Modular Security Apparatus for Managing Distributed Cryptography for Command-and-Control Messages on Operational Technology Networks (Module-OT)

Danish Saleem,[1] Steve Granda,[1] MD Touhiduzzaman,[1] Adarsh Hasandka,[1] William Hupp,[1] Maurice Martin,[1] Shamina Hossain-McKenzie,[2] Patricia Cordeiro,[2] Ifeoma Onunkwo,[2] and Deepu Jose[2]

1 National Renewable Energy Laboratory
2 Sandia National 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-5R00-79974
January 2022

Modular Security Apparatus for Managing Distributed Cryptography for Command-and-Control Messages on Operational Technology Networks (Module-OT)

Danish Saleem,[1] Steve Granda,[1] MD Touhiduzzaman,[1] Adarsh Hasandka,[1] William Hupp,[1] Maurice Martin,[1] Shamina Hossain-McKenzie,[2] Patricia Cordeiro,[2] Ifeoma Onunkwo,[2] and Deepu Jose[2]

1 National Renewable Energy Laboratory
2 Sandia National Laboratories

Suggested Citation
Saleem, Danish, Steve Granda, MD Touhiduzzaman, Adarsh Hasandka, William Hupp, Maurice Martin, Shamina Hossain-McKenzie, Patricia Cordeiro, Ifeoma Onunkwo, and Deepu Jose. 2022. *Modular Security Apparatus for Managing Distributed Cryptography for Command-and-Control Messages on Operational Technology Networks (Module-OT)*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5R00-79974. https://www.nrel.gov/docs/fy22osti/79974.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-5R00-79974
January 2022

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

NOTICE

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

Acknowledgments

The authors thank the U.S. Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response for their support of this research through the Modular Security Apparatus for Managing Distributed Cryptography for Command-and-Control Messages on Operational Technology Networks (Module-OT) project.

The authors are grateful to Walter Yamben, James Briones, and Carol Hawk of DOE for their valuable guidance and support.

We are also grateful to the superb engagement, technical expertise, guidance, and feedback from Jon Hawkins from the Public Service Company of New Mexico and Miles Russel and Emily Hwang from Yaskawa Solectria Solar. We acknowledge the invaluable support of Bryan Richardson and Keith Schwalm at Patria Security LLC for aiding the testing efforts. We also acknowledge the support and expertise provided early in the project by Nicholas Jacobs, Jeffrey Zhao, Christine Lai Chris Howerter, and Roger James Baker from Sandia National Laboratories. We are 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 test bed; and to NREL's communications team, including Nika Durham, Katie Wensuc, Brittany Conrad, 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 (NREL), Aditya Sundararajan (Oak Ridge National Laboratory), and Ahmad Khan (University of Illinois at Chicago).

List of Acronyms

AES	Advanced Encryption Standard
API	application programming interface
BIOS	Basic Input/Output System
BITW	bump-in-the-wire
CAVP	Cryptographic Algorithm Validation Program
CESER	Cybersecurity, Energy Security, and Emergency Response
CD	continuous delivery
CEEP	Cyber Energy Emulation Platform
CI	continuous integration
CIA	confidentiality, integrity, and availability
CSP	Content Security Policy
DER	distributed energy resource
DNP3	Distributed Network Protocol 3
DOE	U.S. Department of Energy
DoS	denial-of-service
ECDSA	Elliptic Curve Digital Signature Algorithm
EPRI	Electric Power Research Institute
FISP	Federal Information Processing Standard
FLT	firmware load test
HMI	human-machine interface
ICS	Industrial Control System
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPSec	Internet Protocol Security
LAN	local-area network
MITM	man-in-the-middle
Module-OT	Modular Security Apparatus for Managing Distributed Cryptography for Command-and-Control Messages on Operational Technology Networks
NI	New Instructions
NIST	National Institute of Standards and Technology
NREL	National Renewable Energy Laboratory
PCT	pairwise consistency test
PMU	phasor measurement unit
PNM	Public Service Company of New Mexico
PSIL	Power Systems Integration Laboratory
PV	photovoltaic
SDN	software-defined networking
SSH	Secure Shell
SSL	Secure Sockets Layer
SVP	System Validation Platform
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus

