Cybersecurity Certification Recommendations for Interconnected Grid Edge Devices and Inverter Based Resources

William Hupp, Danish Saleem, and Jordan T. Peterson
National Renewable Energy Laboratory

Kenneth Boyce
Underwriters Laboratories

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-5R00-80581
November 2021

Cybersecurity Certification Recommendations for Interconnected Grid Edge Devices and Inverter Based Resources

William Hupp, Danish Saleem, and Jordan T. Peterson
National Renewable Energy Laboratory

Kenneth Boyce
Underwriters Laboratories

Suggested Citation
Hupp, William, Danish Saleem, Jordan T. Peterson and Kenneth Boyce. 2021. *Cybersecurity Certification Recommendations for Interconnected Grid Edge Devices and Inverter Based Resources.* Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-80581. https://www.nrel.gov/docs/fy22osti/80581.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-5R00-80581
November 2021

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

NOTICE

This work was authored in part 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 the 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.

Cover Photos by Dennis Schroeder: (clockwise, left to right) NREL 51934, NREL 45897, NREL 42160, NREL 45891, NREL 48097, NREL 46526.

Preface

Increasing numbers of distributed energy resources (DERs) are being deployed on the electric grid. The growth in grid edge DERs, including distributed generation such as rooftop solar photovoltaics and battery storage systems, could create an expanded attack surface for potential cyberattacks. This paper outlines a certification testing procedure that identifies gaps in DER cybersecurity functionality and mandates secure features at the device, network, and system level. The certification testing procedure can potentially be used in a U.S. industry standard to address diverse manufacturer approaches to cybersecurity and to inform the development of appropriate third-party conformity assessment programs for DER cybersecurity testing and certification.

Acknowledgments

The authors thank the U.S. Department of Energy (DOE) Office of Energy Efficiency and Renewable Energy, Solar Energy Technologies Office for their support of this research through the Distributed Energy Resource Cybersecurity Standards Development project. The authors are grateful to Jeremiah Miller of DOE for his valuable guidance and support.

We are also grateful for the superb engagement, technical expertise, guidance, and feedback from UL (http://www.ul.com).

We are also grateful to the National Renewable Energy Laboratory's (NREL's) Energy Systems Integration Facility operations team, including John Fossum, John Nangle, and Greg Martin, for their outstanding technical support and invaluable help in configuring and maintaining the power-hardware-in-the-loop testbed; and to NREL's communications team, including Nika Durham, Katie Wensuc, and Anthony Castellano, for providing editing, proofreading, and other communications support to the project. Without their invaluable help, this project would not have been possible. The authors also appreciate the knowledgeable input and helpful feedback from our reviewers Richard Macwan and Maurice Martin.

List of Acronyms

CEEP	Cyber Energy Emulation Platform
CESER	Office of Cybersecurity, Energy Security, and Emergency Response
CIGRE	International Council on Large Electric Systems
CISA	Cybersecurity and Infrastructure Security Agency
CRL	certificate revocation list
DER	distributed energy resource
DNP	Distributed Network Protocol
DOE	U.S. Department of Energy
DoS	denial of service
DUT	device under test
EERE	Office of Energy Efficiency and Renewable Energy
EPRI	Electric Power Research Institute
ES-C2M2	Electricity Subsector Cybersecurity Capability Maturity Model
EV	electric vehicle
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IBR	inverter-based resource
ICS	industrial control system
IEA	International Energy Agency
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IT	information technology
MAC	message authentication code
MITM	man in the middle
NARUC	National Association of Regulatory Utility Commissioners
NASEO	National Association of State Energy Officials
NDN	named data networking
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NREL	National Renewable Energy Laboratory
OT	operational technology
PSIL	Power Systems Integration Laboratory
PV	photovoltaic
RMP	risk management process
SCADA	supervisory control and data acquisition
SEP	Smart Energy Profile
SETO	Solar Energy Technologies Office
sPower	Sustainable Power Group
SSH	Secure Shell
TCP	Transmission Control Protocol
TLS	Transport Layer Security

Executive Summary

According to the Department of Energy (DOE) Solar Futures Study, the U.S. must install an average of ~45GW of solar capacity per year between 2020 and 2030 to achieve decarbonization goals[1]. With a recent market shift from utility-scale to distributed generation, the future grid must support the increasing deployment of distributed energy resources (DERs) to reach solar generation milestones. DER systems are complex and must be capable of regulation, utility control, and aggregation of DERs working in sync. These capabilities are enabled through an increased dependence on computer technology which require rich data and advanced control systems in both the information technology (IT) and operational technology (OT) space, but each innovation has the potential to open the door for new vulnerabilities and cyber threats. These vulnerabilities can cause the U.S. electric system to have a larger attack surface and increase its susceptibility to potential cyber-physical attacks. To mitigate the effect of these potential attacks, cybersecurity certification standards and programs need to be established. These standards and programs could aid industry stakeholders in evaluating and validating the cybersecurity posture of their interconnected DERs.

To address the lack of security guidance for DERs, this report was developed with the support of UL to establish a baseline for device-level security and to inform the development of a future voluntary UL cybersecurity certification standard for DER stakeholders. Additional objectives were to verify the certification recommendations with UL, use the recommendations to inform a future equipment standard, and create a market value for cybersecurity certification to motivate industry stakeholders to adopt more secure systems to align with federal efforts to elevate IoT security through enhanced labeling ("Executive Order 14208"). This report demonstrates the laboratory validation of the cybersecurity certification recommendations proposed in a previously published National Renewable Energy Laboratory (NREL) report, *Certification Procedures for Data and Communications Security of Distributed Energy Resources* (Saleem and Carter 2019).

The cybersecurity certification recommendations were informed through working group collaborations among NREL, Sandia National Laboratories, the SunSpec Alliance, and industry partners. Leveraging previous cybersecurity certification research, 10 test cases were proposed to show that DERs possess the cybersecurity functionalities needed to secure systems and devices in an interconnected power system (Saleem and Carter 2019). The certification recommendations include checks for Transport Layer Security, key updates, message authentication codes, a certificate revocation list, expired certificates, authentication management, routine audits, and service versions. The certification recommendation tests were performed twice on photovoltaic (PV) inverters. The first certification test was performed on industry standard PVs. The second certification test was performed on PVs running a bump-in-the-wire (an intrusion detection communication device which can be inserted into existing systems to enhance integrity and reliability of communications) solution called DERCyST.

[1] See https://www.energy.gov/sites/default/files/2021-09/Solar%20Futures%20Study.pdf.

Table 1. Certification Test Results

Test Case	Test 1: PV Certification Test	Test 2: PV Certification Test with DERCyST
Two-Party Application Association	Passed	Passed
Transport Layer Security	Failed	Passed
Transport Layer Security Recovery	Failed	Passed
Key Update	Failed	Passed
Message Authentication Code	Failed	Passed
Certificate Revocation List	Failed	Passed
Expired Certificate	Failed	Passed
Operating System and Service Version	Failed	Passed
Authentication and Password Management	Failed	Passed
Security Management	Failed	Passed

The results of Test 1 show that there exist gaps in the cybersecurity posture of industry standard PVs. As a result, they are vulnerable to common cyberattacks, such as eavesdropping, replay, man-in-the-middle (MITM) attacks, denial-of-service (DoS) attacks, spoofing through security certificates, least-privilege violations, and brute-force credentials. However, these attacks can be mitigated by incorporating software and services, such as DERCyST in Test 2, which enable DERs to pass the certification recommendations into the DER environment. The recommended functionalities have been reviewed and approved by UL to validate their practicality, integrity, and use for industry. UL's support for this report will accelerate the adoption of the certification recommendation features to a UL certification program and a cybersecurity standard for DERs.

This report:

- Explains the rationale for cybersecurity standards in DERs
- Explores existing vulnerabilities in DERs
- Provides certification recommendations for grid edge devices
- Discusses test results of performing the certification procedure against a common industry DER

- Illustrates the results of performing the certification procedure against the same DER devices using DERCyST
- Provides an overview of NREL's testing platform
- Outlines future work for adopting DER cybersecurity standards.

Table of Contents

List of Figures

List of Tables

1 Overview

Newly emergent cyber actors have caused large data breaches and disruptions to critical infrastructure that have led to service interruptions and caused multimillion-dollar losses. The cyber threat landscape is constantly changing, and threat attackers are no longer limiting their scopes to information technology (IT) and traditional Transmission Control Protocol/Internet Protocol (TCP/IP) networks. Recent attacks have shown that threat actors are targeting devices interconnected with critical infrastructure. In February 2020, a ransomware attack targeting operational technology networks of a natural gas compression facility was reported by the U.S. Department of Homeland Security. Leveraging spear phishing, the attacker caused the facility to shut down for 2 days (CISA 2020). In that same month, hackers compromised a water plant in Oldsmar, Florida. Attackers leveraged cross-site scripting to infect a computer with access to water plant controls and attempted to poison the water supply (Kephart 2021). In May 2019, a U.S. electric power grid operator, Sustainable Power Group (sPower), was subjected to a denial-of-service (DoS) attack and was disconnected from its power generation station. This occurred due to an unpatched firewall vulnerability that allowed the attackers to disrupt supervisory control and data acquisition system communications and caused a disruption in power generation (NERC 2019).

To tackle the increasing attack surface resulting from the increase of grid edge devices—such as microgrid controllers and smart inverters—and inverter-based resources (IBRs), a standard set of practices needs to be developed that could later be added to a national certification standard and address major cybersecurity vulnerabilities in grid edge devices and IBRs. This is necessary because there currently exists no certification standards or programs that could aid industry stakeholders in validating and evaluating the cybersecurity posture of their devices before they are connected to the electric grid. For example, the Institute of Electrical and Electronics Engineers (IEEE) 1547-2018, Standard for Interconnection and Interpretability of Distributed Energy Resources with Associated Electric Power Systems Interfaces, considers cybersecurity out of scope (IEEE 2018). The National Institute of Standards and Technology has developed a cybersecurity framework to improve the cybersecurity posture of cyber-physical systems, but even this framework does not provide guidance on how to improve device-level security and implement necessary security functions. To reduce the risk of, and impact from, cyberattacks on grid edge devices and inverter-based resources (IBRs) connected to the distribution grid, the U.S. Department of Energy (DOE) Solar Energy Technologies Office (SETO) directed the National Renewable Energy Laboratory (NREL) and Sandia National Laboratories (Sandia) to research, develop, and harmonize cybersecurity standards for PV systems and other DERs.

To inform a certification standard for DER cybersecurity, NREL worked with solar industry partners and UL to establish certification recommendations and test cases (Saleem and Carter 2019) for evaluating intrinsic design security for DERs. These recommendations were developed to bolster cyber-secure functionalities such as Transport Layer Security (TLS), message authentication codes (MACs), and certificate revocation lists (CRLs); session resumption/renegotiation; and password, system, and service security management within the DER devices. The proposed test cases verify the authentication, authorization, confidentiality, and data integrity for data and communications of DERs that use Transmission Control Protocol/Internet Protocol (TCP/IP). They were also developed to protect DER communications

from man-in-the-middle (MITM), replay, eavesdropping, DoS, least-privilege violations, spoofing through security certificates, and brute force attacks.

This report, which has been developed in conjunction with UL, expands upon these test cases to provide DER cybersecurity certification recommendations that increase DER resilience and help mitigate cyberattacks. We expect that adoption of an independent certification standard for the cybersecurity of grid edge devices will improve energy security nationwide as DER adoption continues.

1.1 Motivation to Establish Cybersecurity Certification Recommendations

The modern electric grid is rapidly changing. To improve system performance, monitoring, and control, grid edge devices are rapidly being deployed on the grid. This shift toward a more distributed grid with numerous interdependencies being added every year makes defending and securing systems from cyberattacks more difficult than ever. The heightened cyber-physical interdependence between the electric grid and DERs allows attackers more ways to pivot between distribution resources and propagate to critical resources, which could lead to data loss or total operation failure.

If vulnerabilities at the device, network, and application level of DERs are not addressed, DERs could potentially serve as attack vectors for the distribution grid. Despite this, it was found that DER device data and communications are often unencrypted, lack secure firmware upgrades and basic authentication procedures, and are thus vulnerable to cyberattacks (EPRI 2013). Cyberattacks on the grid—such as the 2019 DoS on energy provider Sustainable Power Group (sPower) and the Havex malware, which targeted industrial control system (ICS) devices through a remote access Trojan—emphasize the need for secure DERs and grid edge devices (Zhou et al. 2018).

Despite many publicly available standards and guides, there is no certification standard targeted toward the cybersecurity evaluation and validation of DERs before they are connected to the grid. To address this need, NREL has partnered with UL, with support from other national laboratories—including Sandia, Pacific Northwest National Laboratory, Idaho National Laboratory, Lawrence Livermore National Laboratory, and Lawrence Berkeley National Laboratory—to research and support the development of a cybersecurity certification standard for DERs.

1.2 Relevant Cybersecurity Standards and Guides

Standards, guidelines, and procedures around different aspects of cybersecurity are being actively developed and are evolving quickly. Currently, the National Institute of Standards and Technology (NIST) Cybersecurity Framework is the most thorough and holistic approach to achieve cybersecurity. This framework covers 900 controls over five major functions: identify, protect, detect, respond, and recover. These five functions allow an organizations' security and operations teams to prioritize all areas to achieve holistic cybersecurity throughout their organization. Another source of cybersecurity standards development is the cybersecurity working group co-convened by the SunSpec Alliance (SunSpec) and Sandia. This working group has developed a few supporting documents that could inform future cybersecurity standards,

such as secure network architectures, certification procedures for data and communications security of DERs, recommendations for trust and encryption in DER interoperability standards, and data in-flight requirements for DERs. The following are some key cybersecurity guidelines, standards, and best practices that could be used to enhance grid cybersecurity. Because of the vast breadth of the field of cybersecurity, the following list should be considered a starting point only and is not exhaustive.

