NIST Interagency Report
NIST IR 8498

Cybersecurity for Smart Inverters

Guidelines for Residential and Light Commercial Solar Energy Systems

Final

James McCarthy
Jeffrey Marron
Don Faatz
Daniel Rebori-Carretero
Johnathan Wiltberger
Nik Urlaub

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8498

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Interagency Report
NIST IR 8498

Cybersecurity for Smart Inverters

Guidelines for Residential and Light Commercial Solar Energy Systems

Final

James McCarthy*
Jeffrey Marron
Applied Cybersecurity Division
Information Technology Laboratory

Don Faatz
Daniel Rebori-Carretero
Jonathan Wiltberger
Nik Urlaub[#]
The MITRE Corporation

**Former NIST employee; all work for this publication was done while at NIST.*

[#]Former MITRE employee; all work for this publication was done while at MITRE.

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8498

December 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

NIST Technical Series Policies

NIST Technical Series Publication Identifier Syntax

Publication History
Approved by the NIST Editorial Review Board on 2024-12-10

How to Cite this NIST Technical Series Publication
McCarthy J, Marron J, Faatz D, Rebori-Carretero D, Wiltberger J, Urlaub N (2024) Cybersecurity for Smart Inverters: Guidelines for Home and Small Business Solar Energy Systems. (National Institute of Standards and Technology, Gaithersburg, MD). NIST Interagency Report (IR) NIST IR 8498. https://doi.org/10.6028/NIST.IR.8498

Author ORCID iDs
James McCarthy: 0000-0002-5559-733X
Jeffrey Marron: 0000-0002-7871-683X

Contact Information
energy_nccoe@nist.gov

National Institute of Standards and Technology
Attn: National Cybersecurity Center of Excellence, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2002) Gaithersburg, MD 20899-2002

Additional Information
Additional information about this publication is available at https://csrc.nist.gov/pubs/ir/8498/final including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

This report provides practical cybersecurity guidance for small-scale solar inverter implementations that are typically used in homes and small businesses. These guidelines are informed by a review of known smart-inverter vulnerabilities documented in the National Vulnerability Database (NVD), a review of information about known smart-inverter cyber-attacks, and testing of five example smart inverters. The report also provides recommendations to smart-inverter manufacturers on the cybersecurity capabilities needed in their products to implement the seven guidelines. These recommendations build on the Internet of Things (IoT) cybersecurity capability baselines defined in NIST IR 8259A and IR 8259B by providing smart-inverter-specific information for some of the baseline cybersecurity capabilities.

Keywords

IoT cybersecurity capabilities; light commercial inverter; residential inverter; small-scale solar energy system; smart-inverter cybersecurity.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Patent Disclosure Notice

NOTICE: ITL has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Table of Contents

List of Tables

List of Figures

Acknowledgments

The National Cybersecurity Center of Excellence (NCCoE) is grateful to our collaborators on this project for their expertise and equipment in developing this guidance.

Name	Organization
Paul Abbazia	Bedrock Systems
Adrian Beatty	Wunderlich-Malec Engineering
Barbara B. Cuthill	NIST Applied Cybersecurity Division
Eileen Division	The MITRE Corporation[1]
Joel Gil	Bedrock Systems
Siv Hilde Houmb	Norwegian University of Science and Technology
Ian Kittle	U.S. Department of Homeland Security
Trond Oines	Solar Technologies Scandinavia
Jeremy Panicker	Schneider Electric
Sean Plankey	Bedrock Systems
Aleksandr Rakitin	Schneider Electric
Chris Rezendes	Spherical Analytics
Mark Rice	Pacific Northwest National Laboratory
TJ Roe	Radiflow
Thomas P. Roth	NIST Smart Connected Systems Division
Arif Sarwat	Florida International University
Chris Rezendes	Spherical Analytics
John Walsh	Bedrock Systems
Don Wingate	Schneider Electric
Tsion Yimer	Morgan State University

[1] Former MITRE employee; all work for this publication was done while at MITRE.

Executive Summary

This report provides practical cybersecurity guidance for the smart inverters used in small-scale residential and light-commercial solar energy systems connected to the electric distribution network and not directly owned or operated by a utility. Smart inverters manage the flow of energy to and from homes or small businesses and the electrical grid. By sensing conditions on the grid and communicating with the electric utility, these devices contribute to power availability, safety, and grid stability.

Smart inverters often use the internet to connect with cloud-based management capabilities. This connectivity exposes smart inverters to cyber threats and increases the need for effective device cybersecurity that ensures continued safe and reliable operation.

Section 2 of this report provides seven cybersecurity guidelines for homeowners, solar energy system installers, and solar energy system maintainers. These cybersecurity guidelines describe actions that can help ensure that a residential or small business solar energy system is installed, configured, and operated safely and securely.

Section 3 of this report provides ten cybersecurity capability recommendations for smart-inverter manufacturers. These cybersecurity capabilities are derived from the Internet of Things cybersecurity capability core baselines presented in NIST Interagency Report (IR) 8259A and 8259B and enable implementation of the Sec. 2 guidelines.

A collection of appendices provides information that supports the development and use of these guidelines and recommendations.

Appendix A provides a bibliography of publications that were consulted in developing the guidelines and recommendations.

Appendix B provides a list of abbreviations and acronyms.

Appendix C provides a sample Provisioning Checklist that system installers can tailor and use in verifying that they have completed the actions defined in the Sec. 2 guidelines.

Appendix D records the results of testing five installed smart inverters to determine their ability to implement the Sec. 2 guidelines.

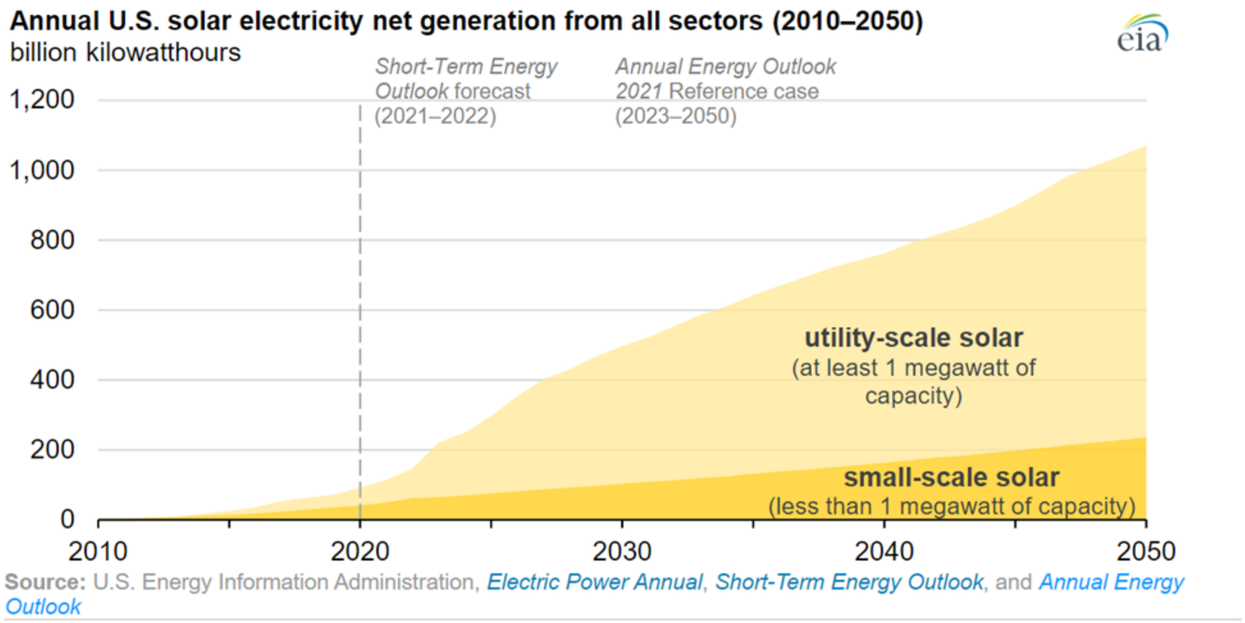
Appendix E maps the Sec. 2 guidelines to six general cybersecurity guidance sources.

Appendix F presents information about known smart-inverter cybersecurity vulnerabilities documented in the National Vulnerability Database (NVD).

1. Introduction

This report provides practical cybersecurity guidance for small-scale residential and light-commercial inverters that are connected to the distribution network, not directly owned and operated by the utility, and typically used in homes and small businesses. It was developed by examining the current smart-inverter threat landscape, currently available smart-inverter cybersecurity capabilities, and potential mitigations that system installers, homeowners, and small business owners can implement. These capabilities and mitigations were validated through testing to demonstrate their practicality. The report provides recommendations to smart-inverter manufacturers for cybersecurity capabilities needed in their products to implement the seven guidelines. These recommendations build on the Internet of Things (IoT) cybersecurity capability baselines defined in NIST Interagency Report (IR) 8259A [1] and IR 8259B [2] by providing smart-inverter-specific information.

As shown in Fig. 1, the U.S. Energy Information Administration [3] projects a continuing increase in solar generation, including small-scale solar such as residential and light commercial solar energy systems.


Annual U.S. solar electricity net generation from all sectors (2010–2050)

Source: U.S. Energy Information Administration, *Electric Power Annual*, *Short-Term Energy Outlook*, and *Annual Energy Outlook*

Fig. 1. U.S. electric generation

The electrical grid is incorporating more IoT and smart devices (e.g., smart inverters) that have less centralized control. These devices often use the internet to connect with cloud-based management capabilities. This internet connectivity increases exposure to cyber threats, thus increasing the need for effective cybersecurity to prevent impacts on the grid.

The compromise of a single residential or light commercial smart inverter connected to the distribution network would have a minimal impact on the grid today. However, as the solar energy market grows, utilities may become more dependent on the supply of power from distributed renewable energy resources during peak daytime power consumption. As this transformation occurs, attacks developed to compromise multiple residential or light commercial smart inverters may have significant impacts. The inverter's safety-critical functions must always be capable of detecting conditions in which providing power flow would be unsafe.

If vendors share software across multiple product lines, weaknesses discovered and exploited in residential and light commercial smart inverters could be leveraged to compromise larger commercial inverters.

Even without impacting the electrical grid, cyber attacks on small-scale solar energy systems can have negative effects on homeowners and small business owners, such as:

- Loss of financial benefit: An inverter disconnecting from the grid would lead to the loss of any expected financial benefits from installing the equipment.
- Damage to the home, business, or installed equipment: An attack on an inverter could damage the inverter or cause the inverter's output to exceed safe operating conditions (e.g., harmonic distortion, overvoltage, incorrect frequency), potentially damaging other home or business equipment (e.g., AC, stove, electronics).
- Loss of equipment at key need: An attack on an inverter could prevent the system from operating when needed (e.g., power outage).

Cybersecurity protections for the smart inverters used in small-scale residential and small business solar energy systems can reduce the likelihood of a successful cyber attack.