WAN	wide-area network

Executive Summary

Modern energy systems are characterized by a shift toward diverse and distributed technologies—a blend of new and legacy energy resources interconnected by data and control networks. Increased interconnectivity improves communications and flexibility on the electric power system, but its effect on cybersecurity can pose challenges. More connections can create more options for cyberattacks, and many cybersecurity standards for devices are either outdated, unenforced, or simply nonexistent for some legacy devices. Such circumstances can leave energy systems unprotected, and a successful cyberattack on even one device—e.g., a photovoltaic (PV) inverter, electric vehicle charger, or an energy storage device—could potentially propagate to other connection points across a utility's network. As the electric power industry continues to adapt standards to include modern cybersecurity practices, the U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response awarded funding to the National Renewable Energy Laboratory (NREL) and Sandia National Laboratories (Sandia) to develop a solution that protects distributed energy resources (DERs) and to advance the state of the art for modern cybersecurity. The project partners include the Public Service Company of New Mexico (PNM) and Yaskawa Solectria Solar (Solectria).

This report describes a demonstrated solution to improve the overall cybersecurity posture of legacy and future DER systems without disrupting the existing infrastructure. The goal of the research was to develop a novel and cost-effective technology securing distributed communications across utility-owned DER systems. To achieve this, our approach was to design a flexible and lightweight cryptographic module for grid-edge devices focusing on end-to-end encryption. This provides integrity to the command-and-control messages in transit to and from DERs mitigating cyber threats, such as man-in-the-middle, and securing DER communications to the electric grid.

The Modular Security Apparatus for Managing Distributed Cryptography for Command-and-Control Messages on Operational Technology Networks (Module-OT) (Hupp et al. 2020) improves the cybersecurity posture of DER systems in a holistic way by providing authentication, authorization, and data integrity to secure DER communications. Additionally, it performs key management, provides data security through whitelisting Internet Protocol addresses and ports, blocks unauthorized connections, controls user access, and allows serial or Ethernet connections for added flexibility. The core software is portable to various Linux-based operating systems and is developed to be customized by the developer and researcher communities. Module-OT is open source and available via GitHub to encourage active development and deployment.

The development of Module-OT involved a comprehensive survey of existing cybersecurity and interoperability standards as well as a stakeholder workshop. Industry feedback came from a mix of utilities and technology vendors in addition to project partners Sandia, PNM, and Solectria. After studying the design constraints and the interoperability requirements for implementing cryptography in DER systems, performing a market survey about the need for developing a holistic way to secure DER systems, and performing large numbers of simulations and analysis, a holistic and comprehensive solution, Module-OT, was developed that can provide wide-scale compatibility and convenience as either a stand-alone bump-in-the-wire hardware or an

embedded software, both equally capable of securing operational technology devices that exist today.

To evaluate the commercialization potential of Module-OT, we held a focus meeting comprising industry stakeholders interested in securing DER and grid-edge device communications. The stakeholders included utilities, equipment vendors, nonprofits/utility service organizations, government agencies, and academics. Feedback was solicited to gauge interest in potential partnerships and other potential features useful to industry. The feedback and interest by the attendees provided another positive indication that Module-OT can be incorporated into an existing or new product line and had the potential to improve DER security on a large scale.

Module-OT has been validated in the lab, has been demonstrated in the field, and has been proven ready to secure operational technology devices. Its core functionality meets current standards, including validation procedures of the National Institute of Standards and Technology Cryptographic Algorithm Validation Program and the *Federal Information Processing Standard (FIPS) (FP 140-2)*. Pending industry's developing standards, Module-OT could potentially serve as an effective technological option to standardize cybersecurity moving forward. This is due to its capability to provide an accessible and affordable option for increasing security across modern energy systems. Its open-source design also allows it to be easily customized for future applications.

