 describes a suite of digital signature algorithms for detecting unauthorized data modifications, and for authenticating a signer's identity. RFC 3447 describes the use of RSA for public key cryptography, including key generation and encryption.

To address authorization, Access Control Lists (ACL) and Network Address Translation (NAT) functions are integral. ACL are used in routers to limit which ports and/or IP addresses are permitted to be accessed by which entities.[108] NAT functions isolate systems from direct access by external systems.[109] They are often included in Wi-Fi network routers, in which a single Internet IP is provided to a site, and is shared by all networked devices at that site. The NAT handles all interactions with the Internet and passes only authorized messages to the systems behind the NAT router, thus providing security against unauthorized traffic.

Finally, for accountability, Intrusion Detection and Intrusion Prevention Systems (IDS and IPS) monitor networks for malicious or impermissible traffic.[110] The IDS can detect such malicious traffic and notify users, while an IPS can actually block malicious traffic and support prevention of additional traffic from a suspect IP address. As such, both IDS and IPS are essential for cyber security defense.

6.2. Recommendations for Grid Operators

Utilities, regional transmission organizations (RTOs), independent system operators (ISOs), and other grid operators may communicate to networked DER. In the past, these organizations are often under-staffed and under-funded to fully address the range of cyber threats that they face, but this is slowly changing. In part this change is due to new NERC CIP compliance requirements but it is also from growing awareness of cyber security concerns.

Grid operators must employ continuous improvement processes to defend against continuously evolving cyber security threats. Tools such as the Electricity Subsector Cybersecurity Capability

[103] *HTTP Over TLS*, RFC 2818, 2000.

[104] W. Strayer and R. Yuan. (2001). *Introduction to Virtual Private Networks* [Online]. Available: http://www.informit.com/articles/article.aspx?p=167809

[105] *The Group Domain of Interpretation*, RFC 6407, 2011.

[106] *Digital Signature Standard (DSS)*, FIPS PUB186-2, 2000.

[107] *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1*, RFC 3447, 2003.

[108] W. Stallings, "Access Control," in *Computer Security: Principles and Practice*, 2nd Ed., Upper Saddle River, NJ: Prentice Hall, 2008.

[109] CISCO. (2014). *Network Address Translation (NAT) FAQ* [Online]. Available: https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html

[110] T. Holland, "Understanding IPS and IDS: Using IPS and IDS together for Defense in Depth," GSEC Practical v1.4b, Option 1, SANS Institute InfoSec Reading Room, Feb. 23rd, 2004.

Maturity Model (ES-C2M2) and DHS US-CERT Cyber Security Evaluation Tool (CSET®) systematically evaluates the network security, identifies and ranks gaps based on threat information, and reports on the assessment to recommend high-priority improvements. [111,112] These tools provide methods for ranking the organization's security posture; e.g., ES-C2M2 uses maturity indicator levels in different domains:

1. Risk Management
2. Asset, Change, and Configuration Management
3. Identity and Access Management
4. Threat and Vulnerability Management
5. Situational Awareness
6. Information Sharing and Communications
7. Event and Incident Response, Continuity of Operations
8. Supply Chain and External Dependencies Management
9. Workforce Management
10. Cybersecurity Program Management

Once specific areas of improvement have been identified, more detailed, targeted improvements should be performed based on guidelines or best practices. These types of self-assessments are essential for DER communication network in order to identify and resolve cyber vulnerabilities. Additional recommendations for utility cyber security practices are also provided by the National Rural Electric Cooperative Association and NREL.[113,114]

6.2.1. Risk Management Suggestions

Managing risk is an important piece of any effective cyber security strategy and should be applied to all stakeholders involved in the DER communication network. Commonly, the process of mitigating attacks is considered to have nine different stages:

1. **Prevention:** Preventing a cyber incident may be achieved through either passive or active security measures. These are incorporated into the system using system design, architecture, and security elements that attempt to ensure a cyber attack never succeeds. Examples of prevention measures include firewalls, Intrusion Prevention Systems (IPS), security enclaves, and more.[115]
2. **Deterrence:** Risks can be mitigated by lowering the incentives for an adversary to attempt an attack and by making it more difficult for the adversary to achieve the objectives of an attack with the resources available. This often achieved through measures that "raise the bar" so that security posture is improved to the point where the resources required to breach the system outweigh the consequences of a successful attack.

[111] " Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), Version 1.1," U.S. Department of Energy and U.S. Department of Homeland Security, Feb. 2014.

[112] National Cybersecurity and Communications Integration Center. (2017). *Cyber Security Evaluation Tool* [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_CSET_S508C.pdf

[113] NRECA, "Guide to Developing a Cyber Security and Risk Mitigation Plan," NRECA / Cooperative Research Network Smart Grid Demonstration Project, 2011.

[114] M. Ingram, M. Martin, "Guide to Cybersecurity, Resilience, and Reliability for Small and Under-Resourced Utilities", NREL Technical Report NREL/TP-5D00-67669, Jan. 2017.

[115] C. K. Veitch, J. M. Henry, B. T. Richardson, D. H. Hart, "Microgrid Cyber Security Reference Architecture," Sandia National Laboratories Technical Report, SAND2013-5472, July 2013.

3. **Detection:** Once an attack occurs, it is crucial to be able to detect it relatively quickly and ensure that the appropriate notifications are sent.[116] This will then expedite efforts to minimize and mitigate damage, requiring either human intervention or automatic system response. Examples of detection include Intrusion Detection Systems (IDS) and network monitoring capabilities.[117]
4. **Assessment:** After a cyber incident, the ability to assess damage and what happened is crucial. This is where logging and forensic study come into play.
5. **Response:** After a threat is assessed, the appropriate action must be taken to respond. This will utilize information gathered from prior steps in detection and assessment to determine the appropriate action to take.
6. **Coping:** The system under attack may have additional measures to cope with system failures or compromise. These may include system switching capabilities, rerouting, and graceful shutdown or failure.
7. **Resilience** is commonly defined as a system's ability to operate under degraded conditions. In Presidential Policy Directive 21 (PPD 21), this was defined as the ability to prepare, adapt, withstand, and recover from disruptions.[118] A resilient system will be designed so that when it is compromised it will minimize disruption to essential operations and is able to recover rapidly.
8. **Recovery:** Once an incident has occurred, it is crucial to be able to restore operations quickly. This stage will include measures such as reflashing devices to a clean state from golden copies of firmware, validation that systems have been cleaned of malware and viruses, password changes, and excess inventory for replacing failed devices.
9. **Reaction:** Following a cyber incident, there will be a reaction to it. This may include auditing, possible legal repercussions if there was any failure to comply with regulations, and system redesign, assessment, and improvement to incorporate lessons learned and prevent further attacks from succeeding.

Notice many of these stages overlap and feed each other. For instance, a reaction to a cyber attack is also preparation against any further attacks that may be performed in the future. It is important to understand these phases in risk management and take appropriate measures to address concerns for each system individually. There is not a "one size fit all" strategy that works for all systems, as each case has different needs, constraints, and purpose. Thus, it is important to analyze each system for its own case and design security around its needs, risks, and consequences.