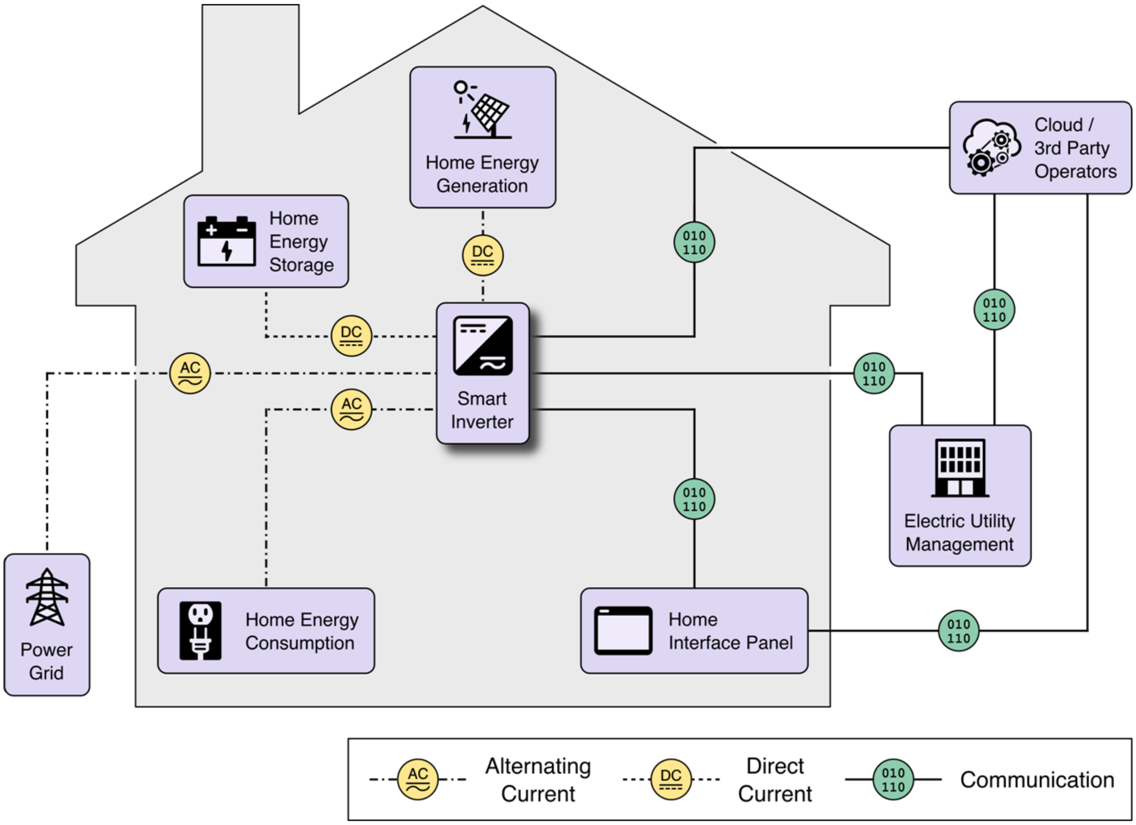


Fig. 2. The role of a smart inverter in a residential or light commercial solar energy system

Fig. 2 illustrates the central role that a smart inverter plays in a residential or light commercial solar energy system. The smart inverter orchestrates the behavior of the solar energy system and its interactions with the electrical grid. The smart inverter receives direct current (DC) power from the system's solar panels and directs that energy to one of three uses:

1. The smart inverter can convert the DC power to alternating current (AC) power and provide it to the home or small business for immediate use.
2. The smart inverter can provide excess AC power to the electric utility by communicating with the electric utility or third-party operators via communications links.
3. If AC power is not needed by the home, business, or local utility, the smart inverter can use the DC power produced by the solar panels to charge the batteries in the home energy storage component of the system.

Additionally, the smart inverter can draw energy from the home energy storage component if the home or business needs more power than the solar panel can provide. The smart inverter can also provide power from home energy storage to support the grid in times of high demand. The smart inverter coordinates providing power from home energy storage by communicating with the electric utility or third-party operators via communications links.

The communication links used for coordination with the electric utility or third-party operators, if not protected, expose the smart inverter to potential cyber-attacks. In the absence of proven-correct software, software defects should be assumed to exist in smart-inverter software. Some defects should be assumed to enable the manipulation of smart-inverter behavior that potentially impacts the home, business, and electrical grid.

1.1. Audience

This paper provides cybersecurity guidance for residential and small commercial smart inverter solar energy system owners, installers, maintainers, and component manufacturers.

System owners, homeowners, and small business owners can use this guidance to understand the cybersecurity capabilities that should be included in their systems and to discuss the cybersecurity of their systems with vendors, installers, and maintainers. System installers can use this guidance to develop installation procedures and checklists to ensure that the systems they install provide appropriate cybersecurity for system owners. System maintainers can use this guidance to define procedures that ensure cybersecurity-related maintenance (e.g., system patching) is being performed and verify that the system continues to provide appropriate security. Manufacturers can use this guidance to ensure that their products provide the cybersecurity capabilities needed to support secure installation and operation.

1.2. Report Organization

The cybersecurity guidance is presented in four main sections, each tailored to a specific audience.

- Section 1 describes why cybersecurity is important for residential and small business solar energy systems and why this cybersecurity guidance focuses on smart inverters.
- Section 2 provides seven guidelines for ensuring that a residential or small business solar energy system is installed, configured, and operated securely.
- Section 3 identifies six technical and four non-technical cybersecurity capabilities that smart-inverter manufacturers should consider including in their products, as defined in IR 8259A and IR 8259B. This section also provides smart-inverter-specific recommendations in the form of additional information for the IR 8259A and IR 8259B cybersecurity capabilities to help ensure that smart inverters are installed, configured, and operated securely.
- Section 4 summarizes the development and presentation of this cybersecurity guidance.

This guidance is augmented by a collection of appendices that provide supporting information for the guidelines and recommendations.

- Appendix A is a bibliography of publications that were consulted in developing this guidance.
- Appendix B provides a list of abbreviations and acronyms.
- Appendix C provides a sample Provisioning Checklist for solar energy system installers. This checklist can be tailored to the activities needed for specific products and environments. Installers can use the tailored checklist to verify that they have completed the actions defined in the guidelines. The completed checklist can be shared with homeowners and small business owners as a record of the cybersecurity-related actions completed with the installation.
- Appendix D records the results of testing five installed smart inverters to determine their ability to implement the guidelines presented in Sec. 2.
- Appendix E maps the guidelines to six general cybersecurity guidance sources. Manufacturers may use these mappings to better understand the recommendations in Sec. 3 and how to implement the recommendations in their products.
- Appendix F presents information about known smart-inverter cybersecurity vulnerabilities documented in the National Vulnerability Database (NVD). This information was used in formulating the guidelines.

2. Cybersecurity Guidelines for Owners and Installers

This section provides seven guidelines for homeowners and solar energy system installers and maintainers. These guidelines define actions that should be taken to help ensure that a residential or small business solar energy system is installed, configured, and operated securely. They encompass smart-inverter configuration actions that should be performed across the solar energy system life cycle by installers, maintainers, and homeowners. These guidelines also provide a collection of cybersecurity protections that should be utilized for a secure solar energy system installation.

The guidelines are informed by a collection of general cybersecurity guidance presented in Appendix E and were tested against the cybersecurity capabilities available in five smart inverters. The results of that testing are presented in Appendix D.

Each guideline contains the following sections:

- A description of the guideline
- A definition of the solar energy system life cycle phases in which the guideline should be implemented
  - There are five phases in the solar energy system life cycle: manufacturing[2], setup (or installation), operation, maintenance, and decommissioning (i.e., retirement). The guidelines in Sec. 2 are implemented in one or more of four life cycle phases:
    - Setup — The smart inverter is installed and configured in a home or business.
    - Operation — The homeowner or business owner uses the smart inverter to perform its intended function.
    - Maintenance — The smart inverter undergoes maintenance to correct a problem or ensure continued safe and reliable operation.
    - Decommissioning — The smart inverter is removed from the home or business.
- Examples of configuration actions to implement the guideline
  - The examples are described at a high level as the process to implement the guideline will vary by manufacturer and smart-inverter model. Consult the manufacturer's documentation for specific instructions.

2.1. Guideline #1: Change Default Passwords and Credentials

Device manufacturers often create preconfigured accounts that may have well-known or easily-discoverable default passwords, individual device-specific passwords, or other access credentials to simplify the installation and setup of a device. However, once installed and

[2] Cybersecurity recommendations implemented in the manufacturing life cycle phase are discussed in Sec. 3.

connected to communication networks, these passwords and credentials may allow anyone who knows the values to access the device and change its configuration.

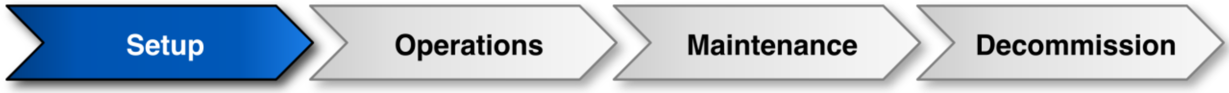


Fig. 3. Guideline #1 life cycle phase

As shown in Fig. 3, during the device setup and installation process, each preconfigured account should be assigned a new, unique password or credential. Any new accounts created as part of installation or operation of the device should be assigned unique passwords or credentials. Multi-factor authentication[3] (MFA) can also improve security, especially for more privileged accounts (see Sec. 2.2)[4].

In addition to interacting with people, smart inverters may also interact with other systems and devices. These interactions need to be mutually authenticated using strong credentials (e.g., digital certificates) that should also be changed from factory defaults during setup.

2.2. Guideline #2: Use Role-Based Access Control (RBAC)

Limiting access to only those capabilities a person needs to perform their responsibilities is a key tenet of good cybersecurity. Various people and organizations may need to access a smart inverter in a home or small business solar energy system. Rather than assigning access permissions directly to each person or organization, a more manageable approach would be to identify roles and the access permissions they need to perform specific tasks. A smart inverter may have defined roles for installers, maintainers, the electric utility, third-party operators, and homeowners. Adding or removing access permissions for a person or organization involves adding their account to or removing it from one or more roles. For a system installer, it may be important to make interface changes and set values for different aspects of the system to ensure that it functions properly in its environment. A homeowner may instead need the ability to view monitor data and historical usage graphs. A homeowner may not need, nor should they be able to reconfigure the smart inverter, and a system installer may not need some of the historical data. Although these roles and permissions may vary, the concept of separate roles is vital to ensuring secure access to the device based on the user.

As shown in Fig. 4, an initial collection of roles with appropriate access permissions should be defined during the setup phase of the smart-inverter life cycle. Roles may need to be created, modified, or deleted during the maintenance phase. For example, software updates may add or remove smart-inverter capabilities that require updates to role definitions. The assignment of people and organizations to roles should be reviewed periodically to ensure they are up to date and appropriate.

[3] MFA is authentication using two or more of the following factors: (i) something you know (e.g., password/personal identification number [PIN]), (ii) something you have (e.g., cryptographic identification device, token), or (iii) something you are (e.g., biometric).

[4] Reference [4] describes current best practices in a variety of authentication techniques, including MFA and passwords. Additional password best-practice guidance is provided by Cybersecurity and Infrastructure Security Agency (CISA) [5] and the Federal Bureau of Investigation (FBI) [6].

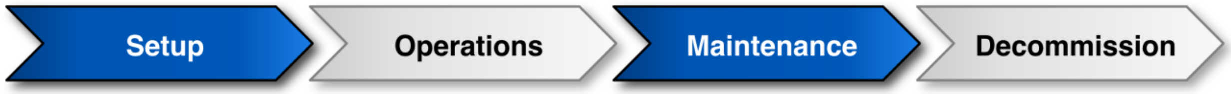


Fig. 4. Guideline #2 life cycle phase

A basic collection of roles for a smart inverter might include:

- An Installer role with the access permissions needed to perform initial setup and configuration of the smart inverter. A smart-inverter manufacturer might include this as a default role along with a default user account, as described in Guideline #1 (Sec. 2.1).
- A Maintainer role with the access permissions needed to install software updates, perform diagnostics, and make repairs.
- A Homeowner role with the access permissions needed to monitor the operation of the smart inverter and respond to alerts.

2.3. Guideline #3: Configure the Recording of Events in a Log

A log of cybersecurity-relevant activities that is stored in another location can help identify the factors that led to an unexpected event, recover from the compromise, and determine how to prevent such compromises in the future.

Logs should contain information about the operation of the smart inverter (e.g., normal or anomalous values of system parameters) when an event is detected and enable reviewers to understand the chain of events with a degree of fidelity. Event logging supports troubleshooting for smart-inverter issues as well as responses to cyber events.