- NISTIR 7628: Guidelines for Smart Grid Cybersecurity[2]
- NIST SP 800-82: Guide to Industrial Control Systems (ICS) Security[3]
- NIST Framework for Improving Critical Infrastructure Cybersecurity[4]
- International Electrotechnical Commission (IEC) 62351: Information Security for Power Systems Control Operations[5]
- Institute of Electrical and Electronics Engineers (IEEE) C37.240: IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems[6]
- IEEE 1686: IEEE Standard for Intelligent Electronic Devices Cybersecurity Capabilities[7]
- IEEE 2030.5: IEEE Standard for Smart Energy Profile Application Protocol[8]
- IEEE P2800: IEEE Draft Standard for Interconnection and Interoperability of Inverter-Based Resources (IBR) Interconnecting with Associated Transmission Electric Power Systems[9]
- DOE/U.S. Department of Homeland Security ES-C2M2: Electricity Subsector Cybersecurity Capability Maturity Model Version 1.1[10]
- DOE/NIST/North American Electric Reliability Corporation: Cybersecurity Risk Management Process (RMP) Guideline[11]
- RFC 3268: Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security[12]
- RFC 4962: Guidance for Authentication, Authorization, and Accounting (AAA) Key Management[13]
- UL 1741: The Standard for Inverters, Converters, Controllers, and Interconnection System Equipment for Use with Distributed Energy Resources[14]

---

[2] See https://nvlpubs.nist.gov/nistpubs/ir/2010/NIST.IR.7628.pdf.
[3] See https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.
[4] See https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
[5] See https://www.ipcomm.de/protocol/IEC62351/en/sheet.html
[6] See https://standards.ieee.org/standard/C37_240-2014.html.
[7] See https://standards.ieee.org/standard/1686-2013.html.
[8] See https://standards.ieee.org/standard/2030_5-2018.html.
[9] See https://standards.ieee.org/project/2800.html.
[10] See https://www.energy.gov/oe/downloads/electricity-subsector-cybersecurity-capability-maturity-model-v-11-february-2014.
[11] See https://www.energy.gov/ceser/downloads/cybersecurity-risk-management-process-rmp-guideline-final-may-2012.
[12] See https://dl.acm.org/doi/10.17487/rfc3268.
[13] See *Guidance for Authentication, Authorization, and Accounting (AAA) Key Management* by R. Housely and B. Aboba.
[14] See *Inverters Converters Controllers and Interconnection System Equipment for Use with Distributed Energy Resources* by Underwriters Laboratories Inc.

- UL 2900-1: The Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements[15]
- CIGRE B5/D2.46: Application and Management of Cybersecurity Measures for Protection and Control Systems[16]
- CIGRE D2.31: Security Architecture Principles for Digital Systems in Electric Power Utilities.[17]

These standards, however, do not address cybersecurity features necessary for securing edge devices on the distribution grid. To address this need, NREL and Sandia were tasked by DOE to research, develop, and harmonize cybersecurity standards for PV and DER integration.

1.3 Role of Policy and Regulatory Authorities

Instituting a statewide or nationwide policy or law for cybersecurity standards is difficult. It can take approximately 3 years for a standard to be completely developed, refined, and adopted[18]. Standards for technologies with limited previous research, such as cybersecurity for grid edge devices, often necessitate additional time for initial development. By the time a standard gets approved and becomes publicly available, the industry already faces new threats and challenges that the newly adopted standard did not address. State energy offices' roles in cybersecurity vary across the United States. Some have an active or a formal role, whereas others do not. State energy offices engaged in cybersecurity generally conduct the following key activities, each of which can be further categorized into policy, programs, and operations (NASEO 2020):

- Supporting cyber risk mitigation and resilience.
- Coordinating within state government and across the public-private nexus.
- Responding to a cyberattack affecting energy infrastructure through consequence management as part of all-hazards energy assurance.

Recently, the National Association of State Energy Officials and the National Association of Regulatory Utility Commissioners have launched a new partnership, with support from SETO, to mitigate cybersecurity risks and consequences in solar energy developments (NARUC 2020). They jointly established the Cybersecurity Advisory Team for State Solar to identify challenges, priorities, and mitigative actions to address cybersecurity issues associated with distributed solar systems. This team enables critical strategies and solution pathways for state decision makers to enhance the security of solar systems. The Cybersecurity Advisory Team for State Solar will tap state, federal, and private cybersecurity, grid, and PV expertise, in partnership with utilities and industry, to identify model state programs and actions to mitigate PV-related cybersecurity risks. This SETO-funded project will provide state stakeholders with education, tools, and access to a nationwide network of technical assistance expertise in the form of a collection of resources.

---

[15] See *Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements* by Underwriters Laboratories Inc.
[16] See https://e-cigre.org/publication/603-application-and-management-of-cybersecurity-measures-for-protection-and-control-systems.
[17] See https://e-cigre.org/publication/615-security-architecture-principles-for-digital-systems-in-electric-power-utilities.
[18] See https://www.iso.org/files/live/sites/isoorg/files/developing_standards/resources/docs/std%20dev%targe0074%20date%20planner.pdf

1.4 Past Work

To help ensure the cybersecurity certification procedure is technically sound and useful to industry, NREL, Sandia, and SunSpec created a working group including utilities, manufacturers, vendors, aggregators, national laboratories, and certification laboratories. Stakeholders shared their thoughts on the need for cybersecurity standards for DERs and proposed security features to counter known problems. The working group allowed stakeholders to share their experiences and brainstorm solutions to problems. Discussions focused on the ease of integrating DER security features into the market and on how to seamlessly integrate features without disrupting grid operations. Working group feedback was used to develop a set of cyber-secure functionalities through which DER devices could be secured from several known vulnerabilities and cyberattacks.

Using working group feedback, NREL published the report on *Certification Procedures for Data and Communication Security of Distributed Energy Resources*, which outlined the test cases for verifying DER authentication, authorization, confidentiality, and data integrity for data and communications. These test cases serve to improve the cybersecurity posture of DERs by protecting against MITM, replay, eavesdropping, certificate spoofing, DoS, least-privilege violations, and brute-force attacks.

The previous certification procedure document was used as a basis for this report; however, several test case improvements are recommended. The ability to perform TLS session resumption/renegotiation was the initial Test Case 3 for the certificate procedures of DERs. The test case ensured that DERs had the ability to both resume and renegotiate TLS sessions. If a connection was disrupted before a set resumption window, the session would be resumed. If a connection was disrupted after a set resumption window, a new TLS session would be created, and a new TLS handshake would occur. After testing this feature in a grid environment located in NREL's Power Systems Integration Laboratory (PSIL), however, it was discovered that implementing time-outs causes multiple DER connections to simultaneously attempt to renegotiate and resume a session at the same time, thus causing connection disruptions. It is possible that this was caused by insufficient delta between time-outs for resumption and renegotiation rather than by the features of resumption and renegotiation, but the additional complexity of implementing TLS session resumption and renegotiation is not necessary because these are not necessary features to ensure DER cybersecurity capabilities. The main difference between session renegotiation and resumption is the renegotiation of the session key. If the session key is renegotiated routinely, which is supported in Test Case 4, then the resumption window has a negligible effect on DER cybersecurity. As a result, Test Case 3 should be changed from the ability to perform session renegotiation and resumption to the ability for TLS to recover from network disruptions. The security of a DER device will not be compromised by refining Test Case 3 if a plan is implemented to routinely update keys. This leads to the addition of Test Case 10, security management, which requires a plan for routine key and certificate updating. The last change made was the differentiation between a master secret key update and a key update test for Test Case 4. It was found that requiring a master key could be overkill for smaller DER sites. Whether DERs employ asymmetric or symmetric encryption, they should be able to update their session keys without disrupting TLS.

2 Distributed Energy Resource Vulnerability Analysis

The term *DER* refers to energy storage and generation technologies on the distribution grid and their associated flexible loads. This includes PV, battery storage, wind turbines, and fuel cells, among other resources essential to grid operations. The cybersecurity risk to the power system increases significantly when extending communications to DER devices because of the increased number of devices connected to the utility supervisory control and data acquisition (SCADA) network. In addition, SCADA control signals may be issued over public internet channels instead of using traditional dedicated telecommunications lines. The interconnection of power electronics interfaced DERs has been constantly increasing because of renewables portfolio standards, environmental standards, and customer preferences. It is possible to disable and/or damage local grid operations by changing the frequency and/or voltage trip settings for grid-interactive inverters; by disabling the underfrequency load-shedding; or by getting unauthorized access to the inverter's controls using eavesdropping, manipulation of the human-machine interface, traffic analysis, or other intrusion methods (Johnson et al. 2019).

Although there is a wide range of communication protocols for power systems equipment, there are only a few standardized protocols for DER equipment. Communication protocols such as IEEE 1815 (commonly known as Distributed Network Protocol 3, or DNP3), SunSpec Modbus, and IEEE 2030.5 (commonly known as the Smart Energy Profile, or SEP 2.0) are currently in use in DER communications and were also considered for inclusion in IEEE 1547-2018. This standard might also support other proprietary protocols if the use of that communication protocol is mutually agreed upon by the area electric power system and DER operator; however, IEEE 1547-2018 considers cybersecurity outside its scope. Therefore, to address the nation's need for a unified approach for cyber-secure functionalities, and the associated standards and certification programs, national laboratories started working with standards development organizations and other stakeholders of the energy industry to develop a national certification standard.

2.1 Photovoltaics

Smart inverter technologies that are being required by California and other states can be fully autonomous, but they often require that inverters be connected to the local electric power system, via communication network, to produce an appropriate response for grid support based on varying conditions. The progression of smart inverter technologies and uptake enables a more dynamic and responsive grid including DERs, but it can also elevate the potential for cyberattacks through mandated communications connectivity. The most common attack vector is through monitoring and control capabilities (Watts, Kline, and Ridge 2018). Sensor measurements can be altered to manipulate voltage (Teymouri, Mehrizi-Sani, and Liu 2018). Previous proof-of-concept attacks on PV inverters have altered the reactive reference point to make the inverter absorb reactive power, which leads to power loss. Additionally, exploited PV inverters can overcharge batteries or cause further grid disruptions (Bellini 2020). PV inverters often use default passwords and lack physical tamper detection, which make them vectors for unauthorized access to the system. Spectre and Meltdown chip vulnerabilities enable attackers to seize passwords and other sensitive information (Hill et al. 2019). Additional vulnerabilities, such as remote code execution, stem from unpatched software and connecting PV to public-facing networks.

2.2 Electric Vehicles

EV chargers are rapidly being deployed on the grid. The EV industry has grown by 60% annually from 2014–2019 (IEA 2020). In January 2021, President Biden pledged to deploy 500,000 EV charging stations in the United States (Koning Beals 2021). EV charging stations contain on-site human-machine interfaces and local and remote interfaces that communicate with building energy management systems, the electric grid, and smartphones. EV charging stations have Universal Serial Bus, serial, and Ethernet ports for updates and maintenance. Configuration of power settings or manufacturing patching can often be achieved over building energy management systems, cellular network, or Wi-Fi. These communication modes often contain known vulnerabilities and methods of exploitation. As a result, attacks on the EV have the potential to propagate to connected peripherals and devices. Additionally, the controller area network bus system, which enables communication with vehicle electric charging units, is prone to malware injections because communications are not encrypted or authenticated (El-Rewini et al. 2020). The same vulnerabilities are present in EV tire pressure monitoring systems and are subject to data injections and spoofing. Wireless EV supply equipment, which are without a wired connection between the EV and the charger, are now being deployed. They accomplish both communications and power transfer wirelessly and would be expected to have a similar vulnerability profile (Harnett et al. 2018).

2.3 Wind Plants

Wind power plants are rapidly being deployed across the United States to harness wind energy and to create electricity. These plants and related equipment are also vulnerable to cyberattacks. Wind turbine fiber and Ethernet switches are subject to MITM attacks—including blocking, fabricating, and manipulating traffic—if the switches do not employ port security. Because of the interconnected nature and unsegmented network of some wind plants, exploiting a vulnerability in a wind plant resource, such as a programmable logic controller, may allow the attacker to pivot and infect other resources. Rogue devices with access to the plant network could potentially transmit OPC XML-DA messages to change the operating state of a turbine if wind turbines do not contain authentication mechanisms for communications (Staggs, Ferlemann, and Shenoi 2017). Additional research has shown that SCADA systems for wind turbines could potentially be used to transmit malicious code to the turbine through compromising unencrypted virtual private network communications and physical locks (DOE EERE 2020). In at least one case, a turbine's human-machine interface listed credentials in plaintext, allowing unauthorized access to critical resources (CISA 2018).

Vulnerabilities in different kinds of DERs—such as EV charging systems, PV systems, and others—can potentially be mitigated by adopting the certification recommendations listed in Section 3 of this report.

3 Securing the Modern Grid

The grid is evolving rapidly, so developing defense mechanisms for such a moving target is difficult. To enable utility features such as remote access and remote control, grid edge devices are often equipped with digital communications and control interfaces that present an exploitable attack surface. Some of the most common attacks that could exploit known vulnerabilities in the electric power systems space are MITM, replay, eavesdropping, DoS, spoofing through security certificates, and brute-force (Sundararajan et al. 2018). Based on working group input and other research, functionalities to address these vulnerabilities were proposed. These functionalities include encryption, authentication, authorization, confidentiality, and data integrity for data at rest and data in transit. To accelerate the adoption of security controls for DERs, NREL researchers incorporated these functionalities into test cases as certification recommendations to be used to standardize security for DERs.

3.1 Certification Recommendations for Distributed Energy Resources and Grid Edge Devices

Attacks on DERs and/or other grid edge devices could be a new cyber threat vector with a potential for high impact. Such attacks would require more sophisticated knowledge on the attacker's part and defending against it would require more sophisticated detection and mitigation techniques. One of the few viable and proven methods for securing critical infrastructure is by using a defense-in-depth approach that ensures that the attacker who could compromise one layer of defense could be stopped by subsequent layers. Information technology (IT) companies have long used the defense-in-depth security model to secure IT infrastructure. But when it comes to securing operational technology networks of electric power systems, this approach is not as common or as well implemented.

Following are a few cybersecurity test cases that could be considered by manufactures, vendors, aggregators, and electric utilities to access the security of DERs and grid edge devices. For this report, we consider grid edge devices and IBRs as DERs. Each is described in detail in the following sections.

1. Two-party application association
2. TLS
3. TLS recovery
4. Key update
5. MAC
6. CRL
7. Expired certificate
8. Operating system security and service version
9. Authentication and password management
10. Security management.

These test cases were developed with the intention to inform a potential U.S. industry standard to address the cybersecurity functionality gap and to support the development of appropriate third-party conformity assessment programs for DER cybersecurity testing and certification. These test cases should be considered a starting point only and are not exhaustive.

Because of the variance in DER site sizes, operational purpose, and on-site needs, physical security is out of scope of this report. Physical security is the duty of each individual operator, and they are responsible for ensuring that the appropriate on-site security measures are taken.

3.1.1 Test 1: Two-Party Application Association

Two-party application association means that two devices can communicate with one another. The purpose of this test is to ensure that there is an active connection between the DER and its tester or controller.

In this test, first, ensure that the DER and tester are on an isolated network. Second, initiate a packet capture between the DER and tester on the configured network interface. Third, ensure that bidirectional packets are observed between the DER and tester. Last, disconnect the DER from the tester, and ensure packets are not observed.