6.3. Recommendations for Aggregators

Aggregators already communicate to their DER equipment for maintenance, billing, and to push firmware updates—typically through encrypted, proprietary communication channels over the internet. In the near future, aggregators will likely relay grid operator commands to the end devices through their communication network. To do this, the aggregator will host a client for

[116] ICS-CERT. (2013). *Targeted Cyber Intrusion Detection and Mitigation Strategies (Update B)* [Online]. Available: https://ics-cert.us-cert.gov/tips/ICS-TIP-12-146-01B

[117] P. Innella and O. McMillan. (2001, Dec. 6). *An Introduction to IDS* [Online]. Available: https://www.symantec.com/connect/articles/introduction-ids

[118] "Presidential Policy Directive 21 Implementation: An Interagency Security Committee White Paper," Interagency Security Committee, Feb. 2015.

grid operator server; once a new command come in from the grid operator, the aggregator will be responsible to issue this command, new setpoint, or measurement request to the appropriate DER equipment. This puts the aggregator in a unique security position to protect not only their connection to the DER equipment, but also the connection to the grid operator. Therefore, the recommendations for the grid operator also apply to the aggregator. Additionally, the aggregator should consider:

- Verify proprietary protocols include confidentiality, integrity, and availability security tenets.
- Any cloud based services require good password hygiene and Role-Based Access Controls (RBAC).

6.4. Protocol-Specific DER Cyber Security Recommendations

The transmission protocols integrated in legacy DER systems and devices were not developed for securing grid systems and applications, but rather for reliability and ease of use. Common DER protocols such as Modbus, IEEE 2030.5, and IEEE 1815 have been updated for reliable and fast communications to utilities and aggregators for maintaining DER state and updates. Background on these protocols and others were provided in Sections 4 and 5, further details are available in Appendix A.

Essentially, DER devices are using modern network services to maintain fast and reliable communications but some DER protocols include advanced cyber security features, while others do not. For those that do not have these capabilities, additional security features must be layered on top of the data to secure the communication. In this section, the native security features of common DER communication protocols are presented along with recommendations for verifying those features. Table 4 summarizes the cyber security features of the different standards and information models and are detailed subsequently. It should be noted that the overall impact to the security and reliability of a system needs to be considered in selecting a protocol. A protocol that does not have security features can be wrapped in a more secure protocol, or it can be addressed at higher and lower layers in the OSI stack.

Table 4: Cyber security features of DER communication standards, information models, and security standards.

DER Protocol Cyber Security Features	Protocol: IEC 61850 Information Model: IEC 61850-90-7 Security Requirements: IEC 62351 Series	Protocol: IEEE 2030.5 Information Model: CSIP Security Requirements: IEEE 2030.5 + CSIP	Protocol: IEEE 1815 Information Model: DNP3 Application Note Security Requirements: IEEE 1815	Protocol: Modbus Information Model: SunSpec or MESA Models Security Requirements: None
Devices Support	DER, Power Systems Devices	DER, Smart Grid devices	Utility, Grid Devices	Utility, Grid, ICS devices
Encryption Capability	Non-Native	Yes	BITW	BITW
Encryption Required	No	Yes	No	No
Supported Transport Protocols	N/A	TCP or UDP	Serial or TCP	Serial or TCP
Supported Networks	N/A	IPv4, IPv6	IPv4	IPv4, IPv6
Authentication Support	Non-Native	Yes	Optional	Non-Native
Type of Communication Protocol	IEC 61850-90-7 contains functions for power converter-based DER systems	Communication protocol for device integration with the Smart Grid	Communication protocol for real-time monitoring and control	Communication protocol for real-time monitoring and control
Type of Information Model	IEC 61850-90-7	CSIP	DNP3 Application Note	SunSpec and MESA are information models for Modbus
Type of Security Requirements	IEC 62351 Series	IEEE 2030.5 + CSIP	IEEE 1815	There are no security requirements for Modbus communications
Type of Data Transmitted	DER settings, control modes, and measurements	DER measurement and control data	Data objects with defined attributes and priority levels	DER measurement and control data
Aggregation Support	Utility or aggregators can collect data	Yes	Yes	Yes

6.4.1. Modbus Recommendations

The Modbus protocol was not built with any consideration to cyber security.[119] The protocol does not have support for securing Modbus messages in the event of a possible cyber attack. In fact, the lack of security with Modbus led to the mantra, "if you can ping a Modbus device, you own it."[42] It is assumed that the vast majority of legacy DER devices utilize this protocol for communications and state updates. In a legacy system, confidentiality for Modbus devices can be provided with bump-in-the-wire (BITW) encryption technologies that use an exterior device to encrypt and decrypt Modbus network traffic. For transitional devices using Modbus, it is recommended that Modbus messages be sent over TCP/IP, allowing the communications to be encrypted using TLS and the packets to be authenticated at the network layer using IPsec. In addition, the use of a network traffic monitor can notify personnel of a possible cyber security incident involving unwarranted or anomalous Modbus messages. This monitor should alert personnel whenever normal Modbus traffic is modified, stopped, or transfers abnormal signals.

6.4.2. IEEE 2030.5 Recommendations

IEEE 2030.5 (SEP2) specifies the use of Transport Layer Security (TLS) 1.2 to secure communications between devices, digital certificates for authentication, and native IPv6 addressing, as discussed in previous sections.[120] The TLS protocol provides communication security over networks, but care must be taken to ensure that holes are not introduced though improper certificate authentication or unencrypted interfaces with older protocols. IEEE 2030.5 also encourages additional security features for "non-native SEP2" devices. If a device possesses adequate hardware resources and has a need for greater security, additional security mechanisms may be implemented.[106]

The California IOUs are adopting this protocol for securing DER communications. Monitoring of IEEE 2030.5 traffic should be implemented to make sure critical information is secured. This can be achieved by installing a network packet analyzer on the same network as the DER. Critical information such as personal data, device identification, and passwords, or any other information that can aid an adversary in a possible cyber attack should be encrypted and not transferred in plain text.

6.4.3. IEEE 1815 Recommendations

IEEE 1815 (DNP3) can utilize TLS to secure DER communications, but TLS support is not required.[121] Current cyber security support for DNP3 includes end-to-end application layer encryption and protocol support for IP, serial, and RF. Additionally, DNP3 has support for addressing the threat of unauthorized spoofing and it meets IEC 62351 security standard including Role-Based Access Control (RBAC). Devices that use DNP3 communications should be verified for the implementation of any mandatory security features, and include TLS whenever the device hardware and network infrastructure is available to support it. Finally,

[119] O. Hersent, D. Boswarthick and O. Elloumi, "ModBus," in *The Internet of Things: Key Applications and Protocols*, Ed. 1, Wiley Telecom, 2012.

[120] *IEEE Adoption of Smart Energy Profile 2.0 Application Protocol Standard*, IEEE Std. 2030.5, 2013.

[121] *IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)*, IEEE Std.1815-2012 (Revision of IEEE Std. 1815-2010), 2012.

monitoring grid communications benefits grid personnel by alerting if abnormal traffic is transferred. If abnormal traffic is transferred, mitigations should be performed to ensure grid status remains operational. Investigation of IEEE 1815 Secure Authentication[122] for DER communications should be considered.