In addition to system parameters, logs should also contain cybersecurity-relevant information, such as:

- Creation or removal of user accounts
- Successful and unsuccessful user authentication, including the identity associated with the authentication
- Changes to smart-inverter configuration settings, including previous and new values and the identity of the user or system making changes to enabled/disabled features, assigned user roles, and role permissions
- Enabling previously disabled features
- Records of software and firmware updates, including how the update was initiated (e.g., by a user, automatically), the source of the update, and any update integrity information (e.g., checksums, hashes)
- Communications events, such as network connections or loss of connectivity
- Actions performed directly from the smart-inverter's control panel

As shown in Fig. 5, logging capabilities should be configured and enabled by the installer during solar energy system setup. During operations and maintenance, the owner or maintenance technician should verify that information is being collected and stored in logs as intended.

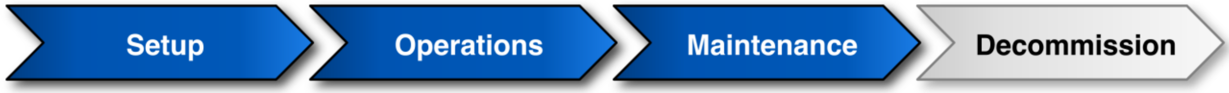


Fig. 5. Guideline #3 life cycle phase

2.4. Guideline #4: Update Software Regularly

Smart inverters depend on software to provide the "smart" elements of their operation. Even well-developed software has vulnerabilities that are discovered after deployment and need to be corrected. Additionally, manufacturers continuously evolve the software capabilities in their devices. Therefore, it is important to provide a secure avenue to update smart-inverter software that verifies the validity, source, and authenticity of updates prior to installation. This ensures that software stays up to date with the latest security and functional capabilities. Updates that impact the security of the smart inverter should be deployed as soon as possible. Keeping smart-inverter software updated helps protect against weaknesses discovered after the device has been set up in a home or small business solar energy system.

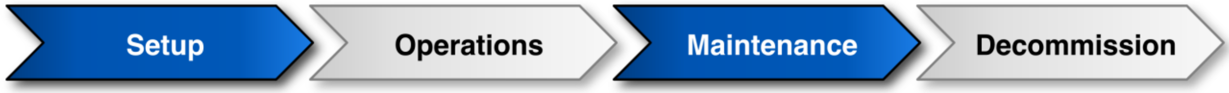


Fig. 6. Guideline #4 life cycle phase

Updating a smart-inverter's software should be part of the device's initial setup and ongoing maintenance[5], as shown in Fig. 6. Manufacturers generally have a limited support life cycle and will stop developing patches for discontinued devices. When this occurs, owners should replace the discontinued device with a current model as soon as possible.

2.5. Guideline #5: Back Up System Information

Smart inverters have configuration parameters or settings that can be customized based on the requirements of a particular home or small business solar energy system. These parameters are normally stored in a configuration file and may include the battery recharge voltage and security settings (e.g., user credentials discussed in Sec. 2.1, permissions and user role assignments discussed in Sec. 2.2).

Creating a configuration backup is the process of copying the current configuration information to a different location. Maintaining a backup of the smart-inverter configuration can help restore operations after an event, either cyber or non-cyber, that leaves the solar energy system in a non-operating state or operating incorrectly. Restoring a configuration backup or performing a factory reset that returns the smart inverter to its default configuration may

[5] Inverters should be designed to only allow updates when it is safe to do so.

correct the problems. Configuration restoration capabilities may also be used to load a pre-built configuration into a smart inverter during setup.

As shown in Fig. 7, a backup should be created after the initial configuration of the smart inverter during setup and after any parameter change or upgrade during maintenance.

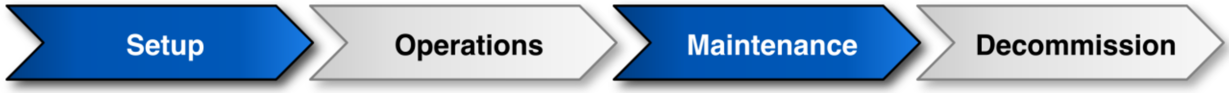


Fig. 7. Guideline #5 life cycle phase

Backups should be stored in a retrievable location, such as a flash drive or cloud storage. The process for creating a configuration backup will be specific to the manufacturer and product.

2.6. Guideline #6: Disable Unused Features

Smart inverters may be built with features and capabilities that support multiple deployment scenarios and user requirements. While having these features and capabilities provides flexibility in deployment, each enabled feature potentially adds to a device's exposure to cybersecurity threats.

Disabling features and capabilities that are not used in a particular device deployment is another key tenet of good cybersecurity. Any features or capabilities that are not required for a particular deployment should be disabled to enhance security and reduce exposure to threats.

In addition to smart-inverter features and capabilities that are necessary to the operation of a solar energy system, there may be features and capabilities that are nice to have or may be a convenience in operating the system. In determining whether to use the features and capabilities, consider whether the benefits they offer outweigh any increase in exposure to cybersecurity threats.

Smart-inverter features and capabilities may be enabled or disabled during the setup and maintenance life cycle phases, as illustrated in Fig. 8.

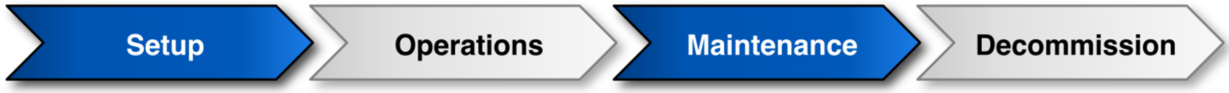


Fig. 8. Guideline #6 life cycle phase

Some features and capabilities that may be included in a smart inverter but may not be needed in a particular deployment include:

- **Remote access protocols and interfaces.** The operation and maintenance of a smart inverter may require remote access to the device. Any remote access protocols or interfaces that are not used in a deployment should be disabled.

- **Wireless communications.** Smart inverters may support both wired and wireless network connectivity. If a deployment uses only wired connectivity, the wireless communications capability should be disabled.
- **Guest and/or anonymous smart-inverter access.** A Guest role that allows access to some smart-inverter features or capabilities without a defined user account should be read-only and prohibited from changing the configuration or operation of a device.

2.7. Guideline #7: Protect Communications Connections

An important aspect of smart inverters is their ability to communicate. A smart-inverter's communication can take many forms, including communications with the electric utility, third-party operators, device manufacturer, or other devices in the local environment. The inverter may communicate operating information to the owner and the local utility. It may also communicate with the device manufacturer or a device's maintenance contractor to receive software updates or share operating information to detect potential problems before they occur. However, this communication capability also provides an avenue for cyber attacks. Therefore, it is important to consider how the smart inverter can be protected from threats while still being able to communicate as needed for its intended purpose.

There are many potential approaches to protecting smart-inverter communications from malicious actors while still allowing needed communications. Inverters may have a dedicated cellular connection to communicate with the local utility without being exposed to a public network, such as the internet. Communication with the owner may occur using a control panel that is directly connected to the inverter. Updates may be performed using portable storage devices, such as USB "thumb drives."[6]

A smart inverter may leverage an existing home internet connection to communicate with the owner, electric utility, third-party operators, and manufacturer. When the inverter uses an existing internet connection, the installation should take steps to separate the inverter from other activity on the network. There are several ways to provide this protection, such as separate logical networks created by the home or business router. Separation techniques depend on the capabilities available from the internet service provider (ISP). Connections used to communicate with the local utility or manufacturer should not be accessible from other devices on the local network. Cybersecurity capabilities can also provide this protection, such as a virtual private network (VPN) connection between the utility or manufacturer.

As shown in Fig. 9, protection should be established during the setup life cycle phase and monitored during the operations life cycle phase to ensure that it remains effective.

[6] Some older smart inverters may provide this update mechanism. Smart inverter installers/operators should be aware of the risks of using external media to perform software updates. Installers/operators should also be certain of the media's origin and that the media are free of malicious software.

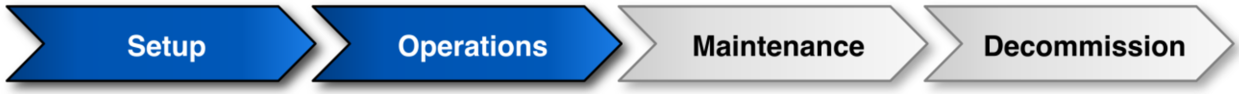


Fig. 9. Guideline #7 life cycle phase

3. Cybersecurity Recommendations for Smart-Inverter Manufacturers

This section provides recommendations for smart-inverter manufactures to provide the cybersecurity capabilities needed to implement the guidelines in Sec. 2 and the capabilities that would better address cyber threats to smart-inverter operations. These recommendations involve changes to inverter design, changes to inverter software and firmware, or the addition of new front-end devices to protect inverter interfaces.

3.1. Recommended Baseline Cybersecurity Capabilities

Smart inverters used in home and small business solar power systems are examples of IoT devices. IR 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers* [7], describes its guidance as applying to devices that "have at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth, Long-Term Evolution [LTE], Zigbee, Ultra-Wideband [UWB]) for interfacing with the digital world." Smart inverters sense the state of the power grid, provide power to the grid, and communicate with owners and grid operators through communications interfaces that satisfy this description. Emerging inverter controllers may also require the autonomous exchange of information between inverters. Hence, the general cybersecurity guidance presented in IR 8259 [7] is applicable to smart inverters.

Two publications in the IR 8259 series provide the baseline cybersecurity capabilities recommended for all IoT devices:

1. IR 8259A, *IoT Device Cybersecurity Core Baseline* [1], defines a baseline of six technical cybersecurity capabilities that IoT devices provide through their own technical means (i.e., device hardware and software).
2. IR 8259B, *IoT Non-Technical Supporting Capability Core Baseline* [2], defines a baseline of four non-technical cybersecurity capabilities that a manufacturer or third-party organization performs in support of the cybersecurity of an IoT device (e.g., providing information about software updates, instructions for configuration settings, and supply chain information).

Used together, technical cybersecurity capabilities and non-technical supporting capabilities can help mitigate cybersecurity risks related to the use of IoT devices while assisting customers in achieving their goals.

As smart inverters are IoT devices, manufacturers should consider including all of the baseline cybersecurity capabilities in their products to enable owners and installers to implement the seven basic guidelines. Table 1 and Table 2 list the cybersecurity capabilities from the IR 8259A [1] and IR 8259B [2] baselines, respectively, in the first column of each table. Additionally, columns 2 and 3 of each table include information about the baseline cybersecurity capability that is specific to smart-inverter cybersecurity capabilities. This additional information was derived in part from the smart-inverter testing presented in Appendix D and the smart-inverter vulnerability research presented in Appendix F.

Table 1. Technical cybersecurity capability recommendations

IR 8259A Technical Device Cybersecurity Capability	Additional Smart-Inverter Cybersecurity Capability Recommendation Information for Manufacturers	Smart-Inverter-Specific Cybersecurity Capability Description
Device Identification: The IoT device can be uniquely identified logically and physically.	The smart inverter has the capability to inventory other components of a solar energy system. This recommendation supports Guideline #3.	Solar energy systems may contain components in addition to the smart inverter (see Fig. 11). These components may include specialty gateway devices, cloud-based services, or even mobile apps. The capability to identify and inventory these components can aid in comprehensively logging system activity and recognizing trusted system components. IR 8425 [8] expands on the unique identification of IoT devices to include inventorying the components of an IoT product (e.g., cloud-based services, mobile apps) as recommended here for smart inverters.
Device Configuration: The configuration of the IoT device's software can be changed, and such changes can be performed by authorized entities only.	The smart inverter can back up its configuration to an external location and restore its configuration from a backup. This recommendation supports Guideline #5.	A backup of smart-inverter configuration parameters and settings enables rapid restoration of the configuration should an accidental or malicious action change the configuration. The smart inverter should be able to create a backup of all parameters and settings that affect its operation, export the backup to an external storage location, verify the integrity of a previously created backup, and restore its configuration from the backup.
	The smart inverter should be able to disable or remove capabilities that are not needed in a deployment. This recommendation supports Guideline #6.	Smart-inverter products need to support a variety of deployment approaches. Hence, they may include capabilities that are not used in all deployments. Enabled but unused capabilities increase the opportunity for a malicious actor to gain unauthorized access to the smart inverter. Capabilities that are not used in all deployment approaches should be disabled by default and require an installer to proactively enable them when needed. This recommendation should also be applied to communications protocols. Smart inverters may include software acquired from third parties. Any capabilities in such software that are not used by the smart inverter should be removed or disabled.
	The smart inverter can reset its configuration to the factory default. This recommendation supports Guideline #5.	For troubleshooting, it may be advantageous to restore a smart inverter to a default configuration. Additionally, when disposing of a smart inverter, it should be reset to the default factory configuration to remove any information that might aid a malicious actor.

