Gap Analysis of Supply Chain Cybersecurity for Distributed Energy Resources

Ryan Cryar, Danish Saleem, Jordan Peterson, and William Hupp

National Renewable Energy Laboratory

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5R00-84752
February 2023

Gap Analysis of Supply Chain Cybersecurity for Distributed Energy Resources

Ryan Cryar, Danish Saleem, Jordan Peterson, and William Hupp

National Renewable Energy Laboratory

Suggested Citation
Cryar, Ryan, Danish Saleem, Jordan Peterson, and William Hupp. 2023. *Gap Analysis of Supply Chain Cybersecurity for Distributed Energy Resources*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-84752.
https://www.nrel.gov/docs/fy23osti/84752.pdf.

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5R00-84752
February 2023

National Renewable Energy Laboratory
15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

NOTICE

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Solar Energy Technologies Office The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government.

Acknowledgments

This work was funded by the U.S Department of Energy Solar Energy Technologies Office.

We thank all contributors who provided their valuable comments and feedback to this document, including, but not limited to, Samuel D. Chanoski (INL), Ron Brash (aDolus Technology), Jake Gentle (INL), Virginia L. Wright (INL), Marissa Morales-Rodriguez (DOE), Anthony Wallace (NREL), Steve Granda (NREL), and Jennifer Guerra (NREL).

List of Acronyms

ARIES	Advanced Research on Integrated Energy Systems
C2M2	Cybersecurity Capability Maturity Model
CECA	Clean Energy Cybersecurity Accelerator
CIP	Critical Infrastructure Protection
CISA	Cybersecurity & Infrastructure Security Agency
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
CyTRICS	Cyber Testing for Resilient Industrial Control Systems
DER	distributed energy resource
DER-CF	Distributed Energy Resource Cybersecurity Framework
DHS	U.S. Department of Homeland Security
DOC	U.S. Department of Commerce
DOE	U.S. Department of Energy
ENISA	European Union Agency for Cybersecurity
ES-C2M2	Electricity Subsector Cybersecurity Capability Maturity Model
HMAC	Hashed-based Message Authentication Code
IBR	inverter-based resource
ICS	industrial control system
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
NATF	North American Transmission Forum
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NREL	National Renewable Energy Laboratory
NVD	National Vulnerability Database
PLC	programmable logic controller
SBOM	software bill of materials

Executive Summary

Cybersecurity has an important impact on many aspects of the supply chain, from firmware arranged on chips, to software packages used at various points in the software development cycle. Equipment or software that has been compromised in the supply chain upstream of the ultimate owner-operator might lead to attacks, such as stealing or rerouting funds; denial of service; breaching confidential or proprietary information from a company, its customers, or its suppliers; ransomware that denies the operation of automated equipment for payment; and malicious control actions that could damage equipment and endanger personnel (Walker et al. 2021). One key area that that needs cybersecurity recommendations and guidance is the security of firmware and programmable logic controllers. To address supply chain vulnerabilities, on February 24, 2021, President Biden issued Executive Order 14017 on America's Supply Chains, which directed a whole-of-government approach to reviewing risks in and strengthening the resilience of supply chains supporting six industries that are critical to U.S. economic prosperity and national security (DOC and DHS 2022). This order directly impacts the renewable energy industry.

Within the realm of inverter-based resources (IBRs), large-scale photovoltaic plant operators face a scarcity of personnel with cybersecurity expertise to counter cyber threats and implement basic cyber hygiene to protect against weak passwords, outdated security software, and failure to frequently back up data. In the current landscape, the supply chain cybersecurity of distributed energy resources (DERs) lacks a nationally adopted and federally accredited standard. Currently, manufacturers and asset owners of DERs and IBRs can refer to other general standards for cybersecurity best practices, but the supply chain is a new space that needs specific recommendations and guidance. Relevant work is being done in the supply chain cybersecurity space that can be identified and leveraged to inform DER supply chain cybersecurity. In information technology, the U.S. Department of Homeland Security (DHS) created the Information and Communications Technology (ICT) Supply Chain Risk Management Task force, a public-private partnership sponsored by the Cybersecurity & Infrastructure Security Agency (CISA 2022). This task force was created to categorize, assess, and understand the risks of ICT components that could be used to inform best practices for common DER components that are shared between the information technology and energy sectors. The reliance of industrial control systems on modern information technology solutions, including intellectual property-based networking and embedded computing, has raised serious security concerns (Basnight et al. 2013). In the energy sector, we can look to the North American Transmission Forum (NATF) Supply Chain Security Assessment Model to address supply chain risk management, but the model does not include specific DER recommendations.

With energy systems relying on large sets of complex code and numerous subcomponents, the risk of vulnerabilities in downstream software supply chain is high. The heterogenous, distributed systems that are operating across DERs can make it difficult to pinpoint a possible attack that comes through a microcontroller that has tampered firmware via an unauthorized patch from the supplier's supply chain.