6.4.4. IEC 61850 Recommendations

IEC has standardized many advanced grid-support functions in IEC 61850-90-7 and IEC Technical Committee 57 is currently updating IEC 61850-7-420 to include these functions.[123] This standard does not include security features, but instead describes the information model use to communicate to DER devices. The security features for DER communications are described in the IEC 62351 series of standards. IEC 61850 can be mapped to other protocols, such as Manufacturing Message Specification (MMS), Generic Object Oriented Substation Event (GOOSE), or flattened to provide data points for SunSpec Models, the DNP3 Application Note, etc. Depending on the application, different IEC 62351 series standards should be referenced. Those most pertinent to securing IEC 61850 traffic, includes:[124]

- IEC 62351-3 — Security for profiles that include TCP/IP
- IEC 62351-4 — Security for MMS protocols
- IEC 62351-6 — Security for peer-to-peer profiles (e.g., GOOSE)
- IEC 62351-7 — Security for network and system management
- IEC 62351-8 — Role-Based Access Control
- IEC 62351-9 — Key Management
- IEC 62351-10 — Security Architecture
- IEC 62351-11 — Security for XML Files

6.5. DER Cryptography Requirements and Recommendations

DER, like other Internet of Things (IoT) devices, use embedded hardware to achieve automated home and process control, supervisory control and data acquisition, and communications to varying degrees. DER systems provide interfaces for customers, vendors, integrators, and others. While existing cryptographic services for these connections have been largely ad-hoc, interoperability requires coordination of, among other considerations, encryption and key distribution mechanisms. The following describes in further detail challenges and recommendations for DER cryptographic protection.

6.5.1. Motivation

A DER's power electronics, controlled by a microcontroller in an embedded system interface, exchanges data and messages regarding system conditions and actions with various entities. Status and control of any DER device may be of interest to several parties, including the local user or smart devices, the equipment manufacturers/owners, aggregators, system operators, and utilities.[125,126] Others such as marketers attempting to target sales may also try to mine data

[122] G. Gilchrist, "Secure authentication for DNP3," 2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, PA, 2008, pp. 1-3.

[123] *IEC/IEEE International Standard - Communication networks and systems for power utility automation*, IEC/IEEE 61850, 2016.

[124] *IEC 62351 Security Standards for the Power System Information Infrastructure*, IEC TC57 WG15, June 2012.

[125] H. Saboori, M. Mohammadi, and R. Taghe, "Virtual Power Plant (VPP), Definition, Concept, Components and

from online devices. Malicious actors may attempt to gain entry to users' networks, or manipulate electric power production. As overall DER interoperability of command and control increases, so will its attack surface increase. Prior cyber security assessments have shown that a malicious hacker could shut down a large amount of solar generation, or could take over networked DER devices to enact malicious attacks on critical energy and information infrastructure.[127] Interoperability therefore requires commensurate protection to prevent embedded system status from being misappropriated and to prevent controls from being misused.

6.5.2. Cryptography Challenges

DER embedded systems have not always had available cryptographic mechanisms. Though increasingly available, the complexity and lack of resources needed for deployment are among the continuing challenges to establishing cryptographic security. The complexity of implementing cryptographic systems can lead to unseen vulnerabilities, and a lack of the needed resources such as infrastructure and coordination, can lead to incomplete defenses.

Security expert Bruce Schneier has noted, "[b]uilding a secure cryptographic system is easy to do badly, and very difficult to do well."[128] In fact, the implementation of cryptographic algorithms and secure interfaces from one level to the next require myriad non-trivial decisions. Implementation errors inevitably follow from this complexity.

Designers providing customized DER device communication solutions face the challenge of selecting an appropriate platform out of a vast array of hardware and programming options, and often stick with what they know.[129] Adding a cryptographic implementation to a previously successful design, however, may not guarantee a successful cryptographic design. Securing an embedded system, or any other system, typically increases its complexity and must be carefully designed. Implementing cryptography without taking other factors into consideration is also not sufficient. For example, a designer might carefully protect the intended communication interface and inadvertently leave others unsecured.

Resource challenges can also result in design tradeoffs that compromise the strength of cryptographic protections. For example, designers might choose to implement a lightweight cryptography scheme meant to save on processor power, system storage, or reduce wait times and inadvertently introduce weak passwords or keys, unsecured key generation or storage, or unprotected transitions between piecewise communication segments. Users themselves may disable cryptographic protections they find onerous to use. That is, despite the benefits, when security is offered in a commercial product, users may not adopt a secure posture if performance degrades.

Types," 2011 Asia-Pacific Power and Energy Engineering Conference, Wuhan, 2011, pp. 1-4.

[126] "Assessment of Demand Response and Advanced Metering," Staff Report, Federal Energy Regulatory Commission, Dec. 2016.

[127] F. Bret-Mounet, "All Your Solar Panels are Belong to Me," DEF CON 24, Las Vegas, Aug 4-7, 2016.

[128] B. Schneier, "Security Pitfalls in Cryptography," Information Management & Computer Security, 1998.

[129] C. Walls. (2016). *CPU selection in embedded systems* [Online]. Available: https://www.embedded.com/design/mcus-processors-and-socs/4442264/CPU-selection-in-embedded-systems

Infrastructure needed for cryptographic solutions includes not only the hardware and software running the algorithms, but also the coordination of an agreed upon authority (whether centralized or decentralized), the adopted standards, and a means of secure key exchange. Without an agreed-upon key infrastructure, for example, entities might be allowed to issue self-signed certificates, which carry no protection against identity spoofing. Creation and adoption of DER standards and the authorities or other structures required for key exchange have lagged behind the implementation and deployment of devices into the field, leaving system owners to manage in a fragmented fashion.

A review of the current state indicates that the evolving scenario has become a patchwork system of defenses, instead of the desired defense-in-depth, in which several layers of security would be deployed in every element of an interconnected system.

6.5.3. Cryptography Recommendations

Cryptographic functions offer a means of protecting ownership, access, and privacy in the digital realm. With rapid expansion in DER installation and interoperability, the best protected path forward is still being defined with new standards, authorities, and protocols. New DER standards requiring cryptographic protections are now being adopted, e.g., IEEE 2030.5. In a landscape with millions of operational DER where many are legacy installations with no room for cryptographic operations, the recommended intermediate solution for complying with such standards will be bolt-on devices enabling the secure communications specified in the new standards. In this way, owners will have the option to cryptographically secure legacy installations without replacing the existing hardware.

In the longer term with cryptographic protections included in requirements, system developers, designers and users will need to plan and train in the 'defense in depth' outlook, accounting for cryptographic infrastructure in their business models, much in the way that the secure console industry for television and video games have successfully done.[130]

Designers will be able to consider the necessary hardware and software resources during (instead of after) the design process, making use of tested crypto libraries, board packages, and reference designs, provided in typical embedded system Integrated Development Environments (IDE) to improve outcomes. Where reference designs do not exist for algorithms and protocols in new DER standards, designers should request that IDEs begin to include such reference designs in their libraries. Software implementations of cryptographic algorithms, once losing ground to hardware accelerators with better resistance to cryptanalysis, are once again gaining ground due to their ability to change designs by updating only their firmware. Such agile design prevents obsolescence when cryptographic algorithms embedded in a system are broken by cryptanalysts and hackers.

Coordination of agreed-upon standards and authorities will enable a stronger stance against issues such as counterfeit certificates. It must, however, also plan to include a response path for

[130] A. Huang. *Hacking the Xbox: An Introduction to Reverse Engineering. San Francisco*. CA: No Starch Press, 2003.

the eventuality of superseded crypto algorithms and key distribution protocols, as cryptographic security is constantly re-defined.