IR 8259A Technical Device Cybersecurity Capability	Additional Smart-Inverter Cybersecurity Capability Recommendation Information for Manufacturers	Smart-Inverter-Specific Cybersecurity Capability Description
Data Protection: The IoT device can protect the data it stores and transmits from unauthorized access and modification.	The smart inverter uses secure communication protocols that provide mutual authentication of the communication endpoints and protect the integrity of data in transit. This recommendation supports Guideline #7.	Communication interfaces to a smart inverter should use communication protocols that provide mutual authentication of the communications channel endpoints, integrity protection of data in transit, and confidentiality protection of data in transit. Smart inverters should either use protocols that inherently provide security capabilities (e.g., such as Transport Layer Security) or wrap protocols that lack security capabilities using techniques such as VPNs.
Logical Access to Interfaces: The IoT device can restrict logical access to its local and network interfaces, and the protocols and services used by those interfaces, to authorized entities only.	The smart inverter supports MFA to determine the identity of entities attempting to access its services. This recommendation supports Guideline #1.	To control access to capabilities, the inverter needs to know who is attempting to access its capabilities and what capabilities they are authorized to use. The inverter authenticates users and systems to establish their identity. Traditionally, a single authentication factor—a password—has been used. However, passwords are no longer an appropriate authentication approach for access to capabilities that could affect critical infrastructure. Smart inverters should use stronger authentication techniques (e.g., MFA) to authenticate users.[7] Smart inverters also communicate with non-person entities (e.g., other devices and systems). These interactions should use strong system-to-system credentials (e.g., digital certificates) and provide mutual authentication.
	The smart inverter supports RBAC and provides the ability to create, modify, and configure the roles. This recommendation supports Guideline #2.	Rather than assigning access permissions directly to each person, a more manageable approach is to define a collection of roles where each role defines the access permissions needed to perform specific responsibilities. An initial collection of roles with appropriate access permissions should be defined during the setup phase of the smart-inverter life cycle. Roles may need to be created, modified, or deleted during the operation and maintenance phases.
	The smart inverter minimizes the amount and type of information and type of services available via unauthenticated access. This recommendation supports Guideline #2.	It may be necessary to provide some information about the smart inverter and its operation to a person or system without authenticating their identity. In providing such access, the manufacturer should follow the cybersecurity principle of least privilege. That is, the smart inverter should minimize the amount of information it will provide to unauthenticated users. Device "fingerprinting" (i.e., learning as much as possible about a device without explicitly gaining access to the device) can help a malicious actor pinpoint

[7] The NIST Special Publication (SP) 800-63 series provides detailed guidance on authentication techniques.

IR 8259A Technical Device Cybersecurity Capability	Additional Smart-Inverter Cybersecurity Capability Recommendation Information for Manufacturers	Smart-Inverter-Specific Cybersecurity Capability Description
		vulnerabilities and weaknesses that can be used to gain unauthorized access. Manufacturers should minimize information shared on non-authenticated interfaces. Information such as product versions, specific software and firmware installed, and network information should likely not be shared to protect against targeted cyber attacks.
Software Update: The IoT device's software can be updated by authorized entities only using a secure and configurable mechanism.	The smart-inverter's software can be updated automatically and without owner action.[8] This recommendation supports Guideline #4.	Installing software updates to correct software flaws that create exploitable vulnerabilities is critical to maintaining smart-inverter cybersecurity. Updates are most effective when installed in a timely manner. However, if update installation depends on explicit action by the owner or maintainer, they may not be installed quickly enough. Automatic updates can ensure that updates are applied as quickly as it is feasible. The owner should be notified when updates are installed. If meaningful, the notification should identify what inverter capabilities and services were affected by the update. The device should also recognize software update failures, rollback any changes made to known-good software, and notify the owner of the update failure. Enabling automatic updates should be configurable as its use may not be appropriate in all deployment scenarios. The automatic update function should be designed to recognize when it is safe to install an update and when current operating conditions require deferring an update. Software updates to safety-critical control functions should only be performed through a local programming interface on the smart inverter.
Cybersecurity State Awareness: The IoT device can report on its cybersecurity state and make that information accessible to authorized entities only.	The smart inverter records a log of all cybersecurity-relevant events. This recommendation supports Guideline #3.	Determining what happened when a smart inverter fails to operate as expected requires information about the activities that led to the failure, including cybersecurity incidents. The smart inverter should monitor and log events related to both device health and cybersecurity. Smart-inverter configuration changes should also be included. This information should be exported to remote storage to ensure that it is not compromised in a cyber incident.

[8] This recommendation is forward-thinking and describes an ideal scenario. Some smart inverters may require user interaction to update software.

IR 8259A Technical Device Cybersecurity Capability	Additional Smart-Inverter Cybersecurity Capability Recommendation Information for Manufacturers	Smart-Inverter-Specific Cybersecurity Capability Description
Device Security[9]: The capability to secure the IoT device to meet organizational requirements.	The smart inverter should protect sensing and control capabilities that interact with the power grid or with power delivery to a home or business from other capabilities that may be exposed to cyber attacks. This recommendation supports Guideline #7.	To better protect operations, smart inverters should control the interactions among different elements and services within the device, including physical or software protection of real-time control functions, safety-critical functions, and power electronics from data communications interfaces. This protection reduces the potential impacts of cyber incidents on interactions with the physical world. For user interaction interfaces, including locally hosted webservers, techniques such as virtualization and out-of-band security monitoring should be employed. Virtualization can separate the user interaction interfaces from the control and monitoring functions that are critical to safe device operations. Whenever possible, these functions should be separated at a hardware level (e.g., by using separate processing units for control functions and assuming zero trust between the control system hardware and the user interaction hardware). Fig. 10 illustrates the control functions in a smart inverter and their interactions with other functional elements of a smart inverter. Control functions may have different interaction needs with other functional elements. Protecting these interactions from compromise is critical to the correct and safe operation of a smart inverter. A software compromise should not result in unsafe operation. To ensure this, electro-mechanical protections (e.g., over-voltage circuit breakers, over-temperature circuit breakers, and electro-mechanical islanding detection) may be needed to ensure continued safe operation when software is compromised. Manufacturers are encouraged to design smart inverters such that the hardware is physically unable to enter an unsafe state, even if inverter software is compromised.
	The smart inverter should only accept software updates from known trustworthy sources whose identity has been verified. This recommendation supports Guideline #4.	To protect against unauthorized or malicious software updates, smart inverters should have a list of known trusted sources from which they will accept software updates. The identity of sources attempting to provide a software update should be authenticated, and the update should only be allowed if the authenticated identity is a known trusted source for software updates.

[9] The device security capability is not part of the IR 8259A baseline but was introduced in SP 800-213A, *IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog* [9]. It is included here because some recommendations for manufacturers align well with the device security technical capability.

IR 8259A Technical Device Cybersecurity Capability	Additional Smart-Inverter Cybersecurity Capability Recommendation Information for Manufacturers	Smart-Inverter-Specific Cybersecurity Capability Description
	The smart inverter should verify the integrity of software updates before installation. This recommendation supports Guideline #4.	Smart inverters should verify that the update received was produced by a trusted source and that the update has not been modified since it was produced. Techniques such as a cryptographic hash and a digital signature can be used to verify the integrity of a software update.