This report:

- Discusses the motivation for developing Module-OT and what sets it apart from current solutions
- Analyzes the impact of using cryptography in DER system operations, reliability, and cybersecurity
- Includes laboratory test results derived by FIPS 140-2 guidelines for cryptographic devices
- Discusses how Module-OT meets FIPS 140-2 Level 1 requirements
- Includes validation results of Module-OT through an emulated environment to demonstrate its scalability and different implementation options
- Illustrates power-hardware-in-the-loop test results using a microgrid setup consisting of PV inverters from various manufacturers, controllers, digital simulators, etc.
- Shows the impact of Module-OT in a DER system
- Discusses test results from the 500-kW PV and battery storage site (Prosperity Energy Storage Project) in Albuquerque, New Mexico
- Provides a conclusion and recommendations related to how Module-OT can be further improved and commercialized.

Table of Contents

List of Figures

List of Tables

1 Overview

Increasing penetration levels of renewable energy and other distributed energy resources (DERs) on the electric grid have provided various benefits, including technological advancements in electric system monitoring and control, but they have also introduced new cyberattack vectors and increased the attack surface across modern energy systems. To address this issue and enhance the security and resilience of the electric grid, the U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response (CESER) awarded funding to the NREL and Sandia to develop a solution that provides security to both information and operational technology systems to better protect data and communications on the distribution grid. Industry partners includes the Public Service Company of New Mexico (PNM) and Yaskawa Solectria Solar (Solectria).

The developed solution, the Modular Security Apparatus for Managing Distributed Cryptography for Command-and-Control Messages on Operational Technology Networks (Module-OT), was designed to be integrated within a communications system at the transport layer of the Open Systems Interconnection model. The technology improves system security through encryption, authentication, authorization, certificate management, and user access control. Module-OT uses the latest industry standard hardware acceleration to enhance cryptographic performance, data throughput, and end-to-end communications latency. It is a lightweight module with interfaces that allow the technology to be embedded into power system devices of all sizes, such as photovoltaic (PV) inverters. The technology mitigates threats from man-in-the-middle (MITM) attacks and other forms of unauthorized access across increasingly diverse, complex, and expansive DER infrastructures. Figure 1 shows how Module-OT can be leveraged to secure different types of DER systems.