We analyzed the current landscape of DER supply chain cybersecurity, formulated an ideal state, and documented gaps and opportunities in the supply chain currently available to the renewable energy sector:

- **Establish a framework for DER supply chain cybersecurity**: This gap can be bridged by adapting the ICT framework to DER supply chain cybersecurity while being influenced by the current cybersecurity frameworks and models, such as the Cybersecurity Capability Maturity Model (C2M2), NIST 800-161, and the NATF Supply Chain Security Assessment Model. Although many general frameworks exist, there can be concern of an overpopulation of frameworks to choose from, which could result in the further fragmentation of standards and homogenous expectations. An alternative to creating a new framework could be modifying an existing framework, such as the National Institute of Standards and Technology's (NIST's) Cybersecurity Framework or utilizing the Distributed Energy Resource Cybersecurity Framework (DER-CF) to support this modification.
- **Engage industry for assessments:** Identify industry stakeholders who could participate in voluntary assessments of their design practices and procedures to inform their own cybersecurity posture by helping to monitor, assess, and manage supply chain risks using quantitative results.
- **Create open-source software guidance:** Although open source is an attractive avenue for developing software, there are considerable risks that need to be addressed. Guidance is needed in the form of standards or best practices to understand the risks and how to mitigate them.
- **Establish a testing and certification ecosystem for DER software supply chain cybersecurity:** Take the lessons learned from Cyber Testing for Resilient Industrial Control Systems (CyTRICS) and the Clean Energy Cybersecurity Accelerator (CECA), which have their own testing methodologies, to develop a new testing ecosystem. Leverage the National Renewable Energy Laboratory's Advanced Research on Integrated Energy Systems (ARIES) to assess and understand mitigation techniques for the supply chain of the software provided. This will drive new partnerships, recommendations, certifications of products or components, and mitigation strategies for supply chain risks.
- **Address the issue of lacking standards for DER supply chain cybersecurity:** Establish a well-versed guidance document for DER supply chain cybersecurity through stakeholder engagement by leveraging subject matter experts in the solar industry after performing deep-dive investigations on available best practices, such as NIST's supply chain cybersecurity risk management and mitigation programs, the North American Electric Reliability Corporation's implementation plan for cybersecurity supply chain risk management (CIP-013-1), and supply chain security tools developed by national labs.
- **Form working groups for best practices:** Obtain industry feedback through a working group to move the current state of supply chain cybersecurity closer to the ideal. Identifying industry best practices, even if they are not made into a standard, can benefit the industry by providing optional recommendations to owner/operators/vendors/aggregators to improve their supply chain cybersecurity postures.

Table of Contents

List of Figures

List of Tables

1 Introduction

A supply chain comprises the ecosystem of resources needed to design, manufacture, and distribute a product (ENISA 2021). In the context of supply chain cybersecurity, the resources that directly influence this ecosystem include software, hardware, data, and/or other digital components. Compromised equipment or software in the supply chain could lead to attacks, such as financial loss; denial of service; breaching confidential or proprietary information from a company, its customers, or its suppliers; ransomware that denies the operation of automated equipment for payment; and malicious control actions that could damage equipment and endanger personnel (Walker et al. 2021).

Currently, 60.8% of U.S. energy comes from fossil fuels, 18.9% comes from nuclear, and the remaining 20.1% comes from renewable resources. Federal Energy Regulatory Commission Order 2222 and Executive Order 14017 are important milestones to help increase renewable resources to a level that can power the entire country and attain carbon neutrality by 2035. The quest to meet renewable energy goals, however, will require collaboration and coordination across electric sector stakeholders, especially to address supply chain cybersecurity concerns. For example, rooftop and small solar electricity production in the Western Interconnection is approximately 30,000 MW, representing approximately 65% of the deployed solar infrastructure, but none of these installations require following the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) reliability standards (Walker et al. 2022). A range of consequences from a successful cyberattack is possible in all cyber-physical energy systems—from the simple loss of power generation to the complete loss of the generating asset itself. It is important to realize that not all distribution cyberattacks are bounded geographically. Failure to address supply chain cybersecurity could have far-reaching consequences to electricity distribution systems and potentially to bulk energy systems. Such consequences may include loss of profits, loss of control of critical resources, and potentially affecting civilians with loss of electricity.

Each year, MITRE identifies the most dangerous software weaknesses and highlights the top 25 easiest to exploit and abuse to take over a system, steal data, or prevent an application from working (MITRE 2022). The 2022 Common Weakness Enumeration (CWE) provides developers, testers, security researchers, and users insight into the most severe and current security weaknesses. It also leverages Common Vulnerabilities and Exposures (CVE) data found in the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) as well as the Common Vulnerability Scoring System (CVSS) scores associated with each CVE record. Using a formula, it assigns a score to each weakness based on prevalence and severity. Using CWE Top 25, a proactive understanding of cybersecurity risks, especially related to the supply chain, can be developed. Table 1 provides the CWE Top 25 for 2022; many of these indicate that the developers and their organizations are not applying robust software practices, are cutting corners, and are missing key security fundamentals.

When there is a lack of personnel with cybersecurity expertise, a lack of cyber hygiene, or a lack of sufficient third-party risk management, the supply chain presents a potential attack vector, with an external organization being used as the pathway to a secured organization. Without proper procedures in place, an attack that comes through the supply chain vector can be

extremely detrimental to a system or a plant, and it can be extremely difficult to pinpoint and stop.