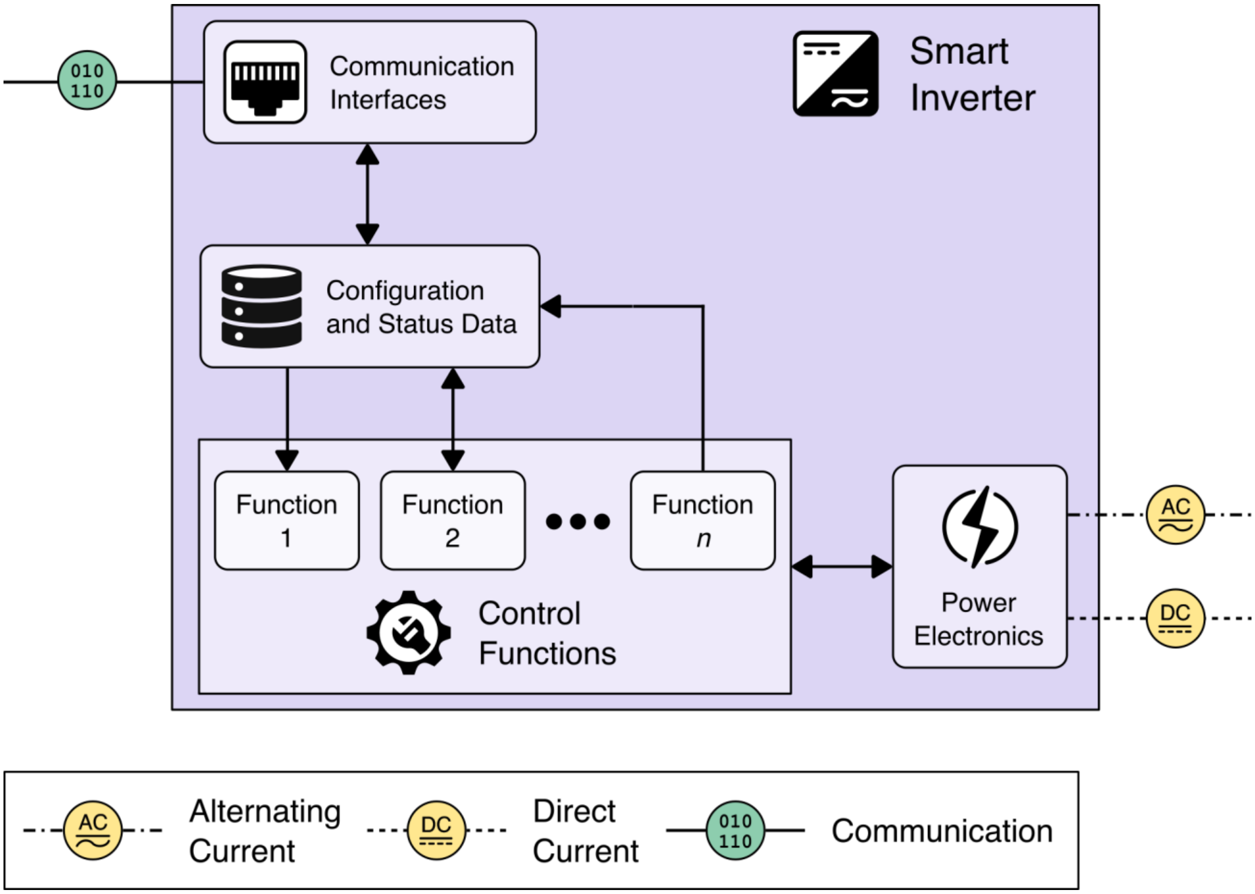


Fig. 10. Functional elements of a smart inverter

Table 2. Non-technical cybersecurity capability recommendations

IR 8259B Non-Technical Device Cybersecurity Capability	Additional Smart-Inverter Cybersecurity Capability Recommendation Information for Manufacturers	Smart-Inverter-Specific Cybersecurity Capability Description
Documentation: The ability for the manufacturer and/or the manufacturer's supporting entity, to create, gather, and store information relevant to cybersecurity of the IoT device prior to customer purchase, and throughout the development of a device and its subsequent lifecycle.	The manufacturer provides and maintains a Software Bill of Materials (SBOM) for the smart inverter. This recommendation supports Guideline #4.	An SBOM provides details on the libraries and software used in a product so that owners and maintainers can determine whether a newly discovered vulnerability applies to the software in a particular device. The SBOM should be maintained throughout the life of a smart inverter and reflect the current state of system software, including changes that result from software updates.
	The manufacturer creates documentation that enables owners and installers to perform Guidelines #1-7.	Extensive documentation may be required to enable owners and installers to perform all recommended Guidelines. This documentation may include how to: • Set up and change authentication techniques (e.g., MFA, passwords) • Create and configure roles • Configure software update settings • Enable and disable features • Configure logging • Enable and configure backups • Configure communication interfaces
Information and Query Reception: The ability for the manufacturer and/or supporting entity to receive information and queries from the customer and others related to cybersecurity of the IoT device.	The manufacturer initiates capabilities to receive information about smart-inverter vulnerabilities. This recommendation supports Guideline #4.	Manufacturers need to have capabilities to receive information about smart-inverter vulnerabilities and other issues with a product in order to develop software updates and improvements.
	The manufacturer initiates capabilities to receive and respond to questions from owners and installers about the smart inverter. This recommendation supports Guidelines #1-7.	Owners and installers may encounter issues during all phases of the smart-inverter life cycle, including installation, initial configuration, and routine maintenance during system operation. Manufacturers should have a way to receive questions from owners and installers and to respond in a timely manner.
Information Dissemination: The ability for the manufacturer and/or supporting entity to broadcast and distribute (e.g., to the customer or others in the IoT device	The manufacturer disseminates updated information that enables owners and installers to perform Guidelines #1-7.	Throughout a smart-inverter's support life cycle, there will likely be new information about relevant threats, vulnerabilities, and risks that impact cybersecurity and the implementation of the guidelines. Manufacturers should have capabilities in place to disseminate updated documentation, bulletins, and/or notices so that owners and installers can successfully perform all recommended guidelines.

IR 8259B Non-Technical Device Cybersecurity Capability	Additional Smart-Inverter Cybersecurity Capability Recommendation Information for Manufacturers	Smart-Inverter-Specific Cybersecurity Capability Description
ecosystem) information related to cybersecurity of the IoT device.		
Education and Awareness: The ability for the manufacturer and/or supporting entity to create awareness of and educate customers and others in the IoT device ecosystem about cybersecurity-related information, considerations, features, etc., of the IoT device.	The manufacturer provides relevant information and awareness materials in a format that is easily understood by owners and installers. This recommendation supports Guidelines #1-7.	The secure and safe installation and maintenance of a smart inverter depends on effective education and awareness. Manufacturers can help ensure that owners and installers successfully perform all recommended guidelines by providing information, resources, and awareness materials in a format that can be easily used and understood.

Homeowners, small business owners, grid operators, and society reasonably expect residential and light-commercial solar energy systems to operate safely and reliably. Smart-inverter manufacturers should fully address these expectations in their products.

4. Conclusion

Smart inverters are exposed to an array of potential cybersecurity threats, creating risks that can affect their intended operation. The growing prevalence of, dependence on, and interconnection of these systems means that risks to smart inverters can create broader risks to the electrical grid.

This report provides seven basic cybersecurity guidelines for solar energy system owners, installers, and maintainers to improve the secure installation and operation of small-scale residential and small-business solar energy systems. This report also provides cybersecurity recommendations for smart-inverter manufacturers. These recommendations provide smart-inverter-specific guidance for some of the IoT cybersecurity capability baselines in IR 8259A [1] and IR 8259B [2]. Manufacturers should consider including all of the baseline cybersecurity capabilities in their products to enable owners and installers to implement the seven basic guidelines.

These guidelines and recommendations were derived from several sources. The NVD was reviewed to identify known vulnerabilities (see Appendix F) in existing smart inverters, and the guidelines suggest actions to reduce the risks from these vulnerabilities where possible. Six sources of general cybersecurity guidance were reviewed to identify specific guidelines and recommendations for smart inverters and solar energy system component manufacturers (see Appendix E). The practicality of the guidelines was verified by applying them to five existing commercially available smart inverters, and only two could implement all seven guidelines (see Appendix D). The recommendations, if followed by manufacturers, should enable future smart inverters to implement all seven guidelines.

References

[1] Fagan MJ, Megas KN, Scarfone KA, Smith M (2020) IoT Device Cybersecurity Capability Core Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8259A. https://doi.org/10.6028/NIST.IR.8259A.

[2] Fagan MJ, Marron JA, Brady KG, Jr., Cuthill BB, Megas K, Herold R (2021) IoT Non-Technical Supporting Capability Core Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8259B. https://doi.org/10.6028/NIST.IR.8259B.

[3] U.S. Energy Information Administration (2024) EIA expects U.S. annual solar electricity generation to surpass hydropower in 2024. Available at https://www.eia.gov/todayinenergy/detail.php?id=60922.

[4] Grassi PA, Newton EM, Perlner RA, Regenscheid AR, Fenton JL, Burr WE, Richer JP, Lefkovitz NB, Danker JM, Choong Y-Y, Greene KK, Theofanos MF (2017) Digital Identity Guidelines: Authentication and Lifecycle Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-63B. Includes updates as of March 02, 2020. https://doi.org/10.6028/NIST.SP.800-63B.

[5] CISA (2019) Choosing and Protecting Passwords | CISA. Available at https://www.cisa.gov/news-events/news/choosing-and-protecting-passwords.

[6] Brennan B, Smith K (2021) FBI Tech Tuesday: Strong Passphrases and Account Protection. Federal Bureau of Investigation. Available at https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-tech-tuesday-strong-passphrases-and-account-protection.

[7] Fagan MJ, Megas KN, Scarfone KA, Smith M (2020) Foundational Cybersecurity Activities for IoT Device Manufacturers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8259. https://doi.org/10.6028/NIST.IR.8259.

[8] Fagan M, Megas KN, Watrobski P, Marron J, Cuthill B (2022) Profile of the IoT Core Baseline for Consumer IoT Products. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8425. https://doi.org/10.6028/NIST.IR.8425.

[9] Fagan MJ, Megas KN, Marron JA, Brady KG, Jr., Cuthill BB, Herold R, Lemire D, Hoehn B (2021) IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-213A. https://doi.org/10.6028/NIST.SP.800-213A.

[10] Joint Task Force (2022) Assessing Security and Privacy Controls in Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 5. https://doi.org/10.6028/NIST.SP.800-53Ar5.

[11] National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. (National Institute of Standards and Technology, Gaithersburg,

MD) NIST Cybersecurity White Paper (CSWP) NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29.

[12] CIS (2021) CIS Critical Security Controls® v8. Available at https://www.cisecurity.org/controls/v8.

[13] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-53r5. Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5.

[14] MITRE, MITRE ATT&CK®. Available at https://attack.mitre.org.

[15] International Society of Automation/International Electrotechnical Commission (2009) *ISA/IEC 62443-2-1-2009 Security for Industrial Automation and Control Systems Part 2-1: Establishing an industrial automation and control system security program*. Available at https://webstore.ansi.org/search/find?in=1&st=ANSI%2FISA-62443-2-1+%2899.02.01%29-2009.

Appendix A. Additional Resources

- NERC (2023) Electric Vehicle Dynamic Charging Performance Characteristics during Bulk Power System Disturbances. Available at https://www.nerc.com/comm/RSTC/Documents/Grid_Friendly_EV_Charging_Recommendations.pdf
- Center for Internet Security CIS Controls Version 8. Available at https://www.cisecurity.org/controls/v8
- National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 6. https://doi.org/10.6028/NIST.CSWP.6
- NIST (2019) National Vulnerability Database – Home. Available at https://nvd.nist.gov/
- P. Ruggiero and M. Heckathorn (2012) Data Backup Options. Available at https://www.cisa.gov/sites/default/files/publications/data_backup_options.pdf
- M. Wilson (2022) Why solar 'tripping' is a grid threat for renewables. E&E News. Available at https://www.eenews.net/articles/why-solar-tripping-is-a-grid-threat-for-renewables/
- National Security Agency (2023) Best Practices for Securing Your Home Network, Version 1.0. (National Security Agency, Ft. Meade, MD). Available at https://media.defense.gov/2023/Feb/22/2003165170/-1/-1/0/CSI_BEST_PRACTICES_FOR_SECURING_YOUR_HOME_NETWORK.PDF
- U.S. Energy Information Administration (2020) Solar generation was 3% of U.S. electricity in 2020, but we project it will be 50% by 2050. Available at U.S. Energy Information Administration - EIA - Independent Statistics and Analysis
- U.S. Department of Energy (2023) Cyber-Informed Engineering Implementation Guide Version 1.0. Available at https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_67122.pdf

Appendix B. List of Symbols, Abbreviations, and Acronyms

AC
Alternating Current

CIS
Center for Internet Security

CISA
Cybersecurity and Infrastructure Security Agency

DC
Direct Current

FBI
Federal Bureau of Investigation

IoT
Internet of Things

ISA/IEC
International Society of Automation/International Electrotechnical Commission

ISP
Internet Service Provider

NCCoE
National Cybersecurity Center of Excellence

NIST
National Institute of Standards and Technology

NIST IR
NIST Interagency or Internal Report

NVD
National Vulnerability Database

RBAC
Role-Based Access Control

SBOM
Software Bill of Material

USB
Universal Serial Bus

US-CERT
United States Computer Emergency Readiness Team

VPN
Virtual Private Network

Appendix C. Residential and Light Commercial Solar Energy System Setup Cybersecurity Checklist

	Action	Notes
Guideline #1 – Change Default Passwords and Credentials	□ Change default or device-specific passwords to unique, secure passwords	
	□ Change other default credentials to unique, secure values	
	□ Use MFA, if available	
Guideline #2 – Use Role-Based Access Control (RBAC)	□ Create user accounts	
	□ Create user roles	
	□ Assign user accounts to roles	
	□ Disable unused accounts	
Guideline #3 – Configure the Recording of Events in a Log	□ Enable and configure logging	
	□ Setup external location for logs	
Guideline #4 – Update Software Regularly	□ Download and verify newest software/firmware version	
	□ Update device with current software/firmware version	
Guideline #5 – Backup and Restore System Information	□ Download device configuration	
	□ Download all available configurations	
	□ Store configuration in retrievable location	
Guideline #6 – Disable Unused Features	□ Disable unused interfaces, features, etc.	
	□ Enable security features	
Guideline #7 – Protect the Communications Connections	□ Device is isolated from a personal network	

Appendix D. Smart-Inverter Testing

Five smart inverters were analyzed to determine their ability to support the cybersecurity guidelines presented in Sec. 2. This testing was performed in Fall 2022 with smart inverters that were commercially available at that time. Testing was conducted in one of two ways: Examine and Test.

- Examine reviewed publicly available documentation to determine whether it was possible to implement the recommendation.
- Tests used interactions with an inverter through one of its communication interfaces to determine whether the guidelines could be implemented.[10]

Each tested inverter implemented one of three connection methods:

1. **Direct connection to the inverter.** This interface method requires the inverter itself to be capable of implementing all of the cybersecurity guidelines.
2. **Gateway device connection to the inverter.** This interface method allows the gateway device to implement some of the cybersecurity guidelines.
3. **Cloud-based service connection to the inverter.** Cloud-based services typically connected to an inverter through a gateway device. This interface method allows for implementation of the cybersecurity guidelines to be distributed among the inverter, the gateway device, and the cloud-based service.

For gateway device connections and cloud-based service connections, testing did not determine which components of the connection implemented the cybersecurity guidelines (see Fig. 11).