3.1.2 Test 2: Transport Layer Security

TLS is a cryptographic communication protocol that secures communications between two devices through features such as message authentication, encryption algorithms, and cryptographic keys. TLS mitigates both MITM and eavesdropping attacks. Power grid operation communications require low latency to ensure real-time data exchange and avoid false data and measurements. To meet these latency requirements, it is recommended for the TLS communication endpoints to use hardware acceleration or high-end processors. The purpose of this test is to ensure that the DER and tester can communicate over TLS while meeting the latency requirements needed for power grid operation.

In this test, first, initiate a packet capture between the DER and tester on the configured network interface. Next, ensure that bidirectional TLS packets of the latest version are observed. Finally, ensure grid communications and capabilities are still functionating as intended with the added latency from TLS.

3.1.3 Test 3: Transport Layer Security Recovery

TLS recovery is the ability for TLS sessions to recover from interruptions. TLS recovery can be tested by ensuring that once a TLS session is interrupted, either because the network interface is inactive or by other means, the session can be resumed or renegotiated.

In this test, first, initiate a packet capture between the DER and tester on the configured network interface and ensure that a TLS handshake has occurred. Second, disable one of the configured network interfaces and ensure that TLS communication is not observed. Last, restart the network interface and confirm that TLS packets are observed again.

3.1.4 Test 4: Key Update

In cryptography, a key is used to encrypt and decrypt data and to help prevent MITM attacks. The purpose of this test is to ensure that the TLS connection is not interrupted when updating keys. Additionally, the test is used to prove that keys can be updated when compromised or have been in use for longer than a predefined window.

In this test, first, establish a TLS connection between the DER and tester on the configured network interface. Once the TLS session is established, provide the DER with an updated TLS

key. Next, using a packet capture, confirm that a new TLS session is negotiated with the new key and that TLS communication occurs. Last, ensure the that the DER operator is informed of the key update.

3.1.5 Test 5: Message Authentication Code

A MAC is a piece of information tagged onto a message to validate whether the message has been altered. MACs protect against replay and MITM attacks. The purpose of this test is to ensure that TLS communication is employing a MAC.

In this test, first, initiate a TLS connection between the DER and tester. Next, using a packet capture software, sniff the traffic between the DER and tester on the configured network interface. Last, verify that the TLS packets use a MAC by checking the last section of the cipher suite employed by TLS in the packet capture. If the TLS packets use a MAC, the type will be specified in the last section of the cipher suite.

3.1.6 Test 6: Certificate Revocation List

A CRL is a list of certificates that have been revoked by the certificate authority. If a revoked certificate is used by TLS, the session is disallowed. This prevents spoofing through certificates. The purpose of this test case is to ensure that the DER is provisioned with a CRL to verify whether a certificate is valid and trustworthy.

In this test, first, use a packet capture software to sniff the traffic between the DER and tester on the configured network interface. Second, initiate a TLS connection with the DER using a certificate in the CRL. Third, using the packet capture, ensure that the TLS handshake is terminated and no TLS communication occurs. Last, confirm that the DER operator is informed of the revoked certificate through logs or error messages.

3.1.7 Test 7: Expired Certificate

An expired certificate is a certificate that is in use past its expiration date. The longer a certificate is used, the more likely it to be compromised; therefore, functionality is needed to ensure that expired certificates are not used. The purpose of this test is to ensure that expired certificates are not used to negotiate TLS sessions. Expired certificate checks prevent replay attacks, MITM, and eavesdropping.

In this test, first, initiate a TLS session with an expired certificate. Next, using a packet capture software, sniff the traffic between the DER and tester on the configured network interface. Third, ensure that no TLS communication is observed. Last, confirm that the DER operator is informed that they are using an expired certificate through logs or error messages.

3.1.8 Test 8: Operating System Security and Service Version

Outdated or unused software, firmware, and services might contain vulnerabilities that can be exploited for cyberattacks. To prevent this, software, firmware, and services should always be updated and patched to the latest secure release. Networked services and software that are not implemented within the DER should be uninstalled or disabled in the DER.

In this test, first, ensure that all applications, services, and firmware are patched, updated, and running secure versions. In addition, confirm that all unused services and software are disabled. Last, ensure that the updates do not break any applications or operations.

3.1.9 Test 9: Authentication and Password Management

The purpose of authentication and password management is to ensure that unauthorized users cannot access the DER or critical components for malicious purposes. Using strong passwords and implementing proper authentication mechanisms prevents attacks, such as least-privilege violations and brute-force credentials.

In this test, first, ensure that all users must authenticate themselves before accessing critical infrastructure or resources. Second, confirm that all users are required to change their default passwords after the first use and that the passwords are complex. The following characteristics are required for a password to be considered complex, as defined by NIST SP 800-63-3 (NIST 2017):

- Use a minimum of eight characters.
- Allow all printable American Standard Code for Information Exchange characters.
- Require capital case (A–Z), lowercase (a–z), and special characters (!,@,#,$,%,^,&,*, ~,`).
- Do not use consecutive and repeatable characters.
- Do not use common dictionary words.

Third, ensure that the DER forces a lockout period and denies access after three unsuccessful log-in attempts. Fourth, confirm that the DER does not allow the user to retry logging in for at least 5 minutes. Finally, ensure that users can only access services and data essential to their work.

3.1.10 Test 10: Security Management

Security management enables organizations to plan for potential cyber threats and mitigate their effect. Security management is ensured by requiring a plan for routinely updating user lists and roles, CRLs, systems, credentials, software, firmware, certificates, and keys.

In this test, check for the existence of a security management plan with systems for routine updates of credentials, certificates, user lists and roles, CRLs, firmware, systems, and software, and keys at least once every 6 months. The plan should include systems for revoking certificates and updating CRLs whenever certificates are replaced or updated. An administrator should generate a new TLS key and renegotiate all sessions at least once every 6 months to ensure that no keys or certificates have been compromised.

3.2 Additional Functionalities for Distributed Energy Resources and Grid Edge Devices

Based on previous research and reports, such as Module-OT and NISTIR 7268, it was found that the following additional cybersecurity features are recommended for DERs.

Table 2. Cybersecurity Functionalities for Distributed Energy Resources and Grid Edge Devices

Functionality	Description	NIST Cybersecurity Framework Function and Category
Network segmentation based on trust levels.	Firewalls should be implemented between network segments to protect against unauthorized access.	Protect – data security
Enabling robust and comprehensive logging.	All device, system, network, and user actions should be logged and monitored for anomalies.	Detect – security continuous monitoring
Unused ports and services should be disabled and inactive.	Only the features necessary for system functionality should be enabled to eliminate potential attack vectors.	Protect – protective technology
Access control should be implemented on all equipment.	Users should only be able to access equipment necessary for their tasks and be required to log in using strong credentials.	Protect – identity management and access control
All interconnected systems and devices should be authenticated.	When pivoting between systems, users should be required to authenticate their identity.	Protect – identity management and access control
Systems and users should be assigned permissions to access data and services.	Sensitive data and services should only be accessed by those with permission.	Protect – identity management and access control
Secure interfaces should be used for user and system updates.	Firewall rules about accessing network interfaces and their specific ports should be implemented.	Protect – protective technology
Role-based access control for interactions among systems, users, and devices	Users should only be able to access equipment and services necessary for their job role.	Protect – identity management and access control
Address space layout randomization enabled on the operating system.	Address space layout randomization randomizes the location, in memory, of an executable, which prevents buffer overflow attacks.	Protect – protective technology
Use the latest stable version of the X.509 certificate.	Updated certificates should be used to validate updates and communication integrity.	Protect – identity management and access control
Software and devices should be actively monitored.	System services should be monitored by intrusion detection services to alert operators of security breaches.	Detect – detection processes
Use Trusted Platform Module and cryptographic device identification at the device level.	All data stored on hardware should be secured through integrated cryptographic keys to prevent tampering.	Protect – protective technology

Functionality	Description	NIST Cybersecurity Framework Function and Category
Validate hashes of remote updates.	All system changes and updates should be validated by comparing the hash of the received update with the original.	Detect – anomalies and events

3.3 Polices to Improve Overall Grid Security

More robust research-and-development programs are needed to improve the effectiveness of cybersecurity guidelines and to ensure that they do not overburden system operators. In the meantime, utilities, aggregators, and equipment manufacturers could consider implementing and testing against appropriate elements of existing cybersecurity standards and guidelines as they become available. As a start, they could align their cyber defenses to NIST's Framework for Improving Critical Infrastructure Cybersecurity. Following are a few recommended general security policies and procedures that could be considered to secure the modern grid (NIST 2018).

1. Isolate internal and external communications from each other. Internal communications are used to communicate with DER controllers, SCADA systems, distributed energy resource management systems, etc. External communications are used to communicate with the internet, vendor, advanced metering infrastructure, cellular systems, etc.
2. Use signature and context-based firewalls, gateways, and secured ports to separate the security domains. Also consider disabling unused ports and services.
3. Use intrusion detection and/or protection systems to monitor communication network traffic.
4. Perform validation of all application software patches and software data updates with rollback capabilities (if applicable).
5. Use Simple Network Management Protocol or similar standards to monitor the health of communication networks and their components.
6. Use role-based access control for all communications, human-machine interfaces, and other places as appropriate. Use role-based access control to authorize any read, write, create, or delete access to stored data. Perform proper validation of the identity of the personnel, vendors, auditors, systems, and applications that are involved in the communications to avoid an insider attack scenario.

4 Case Studies

4.1 Grid Edge Device Compliancy Test Without DERCyST

To demonstrate the resilience of existing DERs against common cyberattacks, 10 test cases, as listed in Section 3, were performed on different DERs.

Two machines were used. A PV inverter, configured for Modbus on Port 502, was the DER under test, and a Kali Linux virtual machine functioning as a DER server was used as the tester. The machines were connected via Ethernet on an isolated network, and the Kali machine's Ethernet interface was bridged and assigned a static IP, as shown in Figure 1.

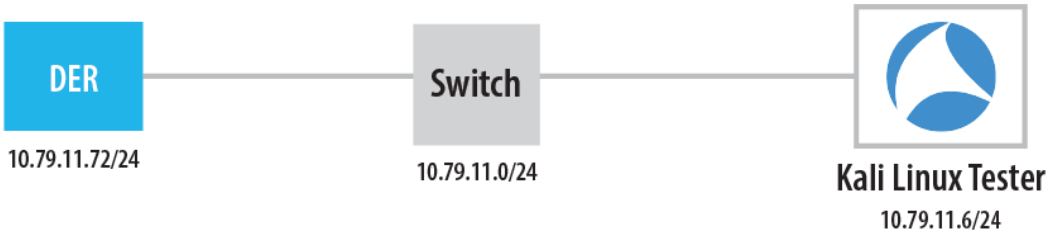


Figure 1. General grid edge device testing architecture

Nine of 10 test cases failed; therefore, the DER device is deemed not secure.

4.1.1 Test 1: Two-Party Application Association

Two-party association is verified by initiating a Hypertext Transfer Protocol (HTTP) session to the DER's web user interface at 10.79.11.72:80 from the Kali virtual machine. Bidirectional two-party communication is observed in a packet capture, as shown in Appendix A, Figure A-1. After waiting 10 minutes and releasing the connection by closing the web browser, no more bidirectional communication is observed.

Result: Passed

4.1.2 Test 2: Transport Layer Security

The connection between the DER and tester does not have TLS enabled. No TLS packets are captured in Wireshark on the Kali Linux tester. Without TLS, communications are subject to MITM and eavesdropping attacks, as shown in Appendix A, Figure A-1. OpenSSL can be used to implement TLS. OpenSSL is installed on the DER server, but for TLS communications to be established, the inverter must be running a TLS server and listening on an available port. An Nmap scan of the PV inverter shows an open port 14729, but it does not respond to TLS requests to verify certificate information, thus proving that the port is not running TLS. The Nmap scan is shown in Appendix A, Figure A-2.

Result: Failed

4.1.3 Test 3: Transport Layer Security Recovery

TLS communications are not supported by the DER; therefore, the TLS network disruption recovery is not supported.

Result: Failed

4.1.4 Test 4: Key Update

TLS communications are not supported by the DER; therefore, there is no key used for the TLS certificate verification.

Result: Failed

4.1.5 Test 5: Message Authentication Code

A MAC is not used in the observed HTTP and Modbus communications. By design, HTTP does not use a MAC. MACs are used by certain cipher suites. No cipher suite is used in traditional Modbus, and therefore a MAC is not used. This is verified in Wireshark packet captures.

Result: Failed

4.1.6 Test 6: Certificate Revocation List

There is no CRL in the DER because the DER does not enable TLS or any communications that require certificates.

Result: Failed

4.1.7 Test 7: Expired Certificate

By design, Modbus and HTTP do not use certificates.

Result: Failed

4.1.8 Test 8: Operating System Security and Service Version

As shown in Appendix A, Figure A-2, the operating system and services are not the latest version. CherryPy is version 3.2.2, but it should be the secure version 18.6.0. Dropbear is version 2012.55, but it should be the latest version 2020.81. Port 80 HTTP should be replaced with port 443 Hypertext Transfer Protocol Secure (HTTPS) to enable a secure HTTP connection. Port 14729 should be closed because it is not necessary for the functionality of the DER, and it is a possible attack vector. The latest Linux Kernel is not used, and the firmware has not been updated since the inverter's date of manufacture.

Result: Failed

4.1.9 Test 9: Authentication and Password Management

Default passwords are not required to be changed after the first use. There is also no lockout for log-in attempts. Complex passwords are not used for access and should be required.

Result: Failed

4.1.10 Test 10: Security Management

There is no required plan for routine credentials, certificates, user lists and roles, CRLs, firmware, systems, and software, and key updates.

Result: Failed

4.2 Grid Edge Device Compliance Test with DERCyST

To enable DER devices to pass the cybersecurity certification procedure, DERCyST was developed. DERCyST is a software, operated as a bump-in-the-wire, based on the open-source Module-OT[19] security module. The software enables DERs to pass the cybersecurity certification procedure when it is deployed on a DER site and control center as a bump-in-the-wire. DERCyST features include encrypted TCP/IP traffic over TLS, a CRL, certificate checks, key updates, and session renegotiation.

To demonstrate that DER devices have the potential to be more resilient, have better security design, and can maintain a strong cybersecurity posture, DERCyST was incorporated into a microgrid testbed in NREL's PSIL, as shown in Figure 2. Figure 3 depicts testbed power connections. The certification procedure test cases were performed on DER devices connected to the DERCyST application. For this compliance test, the microgrid controller was used as the tester.

All test cases passed, thus proving that DER devices have the potential to meet cybersecurity standards and maintain a strong cybersecurity posture. The results are described next.

[19] See https://www.nrel.gov/docs/fy20osti/74697.pdf.