In this report, we:

- Discuss supply chain cybersecurity risks.
- Identify key domains of the supply chain cybersecurity of distributed energy resources (DERs).
- Perform a gap analysis of the current supply chain cybersecurity landscape of DERs.

Table 1. 2022 CWE Top 25 Software Weaknesses (MITRE 2022)

Rank	ID	Name	Score
1	CWE-787	Out-of-bounds Write	64.20
2	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	45.97
3	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22.11
4	CWE-20	Improper Input Validation	20.63
5	CWE-125	Out-of-bounds Read	17.67
6	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17.53
7	CWE-416	Use After Free	15.50
8	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.08
9	CWE-352	Cross-Site Request Forgery (CSRF)	11.53
10	CWE-434	Unrestricted Upload of File with Dangerous Type	9.56
11	CWE-476	NULL Pointer Dereference	7.15
12	CWE-502	Deserialization of Untrusted Data	6.68
13	CWE-190	Integer Overflow or Wraparound	6.53
14	CWE-287	Improper Authentication	6.35
15	CWE-798	Use of Hard-coded Credentials	5.66
16	CWE-862	Missing Authorization	5.53
17	CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	5.42
18	CWE-306	Missing Authentication for Critical Function	5.15
19	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	4.85
20	CWE-276	Incorrect Default Permissions	4.84
21	CWE-918	Server-Side Request Forgery (SSRF)	4.27
22	CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	3.57
23	CWE-400	Uncontrolled Resource Consumption	3.56
24	CWE-611	Improper Restriction of XML External Entity Reference	3.38
25	CWE-94	Improper Control of Generation of Code ('Code Injection')	3.32

2 Supply Chain Cybersecurity Risks

Threat actors have used techniques and patterns found in other attacks for many years. Yet, as we look at the modern threat landscape, two trends are forthcoming for which organizations are not prepared (Loucaides 2021):

- The focus on the advantages of targeting firmware, subcomponents, and tool providers
- The impacts and advantages to attackers associated with supply chain campaigns.

Supply chain cybersecurity is a unique space because there are many different attack vectors from which a possible vulnerability can be exploited. Because supply chains are distributed, it can be very difficult to track the location of a vulnerability and what has been verified throughout a supply chain. Research has shown that breaches originating at third parties are among the costliest cyberattacks and have caused downtime in major network infrastructure, such as for FedEx and Maersk (Johnson 2019). Many risks are associated with the supply chain, including poor security from downstream suppliers and vulnerabilities in code in lower parts of the supply chain.

Software that is used in energy systems includes large sets of complex code (Caddy et al. 2022). Much of modern software relies on many libraries that are open source and maintained by users that are external to the organization using the library. The benefits of open source include saving time and having many reviews of the source code so that it can be improved upon. But with this comes the possibility of a bad actor maliciously modifying the source code to introduce new vulnerabilities or using the source code to produce attacks where the source code is introduced into a system. Lack of upgrades and maintenance by parties integrating these components into larger systems leave vulnerabilities that could be exploited with minimal effort. Although there is the possibility of catching these vulnerabilities if they are introduced into the source code, open-source repositories can be at risk if not being closely maintained.

Foreign suppliers also pose a risk when open and global software supply chains are used (Caddy et al. 2022). Software developed for information technology and operational technology systems are often developed in countries where both a skilled workforce and lower wages meet, making the software lower cost. This reliance is a risk where software is created by a supplier that is under the control of or influenced by a foreign adversary.

Based on interactions we had with DER/inverter-based resource (IBR) industry stakeholders, we categorized the challenges faced by component manufacturers, system integrators, and electric utilities, shown in Figure 1. Concerns around supply chain cybersecurity were a common theme among all stakeholders.

Figure 1. Cybersecurity challenges

3 Gap Analysis

A gap analysis for this context is defined as follows:

- Identify and define the current state.
- Define an ideal state.
- Identify the gaps between the two states.

Within the context of our scope, we identified three pillars of the landscape for the DER supply chain cybersecurity: frameworks and assessments, firmware and software, and standards. When assessing the scope, the perspective was from that of regulated entities, such as utilities and vendors.

3.1 Frameworks and Assessments

A framework is a collection of best practices and components to assess a topic space. A model is similar because it includes best practices for a topic space; however, a model is more theoretical and general, whereas a framework is more focused and guided. An assessment acts as a guide that walks a user through the controls of the framework or model and provides metrics to describe the posture according to the framework. The purpose of the assessment is to aid a user in assessing their posture compared to the framework and best practices and to identify action items to improve their posture.

3.1.1 Current State

From the energy sector, the North American Transmission Forum (NATF) Supply Chain Security Assessment Model addresses supply chain risk management from a supplier's point of view (NATF 2022). This assessment creates a way for a supplier to reduce the load a purchaser must take to evaluate how secure the supplier's product is. This is a general model for the energy sector, and although it does not contain specific guidance for DER supply chain cybersecurity, many of these practices are relevant to DERs.

The Cybersecurity Capability Maturity Model (C2M2) is used to assess the cybersecurity posture. The model itself is derived from best practices in the information technology and operational technology space, to provide a whole evaluation process regardless of the organizations area (CESER 2022). For supply chain cybersecurity, the C2M2 includes the domain third-party risk management, which includes practices for determining third-party risks and third-party management.