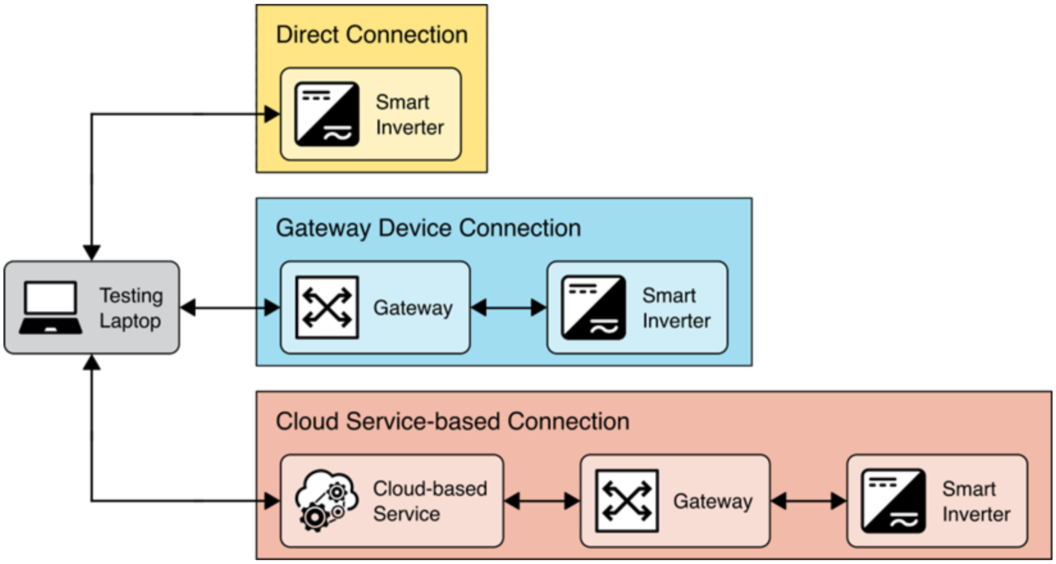


Fig. 11. Inverter connection methods

[10] SP 800-53Ar5 [10] provides additional information on testing methods.

Table 3. Characteristics of tested inverters

System	Inverter Size[11]	External Gateway[12]	Cloud Connectivity[13]
Inverter A	5.5 kW	Yes	Yes
Inverter B	5.5 kW	Yes	No
Inverter C	10.5 kW	Yes	Yes
Inverter D	5 kW	Yes	Yes
Inverter E	15 kW	No	No

D.1. Testing Results for Guideline #1: Change Default Passwords and Credentials

This test verified a smart-inverter's ability to identify all default accounts and change the default credentials associated with those accounts to a unique, secure credential. This test was considered passed if:

- The vendor documentation identified all default account credentials
- All default account credentials could be changed
- The inverter supported MFA

Table 4. Guideline #1 testing results

Inverter	Default Accounts in Vendor Documentation [#]	Identified Default Accounts on Device [#]	Ability to Change Credentials [Yes/No]	Ability to implement MFA [Yes/No]
A	3	3	Yes	No
B	2	2	Yes	No
C	NA[14]	NA	Yes	No
D	NA	NA	Yes	No
E	2	2	Yes	No

D.2. Testing Results for Guideline #2: Use Role-Based Access Control

This test verified a smart-inverter's ability to manage access to features and capabilities using RBAC. Three levels of access control were identified for smart inverters:

1. **Level 1 — Basic.** The smart inverter provides a single user account. The ability to log in to the single user account provides access to all smart-inverter features and capabilities.
2. **Level 2 — Role Account.** The smart inverter provides a single account per defined role, such as Installer, Maintainer, or Owner. The role account credential is shared with people who are authorized to act in that role. The ability to log in to a role account provides access to all features and capabilities associated with that role.

[11] This refers to the rated size of the inverter.
[12] The inverter has an external system that serves as a gateway to access and potentially control the inverter.
[13] The system is designed to support a cloud service to monitor and potentially control the system.
[14] "NA" means that the smart inverter does not utilize traditional accounts. It is configured through a cell phone application that connects via a wireless access point or by using the smart inverter's front panel.

3. **Level 3 — RBAC.** The smart inverter provides the capability to define a collection of roles and associated access permissions. Users are granted access by assigning their accounts to those defined roles.

This test assessed the level of access control supported by the inverter.

Table 5. Guideline #2 testing results

Inverter	Access Control Level Supported
A	Level 3
B	Level 2
C	Level 3
D	Level 3
E	Level 2

Some level of access control based on roles was supported by all five of the smart inverters tested. Most smart inverters supported an “administrator/installer” account/role and a “user” account/role. Some smart inverters also supported a “Guest” account/role.

D.3. Testing Results for Guideline #3: Configure the Recording of Events in a Log

This test verified a smart-inverter’s ability to record security-relevant events in a log and periodically export them to an external source.

This test was considered passed if the device could:

- Record the following security-related events in its log:
  - Successful login
  - Failed login
  - Configuration changes
  - Firmware updates
  - Events, including network connections
- Export the logs to an external source

Table 6. Guideline #3 testing results

Inverter	Supports Logging	Support Security-Related Event Logging
A	Yes	No
B	Yes	No
C	Yes	No
D	Yes	No
E	Yes	Yes

While all of the tested devices supported logging, most of their logging capabilities focused on the functions related to inverter operation (e.g., power output, grid connectivity) and provided little security-related information. Only one of the tested smart inverters fully supported the test criteria.

D.4. Testing Results for Guideline #4: Update Software Regularly

This test verified a smart-inverter's ability to update its software in both the setup and maintenance life cycle phases.

This test was considered passed if:

- The smart inverter had a mechanism to perform software updates.
- The smart-inverter manufacturer provided software updates.
- The integrity of software updates provided to the smart inverter was protected and verifiable.

Table 7. Guideline #4 testing results

Inverter	Fully Supports Software Update
A	Yes
B	Yes
C	Yes
D	Yes
E	Yes

All five of the tested smart inverters provided a complete mechanism to perform software updates. The mechanism varied among the smart-inverter vendors and included web-based interfaces, custom update applications, and pushed updates from cloud services.

D.5. Testing Results for Guideline #5: Back Up System Information

This test verified a smart-inverter's ability to back up and store smart-inverter configurations in a separate location and install a pre-built configuration or restore a configuration from a backup.

This test was considered passed if the smart inverter could:

- Back up its configuration to a separate location
- Restore its configuration from a backup

Table 8. Guideline #5 testing results

Inverter	Supports Configuration Backup	Supports Configuration Restore
A	Yes	Yes
B	No	No
C	No	No
D	No	No
E	No	No

Only one of the tested smart inverters supported backing up and restoring device configurations.

D.6. Testing Results for Guideline #6: Disable Unused Features

This test verified a smart-inverter's ability to enable only those features and capabilities required in a particular deployment. The smart inverter should be able to enable or disable features and capabilities that are not required in all operating conditions.

This test was considered passed if:

- The smart inverter has the ability to disable unused interfaces.
- The smart inverter has the ability to disable unused features and capabilities.

Table 9 Guideline #6 Testing Results

Inverter	Can Disable Functions
A	Yes, Modbus interface
B	Yes, Modbus and Web Server interfaces
C	No
D	No
E	No

Only two of the tested inverters had the ability to disable interfaces, features, and capabilities.

D.7. Testing Results for Guideline #7: Protect Communications Connections

This test verified whether a smart inverter could be located on a different network than personal devices (i.e., a device's ability to operate on a dedicated network).

This test was considered passed if the smart inverter supported:

- An Ethernet or Wi-Fi connection
- A secondary network (e.g., cellular) connection

Table 10. Guideline #7 testing results

Inverter	Connection Type
A	Ethernet
B	Ethernet
C	4G
D	4G
E	Ethernet

Only two of the tested smart inverters supported a cellular network connection, but they did not support Ethernet connectivity. Rather, they used a Wi-Fi access point or the smart-inverter's control panel to configure their cellular connection. The ability to segment an Ethernet network or establish a dedicated Wi-Fi network for smart-inverter connectivity was a function of the network infrastructure and did not depend on smart-inverter capabilities.

Appendix E. Mapping to General Cybersecurity Guidance

This appendix provides mappings between general cybersecurity guidance and the guidelines for installing and operating smart inverters presented in Sec. 2.

E.1. General Cybersecurity Guidance That Informs the Guidelines

Six cybersecurity guidance sources informed the development of these guidelines and recommendations:

1. NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF)
2. Center for Internet Security Critical Security Controls (CSC) v8
3. SP 800-53r5 (Revision 5)
4. SP 800-213A
5. MITRE ATT&CK Framework
6. ISA/IEC 62443

E.1.1. NIST Cybersecurity Framework

The NIST Cybersecurity Framework Version 2.0 (CSF 2.0) [11] provides a taxonomy of cybersecurity outcomes that can help manage cybersecurity risks. The components of the taxonomy are a hierarchy of Functions, Categories, and Subcategories that detail each outcome. The guidelines in this report are mapped to the Subcategories of the CSF to illustrate the contribution of each guideline to achieving cybersecurity outcomes.

E.1.2. Center for Internet Security Critical Security Controls (CSC) Version 8

The Center for Internet Security (CIS) Critical Security Controls (CSC) version 8 [12] describes 18 prioritized controls for securing small to large enterprises. Each control is presented with implementation guidelines for enterprises of different scales as well as overview information on controls, criticality, procedures for implementation, and safeguard descriptions. CSC Version 8 also includes mappings to the NIST Framework for Improving Critical Infrastructure Cybersecurity V1.1 to align with matching controls.

E.1.3. NIST SP 800-53r5

SP 800-53r5 [13] identifies 20 control families that address security and privacy risks within an organization. These controls include potential impact levels to help those with oversight responsibilities establish implementation strategies that are mandatory for federal information systems and applicable to organizations outside of the federal sphere.

E.1.4. NIST SP 800-213A

NIST's Cybersecurity for the Internet of Things (IoT) program supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed. By collaborating with stakeholders across government, industry, international bodies, and academia, the program aims to cultivate trust and foster an environment that enables innovation on a global scale. NIST's Cybersecurity for IoT program has defined a baseline set of capabilities in IR 8259A [1] and IR 8259B [2] that manufacturers should consider integrating into their IoT devices and that consumers should consider enabling/configuring in those devices.

Device cybersecurity capabilities are cybersecurity features or functions that IoT devices provide through their own technical means (i.e., device hardware and software). Non-technical supporting capabilities are actions that a manufacturer or third-party organization performs in support of the cybersecurity of an IoT device (e.g., providing information about software updates, instructions for configuration settings, and supply chain information). Used together, device cybersecurity capabilities and non-technical supporting capabilities can help mitigate cybersecurity risks related to the use of IoT devices while assisting customers in achieving their goals.

NIST's Cybersecurity for IoT Team has also published a larger catalog of device cybersecurity capabilities and non-technical supporting capabilities in SP 800-213A [9]. The capabilities in this catalog are derived from security controls in SP 800-53r5 [13] and include standardized identifiers for easy referencing within the catalog.

Table 11 maps the smart-inverter cybersecurity guidelines to device cybersecurity capabilities and non-technical supporting capabilities in SP 800-213A. Selecting devices and manufacturers that provide these capabilities can support the achievement of the guidelines.

E.1.5. MITRE ATT&CK Framework

The MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework [14] describes adversarial methods and behaviors across the life cycle of a cybersecurity event. It was developed based on observed tactics, techniques, and procedures (TTPs) from advanced persistent threats (APTs) against Microsoft Windows enterprise networks. ATT&CK consists of four core components: tactics, techniques, sub-techniques, and documented adversary usage of those techniques and procedures. Each procedure presented in the ATT&CK matrix describes tactics, techniques, examples, mitigation strategies, and detection strategies.

E.1.6. ISA/IEC 62443-2-1

ISA/IEC 62443*, Security for Industrial Automation and Control Systems* (IACS) [15], is a collection of standards that address the requirements and methods for managing the cybersecurity of control systems and operational technology. The standards are organized in four layers: general, policy and procedures, system, and component. ISA-62443-2-1 defines requirements for security programs that consist of implementing and maintaining procedural, personnel, and technology-based capabilities that may reduce the cybersecurity risks of industrial automation and control systems (IACSs). The security program requirements in this document are intended to mitigate risk by addressing vulnerabilities. Failure to meet the requirements can result in the presence of such vulnerabilities.