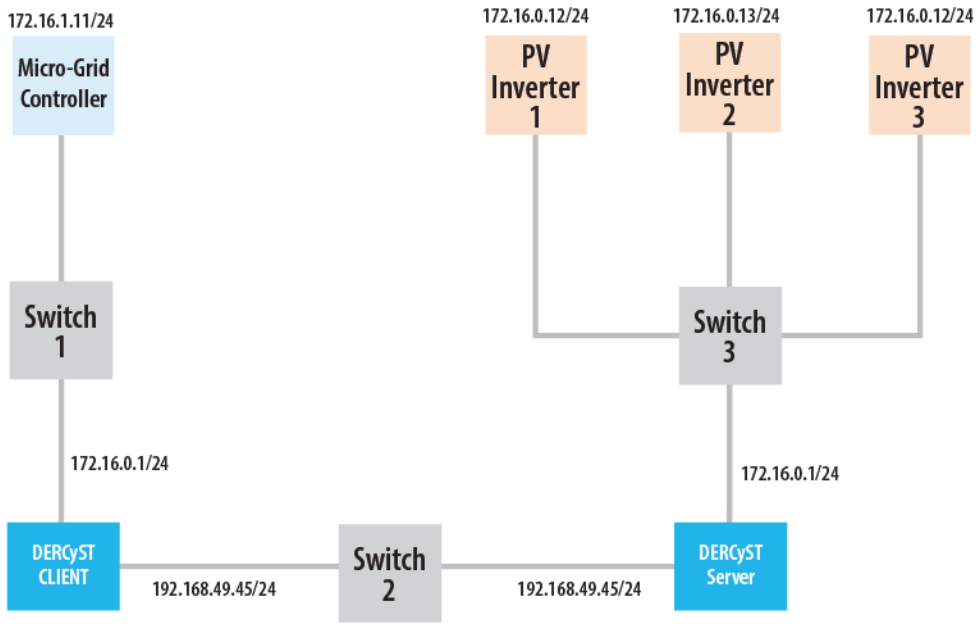


Figure 2. Certification testbed

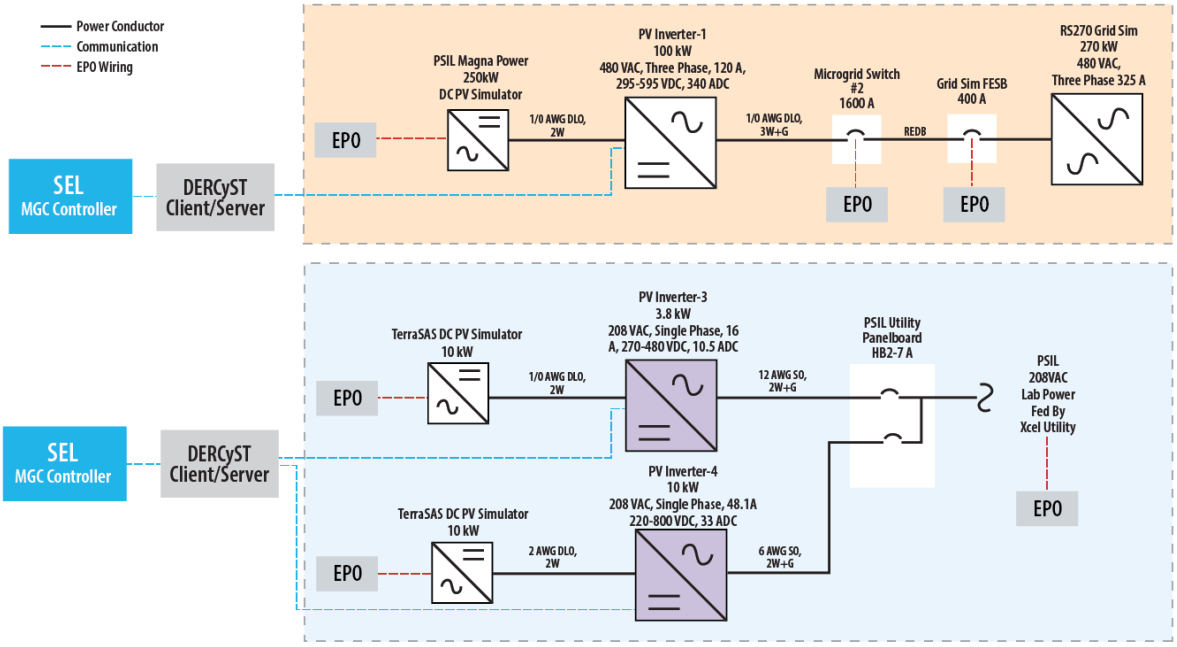


Figure 3. DERCyST power connections

4.2.1 Test 1: Two-Party Application Association

The microgrid controller initiates the Modbus TCP connection to the inverter. The connection between the DER and controller is verified with bidirectional Modbus communications. The

network traffic is shown in Appendix B, Figure B-1. After 10 minutes of communication, the session is terminated, and communications are not observed.

Result: Passed

4.2.2 Test 2: Transport Layer Security

Modbus traffic is being encrypted with TLS over the wide-area network. Instead of seeing Modbus Read registers, only bidirectional TLS packets of the latest version are observed in a packet capture. This is shown in Appendix B, Figure B-2. Modbus read and write operations function as intended, and TLS packets did not cause anomalies in grid operations.

Result: Passed

4.2.3 Test 3: Transport Layer Recovery

A packet capture of the TLS recovery is shown in Appendix B, Figure B-3. When the network interface is brought down at 63 seconds into the packet capture, TLS communications are disrupted. But when the network interface is brought back up at 81 seconds into the capture, TLS communications are observed.

Result: Passed

4.2.4 Test 4: Key Update

Initial TLS communications are established with OpenSSL. Once the client receives an updated key, the old TLS session is terminated. Seconds later, the OpenSSL server creates a new TLS connection with the client via a TLS handshake using the updated OpenSSL key signed by the root certificate authority. TLS communications are restored. DERCyST's output when the new key is issued is shown in Appendix B, Figure B-4. DERCyST's output after the new key is issued is shown in Appendix B, Figure B-5. The network capture of the new TLS handshake and key update is shown in Appendix B, Figure B-6.

Result: Passed

4.2.5 Test 5: Message Authentication Code

The OpenSSL application programming interface used in the DERCyST program allows for specifying the cipher suite. We used TLS_AES_128_CCM_8_SHA256, which contains the SHA256 MAC. Appendix B, Figure B-7 shows the MAC in a packet capture of a TLS packet heading for a DERCyST server.

Result: Passed

4.2.6 Test 6: Certificate Revocation List

A CRL is specified in the DERCyST configuration file, shown in Appendix B, Figure B-8. When DERCyST uses a certificate in the CRL, the TLS handshake fails, and no TLS communication occurs. The operator is informed of the revoked certificate from the DERCyST logs, as shown in Appendix B, Figure B-9.

Result: Passed

4.2.7 Test 7: Expired Certificate

If the certificate used by the TLS server's expiration date is overdue, TLS communications are disallowed. DERCyST is constantly checking the certificate expiration date and comparing it to the current date and time. If an expired certificate is used by the DER, TLS communications are disabled, and the operator is informed of the revoked certificate. The output of DERCyST to the operator is shown in Appendix B, Figure B-10.

Result: Passed

4.2.8 Test 8: Operating System Security and Service Version

Only necessary ports are open—22 for Secure Shell (SSH) access to the machine, and 8000 for TLS communication. The port scan is shown in Appendix B, Figure B-11. The OpenSSH service in Appendix B, Figure B-11 was the latest version at the time of capture; however, OpenSSH 8.6 is currently the latest version. Ubuntu 16.04 LTS, which is common criteria certified, is used as the operating system. Firmware is the latest version and was updated through the manufacturer portal before testing. The latest secure release of OpenSSL (version 1.1.1) and Nmap (version 7.8) are used, and the DER functions with no data loss or anomalies.

Result: Passed

4.2.9 Test 9: Authentication and Password Management

To allow for remote control and monitoring, DERCyST supports the SSH protocol. To limit the potential for abuse of this connection (as well as the device in general), DERCyST allows outside SSH connections only through its least-privileged user. This user account has read-only access to many of the configuration files, and it can be used to monitor the device or view its settings. To change any settings, the active user must be switched to a more privileged account that can request administrative privileges using the "sudo" command. By requiring a passphrase and hardening the SSH server, the device aims to be protected from least-privilege violations that lead to unwanted intrusion and alteration of its configuration. Passwords are complex, are required to be changed upon first use, and a lockout period of 5 minutes is implemented after three unsuccessful log-in attempts.

DERCyST supports the following authorized role for the users (e.g., DER operators) and administrators. By maintaining the authorized roles, DERCyST completes the requirement policy of the Federal Information Processing Standard 140-2.

- **User role:** The role of the user in DERCyST is to perform general services such as cryptographic operations and other security functions.
- **Cryptographic officer role:** In DERCyST, a cryptographic officer performs the DERCyST initialization, the input-output of cryptographic keys, and other audit or management functions, e.g., execute DERCyST cryptographic code, physical access to the operating environment. They are able to access the module before and after installation.

User management is done using Ubuntu's "adduser" feature.

Table 3. DERCyST User Roles

Username	Privileges
Motuser	User (SSH, basic)
Moduleot	Crypto officer (sudo)
Root	Root

Result: Passed

4.2.10 Test 10: Security Management

There exists a plan for routinely updating software, services, firmware, user lists and roles, certificates, and keys. A cryptographic officer user should generate a new TLS key and renegotiate all TLS sessions at least once every 6 months to ensure that no keys have been compromised. A system exists for revoking certificates and updating CRLs whenever certificates are replaced or updated.

Result: Passed

5 DERCyST Integration with Cyber Range

DERCyST is integrated into NREL's Cyber Range,[20] where it is being tested, validated, emulated, and visualized using hardware-in-the-loop. Cyber Range allows for experiments to be created and tested in a fully customizable, large-scale emulation with virtual devices, hardware devices, control flow, power flow, and a visualization application. This is beneficial because Cyber Range allows for scaling and testing the certification procedures in large, virtual grid environments, with power and communication flow, which leverage physical testbed resources, such as the PV inverters in the PSIL. Figure 4 depicts the visualization of the microgrid emulation in Cyber Range that is being used for testing DERCyST.

[20] See https://www.osti.gov/biblio/1659978.

Figure 4. Cyber Range emulation experiment

Communication between Cyber Range and the hardware-in-the-loop testbed is enabled with a software-defined networking switch. A trunk port to the Cyber Range network from the switch allows remote management via a virtual private network. Figure 5 depicts how the microgrid testbed in the PSIL is being incorporated into Cyber Range.

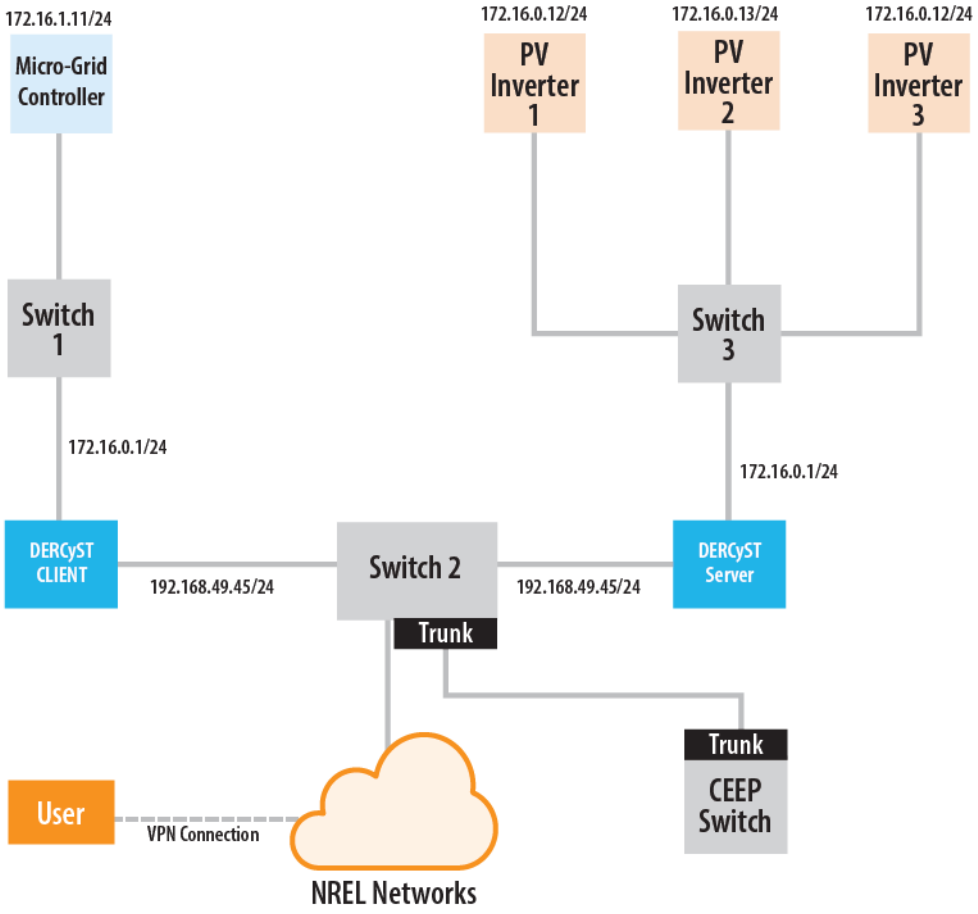


Figure 5. Cyber Range connection to DERCyST testbed

6 Cybersecurity for the Future Grid

6.1 Establish and Foster Partnerships with Industry

Security benefits from a joint effort among stakeholders – such as government, equipment vendors, utilities, aggregators, asset owners, standards development organizations, and academic institutions – sharing data and mutually planning to elevate cybersecurity. Partnerships among all stakeholders promote improved cybersecurity strategies across the electric sector. Regular correspondence and effective communications among electric sector stakeholders, such as utilities and equipment vendors, help promote better device and application security. For example, a government-industry partnership generated practical cybersecurity measures and helped equipment vendors produce more effective equipment in support of the utility operations by creating digital protection and cybersecurity tools for a smart meter network (Hawk and Kaushiva 2014).

6.2 Proactively Develop and Adopt New Tools to Address Future Technological Advancements

Threat actors could adjust to each security measure that is used to protect critical systems; therefore, national laboratories, academic institutions, and private research organizations should continue extending their understanding of cyber attackers and advanced persistent threats and continue sharing their research findings with each other. Further, electric utilities, aggregators, and asset owners should stay current with the cyber vulnerabilities and cyber threat patterns and signatures throughout the electric sector and ICS to develop proactive mitigations. This can be accomplished, to some degree, by checking vulnerability databases such as:

- Common Vulnerabilities and Exposures,[21] which is maintained and updated by the MITRE Corporation
- ICS-CERT's Advisories,[22] which give information about security issues and vulnerabilities

Additionally, periodic third-party vulnerability assessments and penetration testing of their IT and ICS networks will enhance security postures. It is highly recommended to follow the Cyber-Informed Engineering methodology to enable system wide security that enables seamless integration of both legacy and emergent technologies. This methodology ensures cybersecurity is considered throughout product design through a framework consisting of impact analysis, system architecture, engineered controls, resilience planning, procurement and contracting, cybersecurity culture, and other elements (Anderson et al. 2017).