6.6. Cyber Security Roadmap

In December 2017, Sandia National Laboratories completed a roadmap for distributed solar that also has applicability to other DER equipment and communication networks.[131] This roadmap describes the process for improving cyber security for PV systems over the next 5 years, as shown in Figure 9. At the top of the figure, PV system cyber security is nested into the larger context of the cyber security landscape, whereby best practices from a range of communities are being directed into two primary thrusts: stakeholder engagement and cyber security research and development (R&D). Within the stakeholder engagement thrust, public-private partnerships establish workshops, working groups, educational opportunities, and reach out to other cyber security working groups. Within the R&D thrust, cyber security and solar researchers design and evaluate new technologies for securing photovoltaic systems. Both the stakeholder engagement and R&D efforts feed into the creation of cyber security requirements for PV systems. With the adoption of these standards, industry will integrate new cyber security features into PV communication networks and commercialize concepts from the R&D thrust.

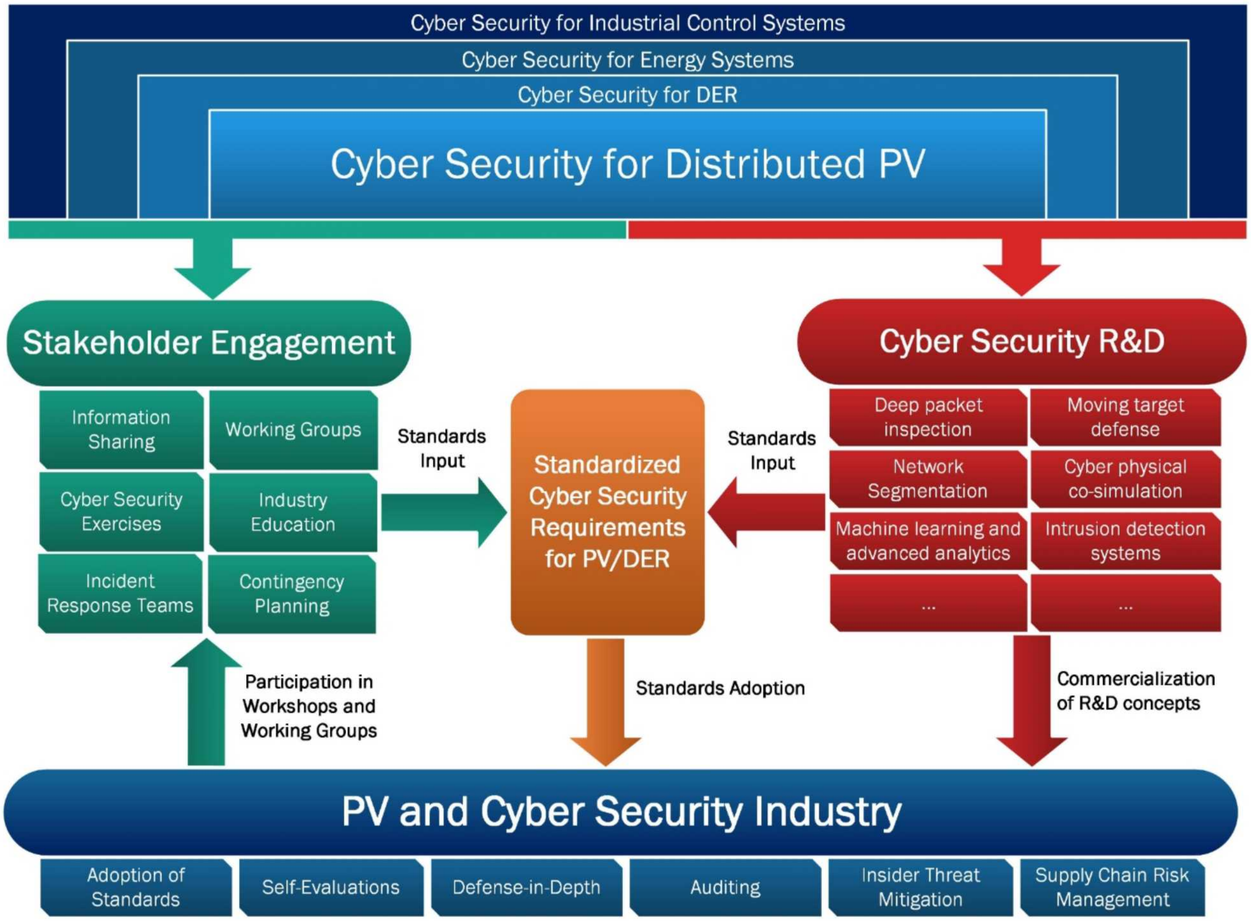
Cyber Security for Industrial Control Systems
Cyber Security for Energy Systems
Cyber Security for DER
Cyber Security for Distributed PV
Stakeholder Engagement
Information Sharing
Working Groups
Cyber Security Exercises
Industry Education
Incident Response Teams
Contingency Planning
Standards Input
Standardized Cyber Security Requirements for PV/DER
Standards Input
Cyber Security R&D
Deep packet inspection
Moving target defense
Network Segmentation
Cyber physical co-simulation
Machine learning and advanced analytics
Intrusion detection systems
...
...
Participation in Workshops and Working Groups
Standards Adoption
Commercialization of R&D concepts
PV and Cyber Security Industry
Adoption of Standards
Self-Evaluations
Defense-in-Depth
Auditing
Insider Threat Mitigation
Supply Chain Risk Management

Figure 9: Process for achieving cyber security of PV systems.

[131] J. Johnson, Roadmap for Photovoltaic Cyber Security, Sandia National Laboratories Technical Report, 2017.

6.7. Industry Collaborations

In 2017, Sandia National Laboratories and the SunSpec Alliance initiated a DER Cyber Security Working Group to discuss DER cyber security requirements that can be used as a basis for national or international codes and standards.[132] This working group is primarily establishing a set of best practices for DER cyber security in the following topic areas:

1. Communication and Protocol Security
2. Secure Network Architectures
3. Access Controls
4. DER/Server Data and Communication Security

It is anticipated that these working groups will establish recommendations by the end of 2018.

[132] SunSpec Alliance. (2017). *SunSpec DER Cybersecurity Workgroup* [Online]. Available: https://sunspec.org/sunspec-cybersecurity-workgroup/

APPENDIX A: DER COMMUNICATION PROTOCOLS, INFORMATION MODELS, AND SECURITY STANDARDS

1. ASHRAE 201

ASHRAE 201-2016 is the Facility Smart Grid Information Model, wherein a "Facility" is defined as a system, typically a building.[133] This model defines an abstracted, object oriented information model that categorizes devices within a system. These categories are structured by UML with four main classes: Generator, Load, Meter, or Energy Manager.