E.2. Guidelines Relationship to General Cybersecurity Guidance

Table 11. Mapping between cybersecurity guidance documents and guidelines for installation and operation

CSF 2.0 Subcategory	CSC v8	SP 800-53r5	SP 800-213A	MITRE ATT&CK Mitigation	62443-2-1
Guideline 1: Change Default Passwords and Credentials					
PR.AA-05	4.7 5.2	Access Enforcement [AC-3]	DC: PRV(1), AUT(1), INT(1), CTL(4d) LA: AUN(1), AUN(2), ACF(2) DO: SMP(5b,c,e), MNT(1g) EA: CSC(2c), CSC(3a,b,c), RSP(1, g)	Access Management [M0801] Password Policies [M0927]	USER 1.11
Guideline 2: Use Role-Based Access Control					
PR.AA-05 PR.AA-03 PR.AT-02	5.1 5.4 6.8	Access Enforcement [AC-3]	DC: PRV(1), AUT(1), LA: ROL(1), ROL(2), ROL(3), ROL(4), ROL(5), ROL(6), ROL(8), ROL(9) DO: SMP(3b), SMP(5j, k.l), DSC(4b), MNT(1g) EA: CSC(2c), CSC(3a, b,c), RSP(1d,e,f,g,h)	Privileged Account Management [M1026] User Account Management [M1018]	USER 1.5 USER 1.8
Guideline 3: Configure the Recording of Events in a Log					
PR.PS-04	8.2	Event Logging [AU-2]	DI: AID(2) CS: AEI(2), EIM(1), EIM(2), EIM(3), LCT(1), RDL(1), RDL(2), RDL(3), RDL(4), RDL(5), RDL(6), LSR(1), LSR(2), LSR(3), LSR(4), SRT(1), SRT(2), SRT(3), SRT(4), AUP(3), AUP(4), AUP(7) DS: OPS(1) DO: SMP(8) ID: CRI(7b)	Remote Data Storage [M1029]	EVENT 1.1
Guideline 4: Update Software Regularly					
PR.DS-10	7.3	Flaw Remediation [SI-2]	DI: AID(3), DP: CRY(3), CRY(4), CRY(5), STX(3) SU: UPD(1), UPD(6), APP(1). APP(2), APP(3) DO: SMP(12), IQ: BUG(1a,b,c,d,e) ID: CRI(1a,b,c), CRI(2a,c), CRI(3a,b,c)	Update Software [M0951]	COMP 3.1 COMP 3.2

CSF 2.0 Subcategory	CSC v8	SP 800-53r5	SP 800-213A	MITRE ATT&CK Mitigation	62443-2-1
			EA: CSC(4a,b), EOL(1a,b), VMG(2a,b)		
Guideline 5: Back Up System Information					
ID.AM-03 PR.IR-03 RC.RP-01	11.1 11.2	System Backup [CP-9] System Recovery & Reconstitution [CP-10]	DC: CTL(2) DP: STO(3) EA: BAK(1a,b,c)	Data Backup [M0953]	AVAIL 1.1 AVAIL 2.5
Guideline 6: Disable Unused Features					
ID.AM-01 ID.AM-02	2.1 4.8	Baseline Configuration [CM-2] Least Functionality [CM-7]	DC: CTL(1), CTL(2) LA: IFC(2), IFC(3), IFC(6) DS: OPS(8) DO: SMP(10) EA: EXP(1)	Software Configuration [M0954] Disable or Remove Feature or Program [M0942] Limit Software Installation [M1033]	CM 1.1 COMP 1.1
Guideline 7: Protect Communications Connections					
PR.IR-01	12.2	Boundary Protection [SC-7]	DS: COM(1) DO: SMP(5h)	Network Segmentation [M0930]	NET 1.1

Appendix F. Smart Inverter Vulnerability Survey

The NVD was reviewed in early 2022 to better understand known cybersecurity vulnerabilities that have been identified in smart inverters. Table 12 was created from several point-in-time searches of the NVD that used both generic (e.g., solar, inverter, photovoltaic) and manufacturer-specific keywords. The entries in the table are a subset of applicable Common Vulnerabilities and Exposures (CVEs) from the NVD. This research identified real cybersecurity concerns that the guidelines should address.

Table 12. Smart inverter vulnerability survey

ID	Vuln ID	Summary	Published	CVSS v3 Severity
1	CVE-2019-19229	admincgi-bin/service.fcgi on Fronius Solar Inverter devices before 3.14.1 (HM 1.12.1) allows action=download&filename= Directory Traversal.	4-Dec-19	V3.1: 6.5 MEDIUM
2	CVE-2019-19228	Fronius Solar Inverter devices before 3.14.1 (HM 1.12.1) allow attackers to bypass authentication because the password for the today account is stored in the /tmp/web_users.conf file.	4-Dec-19	V3.1: 9.8 CRITICAL
3	CVE-2018-12927	Northern Electric & Power (NEP) inverter devices allow remote attackers to obtain potentially sensitive information via a direct request for the nep/status/index/1 URI.	28-Jun-18	V3.0: 7.5 HIGH
4	CVE-2018-12735	SAJ Solar Inverter allows remote attackers to obtain potentially sensitive information via a direct request for the inverter_info.htm or english_main.htm URI.	25-Jun-18	V3.0: 7.5 HIGH
5	CVE-2017-9863	** DISPUTED ** An issue was discovered in SMA Solar Technology products. If a user simultaneously has Sunny Explorer running and visits a malicious host, cross-site request forgery can be used to change settings in the inverters (for example, issuing a POST request to change the user password). All Sunny Explorer settings available to the authenticated user are also available to the attacker. (In some cases, this also includes changing settings that the user has no access to.) This may result in complete compromise of the device. NOTE: The vendor reports that exploitation is unlikely because Sunny Explorer is used only rarely. Also, only Sunny Boy TLST-21 and TL-21 and Sunny Tripower TL-10 and TL-30 could potentially be affected.	5-Aug-17	V3.0: 8.8 HIGH

ID	Vuln ID	Summary	Published	CVSS v3 Severity
6	CVE-2017-9860	** DISPUTED ** An issue was discovered in SMA Solar Technology products. An attacker can use Sunny Explorer or the SMAdata2+ network protocol to update the device firmware without ever having to authenticate. If an attacker can create a custom firmware version that is accepted by the inverter, the inverter is compromised completely. This allows the attacker to do nearly anything: for example, giving access to the local OS, creating a botnet, using the inverters as a steppingstone into companies, etc. NOTE: the vendor reports that this attack has always been blocked by "a final integrity and compatibility check." Also, only Sunny Boy TLST-21 and TL-21 and Sunny Tripower TL-10 and TL-30 could potentially be affected.	5-Aug-17	V3.0: 9.8 CRITICAL
7	CVE-2017-9859	** DISPUTED ** An issue was discovered in SMA Solar Technology products. The inverters make use of a weak hashing algorithm to encrypt the password for REGISTER requests. This hashing algorithm can be cracked relatively easily. An attacker will likely be able to crack the password using offline crackers. This cracked password can then be used to register at the SMA servers. NOTE: the vendor's position is that "we consider the probability of the success of such manipulation to be extremely low." Also, only Sunny Boy TLST-21 and TL-21 and Sunny Tripower TL-10 and TL-30 could potentially be affected.	5-Aug-17	V3.0: 9.8 CRITICAL
8	CVE-2017-9858	** DISPUTED ** An issue was discovered in SMA Solar Technology products. By sending crafted packets to an inverter and observing the response, active and inactive user accounts can be determined. This aids in further attacks (such as a brute force attack) as one now knows exactly which users exist and which do not. NOTE: the vendor's position is that this "is not a security gap per se." Also, only Sunny Boy TLST-21 and TL-21 and Sunny Tripower TL-10 and TL-30 could potentially be affected.	5-Aug-17	V3.0: 7.5 HIGH
9	CVE-2017-9855	** DISPUTED ** An issue was discovered in SMA Solar Technology products. A secondary authentication system is available for Installers called the Grid Guard system. This system uses predictable codes, and a single Grid Guard code can be used on any SMA inverter. Any such code, when combined with the installer account, allows changing very sensitive parameters. NOTE: the vendor reports that Grid Guard is not an authentication feature; it is only a tracing feature. Also, only Sunny Boy TLST-21 and TL-21 and Sunny Tripower TL-10 and TL-30 could potentially be affected.	5-Aug-17	V3.0: 9.8 CRITICAL
10	CVE-2017-9853	** DISPUTED ** An issue was discovered in SMA Solar Technology products. All inverters have a very weak password policy for the user and installer password. No complexity requirements or length requirements are set. Also, strong passwords are impossible due to a maximum of 12 characters and a limited set of characters. NOTE: the vendor reports that the 12-character limit provides "a very high security standard." Also, only Sunny Boy TLST-21 and TL-21 and Sunny Tripower TL-10 and TL-30 could potentially be affected.	5-Aug-17	V3.0: 9.8 CRITICAL

ID	Vuln ID	Summary	Published	CVSS v3 Severity
11	CVE-2012-5861	Multiple SQL injection vulnerabilities on the Sinapsi eSolar Light Photovoltaic System Monitor (aka Schneider Electric Ezylog photovoltaic SCADA management server), Sinapsi eSolar, and Sinapsi eSolar DUO with firmware before 2.0.2870_2.2.12 allow remote attackers to execute arbitrary SQL commands via (1) the inverterselect parameter in a primo action to dettagliinverter.php or (2) the lingua parameter to changelanguagesession.php.	23-Nov-12	N/A
12	CVE-2019-13529	An attacker could send a malicious link to an authenticated operator, which may allow remote attackers to perform actions with the permissions of the user on the Sunny WebBox Firmware Version 1.6 and prior. This device uses IP addresses to maintain communication after a successful login, which would increase the ease of exploitation.	9-Oct-19	V3.1: 8.8 HIGH
13	CVE-2017-9864	** DISPUTED ** An issue was discovered in SMA Solar Technology products. An attacker can change the plant time even when not authenticated in any way. This changes the system time, possibly affecting lockout policies and random-number generators based on timestamps and makes timestamps for data analysis unreliable. NOTE: the vendor reports that this is largely irrelevant because it only affects log-entry timestamps, and because the plant time would later be reset via NTP. (It has never been the case that a lockout policy or random-number generator was affected.) Also, only Sunny Boy TLST-21 and TL-21 and Sunny Tripower TL-10 and TL-30 could potentially be affected.	5-Aug-17	V3.0: 7.5 HIGH
14	CVE-2017-9862	** DISPUTED ** An issue was discovered in SMA Solar Technology products. When signed into Sunny Explorer with a wrong password, it is possible to create a debug report, disclosing information regarding the application and allowing the attacker to create and save a .txt file with contents to his liking. An attacker may use this for information disclosure, or to write a file to normally unavailable locations on the local system. NOTE: the vendor reports that "the information contained in the debug report is of marginal significance." Also, only Sunny Boy TLST-21 and TL-21 and Sunny Tripower TL-10 and TL-30 could potentially be affected.	5-Aug-17	V3.0: 7.5 HIGH