6.3 Areas That Require Further Research and Development

As the modern grid advances from centralized generation to more distributed generation, the potential vulnerabilities and the cyber threats to the electric grid will also advance. Each connected device could open a potential doorway for hackers. As outlined in DOE's *Multiyear Plan for Energy Sector Cybersecurity*, game-changing technologies are needed that enable a fully distributed grid while protecting national security (DOE EERE 2014); therefore, to

[21] See https://www.cve.mitre.org/cve/index.html.
[22] See https://us-cert.cisa.gov/ics/advisories.

proactively address cybersecurity concerns related to the evolving modern grid, research and development for cutting-edge technologies are needed. Some basic research questions are: how to use redundant communication paths (to eliminate the impacts of losing one path); how to actively monitor and alarm if redundant communication paths are lost; how to maintain a "gold copy" of system device configuration files to greatly expedite recovery after a disabling attack or a ransom situation; and how to securely update software/firmware using code-signing and boot-loader processes. Following are some specific game-changing topics that could help enable a fully distributed grid.

6.3.1 Named Data Networking

Named data networking (NDN) has increasing potential to change the way DER communications are handled in the future. Through design principles that increase security and resilience, the adoption of NDN in power communications is becoming more practical as research and implementation of this technology develop. NDN is an information-centric networking architecture that differs from traditional IP networking in multiple ways. The communication paradigm for IP networking is establishing a connection between two endpoints to facilitate data transfer. NDN, however, distributes data throughout the network infrastructure, eliminating the need for end-to-end tunneling. This is possible through data producers digitally signing their data, which can be stored, fetched, and validated by the data consumers. Standardizing this technology has the potential to increase the minimum-security posture for those who observe the standard. Standardization of this technology also will not be as disruptive as one might think. NDN is considered a *universal overlay*, meaning that it can be implemented on top of existing TCP/User Datagram Protocol/IP infrastructures.

6.3.1.1 Security by Design

In traditional communications through TCP/IP, a tunnel is created connecting two endpoints. This facilitates the end-to-end principle, where intermediate routing and forwarding hardware is minimal in complexity and function. With the inclusion of TLS, an encrypted tunnel is created connecting two endpoints. NDN removes this dependence of tunneling for data integrity. In practice, this does not remove the need for encryption between hosts to preserve confidentiality of the data in transit. This allows for distribution of these data through the underlying network infrastructure. Each piece of data is digitally signed by the producer, ensuring that the data have not been tampered with during transit and providing verifiable proof that the data came from the expected producer.

6.3.1.2 Resilience by Design

Network resilience is essential in the power communication space. Loss of connectivity can lead to safety and operational issues. NDN is designed to incorporate distributed redundance of data within the network infrastructure. Given multiple paths of communication between producers and consumers, data can still be produced and consumed even during link outages. Each forwarding node in the network stores a copy of the data produced in a module called the content store. These forwarding nodes can share these data and serve them with consumers even if the producer becomes unreachable to the network. This is advantageous to resilience because sections of the network can become unreachable without eliminating the availability of data sharing between consumers and producers.

6.3.1.3 Network Load Reduction by Design

As NDN forwarding nodes store produced data in the content store, they can also serve these data without linking the consumer to the producer. This has the potential to limit the amount of data being transferred throughout the underlying network infrastructure. Communications are established only between the consumer and the nearest NDN forwarder that has the requested data in its content store. For example, this could reduce the number of hops the data need to travel between the consumer and producer from five to only one if the next hop from the consumer has the requested data in its content store.

6.3.2 Zero-Trust Network for Grid Operations and Management

Zero-trust networking (ZTN) as defined in NIST SP 800-207[23] is becoming the security best practice for organizations ("Executive Order 14208"). This networking style moves defense from static, network-based parameters to dynamic aspects such as users, assets, and resources. Traditional network design relies on a border defense; everything inside the border is trusted. Zero trust assumes no implicit trust is gained to an individual or device from just being on the network. Zero-trust design is essential when working with users that have remote access. One key aspect of zero trust architectures is protecting the resources of a network instead of the network segments. This increases authorization and authentication checkpoints but mitigates the risks of compromised devices or user accounts on the network.

The integration of zero-trust networks into grid operations will increase the security posture and potentially the overall health of the U.S. electric grids. NIST defines tenets of zero trust, which are principles that must be followed to establish a zero-trust posture.

6.3.2.1 Variations of Zero-Trust Networks

There are various ways to implement a zero-trust architecture workflow. Each variation is associated with different requirements and components; however, a comprehensive solution will include a combination of the following three variations as stated by NIST in SP 800-207.

- Zero-trust architecture using enhanced identity governance
- Zero-trust architecture using micro-segmentation
- Zero-trust architecture using network infrastructure and software-defined perimeters.

6.3.2.2 Trust Algorithm

The trust algorithm determines if system requests are allowed or denied. (In a zero-trust network the trust algorithm resides in a module called the policy engine.) The trust algorithm uses a variety of inputs when making allow/deny decisions. The trust algorithm takes as inputs

- Request type (e.g., access)
- Policy
- Subject Database
- Asset database
- Resource requirements
- Threat intelligence

[23] See https://csrc.nist.gov/publications/detail/sp/800-207/final.

Each data source that influences this algorithm can be weighted to reflect the importance of each source.

6.3.2.3 Network/Environment Components

A zero-trust architecture comprises various components. To be considered zero-trust, an architecture must incorporate all of the following:

- Zero-trust architectures require basic network connectivity to exist.
- Zero-trust architectures require the ability to distinguish between owned assets and managed assets.
- Zero-trust architectures require the ability to observe of all network traffic.
- Zero-trust architectures require resources to be locked behind a policy enforcement point.
- Zero-trust architectures require the data and control plane to be logically separate.
- Zero-trust architectures require that assets can reach a policy enforcement point.
- Zero-trust architectures require that a policy enforcement point is the only component with access to the policy administrator.
- Zero-trust architectures require the ability for remote assets to access resources.
- Zero-trust architectures require a scalable infrastructure.

6.3.3 Quantum-Resistant Cryptographic Algorithms

It has long been known that the emergence of quantum computing could destabilize our current cryptography efforts. The current research into "quantum-resistant" cryptographic techniques is cutting edge but targeted at general / large computing. However, we should also be thinking of our legacy systems (including IoT and DER devices) which may have resource constraints. If quantum-resistant techniques are too computationally intense for these low-cost devices, then they will be vulnerable. In the field of cybersecurity, we know that a system is only as strong as its weakest link. In this case that link would be the entirety of our distributed energy infrastructure. Therefore, considering research into the interoperability of DER and quantum-resistant cryptography is a worthwhile endeavor.

Currently, there are two categories of cryptography being researched for quantum-resistant algorithms. First, there are public-key encryption and key establishment. Second, there are digital signatures. Both concepts are integral in our everyday lives—from banking to online web browsing—but they are also required for any secure communication, authentication, message integrity checks, and non-repudiation. As we look toward the future where quantum computing will be commonplace, standardization of quantum-resistant cryptographic algorithms in DERs will become a necessity for the integrity of our systems. Most QRCAs do not need quantum hardware to run, so adoption of these algorithms into existing DER technology may be possible without fundamental redesign of equipment.

6.3.4 5G for Modern Grid and Power Communications

Edge devices are becoming ubiquitous across many areas of the energy landscape, such as power systems, EVs, DERs (solar and wind), smart cities and energy-efficient buildings, energy storage, hybrid energy systems, energy infrastructure, and grid cybersecurity. 5G communication provides a multitude of capabilities that could prove useful in the context of DERs. One such

capability is network slicing[24]. In essence, this capability uses concepts akin to SDN and network function virtualization to create a dynamic structure of virtual networks on top of physical broadband. This provides increased flexibility of each network's functions, resources, and performance. Bringing this technology to DER edges could provide a dynamic and flexible communication infrastructure by way of increased mutability and management. In addition, the frequency, and the speed of the data transfer via 5G have increased from 4G (Reka et al. 2019). Reka et. al, in "Future Generation 5G Wireless Networks for Smart Grid: A Comprehensive Review," stated that 5G can transfer up to 10 Gbps at frequencies from 3–90 GHz. This improvement in speed enables low-latency communications to a degree that we have not experienced with earlier eras of wireless communications, such as 4G and 3G. These improvements in speed, latency, and control have the potential to greatly benefit the DER space. Standardization of this technology could lead to an increase of minimum networking performance and system efficiency between DER endpoints.

[24] See https://www.nrel.gov/docs/fy21osti/78055.pdf.

7 Conclusions and Future Work

The proposed certification procedures can be used as a basis for a cybersecurity standard for DER devices. Through implementing the certification recommendations, DERs incorporate authentication, authorization, confidentiality, and data integrity features. These features have been shown to prevent common cyberattacks, such as MITM, replay, eavesdropping, DoS, least-privilege violations, and brute force attacks. By documenting that DER devices pass the certification procedures test cases without impacting critical functions needed for power system operation, a standard of security can support DER adoption into the grid without risk of compromising grid security.

SETO has established a Laboratory Coordination Committee comprising six national laboratories—NREL, Sandia, Pacific Northwest National Laboratory, Idaho National Laboratory, Lawrence Livermore National Laboratory, and Lawrence Berkeley National Laboratory—to support and coordinate the development of cybersecurity standards among industry stakeholders, standards development organizations, state and federal regulatory bodies, and national laboratories. The goal of this newly formed committee is to accelerate the adoption and implementation of cybersecurity standards through supporting the development of equipment and communication cybersecurity standards for DERs and the development of a national cybersecurity certification standard that could become the reference for the industry. Specific future work plans include:

- Publishing the outline of investigation for DER cybersecurity testing protocols and potentially carrying that forward to a U.S. consensus standard with the help of other standards development organizations.
- Supporting the development of appropriate third-party conformity assessment programs for DER cybersecurity testing and certification.
- Developing white papers, industry webinars, and related activities to increase awareness of DER cybersecurity requirements and conformity assessment programs.
- Organizing and hosting a DER cybersecurity summit by engaging thought leaders and key stakeholders from national laboratories, utilities, and the energy and renewables industries (such as solar, energy storage, EV charging, and wind) to promote awareness and to establish practical and actionable plans to move forward.

References

Anderson, Robert S., Jacob Benjamin, Virginia L. Wright, Luis Quinones, and Jonathan Paz. 2017. *Cyber-informed engineering*. Idaho Falls, ID (United States): Idaho National Lab. (INL). No. INL/EXT-16-40099. https://inl.gov/wp-content/uploads/2021/05/CIE_March2017.pdf.

Bellini, Emiliano. 2020. "Solar Inverters vs. Cyber Attacks." *PV Magazine*, August 17, 2020. https://www.pv-magazine.com/2020/04/17/solar-inverters-vs-cyberattacks/.

Cybersecurity and Infrastructure Security Agency (CISA). 2018. "ICS Advisory (ICSA-15-162-01A): RLE Nova-Wind Turbine HMI Unsecure Credentials Vulnerability (Update A)." August 27, 2018. Arlington, VA. https://us-cert.cisa.gov/ics/advisories/ICSA-15-162-01A.

———. 2020. "ICS Alert (AA20-049A): Ransomware Impacting Pipeline Operation." October 24, 2020. Arlington, VA. https://us-cert.cisa.gov/ncas/alerts/aa20-049a.

Electric Power Research Institute (EPRI). 2013. *Cyber Security for DER Systems: Version 1*. Palo Alto, CA. https://smartgrid.epri.com/doc/der-rpt-07-25-13.pdf.
Hawk, Carol, and Akhlesh Kaushiva. 2014. "Cyber Security and the Smarter Grid." *The Electricity Journal*: 89–90.

El-Rewini, Zeinab, Karthikeyan Sadatsharan, Daisy Flora Selvaraj, Siby Jose Plathottam, and Prakash Ranganathan. 2020. "Cybersecurity challenges in vehicular communications." *Vehicular Communications* 23 (2020): 100214. https://www.sciencedirect.com/science/article/pii/S221420961930261X.

"Executive Order 14208 of May 12, 2021, Improving the Nation's Cybersecurity" Code of Federal Regulations, title 3 (2021 comp.). https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

Harnett, Kevin, Brendan Harris, Daniel Chin, and Graham Watson. 2018. *Doe/dhs/dot volpe technical meeting on electric vehicle and charging station cybersecurity report*. John A. Volpe National Transportation Systems Center (US). No. DOT-VNTSC-DOE-18-01. https://rosap.ntl.bts.gov/view/dot/34991.

Hill, Mark D., John Masters, Parthasarathy Ranganathan, Paul Turner, and John L. Hennessy. 2019. "On the Spectre and Meltdown Process Security Vulnerabilities." *IEEE Micro* 39 (2): 9–19. https://ieeexplore.ieee.org/abstract/document/8634886/.

Institute of Electrical and Electronics Engineers (IEEE). 2018. IEEE 1547-2018 – IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces. Piscataway, N.J. https://standards.ieee.org/standard/1547-2018.html.

International Energy Agency (IEA). 2020. *Global EV Outlook 2020*. Paris, France. https://www.iea.org/reports/global-ev-outlook-2020.

Johnson, Jay, Jimmy Quiroz, Ricky Concepcion, Felipe Wilches-Bernal, and Mathew J. Reno. 2019. "Power System Effects and Mitigation Recommendations for DER Cyberattacks." *IET Cyber-Physical Systems: Theory & Applications*. https://doi.org/10.1049/iet-cps.2018.5014.

Kephart, Tim. 2021. "Report: Oldsmar Water Hack Came After City Computer Visited Compromised Website." *ABC Action News*, May 19, 2021. https://www.abcactionnews.com/news/region-pinellas/report-oldsmar-water-hack-came-after-city-computer-visited-compromised-website.

Koning Beals, Rachel. 2021. "The Big Challenges to Biden's Electric Vehicle Pledge—Not Every State Is On Board." *MarketWatch*, February 6, 2021. https://www.marketwatch.com/story/the-big-challenge-to-bidens-electric-vehicle-pledge-every-state-is-different-11612389231.