ASHRAE 201 does mention security concerns in multiple places throughout its standard, such as at gateway devices, but does not define requirements or specifications for cyber security. Because of this other standards that may be used together with ASHRAE 201 will be needed, such as TLS, BITW, RBAC, and more. See IEC 62351 and IEEE 1547.3 for more background information on viable concerns and mitigation strategies.[134,135]

2. ASHRAE 135

ASHRAE 135 (BACnet-W5) is an effort to integrate consumer devices into the smart buildings management systems which currently encompasses elevator and lighting controllers.[136,137] This standard is designed specifically to meet the communication needs of building automation and control systems for applications such as heating, ventilating, and air-conditioning control; fire and other life safety and security systems; energy management; lighting control; physical access control; and elevator monitoring systems. BACnet-W5 can be used for mobile and cloud-hosted devices, head-end computers, general-purpose direct digital controllers, and application-specific or unitary controllers.

The purpose of Standard 135 is to define data communication services and protocols for computer equipment used for monitoring and control of HVAC&R and other building systems, and to define, for application interoperability, an abstract, object-oriented representation of information communicated between such equipment, thereby enabling the application and use of digital control technology in buildings.

This protocol provides a comprehensive set of messages for conveying encoded building automation data between devices including, but not limited to:

- hardware binary input and output values
- hardware analog input and output values
- software data values
- schedule information

[133] *Advisory Public Review Draft: Facility Smart Grid Information Model*, BSR/ASHRAE/NEMA Standard 201P, 2012.

[134] *Power systems management and associated information exchange - Data and communications security - ALL PARTS*, IEC 62351:2017 SER Series, 2017.

[135] *IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems*, IEEE Std. 1547, 2003.

[136] *BACnet-A Data Communication Protocol for Building Automation and Control Networks*, ASHRAE 135-2016, 2016.

[137] S. Bushby. (1997). *BACnetTM - A standard communication infrastructure for intelligent buildings* [Online]. Available: http://www.bacnet.org/Bibliography/AIC-97/AIC1997.htm

- alarm and event information
- trend and event logs
- files
- control logic
- application specific data for a large range of building services
- network configuration, including security

Although the BACnet protocol does incorporate some level of security, NIST, DoD, and DoE have published their knowledge of known threats and countermeasures.[138] Because BACnet devices broadcast not just their network information but also their physical location and other physical data, it is relatively easy for an adversary or cyber criminal to plant malware on BACnet enabled systems. To a large degree, the measures that can be taken to increase network and physical security are available as commercial solutions.

3. IEEE 1815 (DNP3)

The Distributed Network Protocol (DNP3), which is defined in IEEE Std. 1815, is another protocol in common use today.[139,140,141,142] It is based on the IEC 60870 standard, which was originally released in 1993.[143] DNP3 is an object-oriented protocol in which each object contains very specific attributes. While this represents a more complicated data structure than a protocol such as Modbus utilizes, it allows data to be transmitted via a standard data structure and adds the capability to define different priority levels for different variables, so that high priority messages are given precedence over lower priority messages. This aids traffic scheduling algorithms in ensuring that the most important messages reach their destination in a timely manner. DNP3 messages are also timestamped and are designed to be highly interoperable among devices of different manufacturers. For these reasons, DNP3 is extremely prevalent among power systems communications between utilities and substations.

Like Modbus, DNP3 was not originally designed with any built-in security features and still lacks any form of encryption capability. However, an updated version was released in 2007 that added secure authentication mechanisms using a challenge-response exchange between devices. That is, if Device A makes an access or data request to Device B, Device B will issue a challenge. It is then the responsibility of Device A to prove its identity (authentication) and sufficient privilege level (access control). Since these new authentication features are not mandatory, they are not necessarily implemented in the field.

[138] D. Holmberg, "BACnet Wide Area Network Security Threat Assessment," NISTIR 7009, National Institute of Standards and Technology, July 2003.

[139] *IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)*, IEEE Std.1815-2012 (Revision of IEEE Std. 1815-2010), 2012.

[140] DNP Users Group. (2005). *A DNP3 Protocol Primer* [Online]. Available: https://www.dnp.org/AboutUs/DNP3%20Primer%20Rev%20A.pdf

[141] "Modbus and DNP3 Communication Protocols," Triangle MicroWorks, Inc., Raleigh, NC.

[142] "Why IEEE 1815 (DNP3) Secure Authentication?," Distributed Networks Protocol, 2016.

[143] *Telecontrol equipment and systems. Part 5: Transmission protocols - Section One: Transmission frame formats*, IEC 60970-5-1:1990, 1990.

While DNP3 lacks encryption, when transmitted over TCP/IP it should utilize TLS to achieve confidentiality. Moreover, the secure authentication features now built in to DNP3 should always be implemented if possible. IEC 62351, specifically IEC 62351-4, should be referenced for a more complete set of security standards that should be required for DNP3 communications.

4. IEC 61850

IEC 61850-7-420 is an information model for communication and control of DER devices that covers the types of data that must be exchanged and the logical connections required[144]. A second version is nearing release which will update the standard to include the object models currently associated with IEC 61850-90-7.[145,146,147] The model defines the general logical connections required for DER, with a hierarchical structure containing standard data types, common attributes, common data classes, data objects, logical nodes, and logical devices. This standard has no cyber security requirements to date.

The namespace "IEC 61850-90-7" is considered to be "transitional" since the models are expected to be rolled into IEC 61850-7-420. Potential extensions and modifications to the standard may occur when the models are moved to International Standard status. IEC 61850-90-7 defines information object models for any controllable power converter-based DER systems, including rectifiers, inverters, DC-to-DC, and AC-to-AC converters. These can include photovoltaic systems, battery storage systems, and electric vehicle charging systems, as well as other transmission and distribution systems. The object models also define power converter functions to control various factors including generation level, power factor, watts/vars/volt-amps, power ramp rate, frequency, voltage phase, and charging settings. As described in 61850-7-420, these are sent to DERs as control signals to manage their power generation capabilities. Since this is a high-level information model, no security requirements or specifications are discussed.

5. IEC 62351

IEC 62351 is a cyber security standard for power systems[148] that has been developed to help cover the gaps in other communication protocols and standards, with direct ties to several IEC standards, including IEC 60870 (related to DNP3), IEC 61850, IEC 61970, and IEC 61968.[149] The IEC 62351 standard provides direction on the end-to-end security requirements of power systems, including security for TCP/IP communications, Manufacturing Message Specification

[144] *IEC/IEEE International Standard - Communication networks and systems for power utility automation*, IEC/IEEE 61850, 2016.

[145] *Communication networks and systems for power utility automation - Part 90-7: Object models for power converters in distributed energy resources (DER) systems*, IEC 61850-90-7:2013, 2013.

[146] International Electrotechnical Commission (IEC) Technical Committee 57 Working Group 17, "Distributed Energy Management (DER): Advanced Power System Management Functions and Information Exchanges for Inverter-based DER Devices, Modelled in IEC 61850-90-7, Version 27," June 2012.

[147] J. Johnson, S. Gonzalez, M. Ralph, A. Ellis, and R. Broderick, "Test Protocols for Advanced Inverter Interoperability Functions – Appendices," SAND2013-9875, Sandia Report, Sandia National Laboratories, Nov. 2013.

[148] *Power systems management and associated information exchange - Data and communications security - ALL PARTS*, IEC 62351:2017 SER Series, 2017.

[149] F. Cleveland, "IEC TC57 WG15: IEC 62351 Security Standards for the Power System Information Infrastructure," International Electrotechnical Commission, June 2012.