The Distributed Energy Resources Cybersecurity Framework (DER-CF) was created by the National Renewable Energy Laboratory (NREL) to assess the cybersecurity posture of facilities with renewable resources (Powell et al. 2019). The DER-CF was informed by the C2M2, NIST CSF and NIST 800-53 by adapting controls to fit the DER space. The DER-CF assessment includes a streamlined process for a user to answer questions relating to their own cybersecurity practices, culminating in a final report that displays their maturity level, posture, and how to improve their posture through a series of action items given once completed. The framework includes the third-party domain for assessing that level of the supply chain, but it could be expanded to include more questions to evaluate the posture of supply chain cybersecurity.

3.1.2 Ideal State

With a lack of specific frameworks, a key ideal state would include having a framework to assess DER supply chain cybersecurity.

In the information technology space, the U.S. Department of Homeland Security (DHS) created the Information and Communications Technology (ICT) Supply Chain Risk Management Task force, a public-private partnership sponsored by the Cybersecurity & Infrastructure Security Agency (CISA 2022). This task force was created to categorize, assess, and understand the risks of ICT components. The work being done by this task force can be used to inform best practices for common DER components that are shared between the information technology and energy sectors. The task force gathered and created the ICT framework outlined in Figure 2.

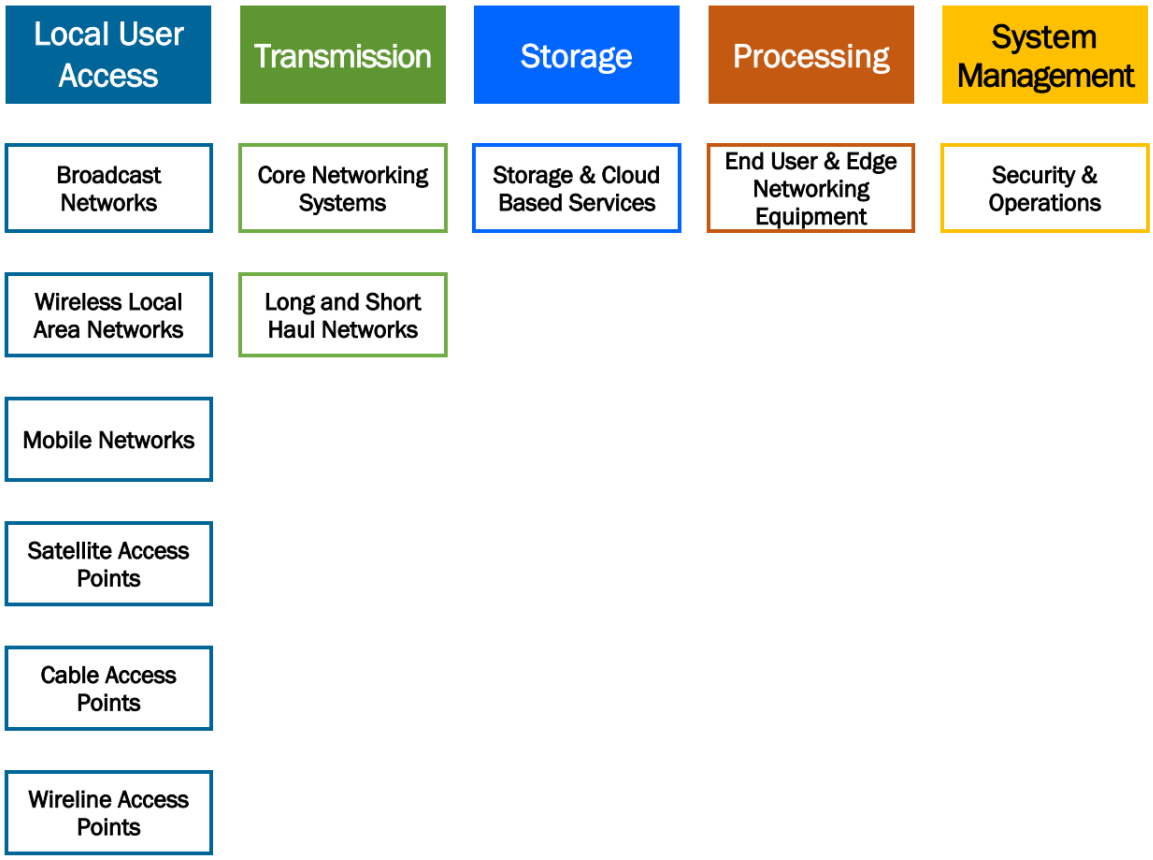

Figure 2. The ICT framework developed by DHS with input from Argonne National Laboratory and Sandia National Laboratories

The components of the ICT framework are National Critical Functions that drive U.S. critical infrastructure. These elements were broken into 5 roles and 11 sub-roles within the framework to categorize each element. Once categorized, the criticality of each element was assessed to further understand its role within the ICT supply chain. A white paper was published presenting the framework and the assessment of criticalities, with a section informing the future analysis of these elements and possible areas that will be expanded (CISA 2020). A framework such as this

specific to DERs is ideal for focusing on the National Critical Functions that are most impacted by supply chain attacks.