National Association of Regulatory Utility Commissioners (NARUC). 2020. "NASEO and NARUC Announce Initiative on Cybersecurity in Solar Projects: Cybersecurity Advisory Team for State Solar (CATSS)." June 18, 2020. Washington, D.C. https://www.naruc.org/about-naruc/press-releases/naseo-and-naruc-announce-initiative-on-cybersecurity-in-solar-projects-cybersecurity-advisory-team-for-state-solar-catss/.

National Association of State Energy Officials (NASEO). 2020. *Enhancing Energy Sector Cybersecurity: Pathways for State and Territory Energy Offices*. Arlington, VA. http://www.naseo.org/data/sites/1/documents/publications/Final%20NASEO_Cybersecurity%20Report%20(062020).pdf.

National Institute of Standards and Technology (NIST). 2017. *NIST Special Publication 800-63-3: Digital Identity Guidelines*. Gaithersburg, MD. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

Rose, Scott, et al. 2020. *SP 800-207: Zero Trust Architecture*. Gaithersburg, MD: National Institute of Standards and Technology, Computer Security Resource Center. https://csrc.nist.gov/publications/detail/sp/800-207/final.

———. 2018. *Framework for Improving Critical Infrastructure Cybersecurity: Version 1.1.* Gaithersburg, MD. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

North American Electric Reliability Corporation (NERC). 2019. "Lessons Learned: Risks Posed by Firewall Firmware Vulnerabilities." Atlanta, GA. www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/20190901_Risks_Posed_by_Firewall_Firmware_Vulnerabilities.pdf.

Reka, S. Sofana, Tomislav Dragicevic, Siano Pierluigi, and S. R. Sahaya Prabaharan. 2019. "Future Generation 5G Wireless Networks for Smart Grid: A Comprehensive Review." *Energies* 12 (11). https://doi.org/10.3390/en12112140.

Saleem, Danish, and Cedric Carter. 2019. *Certification Procedures for Data and Communications Security of Distributed Energy Resources*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-73628. https://www.nrel.gov/docs/fy19osti/73628.pdf.

Staggs, Jason, David Ferlemann, and Fugeet Shenoi. 2017. "Wind Farm Security: Attack Surface, Targets, Scenarios, and Mitigation." *International Journal of Critical Infrastructure Protection* 17: 3–14. https://www.sciencedirect.com/science/article/pii/S1874548217300434?casa_token=n-1dLY5Q2cwAAAAA:wE0v5GrVUkRaaeWEDjohjK_VkQ1i5MFpryA7Zhq2zQSp674uV6LKHUKY_ShaznflyFnYnxMkdQ.

Sundararajan, Aditya, Aniket Chavan, Danish Saleem, and Arif I. Sarwat. 2018. "A Survey of Protocol-Level Challenges and Solutions for Distributed Energy Resource Cyber-Physical Security." *Energies* 11(9): 2360. https://www.mdpi.com/1996-1073/11/9/2360/htm.

Teymouri, A., A. Mehrizi-Sani, and C. C. Liu. 2018. "Cyber Security Risk Assessment of Solar PV Units with Reactive Power Capability." Presented at the IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society, 2,872–77.

U.S. Department of Energy (DOE) Office of Energy Efficiency and Renewable Energy (EERE). 2020. *Roadmap for Wind Cybersecurity*. Washington, D.C. https://www.energy.gov/sites/prod/files/2020/07/f76/wind-energy-cybersecurity-roadmap-2020v2.pdf.

———. 2018. *Multiyear Plan for Energy Sector Cybersecurity*. Washington, D.C. https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf.

Watts, Raymond, Brian Kline, and Tom Ridge. 2018. *Potential Electric Grid Vulnerability from Cyber Enabled Foreign Actors: A Risk Assessment Study of Solar Inverter Technology*. Washington, D.C.: Protect Our Power. https://protectourpower.org/wp-content/uploads/2018/11/Ridge-Global-and-Potential-Electric-Grid-Vulnerability.pdf.

Zhou, Xiaojun, Zhen Xu, Liming Wang, Kai Chen, Cong Chen, and Wei Zhang. 2018. "Kill Chain for Industrial Control System." Presented at the 2018 International Conference on Smart Materials, Intelligent Manufacturing and Automation (SMIMA 2018). https://www.matec-conferences.org/articles/matecconf/abs/2018/32/matecconf_smima2018_01013/matecconf_smima2018_01013.html.

Bibliography

Chown, P. 2002. "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)." *RFC*. https://dl.acm.org/doi/10.17487/rfc3268.

Cybersecurity and Infrastructure Security Agency (CISA). "ICS-CERT Advisories." 2016. Access May 6, 2016. https://us-cert.cisa.gov/ics/advisories.

Bennet, Daniel, Adarsh Hasandka, M.D. Touhiduzzaman, and Evan Vaughan. 2021. "Service-Based, Segmented, 5G Network-Based Architecture for Securing Distributed Energy Resources: Preprint." Presented at the 2021 IEEE Power & Energy Society General Meeting, July 25-29, 2021. https://www.nrel.gov/docs/fy21osti/78055.pdf.

Hasandka, Adarsh, Joshua Rivera, and Joshua Van Natta. 2020. *NREL's Cyber-Energy Emulation Platform for Research and System Visualization*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-74142. https://www.osti.gov/biblio/1659978.

Housley, R., and B. Aboba. 2007. "Guidance for Authentication, Authorization, and Accounting (AAA) Key Management." *BCP* 132, *RFC* 4962 (July).

Hupp, William, Adarsh Hasandka, Ricardo Siqueria de Carvalho, and Danish Saleem. 2020. "ModuleOT: A Hardware Security Module for Operational Technology: Preprint." Presented at the IEEE Texas Power and Energy Conference (TPEC), College Station, Texas, February 6−7, 2020. https://www.nrel.gov/docs/fy20osti/74697.pdf.

Institute of Electrical and Electronics Engineers (IEEE). 2013. IEEE 1686-2013 – IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities. Piscataway, NJ. https://standards.ieee.org/standard/1686-2013.html.

———. 2014. IEEE C37.240-2014 – IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control System. Piscataway, NJ. https://standards.ieee.org/standard/C37_240-2014.html.

———. 2018. IEEE 2030.5-2018 – IEEE Standard for Smart Energy Profile Application Protocol. Piscataway, NJ. https://standards.ieee.org/standard/2030_5-2018.html.

———. 2020. IEEE P2800 – IEEE Draft Standard for Interconnection and Interoperability of Inverter-Based Resources (IBR) Interconnecting with Associated Transmission Electric Power Systems. Piscataway, NJ. https://standards.ieee.org/project/2800.html.

International Council on Large Electric System (CIGRE). 2014. *Application and Management of Cybersecurity Measures for Protection and Control Systems*. Paris, France. https://e-cigre.org/publication/603-application-and-management-of-cybersecurity-measures-for-protection-and-control-systems.

———. 2015. *Security architecture principles for digital systems in Electric Power Utilities*. Paris, France. https://e-cigre.org/publication/615-security-architecture-principles-for-digital-systems-in-electric-power-utilities.

IPCOMM. 2021. “IEC 62351.” https://www.ipcomm.de/protocol/IEC62351/en/sheet.html.

ISO. 2021. “Stages and Resources for Standards Development.” https://www.iso.org/stages-and-resources-for-standards-development.html.

National Institute of Standards and Technology (NIST). 2010. *Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements*. Gaithersburg, MD. https://nvlpubs.nist.gov/nistpubs/ir/2010/NIST.IR.7628.pdf.

———. 2015. *NIST Special Publication 800-82 Revision 2: Guide to Industrial Control Systems (ICS) Security—Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations Such as Programmable Logic Controllers (PLC)*. Gaithersburg, MD. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

———. 2020. *NIST Special Publication 800-207: Zero Trust Architecture*. Gaithersburg, MD. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

The MITRE Corporation. 2016. “Common Vulnerabilities and Exposures.” Accessed May 6, 2016. https://cve.mitre.org/cve/index.html.

U.S. Department of Energy (DOE) Office of Energy Efficiency and Renewable Energy (EERE) Office of Electricity. 2012. “Electricity Subsector Cybersecurity Capability Maturity Model, v. 1.1 (February 2014). https://www.energy.gov/oe/downloads/electricity-subsector-cybersecurity-capability-maturity-model-v-11-february-2014.

U.S. Department of Energy (DOE) Office of Energy Efficiency and Renewable Energy (EERE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER). 2012. “Cybersecurity Risk Management Process (RMP) Guideline – Final (May 2012). https://www.energy.gov/ceser/downloads/cybersecurity-risk-management-process-rmp-guideline-final-may-2012.

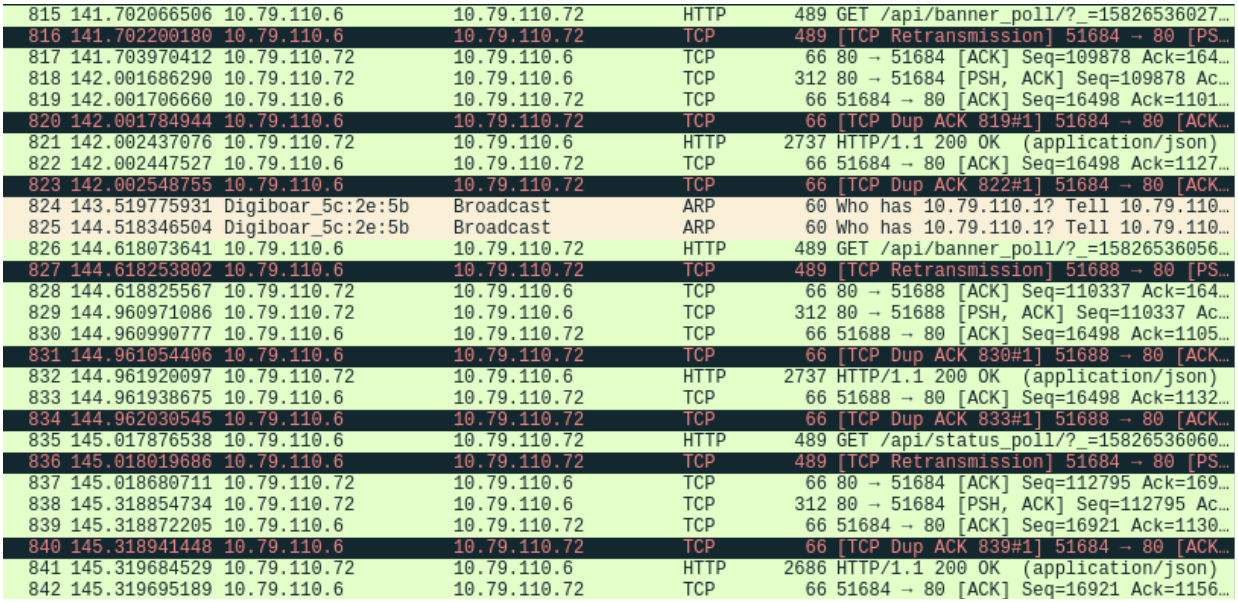
U.S. Department of Energy (DOE) Office of Energy Efficiency and Renewable Energy (EERE). 2021. “Solar Futures Study (September 2021). https://www.energy.gov/sites/default/files/2021-09/Solar%20Futures%20Study.pdf

Underwriters Laboratories Inc. 2010. UL 1741, Ed. 2, Standard for Inverters, Converters, Controllers, and Interconnection System Equipment for Use with Distributed Energy Resources. Northbrook, IL.

Underwriters Laboratories Inc. 2017. UL 2900-1, Ed. 1, Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements. Northbrook, IL.

Appendix A. Photovoltaic Inverter Certification

This appendix contains screenshots from the grid edge device compliancy test without DERCyST.



815	141.702066506	10.79.110.6	10.79.110.72	HTTP	489 GET /api/banner_poll/?_=15826536027…
816	141.702200180	10.79.110.6	10.79.110.72	TCP	489 [TCP Retransmission] 51684 → 80 [PS…
817	141.703970412	10.79.110.72	10.79.110.6	TCP	66 80 → 51684 [ACK] Seq=109878 Ack=164…
818	142.001686290	10.79.110.72	10.79.110.6	TCP	312 80 → 51684 [PSH, ACK] Seq=109878 Ac…
819	142.001706660	10.79.110.6	10.79.110.72	TCP	66 51684 → 80 [ACK] Seq=16498 Ack=1101…
820	142.001784944	10.79.110.6	10.79.110.72	TCP	66 [TCP Dup ACK 819#1] 51684 → 80 [ACK…
821	142.002437076	10.79.110.72	10.79.110.6	HTTP	2737 HTTP/1.1 200 OK (application/json)
822	142.002447527	10.79.110.6	10.79.110.72	TCP	66 51684 → 80 [ACK] Seq=16498 Ack=1127…
823	142.002548755	10.79.110.6	10.79.110.72	TCP	66 [TCP Dup ACK 822#1] 51684 → 80 [ACK…
824	143.519775931	Digiboar_5c:2e:5b	Broadcast	ARP	60 Who has 10.79.110.1? Tell 10.79.110…
825	144.518346504	Digiboar_5c:2e:5b	Broadcast	ARP	60 Who has 10.79.110.1? Tell 10.79.110…
826	144.618073641	10.79.110.6	10.79.110.72	HTTP	489 GET /api/banner_poll/?_=15826536056…
827	144.618253802	10.79.110.6	10.79.110.72	TCP	489 [TCP Retransmission] 51688 → 80 [PS…
828	144.618825567	10.79.110.72	10.79.110.6	TCP	66 80 → 51688 [ACK] Seq=110337 Ack=164…
829	144.960971086	10.79.110.72	10.79.110.6	TCP	312 80 → 51688 [PSH, ACK] Seq=110337 Ac…
830	144.960990777	10.79.110.6	10.79.110.72	TCP	66 51688 → 80 [ACK] Seq=16498 Ack=1105…
831	144.961054406	10.79.110.6	10.79.110.72	TCP	66 [TCP Dup ACK 830#1] 51688 → 80 [ACK…
832	144.961920097	10.79.110.72	10.79.110.6	HTTP	2737 HTTP/1.1 200 OK (application/json)
833	144.961938675	10.79.110.6	10.79.110.72	TCP	66 51688 → 80 [ACK] Seq=16498 Ack=1132…
834	144.962030545	10.79.110.6	10.79.110.72	TCP	66 [TCP Dup ACK 833#1] 51688 → 80 [ACK…
835	145.017876538	10.79.110.6	10.79.110.72	HTTP	489 GET /api/status_poll/?_=15826536060…
836	145.018019686	10.79.110.6	10.79.110.72	TCP	489 [TCP Retransmission] 51684 → 80 [PS…
837	145.018680711	10.79.110.72	10.79.110.6	TCP	66 80 → 51684 [ACK] Seq=112795 Ack=169…
838	145.318854734	10.79.110.72	10.79.110.6	TCP	312 80 → 51684 [PSH, ACK] Seq=112795 Ac…
839	145.318872205	10.79.110.6	10.79.110.72	TCP	66 51684 → 80 [ACK] Seq=16921 Ack=1130…
840	145.318941448	10.79.110.6	10.79.110.72	TCP	66 [TCP Dup ACK 839#1] 51684 → 80 [ACK…
841	145.319684529	10.79.110.72	10.79.110.6	HTTP	2686 HTTP/1.1 200 OK (application/json)
842	145.319695189	10.79.110.6	10.79.110.72	TCP	66 51684 → 80 [ACK] Seq=16921 Ack=1156…

Figure A.1. HTTP communications between the PV inverter and tester

Figure A.1 shows a Wireshark packet capture of HTTP traffic between the PV inverter and tester that confirms Test 1: Two-Party Application Association passes.