(MMS) communications, network and system management (NSM), role-based access control (RBAC), key management, network architecture, and extensible markup language (XML), as well as other IEC standards. Note that this standard rides on top of the communication protocols and standards in use in a power system, and does not replace them. The use cases included in the standard should be inspected to determine applicability.

6. IEEE 1547.3

The IEEE 1547 series of standards defines the interconnection of DER systems to the grid, with the criterion for applicability being any generation with aggregate capacity of 10 MVA or less at the point of common coupling (PCC).[150] IEEE 1547.3-2007 is the Guide for Monitoring Information Exchange and Control of Distributed Resources with Electric Power Systems (EPS), and is the only standard in this series that discusses cyber security requirements. [151] 1547.3 declares the information models required, discusses security challenges, and offers guidelines for DER connected to EPS. The documentation includes dialogue on critical issues in information security, physical security, reliability, personnel security, as well as the triad of confidentiality, integrity, availability, and accountability and recommended security measures. As noted in the standard, these lists are not exhaustive, and other security standards, such as IEC 62351, are referenced as suggested background.[164]

7. IEEE 2030.2

IEEE 2030.2 is the IEEE guide for the interoperability of energy storage systems with electric power infrastructure.[152] It provides a framework for identifying and organizing key information when connecting energy storage systems to the electric power system. As such, it provides direction on commands for frequency regulation, volt/var, renewable integration, substations, DER services, and microgrids when connecting DER to the power grid. This includes the roles of DER management systems (DDEMS, DERMS), as well as Facility DER Management Systems (FDEMS), and how these entities coordinate aggregation of DER resources. Interoperability is a key feature throughout this standard and is discussed at length.

IEEE 2030.2 provides guidance on cyber security issues relevant to smart grid connectivity, but does not define specifications or requirements. It is recommended that the suggestions included are implemented as best practices, along with direction taken from other standards such as IEC 62351.

8. IEEE 2030.5 (SEP 2.0)

Smart Energy Profile (SEP) 2.0, based on Zigbee Smart Energy 1.X, outlines standards for integrating consumer devices and Home Area Networks (HANs) into the smart grid.[153,154] HANs provide customers with performance and management functions such as energy usage

[150] *IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems*, IEEE Std. 1547, 2003.

[151] *Guide for Monitoring Information Exchange and Control of Distributed Resources with Electric Power Systems*, IEEE Std. 1547-2007, 2007.

[152] *IEEE Guide for the Interoperability of Energy Storage Systems Integrated with the Electric Power Infrastructure*, IEEE 2030.2-2015, 2015.

[153] *IEEE Adoption of Smart Energy Profile 2.0 Application Protocol Standard*, IEEE Std. 2030.5, 2013.

[154] R. Simpson. (2015). *IEEE 2030.5™-2013 - (Smart Energy Profile 2.0) - An Overview for KSGA* [Online]. Available: http://robbysimpson.com/prezzos/IEEE_2030_5_Seoul_Simpson_20150424.pdf

information, pricing and billing, demand response and load control, device discovery, and service provider alerts. While Smart Energy 1.X is limited to IEEE 802.15.4 Zigbee Pro 2.4 GHz communications, SEP 2.0 additionally provides multiple link layer support for IEEE 802.11 Wi-Fi, 802.15 Bluetooth, 802.3 Ethernet, and 1901 broadband over power lines (BPL). Although most residential smart meters are currently capable of Zigbee communications, most do not natively support SEP 2.0.

SEP 2.0 operates over both User Datagram Protocol (UDP) and TCP/IP, with support for both IPv4 and IPv6, though it can also operate over a serial link using a hardware translator. Client-server communications are conducted over HTTPS with TLS v1.2. Payloads are encoded in XML, with Efficient XML Interchange (EXI) for compression. Encryption is required for all HTTP communications using the TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 cipher and secp256r1 elliptic curve. In addition to encryption, the SEP 2.0 specification addresses many of the AAA (authentication authorization, and accounting) requirements missing from earlier protocols.

The California Investor-Owned Utilities have adopted Common Smart Inverter Profile (CSIP)[155] as the IEEE 2030.5 information model. CSIP compliant equipment must have a X.509 v3 device certificate installed that chains back to the Root Certificate Authority (Root-CA). Clients and servers perform mutual authentication during the TLS handshake through verification with the Root-CA. The certificate fingerprint is the result of performing a SHA256 operation over the whole DER-encoded certificate and consists of 256-bits (32 octets). Truncated versions of the certificate fingerprint, called the LFDI and SFDI, are used for device identification. The LFDI is the certificate fingerprint left-truncated to 160-bits (20 octets). The LFDI has sufficient entropy (2160) to be considered globally unique. The LFDI is used when a globally unique identity is required. The SFDI is the certificate fingerprint left-truncated to 36-bits. For display purposes, the SFDI is expressed as 11 decimal (base 10) digits, with an additional right-concatenated sum-of-digits checksum digit. The SFDI has sufficient entropy (236 bits) to uniquely identify the device in the context of its usage, and is used to identify a device within a HAN or site domain. It should not be used in a truly global context. The SunSpec Alliance is responsible for the CA Rule 21 Phase 2 (communications) Certification Program for DER equipment. This program will establish the certificate authority, communications probing routine, and test scripts to certify the equipment.[156]

Each server maintains a list of clients that are authorized to communicate. The LFDI should be used for this purpose, since the SFDI may be susceptible to collisions as the number of entries in the device list grows. After receiving the client device certificate during the TLS handshake, the server should calculate its LFDI and verify that the LDFI is in the authorized list. If the LFDI is not in the list, the Server should return an HTTP error code (e.g. 404 Not Found) to terminate the transaction.

Once a client device has been authenticated and authorized, it potentially has access to resources on the server. The server controls access to resources based on access control lists (ACLs). If a

[155] "IEEE 2030.5 Common California IOU Rule 21 Implementation Guide for Smart Inverters, Version 1.0," California Smart Inverter Implementation Working Group, Aug. 31, 2016.
[156] T. Tansy, "SunSpec Alliance CA Rule 21 Phase 2 Certification Program," Nov. 2016.

device is in the ACL for the resource, it is authorized and has access to that resource. Otherwise, it does not. In theory, every resource on the server can have its own ACL. Clients and servers establish the permissions for read, write, control, and other interactions based upon agreements that determine which interactions are authorized between each client and each server. For example, RBAC may be used to establish these permissions for different roles. Another aspect of access control is that the server may present different resource information based on the identity of the client making the request. This is done for both efficiency and/or privacy reasons. The Server should return an HTTP error code if a device tries to access a resource it is not permitted to access.

For example, if an Inverter A tries to access the End Device information associated with Inverter B, the Server should return an HTTP error code. On the other hand, if the Aggregator tries to access the End Device information associated with Inverter A or Inverter B, it should be allowed to do so. In the Aggregator model, when an Aggregator accesses the End Device list, the Server should only present End Devices (i.e. inverters) that are under the control of that Aggregator. This means the Server will present each Aggregator with a different End Device list. This is done for both efficiency (Aggregators know that all inverters in the list are under its control) and privacy (Aggregators will not see any information related to inverters not under its control).

9. LONTALK STACK

The LonTalk Stack was developed by Echelon Corporation and enables optimized performance for the ISO/IEC 14908, the Open Data Communication in Building Automation, Controls and Building Management – Control Network Protocol.[157,158] With the LonTalk Stack, the control networking interface from ISO/IEC 14908 can be added to any product with a microprocessor, microcontroller, or embedded processor. The protocol itself is called LonTalk while the network platform is called LonWorks, and it is frequently employed in the smart grid.