With the introduction of a new framework, an assessment is beneficial to industry members to assess their posture with the practices outlined. In this case, the capabilities of the DER-CF could be leveraged to provide the assessment. The existing functionalities of the tool make it an ideal option.

To align with this framework, industry engagement is needed to identify which current practices are in place, best practices, and agreements on methods of implementation where practices are not established.

3.1.3 Gaps

After addressing the current state of existing frameworks/tools and identifying an ideal state, gaps were identified along with potential solutions:

- **Establish a framework for DER supply chain cybersecurity**: This gap can be bridged by adapting the ICT framework to DER supply chain cybersecurity while being influenced by the current cybersecurity frameworks and models, such as the C2M2, NIST 800-161, and the NATF Supply Chain Security Assessment Model. Although many general frameworks exist, there can be concern of an overpopulation of frameworks to choose from, which could result in the further fragmentation of standards and homogenous expectations. An alternative to creating a new framework could be modifying an existing framework, such NIST's Cybersecurity Framework or utilizing the DER-CF to support this modification.
- **Engage industry for assessments:** Identify industry stakeholders who could participate in voluntary assessments of their design practices and procedures to inform their own cybersecurity postures by helping to monitor, assess, and manage supply chain risks using quantitative results.

3.2 Firmware and Software

With the heterogenous, distributed systems that are operating across DERs, pinpointing a possible attack that comes through a microcontroller that has tampered firmware via an unauthorized patch from the supplier's supply chain can be a large task. The reliance of industrial control systems on modern information technology solutions, including IP-based networking and embedded computing, has raised serious security concerns (Basnight et al. 2013). With energy systems relying on large sets of complex code and numerous subcomponents, the risk of vulnerabilities in downstream software supply chain is high.

3.2.1 Current State

Programmable logic controllers (PLCs) are critical to the operation of critical infrastructure assets. PLCs are embedded devices that are programmed to manage and control the physical components based on system inputs and requirements (Basnight et al. 2013). For DERs, these components include tracking the sun's location for photovoltaics, which if lost would significantly reduce power delivery and thus cause financial loss. The lowest programming abstraction layer of a PLC is the firmware. Malicious modification or counterfeiting PLC

firmware can provide an adversary with complete control over an industrial control device and any physical system components that come under its purview (Basnight et al. 2013).

It is possible that within the supply chain, firmware can be modified or a rootkit can be installed at the firmware level to keep the core firmware intact. Reverse engineering firmware through a step-by-step analysis can include a manual process of black-box testing on the binary, disassembly, and analyzing the disassembly through GNU debugger or another black-box modification testing. A target can be modified by obtaining the dynamic functions that are coded into the software to understand changes needed for an attack. This method allows the firmware to still act and reflect as the core firmware functionality while also inserting the code needed to conduct the attack (Basnight et al. 2013). Ideally, attacks should be prevented at all stages of the supply chain, and detection, containment, and prevention measures should be used to mitigate attacks.

A software bill of materials (SBOM) is a machine-readable list of software components and their dependencies, including information about the software and the relationship of all its components (Idaho National Laboratory 2022b). With an SBOM, an analysis service can be conducted before a piece of software is implemented to see whether deviations exist between the software that was supplied and the accompanying SBOM. An SBOM is limited in what it can provide to discover tampering, but it can be used to discover vulnerabilities in the supplied software to understand the risks to the consumer.

Although the integrity of software and firmware can be checked via hashing algorithms, digests, or hash-based message authentication code (HMAC), verification can still be a potential area for improvement within emerging technologies. Typically, verification of the binary using a signature digest by the vendor of the original firmware is sufficient; however, this relies on either the vendor or the purchaser to verify the signature. If the hash matches or the signature is valid, this does not guarantee that the software is secure, only that it has maintained its integrity between the two agreeing parties. The verification must be at all parts of the software supply chain as well. It is possible that a library used in the development of the firmware could have been tampered with and be completely unknown to the purchaser.

Open-source software is a growing area in energy systems software development. There are many benefits to using open-source software, such as saving time and money because many are free. Also, the open nature of the software benefits from being reviewed by multiple contributors. Multiple reviewers give more input into how the software performs and create new or novel solutions to the problem that is being solved. Time savings, reduced cost, and novel solutions to problems make open-source software an attractive path to developing solutions for the energy system. Downstream dependencies are software packages included in the code that are relied on to run. These dependencies can include other software packages that can form a tree structure, which could become very large and increase the attack surface and vulnerabilities.

Vulnerabilities in downstream dependencies pose risks to systems using bloated, aging software packages. Closed-source code (requiring support contracts) is also susceptible to cyberattacks. Dependency lists of some software packages can often be very large, making it difficult to identify and correct issues that might be in downstream-dependent software packages. Further, many reference designs based on software development kits are used to deploy the product in the

field without updating third-party libraries and code. Also, the entire build process for a product could be outsourced, and once it is deployed, it does not receive updates.

To aid in combating these issues for energy systems, several efforts funded by the U.S. Department of Energy (DOE) were created to aid in testing and understanding components and their software to quantify risk and mitigation tactics.