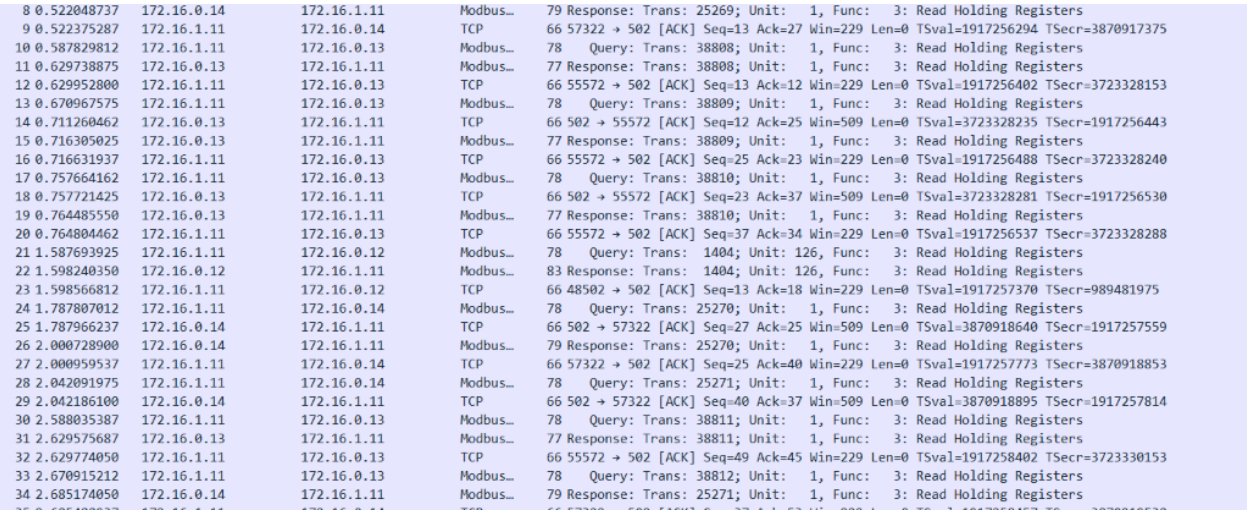
```
root@kali:~# nmap -p 1-65535 -sV -O 10.79.110.72
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-25 12:45 MST
Nmap scan report for 10.79.110.72
Host is up (0.00093s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd (broken: cannot locate user specified in 'ftp_username':ftp)
22/tcp    open  ssh         Dropbear sshd 2012.55 (protocol 2.0)
80/tcp    open  http        CherryPy httpd 3.2.2
427/tcp   open  svrloc?
502/tcp   open  modbus      Modbus TCP
14729/tcp open  ssl/unknown
MAC Address: 00:40:9D:5C:2E:5B (DigiBoard)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.19 - 2.6.36
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Figure A.2. Port and service scan on the PV inverter

Figure A.2 shows open ports and services on the DER found during a nmap scan. The nmap scan confirms that Test 2: Transport Layer Security fails because the PV inverter is not running TLS on any port.

Appendix B. DERCyST Certification

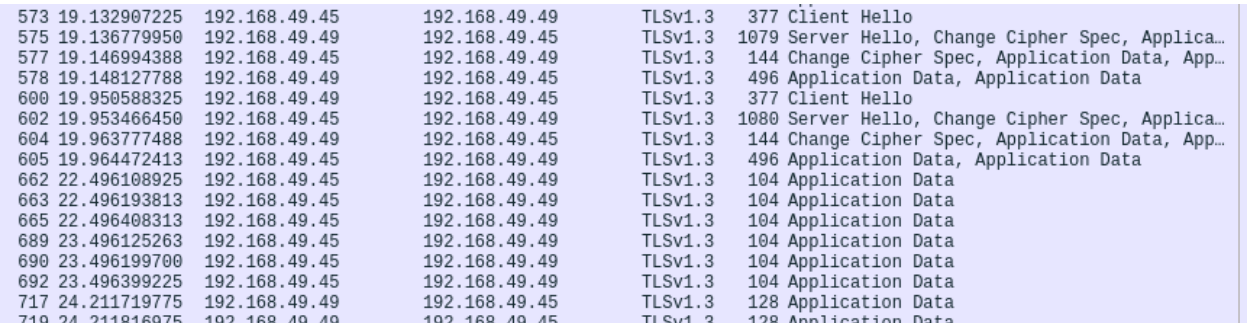
This appendix contains screenshots from the grid edge device compliancy test with DERCyST.



8	0.522048737	172.16.0.14	172.16.1.11	Modbus…	79	Response: Trans: 25269; Unit: 1, Func: 3: Read Holding Registers
9	0.522375287	172.16.1.11	172.16.0.14	TCP	66	57322 → 502 [ACK] Seq=13 Ack=27 Win=229 Len=0 TSval=1917256294 TSecr=3870917375
10	0.587829812	172.16.1.11	172.16.0.13	Modbus…	78	Query: Trans: 38808; Unit: 1, Func: 3: Read Holding Registers
11	0.629738875	172.16.0.13	172.16.1.11	Modbus…	77	Response: Trans: 38808; Unit: 1, Func: 3: Read Holding Registers
12	0.629952800	172.16.1.11	172.16.0.13	TCP	66	55572 → 502 [ACK] Seq=13 Ack=12 Win=229 Len=0 TSval=1917256402 TSecr=3723328153
13	0.670967575	172.16.1.11	172.16.0.13	Modbus…	78	Query: Trans: 38809; Unit: 1, Func: 3: Read Holding Registers
14	0.711260462	172.16.0.13	172.16.1.11	TCP	66	502 → 55572 [ACK] Seq=12 Ack=25 Win=509 Len=0 TSval=3723328235 TSecr=1917256443
15	0.716305025	172.16.0.13	172.16.1.11	Modbus…	77	Response: Trans: 38809; Unit: 1, Func: 3: Read Holding Registers
16	0.716631937	172.16.1.11	172.16.0.13	TCP	66	55572 → 502 [ACK] Seq=25 Ack=23 Win=229 Len=0 TSval=1917256488 TSecr=3723328240
17	0.757664162	172.16.1.11	172.16.0.13	Modbus…	78	Query: Trans: 38810; Unit: 1, Func: 3: Read Holding Registers
18	0.757721425	172.16.0.13	172.16.1.11	TCP	66	502 → 55572 [ACK] Seq=23 Ack=37 Win=509 Len=0 TSval=3723328281 TSecr=1917256530
19	0.764485550	172.16.0.13	172.16.1.11	Modbus…	77	Response: Trans: 38810; Unit: 1, Func: 3: Read Holding Registers
20	0.764804462	172.16.1.11	172.16.0.13	TCP	66	55572 → 502 [ACK] Seq=37 Ack=34 Win=229 Len=0 TSval=1917256537 TSecr=3723328288
21	1.587693925	172.16.1.11	172.16.0.12	Modbus…	78	Query: Trans: 1404; Unit: 126, Func: 3: Read Holding Registers
22	1.598240350	172.16.0.12	172.16.1.11	Modbus…	83	Response: Trans: 1404; Unit: 126, Func: 3: Read Holding Registers
23	1.598566812	172.16.1.11	172.16.0.12	TCP	66	48502 → 502 [ACK] Seq=13 Ack=18 Win=229 Len=0 TSval=1917257370 TSecr=989481975
24	1.787807012	172.16.1.11	172.16.0.14	Modbus…	78	Query: Trans: 25270; Unit: 1, Func: 3: Read Holding Registers
25	1.787966237	172.16.0.14	172.16.1.11	TCP	66	502 → 57322 [ACK] Seq=27 Ack=25 Win=509 Len=0 TSval=3870918640 TSecr=1917257559
26	2.000728900	172.16.0.14	172.16.1.11	Modbus…	79	Response: Trans: 25270; Unit: 1, Func: 3: Read Holding Registers
27	2.000959537	172.16.1.11	172.16.0.14	TCP	66	57322 → 502 [ACK] Seq=25 Ack=40 Win=229 Len=0 TSval=1917257773 TSecr=3870918853
28	2.042091975	172.16.1.11	172.16.0.14	Modbus…	78	Query: Trans: 25271; Unit: 1, Func: 3: Read Holding Registers
29	2.042186100	172.16.0.14	172.16.1.11	TCP	66	502 → 57322 [ACK] Seq=40 Ack=37 Win=509 Len=0 TSval=3870918895 TSecr=1917257814
30	2.588035387	172.16.1.11	172.16.0.13	Modbus…	78	Query: Trans: 38811; Unit: 1, Func: 3: Read Holding Registers
31	2.629575687	172.16.0.13	172.16.1.11	Modbus…	77	Response: Trans: 38811; Unit: 1, Func: 3: Read Holding Registers
32	2.629774050	172.16.1.11	172.16.0.13	TCP	66	55572 → 502 [ACK] Seq=49 Ack=45 Win=229 Len=0 TSval=1917258402 TSecr=3723330153
33	2.670915212	172.16.1.11	172.16.0.13	Modbus…	78	Query: Trans: 38812; Unit: 1, Func: 3: Read Holding Registers
34	2.685174050	172.16.0.14	172.16.1.11	Modbus…	79	Response: Trans: 25271; Unit: 1, Func: 3: Read Holding Registers

Figure B.1. Modbus traffic captured over the local-area network in Wireshark

Figure B.1 shows a Wireshark packet capture of bidirectional Modbus traffic between the PV inverter and controller that confirms Test 1: Two-Party Application Association passes.



573	19.132907225	192.168.49.45	192.168.49.49	TLSv1.3	377	Client Hello
575	19.136779950	192.168.49.49	192.168.49.45	TLSv1.3	1079	Server Hello, Change Cipher Spec, Applica…
577	19.146994388	192.168.49.45	192.168.49.49	TLSv1.3	144	Change Cipher Spec, Application Data, App…
578	19.148127788	192.168.49.49	192.168.49.45	TLSv1.3	496	Application Data, Application Data
600	19.950588325	192.168.49.49	192.168.49.45	TLSv1.3	377	Client Hello
602	19.953466450	192.168.49.45	192.168.49.49	TLSv1.3	1080	Server Hello, Change Cipher Spec, Applica…
604	19.963777488	192.168.49.49	192.168.49.45	TLSv1.3	144	Change Cipher Spec, Application Data, App…
605	19.964472413	192.168.49.45	192.168.49.49	TLSv1.3	496	Application Data, Application Data
662	22.496108925	192.168.49.45	192.168.49.49	TLSv1.3	104	Application Data
663	22.496193813	192.168.49.45	192.168.49.49	TLSv1.3	104	Application Data
665	22.496408313	192.168.49.45	192.168.49.49	TLSv1.3	104	Application Data
689	23.496125263	192.168.49.45	192.168.49.49	TLSv1.3	104	Application Data
690	23.496199700	192.168.49.45	192.168.49.49	TLSv1.3	104	Application Data
692	23.496399225	192.168.49.45	192.168.49.49	TLSv1.3	104	Application Data
717	24.211719775	192.168.49.49	192.168.49.45	TLSv1.3	128	Application Data

Figure B.2. TLS traffic captured over the wide-area network in Wireshark

Figure B.2 shows a Wireshark packet capture of bidirectional TLS communication between the PV inverter and controller that confirms Test 2: Transport Layer Security passes. The TLS packets did not cause anomalies in grid operations.

2185	62.622421975	192.168.49.49	192.168.49.45	TLSv1.3	128	Application Data
2186	62.622492325	192.168.49.49	192.168.49.45	TLSv1.3	103	Application Data
2187	62.622550613	192.168.49.49	192.168.49.45	TLSv1.3	128	Application Data
2192	62.647889775	192.168.49.45	192.168.49.49	TLSv1.3	103	Application Data
2194	62.647978963	192.168.49.45	192.168.49.49	TLSv1.3	104	Application Data
2196	62.648117400	192.168.49.45	192.168.49.49	TLSv1.3	141	Application Data, Application Data
2215	63.648074850	192.168.49.45	192.168.49.49	TLSv1.3	103	Application Data
2216	63.648300375	192.168.49.45	192.168.49.49	TLSv1.3	104	Application Data
2217	63.648311625	192.168.49.45	192.168.49.49	TLSv1.3	141	Application Data, Application Data
2290	81.622784700	192.168.49.49	192.168.49.45	TLSv1.3	1514	Application Data, Application Data, Application
2291	81.622794600	192.168.49.49	192.168.49.45	TLSv1.3	2230	Application Data, Application Data, Application
2293	81.623309525	192.168.49.49	192.168.49.45	TLSv1.3	165	Application Data, Application Data
2318	82.622248700	192.168.49.49	192.168.49.45	TLSv1.3	128	Application Data

Figure B.3. TLS packets are resumed after the network interface controller was powered on.

Figure B.3 shows a Wireshark packet capture of TLS packets between the PV inverter and controller resuming after a 15-second interruption that confirms Test 3: Trasport Layer Recovery passes. The network interface on the DER was disabled 63 seconds into the capture and brought back up at the 81-second mark of the catpure. During the 63–81-second mark, no TLS communication is observed. Outside of that window, TLS 1.3 packets are observed in the packet capture.