LonTalk has four parts: the Protocol Stack, Twisted Pair Communication, Power Line Channel Communication, and IP Communication (IPv4 and IPv6). As the protocol provides supervisory control, monitoring, and configuration support, it may be utilized for distribution and aggregation of smart grid resources. It also provides support for remote access and application management services. To send information, LonTalk defines a "Network Variable" which is a data object that a device will expect to receive, such as measurement or control information.

LonTalk is often applied with the Open Smart Grid Protocol (OSGP), which provides session layer authentication. However, OSGP has known security flaws in its implementation of authentication, so additional security measures are recommended when using LonTalk and OSGP. See other standards such as IEC 62351 and IEEE 1547.3 for further recommendations.[159, 165]

[157] *Information technology -- Control network protocol -- Part 1: Protocol stack*, ISO/IEC 14908-1:2012 , 2012.

[158] "LonTalk® Stack Developer's Guide," Echelon Corporation, 2012.

[159] *Power systems management and associated information exchange - Data and communications security - ALL PARTS*, IEC 62351:2017 SER Series, 2017.

10. MODBUS

Modbus is a control protocol that was originally developed by Modicon (now Schneider Electric) in 1979.[160,161],[162] Due to its long life and simple construction it is very widely employed across a broad range of ICS systems, including the digital infrastructure for controlling power systems and DER. Measurement and control are performed through what are called Modbus registers, which are merely functional addresses on a device that are tied to a certain input or output. While it was originally a serial protocol, Modbus has been extended in recent years to work over TCP/IP.

As Modbus was developed before the modern networking protocols and equipment, it was designed to be simple, fast, and efficient, and does not include any security measures in its construction. It is trivial to tap into a Modbus network and modify components at will, as devices automatically assume that any commands they receive are coming from their master controller. Unless Modbus communications are wrapped in a secure protocol such as TCP/IP with TLS, encryption and authentication should be added in order to create a more secure environment.

8. SUNSPEC ALLIANCE MODELS

SunSpec Alliance Interoperability Specifications describe information models, data exchange formats and communication protocols used with DER systems.[163,164] The SunSpec models are based on IEC 61850-90-7 information models and include nameplate information, monitoring data, and advanced grid support functions.[165] These models are used by a number of PV inverter manufacturers.

The Modbus protocol, which is employed by SunSpec DER devices, is often cited as a "weak link" in the security chain because of its lack of security.[166] The SunSpec Alliance describes a simple bump-in-the-wire attack in their "Best Practice Guide for Security Recommendations" report.[167] This report also discusses availability, confidentiality, integrity, and accountability for SunSpec Modbus systems. End-to-end data integrity and non-repudiation is achieved in the SunSpec architecture through the application of digital signatures at the source of the data generation and carried all the way through to the end consuming application. The SunSpec security models accommodate a variable-length digital signature and algorithm for flexibility. The signature must be a minimum of 4 registers (64 bits) and an integral of 16 bit registers.

[160] O. Hersent, D. Boswarthick and O. Elloumi, "ModBus," in *The Internet of Things: Key Applications and Protocols*, Ed. 1, Wiley Telecom, 2012.

[161] "Modbus and DNP3 Communication Protocols," Triangle MicroWorks, Inc., Raleigh, NC.

[162] "Modicon Modbus Protocol Reference Guide," PI–MBUS–300 Rev. J, Modicon, June 1996.

[163] "SunSpec® Modbus® Interface for SUNNY BOY / SUNNY TRIPOWER," SMA Solar Technology AG, 2014.

[164] "SunSpec Energy Storage Models: SunSpec Alliance Interoperability Specifications, Document #: 12032 , Status: Draft, Version 4," SunSpec Alliance, 2016.

[165] International Electrotechnical Commission (IEC) Technical Committee 57 Working Group 17 , "Distributed Energy Management (DER): Advanced Power System Management Functions and Information Exchanges for Inverter-based DER Devices, Modelled in IEC 61850-90-7, Version 27," June 2012.

[166] "Guidelines for SmartGrid Cyber Security, NIST Interagency Report 7628," National Institute of Standards and Technology, Aug. 2010.

[167] J. Blair, J. Nunneley, R. Kaisler, B. Fox, F. Nagy, B. Randle, L. Linse, T. Tansy, "Security Recommendations: SunSpec Alliance Best Practice Guide," Version 1.1., approved 6-19-2013.

9. MESA STANDARDS FOR ESS

The Modular Energy Storage Architecture (MESA) Standards are designed for Energy Storage Systems (ESS) and composed of 4 different components: one utility-facing standard called MESA-ESS that is based on DNP3, and 3 other Modbus information models that represent the ESS components of storage, Power Conditioning System (PCS), and meter—collectively called a MESA-Device.[168] MESA is a set of open specifications and standards developed by an industry consortium of electric utilities and technology suppliers. The MESA-ESS specification addresses monitoring, orchestration, and control system communications between utilities and energy storage systems. The MESA-Device specification is an extension of SunSpec Alliance standards for interoperability between components of an energy storage system (power meters, power conversion systems, and batteries) to communicate with one another. A summary of these standards is provided in Figure 10 and detailed further in Table 5.

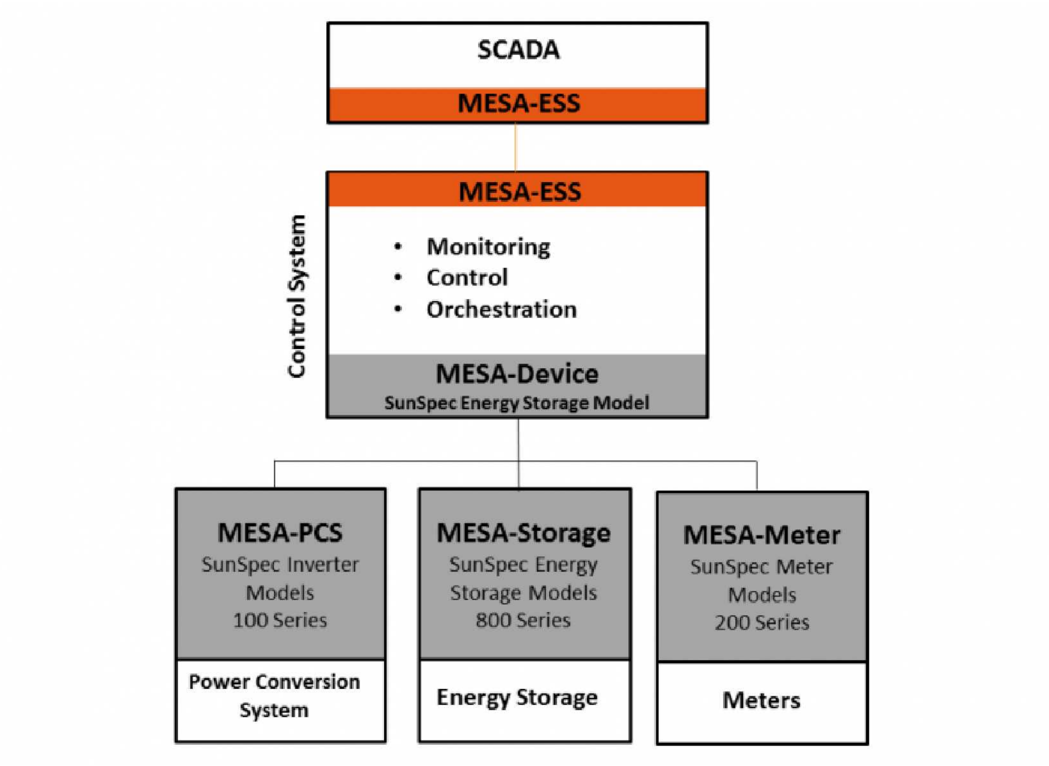

Figure 10: Summary of MESA Standards.[169]