Cyber Testing for Resilient Industrial Control Systems (CyTRICS), created by DOE, is a program for identifying and testing for cybersecurity vulnerabilities in operational technology and industrial control systems (Idaho National Laboratory 2022a). This program uses the information found while testing the components to create best practices for supply chain cybersecurity risk management for energy system components (Caddy et al. 2022). The program is voluntary; industry partners supply the energy system components to test.

The Clean Energy Cybersecurity Accelerator (CECA), led by NREL, is a testing program for cyber risk solutions for renewable energy (NREL 2022). NREL facilitates the testing through the Advanced Research on Integrated Energy Systems (ARIES) to provide simulations to test scenarios against with supplied solutions from industry. Industry members gain partnership opportunities as well as a world-class evaluation of the supplied solutions.

3.2.2 Ideal State

CyTRICS and CECA represent key programs for the testing and verification of energy system components and risk mitigation solutions. Combining the knowledge and analysis from CyTRICS with the capability of NREL's ARIES creates a testing ecosystem to assess, analyze, and understand risks and to pinpoint mitigations and solutions in the DER supply chain.

Ideally, open-source software includes many contributors, skilled or unskilled, to review and add to the library for the best outcomes. When there is a lack of contributors or a lesser-known library, a rigorous review process should be conducted for each software package that is to be included. Such rigor should include an SBOM to be fed into a vulnerability analysis of the package and its versions. After the risks and vulnerabilities that are found from the automated scanning analysis are assessed, a decision must be made regarding whether the software is a security risk if it is included in the product being developed.

Also, ideally, open-source software should have stamps of approval from industry members that are using the software. These stamps of approval show that industry members trust the software, which can enhance the trust of other potential end users who are also considering using the software. These stamps of approval do not mean that the software is secure, however; they denote only that another company is using the software and trusts it. The stamps of approval could aid in decision making but should not be the end solution for determining whether a software package has been validated. Particularly in systems of systems, there could be challenges with the interoperability between two certified components of different origins.

Vulnerabilities in downstream dependencies should also be considered when assessing software. Downstream dependencies that contain vulnerabilities must be assessed to patch the vulnerable package or to create a risk mitigation strategy for that vulnerability. Risk management of the

vulnerability might include closing certain ports, removing parts of the affected package that are compromised, or reducing dependencies on the vulnerable package.

Firmware that is included in supplier PLCs also needs to be verifiably secure. For suppliers to create trust, a demonstration of functionality before and after purchase is needed before production deployment. Although functionality verification does not guarantee security, trust between organizations to provide the best product and to prevent cyberattacks from both ends create incentives to work together to provide secure functionality.

3.2.3 Gaps

When comparing the current landscape to the ideal state, we found gaps between the two:

- **Open-source software guidance:** Although open source is an attractive avenue for developing software, there are considerable risks that need to be addressed. Guidance is needed in the form of standards or best practices to understand the risks and how to mitigate them.
- **Establish a testing and certification ecosystem for DER software supply chain cybersecurity:** Take the lessons learned from CyTRICS and the CECA, which have their own testing methodologies, to develop a new testing ecosystem. Leverage NREL's ARIES to assess and understand mitigation techniques for the supply chain of the software provided. This will drive new partnerships, recommendations, certifications of products or components, and mitigation strategies for supply chain risks.

3.3 Standards

3.3.1 Current Landscape

Many standards exist to inform increases in cybersecurity postures and to protect against cyberattacks. The current landscape of recommendations and standards includes several that can be used by DER utilities, vendors, aggregators, or manufacturers (Walker et al. 2021):

- DOE/DHS Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)
- International Electrotechnical Commission (IEC) 62351 – Power Systems Management and Associated Information Exchange – Data and Communications Security
- IEC 62443 – Industrial Automation and Control Systems Security
- Institute of Electrical and Electronics Engineers (IEEE) 1547.3 – Guide for Cybersecurity of DERs Interconnected with Electric Power Systems
- IEEE 2030.5-2018 – IEEE Standard for Smart Energy Profile Application Protocol
- IEEE C37.240-2014 – IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems
- NERC Reliability Guideline – Cyber Intrusion Guide for System Operators
- NIST 7628 – Guidelines for Smart Grid Cybersecurity
- NIST SP 800-82 Revision 2 – Guide to Industrial Control Systems (ICS) Security
- UL 2941 – Cybersecurity Certification Standard for IBRs.

Although this is not a complete list, these are recommended standards to assess and implement for DER cybersecurity. Idaho National Laboratory posted the standards to a secure energy

infrastructure website that allows an organization to select the filters that match their own organizational structure, the purpose of the standard they are looking for, as well as the type. The site then displays standards that fit that query (CESER 2021). These standards can also be used to inform recommendations, certifications, or another standard for DER supply chain cybersecurity as well, which helps to fill gap in what are currently available. There is potential for new standards to exist in this space to help guide utilities, vendors, aggregators, and manufacturers to assess their supply chain cybersecurity postures.