ID	Vuln ID	Summary	Published	CVSS v3 Severity
15	CVE-2017-9861	** DISPUTED ** An issue was discovered in SMA Solar Technology products. The Session Initiation Protocol (SIP) implementation does not properly use authentication with encryption: it is vulnerable to replay attacks, packet injection attacks, and man in the middle attacks. An attacker can successfully use SIP to communicate with the device from anywhere within the Local Area Network (LAN). An attacker may use this to crash the device, stop it from communicating with the SMA servers, exploit known SIP vulnerabilities, or find sensitive information from the SIP communications. Furthermore, because the SIP communication channel is unencrypted, an attacker capable of understanding the protocol can eavesdrop on communications. For example, passwords can be extracted. NOTE: the vendor's position is that authentication with encryption is not required on an isolated subnetwork. Also, only Sunny Boy TLST-21 and TL-21 and Sunny Tripower TL-10 and TL-30 could potentially be affected.	5-Aug-17	V3.0: 9.8 CRITICAL
16	CVE-2017-9857	** DISPUTED ** An issue was discovered in SMA Solar Technology products. The SMAdata2+ communication protocol does not properly use authentication with encryption: it is vulnerable to man in the middle, packet injection, and replay attacks. Any setting change, authentication packet, scouting packet, etc., can be replayed, injected, or used for a man in the middle session. All functionalities available in Sunny Explorer can effectively be done from anywhere within the network if an attacker gets the packet setup correctly. This includes the authentication process for all (including hidden) access levels and the changing of settings in accordance with the gained access rights. Furthermore, because the SMAdata2+ communication channel is unencrypted, an attacker capable of understanding the protocol can eavesdrop on communications. NOTE: the vendor's position is that authentication with encryption is not required on an isolated subnetwork. Also, only Sunny Boy TLST-21 and TL-21 and Sunny Tripower TL-10 and TL-30 could potentially be affected.	5-Aug-17	V3.0: 8.1 HIGH
17	CVE-2017-9856	** DISPUTED ** An issue was discovered in SMA Solar Technology products. Sniffed passwords from SMAdata2+ communication can be decrypted very easily. The passwords are "encrypted" using a very simple encryption algorithm. This enables an attacker to find the plaintext passwords and authenticate to the device. NOTE: the vendor reports that only Sunny Boy TLST-21 and TL-21 and Sunny Tripower TL-10 and TL-30 could potentially be affected.	5-Aug-17	V3.0: 9.8 CRITICAL
18	CVE-2017-9854	** DISPUTED ** An issue was discovered in SMA Solar Technology products. By sniffing for specific packets on the localhost, plaintext passwords can be obtained as they are typed into Sunny Explorer by the user. These passwords can then be used to compromise the overall device. NOTE: the vendor reports that exploitation likelihood is low because these packets are usually sent only once during installation. Also, only Sunny Boy TLST-21 and TL-21 and Sunny Tripower TL-10 and TL-30 could potentially be affected.	5-Aug-17	V3.0: 9.8 CRITICAL

ID	Vuln ID	Summary	Published	CVSS v3 Severity
19	CVE-2017-9852	** DISPUTED ** An Incorrect Password Management issue was discovered in SMA Solar Technology products. Default passwords exist that are rarely changed. User passwords will almost always be default. Installer passwords are expected to be default or similar across installations installed by the same company (but are sometimes changed). Hidden user accounts have (at least in some cases, though more research is required to test this for all hidden user accounts) a fixed password for all devices; it can never be changed by a user. Other vulnerabilities exist that allow an attacker to get the passwords of these hidden user accounts. NOTE: the vendor reports that it has no influence on the allocation of passwords, and that global hardcoded master passwords do not exist. Also, only Sunny Boy TLST-21 and TL-21 and Sunny Tripower TL-10 and TL-30 could potentially be affected.	5-Aug-17	V3.0: 9.8 CRITICAL
20	CVE-2017-9851	** DISPUTED ** An issue was discovered in SMA Solar Technology products. By sending nonsense data or setting up a TELNET session to the database port of Sunny Explorer, the application can be crashed. NOTE: the vendor reports that the maximum possible damage is a communication failure. Also, only Sunny Boy TLST-21 and TL-21 and Sunny Tripower TL-10 and TL-30 could potentially be affected.	5-Aug-17	V3.0: 7.5 HIGH
21	CVE-2015-3964	SMA Solar Sunny WebBox has hardcoded passwords, which makes it easier for remote attackers to obtain access via unspecified vectors.	11-Sep-15	V3.x:(not available)
22	CVE-2018-7797	A URL redirection vulnerability exists in Power Monitoring Expert, Energy Expert (formerly Power Manager) - EcoStruxure Power Monitoring Expert (PME) v8.2 (all editions), EcoStruxure Energy Expert 1.3 (formerly Power Manager), EcoStruxure Power SCADA Operation (PSO) 8.2 Advanced Reports and Dashboards Module, EcoStruxure Power Monitoring Expert (PME) v9.0, EcoStruxure Energy Expert v2.0, and EcoStruxure Power SCADA Operation (PSO) 9.0 Advanced Reports and Dashboards Module, which could cause a phishing attack when redirected to a malicious site.	17-Dec-18	V3.0: 6.1 MEDIUM
23	CVE-2012-5864	The management web pages on the Sinapsi eSolar Light Photovoltaic System Monitor (aka Schneider Electric Ezylog photovoltaic SCADA management server), Sinapsi eSolar, and Sinapsi eSolar DUO with firmware before 2.0.2870_2.2.12 do not require authentication, which allows remote attackers to obtain administrative access via a direct request, as demonstrated by a request to ping.php.	23-Nov-12	V3.x:(not available)
24	CVE-2012-5863	ping.php on the Sinapsi eSolar Light Photovoltaic System Monitor (aka Schneider Electric Ezylog photovoltaic SCADA management server), Sinapsi eSolar, and Sinapsi eSolar DUO with firmware before 2.0.2870_2.2.12 allows remote attackers to execute arbitrary commands via shell metacharacters in the ip_dominio parameter.	23-Nov-12	V3.x:(not available)

ID	Vuln ID	Summary	Published	CVSS v3 Severity
25	CVE-2012-5862	login.php on the Sinapsi eSolar Light Photovoltaic System Monitor (aka Schneider Electric Ezylog photovoltaic SCADA management server), Sinapsi eSolar, and Sinapsi eSolar DUO with firmware before 2.0.2870_2.2.12 establishes multiple hardcoded accounts, which makes it easier for remote attackers to obtain administrative access by leveraging a (1) cleartext password or (2) password hash contained in this script, as demonstrated by a password of astridservice or 36e44c9b64.	23-Nov-12	V3.x:(not available)
26	CVE-2012-5861	Multiple SQL injection vulnerabilities on the Sinapsi eSolar Light Photovoltaic System Monitor (aka Schneider Electric Ezylog photovoltaic SCADA management server), Sinapsi eSolar, and Sinapsi eSolar DUO with firmware before 2.0.2870_2.2.12 allow remote attackers to execute arbitrary SQL commands via (1) the inverterselect parameter in a primo action to dettagliinverter.php or (2) the lingua parameter to changelanguagesession.php.	23-Nov-12	V3.x:(not available)
27	CVE-2017-6019	An issue was discovered in Schneider Electric Conext ComBox, model 865-1058, all firmware versions prior to V3.03 BN 830. A series of rapid requests to the device may cause it to reboot.	7-Apr-17	V3.0: 7.5 HIGH
28	CVE-2021-33209	An issue was discovered in Fimer Aurora Vision before 2.97.10. The response to a failed login attempt discloses whether the username or password is wrong, helping an attacker to enumerate usernames. This can make a brute-force attack easier.	3-Nov-21	V3.1: 5.3 MEDIUM
29	CVE-2021-33210	An issue was discovered in Fimer Aurora Vision before 2.97.10. An attacker can (in the WebUI) obtain plant information without authentication by reading the response of APIs from a kiosk view of a plant.	11/3/2021	V3.1: 4.3 MEDIUM
30	CVE-2020-25755	An issue was discovered on Enphase Envoy R3.x and D4.x (and other current) devices. The upgrade_start function in /installer/upgrade_start allows remote authenticated users to execute arbitrary commands via the force parameter.	16-Jun-21	V3.1: 8.8 HIGH
31	CVE-2020-25754	An issue was discovered on Enphase Envoy R3.x and D4.x devices. There is a custom Pluggable Authentication Module (PAM) for user authentication that circumvents traditional user authentication. This module uses a password derived from the MD5 hash of the username and serial number. The serial number can be retrieved by an unauthenticated user at /info.xml. Attempts to change the user password via passwd or other tools have no effect.	16-Jun-21	V3.1: 7.5 HIGH
32	CVE-2020-25753	An issue was discovered on Enphase Envoy R3.x and D4.x devices with v3 software. The default admin password is set to the last 6 digits of the serial number. The serial number can be retrieved by an unauthenticated user at /info.xml.	16-Jun-21	V3.1: 9.8 CRITICAL

ID	Vuln ID	Summary	Published	CVSS v3 Severity
33	CVE-2020-25752	An issue was discovered on Enphase Envoy R3.x and D4.x devices. There are hardcoded web-panel login passwords for the installer and Enphase accounts. The passwords for these accounts are hardcoded values derived from the MD5 hash of the username and serial number mixed with some static strings. The serial number can be retrieved by an unauthenticated user at /info.xml. These passwords can be easily calculated by an attacker; users are unable to change these passwords.	16-Jun-21	V3.1: 5.3 MEDIUM
34	CVE-2019-7678	A directory traversal vulnerability was discovered in Enphase Envoy R3.*.* via images/, include/, include/js, or include/css on Transmission Control Protocol (TCP) port 8888.	9-Feb-19	V3.0: 9.8 CRITICAL
35	CVE-2019-7677	Cross-site Scripting (XSS) exists in Enphase Envoy R3.*.* via the profileName parameter to the /home URI on TCP port 8888.	9-Feb-19	V3.0: 6.1 MEDIUM
36	CVE-2019-7676	A weak password vulnerability was discovered in Enphase Envoy R3.*.*. One can login via TCP port 8888 with the admin password for the admin account.	9-Feb-19	V3.0: 7.2 HIGH
37	CVE-2021-20662	Missing authentication for critical function in SolarView Compact SV-CPT-MC310 prior to Ver.6.5 allows an attacker to alter the setting information without the access privileges via unspecified vectors.	24-Feb-21	V3.1: 7.5 HIGH
38	CVE-2021-20661	Directory traversal vulnerability in SolarView Compact SV-CPT-MC310 prior to Ver.6.5 allows authenticated attackers to delete arbitrary files and/or directories on the server via unspecified vectors.	24-Feb-21	V3.1: 8.1 HIGH
39	CVE-2021-20660	Cross-site scripting vulnerability in SolarView Compact SV-CPT-MC310 prior to Ver.6.5 allows an attacker to inject an arbitrary script via unspecified vectors.	24-Feb-21	V3.1: 6.1 MEDIUM
40	CVE-2021-20659	SolarView Compact SV-CPT-MC310 prior to Ver.6.5 allows an authenticated attacker to upload arbitrary files via unspecified vectors. If the file is PHP script, an attacker may execute arbitrary code.	24-Feb-21	V3.1: 8.8 HIGH
41	CVE-2021-20658	SolarView Compact SV-CPT-MC310 prior to Ver.6.5 allows an attacker to execute arbitrary OS commands with the web server privilege via unspecified vectors.	24-Feb-21	V3.1: 9.8 CRITICAL

ID	Vuln ID	Summary	Published	CVSS v3 Severity
42	CVE-2021-20657	Improper access control vulnerability in SolarView Compact SV-CPT-MC310 prior to Ver.6.5 allows an authenticated attacker to obtain and/or alter the setting information without the access privilege via unspecified vectors.	24-Feb-21	V3.1: 5.4 MEDIUM
43	CVE-2021-20656	Exposure of information through directory listing in SolarView Compact SV-CPT-MC310 prior to Ver.6.5 allows an authenticated attacker to obtain the information inside the system, such as directories and/or file configurations via unspecified vectors.	24-Feb-21	V3.1: 4.3 MEDIUM
44	CVE-2021-34544	An issue was discovered in Solar-Log 500 before 2.8.2 Build 52 23.04.2013. In /export.html, email.html, and sms.html, cleartext passwords are stored. This may allow sensitive information to be read by someone with access to the device.	7-Dec-21	V3.1: 6.5 MEDIUM
45	CVE-2021-34543	The web administration server in Solar-Log 500 before 2.8.2 Build 52 does not require authentication, which allows remote attackers to gain administrative privileges by connecting to the server. As a result, the attacker can modify configuration files and change the system status.	7-Dec-21	V3.1: 7.5 HIGH