[168] (2014). *MESA: Open Standards for Energy Storage* [Online]. Available: http://mesastandards.org/

[169] (2014). *MESA: Open Standards for Energy Storage*: *MESA Standards* [Online]. Available: http://mesastandards.org/mesa-standards/

Table 5

Name	Description	Protocol	Status
MESA-ESS DNP3 Profile	Provides a standard framework for utility-scale ESS data exchanges. Specifically addresses ESS configuration management, ESS operational states, and the applicable ESS functions from the IEEE 1815 (DNP3) profile for advanced DER.	DNP3 (references a DNP3 spreadsheet which will be used to update the DNP3 App Note)	MESA-ESS is aligned with the DNP3 App Note, which is being updated by EPRI, *et al.* to align with updates to IEC 61850 due to updates in IEEE 1547.
MESA-Device	Proposes standards for how the components of an energy storage system (power meters, power conversion systems, and batteries) communicate with one another.	Umbrella for MESA-Storage, MESA-PCS, and MESA-Power Meter	
MESA-Storage	Defines new storage models that address the capabilities and requirements of energy storage devices. Currently includes: Lithium-Ion Battery Bank Model, Lithium-Ion String Model, Lithium-Ion Module Model, Flow Battery Model, Flow Battery String Model, Flow Battery Module Model, and Flow Battery Stack Model.	SunSpec Modbus	The storage models have not been ratified by a consensus process to date, but do include multiple battery types.
MESA-PCS (Power Conditioning System - Inverter)	SunSpec 100 Series Models. Includes the DER advanced grid functions and DER nameplate values.	SunSpec Modbus	Updated at the same rate as Rule 21 and IEEE 1547 to ensure harmonization.
MESA-Power Meter	SunSpec 800 Series Models – includes the measured power data.	SunSpec Modbus	Fairly static models. Changes made as necessary.

12. OPENADR 2.0

OpenADR is being developed to improve optimization between electric supply and demand[170] and designed to facilitate automated Demand Response (DR) actions at the customer location, including electric load shedding and shifting. OpenADR is also designed to provide continuous dynamic price signals such as hourly, day-ahead, or day-of pricing. It has been field tested and deployed in a number of DR programs in the U.S. and worldwide. While OpenADR focuses on signals for DR events and prices, significant work has also been done in the development of DR strategies and techniques to automate DR within facilities. OpenADR interacts with facility control systems that are pre-programmed to take action based on a DR signal, allowing a response to a DR event or a price to be fully automated with no manual intervention.

[170] R. Bienert and B. Haaser. *Enabling The Standard for Automated Demand Response: Understanding OpenADR 2.0* [Online]. Available: http://www.openadr.org/assets/docs/understanding%20openadr%202%200%20webinar_11_10_11_sm.pdf

The profile specification is a flexible data model that facilitates common information exchange between electricity service providers, aggregators, and end-users. The open specification is intended to allow anyone to implement the two-way signaling systems and provide the servers, which publish information (Virtual Top Nodes or VTNs) to the automated clients that subscribe to the information (Virtual End Nodes, or VENs).

OpenADR 2.0 aspires to conform to NIST Cyber Security requirements and to follow the guidelines provided by the "Security Profile for OpenADR" prepared by The UCAIug OpenADR Task Force and SG Security Joint Task Force.[171] OpenADR 2.0 specifies the necessary level of security that is essential to meet the NIST cyber security requirements for confidentiality, integrity, authentication and message-level security.

OpenADR 2.0 adopts an open architecture for security and will not restrict itself to specific proprietary technologies. The VENs and VTNs use Public Key Infrastructure (PKI) certificates for HTTP client authentication, non-repudiation, and integrity, and favor the user of RSA due to both its efficiency over ECC in embedded devices and its wider acceptance by public web certificate providers. The OpenADR Alliance is also leveraging existing standards from OASIS and WS-Calendar.

13. OPENFMB

Open Field Message Bus (OpenFMB^{TM}) is a framework developed by Duke Energy, Coalition of the Willing (COW) and SGIP to provide grid edge interoperability and distributed intelligence by enabling distributed nodes to communicate with each other.[172] OpenFMB is not a semantic model or communication standard; it is a publish/subscribe architecture for distributed node interaction in grid models, business networks, and other use cases.[173] The framework allows distributed intelligent devices to interact with each other through loosely coupled, peer-to-peer messaging on fielded devices and systems at the grid edge. It is currently open sourced and can be used with PV devices, batteries, reclosers/switches, meter, optimizers, and central communications to fetch device information such as active power, reactive power, voltage, current, phase angle, timestamps, and states of charge. In addition, OpenFMB is backwards compatible with previously developed devices and communication protocols, including the Internet Protocol (IP) and Internet of Things (IoT) messaging protocols.

The application layer included in OpenFMB nodes contains translators that use data profiles based upon the CIM (IEC 61970 and IEC 61698) and IEC 61850 information models. Specific data formats such as XML and specific publish-subscribe protocols are selected based upon use case specific requirements. Since OpenFMB is still nascent, there is limited information regarding security requirements. The developers currently host a working group to develop a security roadmap and have indicated their intention to align with a variety of best practices.[174]

[171]The UCAIug OpenADR Task Force and SG Security Joint Task Force ,"Security Profile for OpenADR, Version 0.02," 2011.

[172](2017). *OpenFMB™* [Online]. Available: http://www.sgip.org/openfmb/

[173] S. McCafferty, "Open Field Message Bus (OpenFMB) Overview," Innovation for Cool Earth Forum, Tokyo, Japan, 4 Oct. 2016.

[174](2017). *Smart Grid Cyber Security Committee (SGCC)* [Online]. Available: http://www.sgip.org/committees-member-groups-original/working-groups/standing-member-committee-smc/smart-grid-cybersecurity-committee-

DISTRIBUTION

1 Guohui Yuan
U.S. Department of Energy
1000 Independence Avenue SW
Washington, DC 20585

1 Kemal Celik
U.S. Department of Energy
1000 Independence Avenue SW
Washington, DC 20585

1 Dan Ton
U.S. Department of Energy
1000 Independence Avenue SW
Washington, DC 20585

1	MS0671	Jennifer Depoy	05628
1	MS0671	William Waugaman	05628
1	MS0671	Jason Stamp	05623
1	MS1033	Abraham Ellis	08812
1	MS1033	Jimmy Quiroz	08812
1	MS1033	Jay Johnson	08812
1	MS0161	Legal Technology Transfer Center	11500
1	MS0899	Technical Library (electronic copy)	

Sandia National Laboratories