Resources that are individually 20 MW, or 75 MW in aggregate, must comply with applicable NERC reliability standards. In addition, NIST's 800 series, which uses the NIST Risk Management Framework and the NIST Cybersecurity Framework, provides many documents from which to derive recommendations and guidelines. The series is widely used by many organizations to increase their cybersecurity postures (Johnson 2017).

3.3.2 Ideal Landscape

Currently, providers and manufacturers can reference other general standards for best practices, but the DER supply chain is a new space that needs specific recommendations and guidance.

In 2015, NIST organized a workshop on supply chain cybersecurity best practices for general audiences. The workshop identified areas to ask cybersecurity questions to find which risks might be included in the supply chain (NIST 2015):

- How does the vendor stay current in their compliance to new and existing standards?
- What controls are in place to manage and monitor production for compromise?
- What physical security measures are in place for critical assets to the organization?
- What levels of malware protection are in end products?

These guiding questions create a need for industry involvement and directly influence what to include in supply chain cybersecurity recommendations. For an ideal state, questions that underlie these recommendations to industry should be asked from a consumer's point of view:

- What are processes for identifying secure PLCs before implementation?
- What software integrity verification processes are in place?
- Is firmware functionality verified during the acquisition process?
- Are multiple vendors assessed before purchase? How are they assessed?
- Are vendors assessed on their own supply chain cybersecurity posture? What results from such assessments would disqualify a supplier from acquisition?
- What are steps for a supplier to take to remediate being disqualified or removed from acquisition lists?
- What are the requirements for foreign suppliers to be approved for acquisition? Are these requirements stricter or the same as local suppliers? Are local suppliers any better, or are they using foreign relabeled components?

This is not an inclusive list; this is expandable to guide research into what other questions to ask to identify best practices that inform standards.

The audience to ask these questions should be a working group of DER industry members. A working group that can provides feedback on their own supply chain practices will generate strength for the controls and recommendations. Ideally, the group should comprise members from different organizations, such as vendors and utilities, for diverse representation of the problems each organization faces. The resulting practices and recommendations should include bidirectional perspective. For example, a supplier's point of view should be its own set of recommendations within the standard; a supplier can assess their own practices, and a potential end user can see whether those practices were informed by the standard. Similarly, an end user who is purchasing from the supplier can assess their own supply chain practices from their perspective.

Including both sides on drafting proper contractual language requirements and recommendations removes the risk of poor accountability of control implementation. Enforcing said practices through contractual language such that every party involved is implementing the necessary level of security, removes either side from taking a lack of responsibility in the event of a cyber-attack. In addition, neither puts in minimum security for passing initial checks as these enforced contracts could result in large consequences from a legality perspective, not just a cyber perspective.

3.3.3 Gaps

When comparing the current landscape to the ideal, we found gaps between the two:

- **Address the issue of lacking standards for DER supply chain cybersecurity:** Establish a well-versed guidance document for DER supply chain cybersecurity through stakeholder engagement by leveraging subject matter experts in the solar industry after performing deep-dive investigations on available best practices, such as NIST's supply chain cybersecurity risk management and mitigation programs, NERC's implementation plan for cybersecurity supply chain risk management (CIP-013-1), and supply chain security tools developed by national labs.
- **Form working groups for best practices:** Obtain industry feedback through a working group to move the current state of supply chain cybersecurity closer to the ideal. Identifying industry best practices, even if they are not made into a standard, can benefit the industry by providing optional recommendations to owner/operators/vendors/aggregators to improve their supply chain cybersecurity postures.

4 Conclusion

As the energy sector evolves and moves toward new technologies, cybersecurity must be an integral part to ensure the continued delivery of safe and reliable energy services. Supply chain cybersecurity plays an important role in this evolution as technologies advance and evolve. Attack vectors that exist because of out-of-date technology can be detrimental to the system. In this paper, we analyzed the current landscape of DER supply chain cybersecurity, formulated an ideal state, and identified gaps in the current state of the cybersecurity supply chain available to the renewable energy sector:

- **Establish a framework for DER supply chain cybersecurity**: This gap can be bridged by adapting the ICT framework to DER supply chain cybersecurity while being influenced by the current cybersecurity frameworks and models, such as the C2M2, NIST 800-161, and the NATF Supply Chain Security Assessment Model. Although many general frameworks exist, there can be concern of an overpopulation of frameworks to choose from, which could result in the further fragmentation of standards and homogenous expectations. An alternative to creating a new framework could be modifying an existing framework, such as NIST's Cybersecurity Framework or utilizing the DER-CF to support this modification.
- **Engage industry for assessments:** Identify industry stakeholders who could participate in voluntary assessments of their design practices and procedures to inform their own cybersecurity postures by helping to monitor, assess, and manage supply chain risks using quantitative results.
- **Open-source software guidance:** Although open source is an attractive avenue for developing software, there are considerable risks that need to be addressed. Guidance is needed in the form of standards or best practices to understand the risks and how to mitigate them.
- **Establish a testing and certification ecosystem for DER software supply chain cybersecurity:** Take the lessons learned from CyTRICS and CECA, which have their own testing methodologies, to develop a new testing ecosystem. Leverage NREL's ARIES to assess and understand mitigation techniques for the supply chain of the software provided. This will drive new partnerships, recommendations, certifications of products or components, and mitigation strategies for supply chain risks.
- **Address the issue of lacking standards for DER supply chain cybersecurity:** Establish a well-versed guidance document for DER supply chain cybersecurity through stakeholder engagement by leveraging subject matter experts in the solar industry after performing deep-dive investigations on available best practices, such as NIST's supply chain cybersecurity risk management and mitigation programs, NERC's implementation plan for cybersecurity supply chain risk management (CIP-013-1), and supply chain security tools developed by national labs.
- **Form working groups for best practices:** Obtain industry feedback through a working group to move the current state of supply chain cybersecurity closer to the ideal. Identifying industry best practices, even if they are not made into a standard, can benefit the industry by providing optional recommendations to owner/operators/vendors/aggregators to improve their supply chain cybersecurity postures.