```
2020/09/01 12:22:20 Got TCP Discover update:  {  172.16.0.14 502 OPEN []}
2020/09/01 12:22:25 TCP client (Remote Src:  172.16.1.11 : 43602 ) connecting to
 server at  172.16.0.13 : 502
2020/09/01 12:22:25 TCP client (Remote Src:  172.16.1.11 : 36528 ) connecting to
 server at  172.16.0.12 : 502
2020/09/01 12:22:25 TCP client (Remote Src:  172.16.1.11 : 43602 ) connected:  1
72.16.0.13:502
2020/09/01 12:22:25 TCP client (Remote Src:  172.16.1.11 : 36528 ) connected:  1
72.16.0.12:502
2020/09/01 12:22:29 TCP client (Remote Src:  172.16.1.11 : 45344 ) connecting to
 server at  172.16.0.14 : 502
2020/09/01 12:22:29 TCP client (Remote Src:  172.16.1.11 : 45344 ) connected:  1
72.16.0.14:502
2020/09/01 12:25:09 TCP client (Remote Src:  172.16.1.11 : 45360 ) connecting to
 server at  172.16.0.14 : 502
2020/09/01 12:25:09 TCP client (Remote Src:  172.16.1.11 : 45360 ) connected:  1
72.16.0.14:502
2020/09/01 12:27:51 Scores dont match. Got Cert Update. Resetting TLS Server
2020/09/01 12:27:51 TLS Server Closing from Cert error
2020/09/01 12:27:51 ERROR: OpenSSL Server Failed -  RESETTING TLS SERVER FROM CE
RT UPDATE ERROR
```

Figure B.4. DERCyST terminates TLS once a new key is issued.

Figure B.4 shows the output of DERCyST, connected to the DER, when an updated key is issued to the DER for Test 4: Key Update. DERCyST output proves that the operator is informed when TLS communication is interrupted, and then the DER attempts to renegotiate a TLS session with the controller using the new key.

```
2020/09/01 12:27:56 NETWORK DISCOVERY Started On  [192.168.49.49]
2020/09/01 12:27:56 NETWORK DISCOVERY Started On  [172.16.1.1 172.16.0.12 172
2020/09/01 12:27:56 INITIAL SCORE: 1713594466
2020/09/01 12:27:58 Nmap done: 1 hosts up scanned in 0.690000 seconds
2020/09/01 12:28:00 Got TLS Discover update:  {  192.168.49.49 8000 OPEN []}
2020/09/01 12:28:00 TLS client dialing server at  192.168.49.49 : 8000
2020/09/01 12:28:00 TLS client connected to server at  192.168.49.49 : 8000
2020/09/01 12:28:01 New ModuleOT client connected: 192.168.49.49:8000
2020/09/01 12:28:03 Nmap done: 7 hosts up scanned in 5.850000 seconds
2020/09/01 12:28:03 Got TCP Discover update:  {  172.16.0.12 502 OPEN []}
2020/09/01 12:28:03 Got TCP Discover update:  {  172.16.0.13 502 OPEN []}
2020/09/01 12:28:03 Got TCP Discover update:  {  172.16.0.14 502 OPEN []}
2020/09/01 12:28:05 TCP client (Remote Src:  172.16.1.11 : 43660 ) connecting
2020/09/01 12:28:05 TCP client (Remote Src:  172.16.1.11 : 36592 ) connecting
2020/09/01 12:28:05 TCP client (Remote Src:  172.16.1.11 : 45406 ) connecting
2020/09/01 12:28:05 TCP client (Remote Src:  172.16.1.11 : 36592 ) connected:
2020/09/01 12:28:05 TCP client (Remote Src:  172.16.1.11 : 43660 ) connected:
2020/09/01 12:28:05 TCP client (Remote Src:  172.16.1.11 : 45406 ) connected:
```

Figure B.5. DERCyST creates new TLS connections with the updated key.

Figure B.5 shows the output of DERCyST, connected to the DER, after a new key is issued to the DER for Test 4: Key Update. DERCyST output proves the operator is informed of a TLS session being established between the PV inverter and controller with the new key after the previous session key was replaced.

```
486 10.278485613  192.168.49.49   192.168.49.45   TLSv1.2   132 Application Data
488 10.298266213  192.168.49.49   192.168.49.45   TLSv1.2   132 Application Data
490 10.331336838  192.168.49.45   192.168.49.49   TLSv1.2   131 Application Data
494 10.372993525  192.168.49.49   192.168.49.45   TLSv1.2   132 Application Data
496 10.378604275  192.168.49.45   192.168.49.49   TLSv1.2   131 Application Data
498 10.424699838  192.168.49.45   192.168.49.49   TLSv1.2    82 Application Data
500 10.425182713  192.168.49.49   192.168.49.45   TLSv1.2    82 Application Data
504 10.515779375  192.168.49.49   192.168.49.45   TLSv1.2    82 Application Data
573 19.132907225  192.168.49.45   192.168.49.49   TLSv1.3   377 Client Hello
575 19.136779950  192.168.49.49   192.168.49.45   TLSv1.3  1079 Server Hello, Change Cipher Spec, Applica…
577 19.146994388  192.168.49.45   192.168.49.49   TLSv1.3   144 Change Cipher Spec, Application Data, App…
578 19.148127788  192.168.49.49   192.168.49.45   TLSv1.3   496 Application Data, Application Data
600 19.950588325  192.168.49.49   192.168.49.45   TLSv1.3   377 Client Hello
602 19.953466450  192.168.49.45   192.168.49.49   TLSv1.3  1080 Server Hello, Change Cipher Spec, Applica…
604 19.963777488  192.168.49.49   192.168.49.45   TLSv1.3   144 Change Cipher Spec, Application Data, App…
605 19.964472413  192.168.49.45   192.168.49.49   TLSv1.3   496 Application Data, Application Data
662 22.496108925  192.168.49.45   192.168.49.49   TLSv1.3   104 Application Data
663 22.496193813  192.168.49.45   192.168.49.49   TLSv1.3   104 Application Data
665 22.496408313  192.168.49.45   192.168.49.49   TLSv1.3   104 Application Data
689 23.496125263  192.168.49.45   192.168.49.49   TLSv1.3   104 Application Data
690 23.496199700  192.168.49.45   192.168.49.49   TLSv1.3   104 Application Data
692 23.496399225  192.168.49.45   192.168.49.49   TLSv1.3   104 Application Data
717 24.211719775  192.168.49.49   192.168.49.45   TLSv1.3   128 Application Data
719 24.211816975  192.168.49.49   192.168.49.45   TLSv1.3   128 Application Data
```

Figure B.6. Wireshark capture of the TLS handshake occurring with the updated key

Figure B.6 shows a Wireshark packet capture between the DER and controller and confirms Test 4: Key Update passes because a new TLS handshake occurs after the key was updated at the 10-second mark of the packet capture. This means that a new TLS session was renegotiated with the updated key.

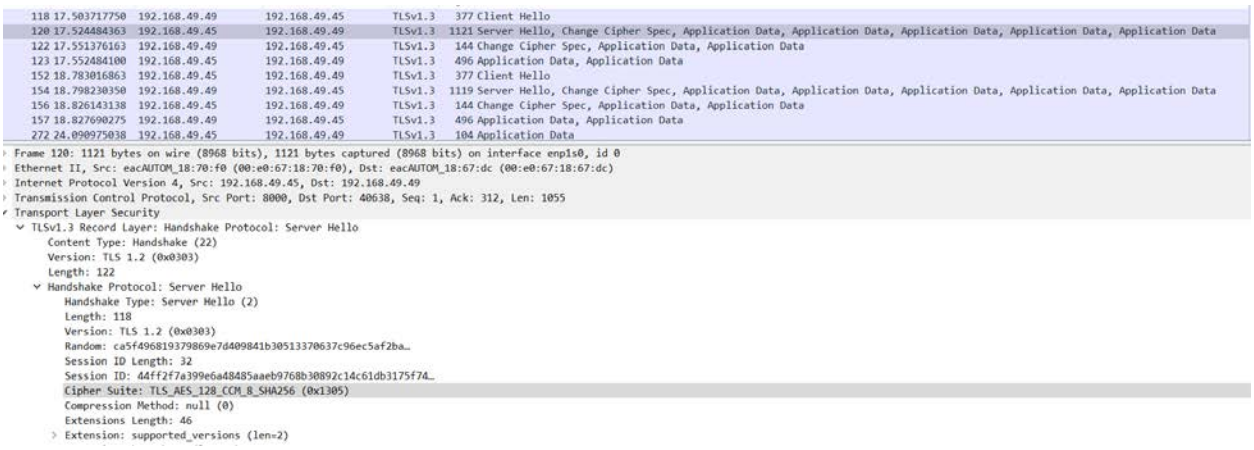


Figure B.7. SHA256 MAC used in TLS communications shown in the packet capture

Figure B.7 shows a TLS packet in a Wireshark capture between the DER and controller. The analyzed TLS packet's cipher suite ends in SHA256 which confirms Test 5: Message Authentication Code passes because the TLS cipher suite employs the SHA256 MAC.

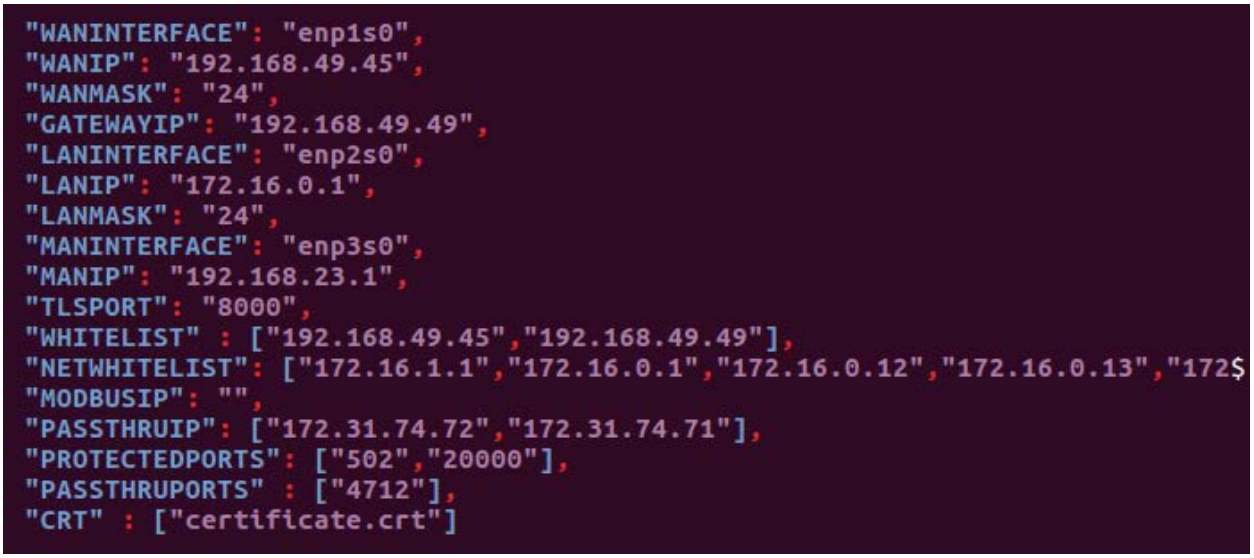


Figure B.8. DERCyST configuration file with 'certificate.crt' in the CRL

Figure B.8 shows the DERCyST confirguration file, which specifices certificates to be included in the CRL.

```
2020/09/01 15:52:19 Firewall Add Default Gateway Error:  exit status 7
2020/09/01 15:52:20 NETWORK DISCOVERY Started On  [192.168.49.49]
2020/09/01 15:52:20 NETWORK DISCOVERY Started On  [172.16.1.1 172.16.0.12 172.1$
2020/09/01 15:52:20 INITIAL SCORE: 1713594943
2020/09/01 15:52:20 certificate.crt in CRL. Killing connection
2020/09/01 15:52:20 ERROR: OpenSSL Server Failed -  Cert in CRL. Killing connec$
2020/09/01 15:52:21 Attempting to restart Server
2020/09/01 15:52:21 INITIAL SCORE: 1713594943
2020/09/01 15:52:21 TLS Server Closing...
2020/09/01 15:52:21 ERROR: OpenSSL Server Failed -  listen tcp 192.168.49.45:80$
2020/09/01 15:52:22 Nmap done: 1 hosts up scanned in 0.610000 seconds
2020/09/01 15:52:22 Attempting to restart Server
2020/09/01 15:52:22 Got TLS Discover update:  {  192.168.49.49 8000 OPEN []}
2020/09/01 15:52:22 TLS client dialing server at  192.168.49.49 : 8000
2020/09/01 15:52:22 INITIAL SCORE: 1713594943
2020/09/01 15:52:22 certificate.crt in CRL. Killing connection
2020/09/01 15:52:22 ERROR: OpenSSL Server Failed -  Cert in CRL. Killing connec$
2020/09/01 15:52:22 TLS client connected to server at  192.168.49.49 : 8000
2020/09/01 15:52:23 Attempting to restart Server
```

Figure B.9. DERCyST log showing TLS communications are unable to be established with a certificate in the CRL

Figure B.9 shows the output of DERCyST, connected to the DER, after a key specified in the CRL is used to establish a TLS session between the DER and controller for Test 6: Certificate Recovation List. DERCyST output proves the operator is informed that the certificate used by DERCyST to connect the DER and controller over TLS is in the CRL. As a result, no TLS communication takes places, which proves that Test 6: Certificate Recovation List passes.

```
2020/09/01 16:32:03 Got TCP Discover update:  {  172.16.0.12 502 OPEN []}
2020/09/01 16:32:03 Got TCP Discover update:  {  172.16.0.13 502 OPEN []}
2020/09/01 16:32:03 Got TCP Discover update:  {  172.16.0.14 502 OPEN []}
2020/09/01 16:32:05 TCP client (Remote Src:  172.16.1.11 : 47780 ) connecting to server at  172.16.0.14 : 502
2020/09/01 16:32:05 TCP client (Remote Src:  172.16.1.11 : 38966 ) connecting to server at  172.16.0.12 : 502
2020/09/01 16:32:05 TCP client (Remote Src:  172.16.1.11 : 46034 ) connecting to server at  172.16.0.13 : 502
2020/09/01 16:32:05 TCP client (Remote Src:  172.16.1.11 : 46034 ) connected:  172.16.0.13:502
2020/09/01 16:32:05 TCP client (Remote Src:  172.16.1.11 : 47780 ) connected:  172.16.0.14:502
2020/09/01 16:32:05 TCP client (Remote Src:  172.16.1.11 : 38966 ) connected:  172.16.0.12:502
2020/09/01 16:32:50 Expired Certificate. TLS Server Closing
2020/09/01 16:32:50 ERROR: OpenSSL Server Failed -  RESETTING TLS SERVER. FROM EXPIRED CERT
```

Figure B.10. DERCyST log showing TLS communications are unable to be established with an expired certificate

Figure B.10 shows the output of DERCyST, connected to the DER, after an expired certificate is used to establish a TLS session between the DER and controller for Test 7: Expired Certificate. DERCyST output proves the operator is informed that the certificate DERCyST is using to connect the DER and controller over TLS is expired. As a result, no TLS communication takes place, which proves that Test 7: Expired Certificate passes.

Figure B.11. Nmap scan of DERCyST server

Figure B.11 shows the output of a port scan, using nmap, on the DER. This port scan confirms that the latest versions of services are used, and only necessary ports are open for Test 8: Operating System Security and Service Version.