References

Basnight, Z., J. Butts, J. Lopez, and T. Dube. 2013. "Firmware Modification Attacks on Programmable Logic Controllers." *International Journal of Critical Infrastructure Protection* 6 (2): 76–84. https://doi.org/10.1016/j.ijcip.2013.04.004.

Caddy, C., E. Begoli, S. Chanowski, A. Gates, P. Stockton, and V. Wright. 2022. *Cybersecurity and Digital Components: Supply Chain Deep Dive Assessment*. Washington, D.C.: U.S. Department of Energy. https://www.energy.gov/sites/default/files/2022-02/Cybersecurity%20Supply%20Chain%20Report%20-%20Final.pdf.

Cybersecurity Infrastructure and Security Agency (CISA). 2020. Executive Order 13873 Response: Methodology for Assessing the Most Critical Information and Communications Technologies and Services. Washington, D.C. https://www.cisa.gov/sites/default/files/publications/eo-response-methodology-for-assessing-ict_v2_508.pdf.

———. 2022. "ICT Supply Chain Risk Management Task Force." Accessed August 8, 2022. https://www.cisa.gov/ict-scrm-task-force.

European Union Agency for Cybersecurity (ENISA). 2021. "Understanding the Increase in Supply Chain Security Attacks." Press release, July 29, 2021. https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks.

Idaho National Laboratory. 2022a. "CyTRICS: Cyber Testing for Resilient Industrial Control Systems—Incorporating Context for Better Threat Detection." https://cytrics.inl.gov/cytrics/.

———. 2022b. "Software Bill of Materials: Exploring a Proof-of-Concept for the Energy Community." https://sbom.inl.gov/sbom/.

Johnson, J. 2017. *Roadmap for Photovoltaic Cyber Security*. Albuquerque, NM: Sandia National Laboratories. SAND2017-13262. https://sunspec.org/wp-content/uploads/2020/01/Roadmap-for-Photovoltaic-Cyber-Security-SAND2017-13262-4-10-2018.pdf.

Johnson, K. 2019. "NERC CIP-013-1: Start Date, Preparation Strategies, & Impact." *BitSight*, April 9, 2019. https://www.bitsight.com/blog/nerc-cip-013-1-effective-date-preparation-strategies-and-impact.

Loucaides, J. 2021. "Threats Below The Surface in High-Risk Devices." BrightTALK. https://www.brighttalk.com/webcast/17865/479187.

MITRE. 2022. "2022 CWE Top 25 Most Dangerous Software Weaknesses." Common Weakness Enumeration. https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html.

National Institute of Standards and Technology (NIST). 2015. "Best Practices in Cyber Supply Chain Risk Management: Conference Materials." Gaithersburg, MD. https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf

National Renewable Energy Laboratory (NREL). 2022. "Clean Energy Cybersecurity Accelerator." Accessed October 19, 2022. https://www.nrel.gov/innovate/cybersecurity-accelerator.html.

North American Transmission Forum (NATF). 2022. "Supply Chain Cyber Security Industry Coordination." https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.

Office of Cybersecurity, Energy Security, and Emergency Response (CESER). 2021. "Standards to Secure Energy Infrastructure." Washington, D.C.: U.S. Department of Energy. https://energyicsstandards.inl.gov/.

———. 2022. *Cybersecurity Capability Maturity Model (C2M2)*. Washington, D.C. https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf. Washington, D.C.: U.S. Department of Energy.

Powell, C., K. Hauck, A. Sanghvi, A. Hasandka, J. Van Natta, and T. Reynolds. 2019. *Guide to the Distributed Energy Resources Cybersecurity Framework*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-75044. https://www.nrel.gov/docs/fy20osti/75044.pdf.

U.S. Department of Commerce (DOC) and U.S. Department of Homeland Security (DHS). 2022. *Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry*. Washington, D.C. https://www.dhs.gov/sites/default/files/2022-02/ICT%20Supply%20Chain%20Report_2.pdf.

Walker, A., J. Desai, D. Saleem, and T. Gunda. 2021. *Cybersecurity in Photovoltaic Plant Operations*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5D00-78755. https://www.nrel.gov/docs/fy21osti/78755.pdf.

Bibliography

King, A. 2021. “Cybersecurity Tips: Supply Chain Security.” Security Industry Association, October 22, 2021. https://www.securityindustry.org/2021/10/22/cybersecurity-tips-supply-chain-security/.