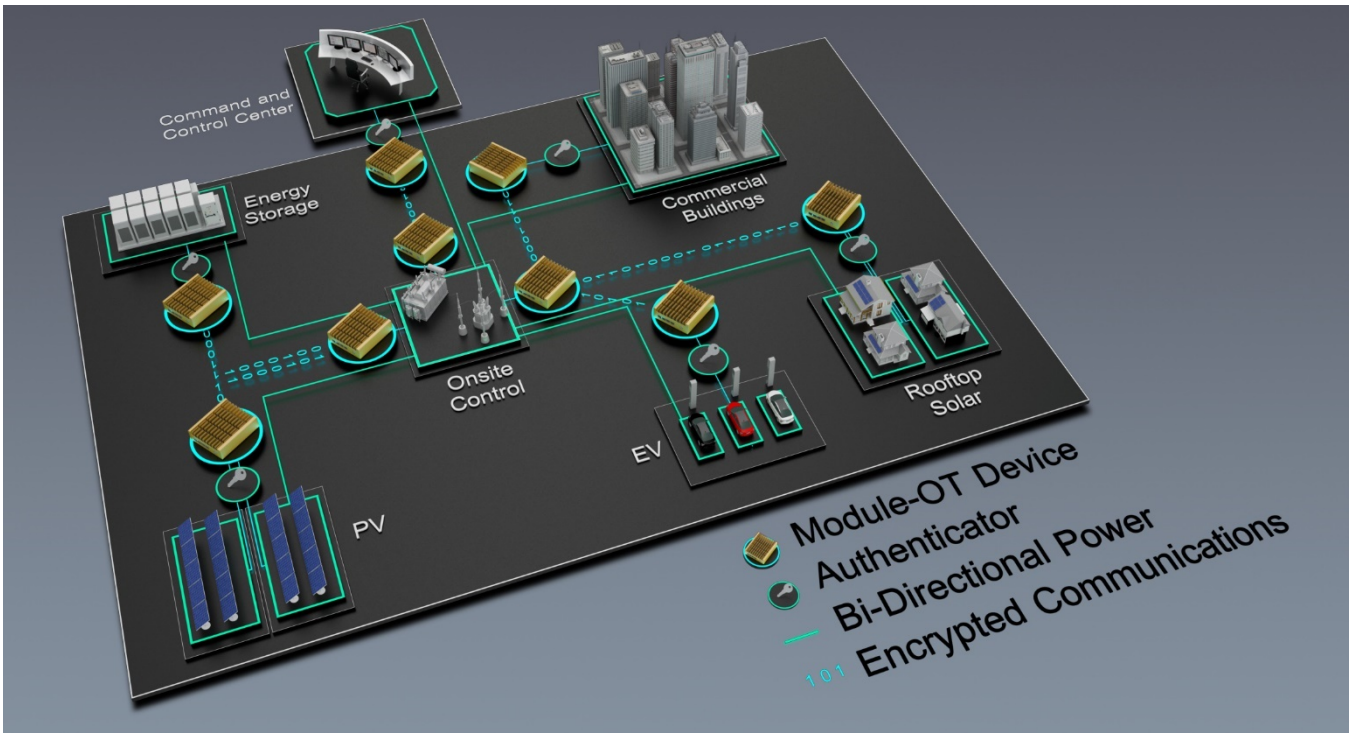


Figure 1. Module-OT landscape

Cryptographic solutions on the market today typically have large-form factors reflecting their memory, processing, and networking resources; this makes it difficult to scale down for application to DERs. Although it might be intuitive for utilities, manufacturers, aggregators, or other industry stakeholders to purchase commercial, off-the-shelf security modules to enhance cybersecurity posture, the available solutions in the market do not provide all the features that are critical for comprehensive cybersecurity coverage. Table 1 captures all the features that Module-OT provides.

Table 1. Features Offered by Module-OT

	Vendor 1	Vendor 2	Vendor 3	Module-OT
AES encryption	×	✓	✓	✓
Trusted platform module	×	×	✓	✓
Client authentication (whitelisting)	×	✓	✓	✓
Device authentication (firmware hash-checking)	✓	✓	Unable to verify	✓
Authorization (using certificate authority)	×	✓	✓	✓
Encryption algorithm and bit length	RSA 2048	AES 128 or 256	AES 256	AES 128 or 256
Key management	✓	×	Unable to verify	✓
Potential for bare-metal solution	✓	✓	✓	✓
Self-test on boot	✓	✓	Unable to verify	✓
Optimized for DERs	×	×	×	✓
Can run as a virtual machine/container	N/A	×	✓	✓
Computation power	Embedded appliance	Embedded appliance	X86 hardware	X86 hardware
Base hardware/software platform	Linux, Win, MAC	Embedded appliance	CentOS	Ubuntu, Debian
Supports SunSpec Modbus over serial	×	✓	×	✓
Supports SunSpec Modbus over TCP	×	✓	×	✓
Supports IEEE 1815 (DNP3)	×	✓	×	✓
Supports IEEE 2030.5 (SEP 2.0)	×	×	×	✓
Open source	✓	×	×	✓
Meets DER latency requirements	✓	✓	✓	✓
Cost	$650	$2800	$7.5k–$20k	Approx. $300

1.1 Motivation for Developing Module-OT

The modern electric grid is dependent on many cyber-physical systems, such as intelligent electronic devices and advanced metering infrastructure, to enhance systemwide command and control operations, monitor energy usage, and even help support newer DER systems; however, traditionally, electric grid communications used dedicated lines for supervisory control and data acquisition system communications, but modernization efforts and the adoption of DERs have started seeing the use of the Internet as a resilient, distributed, and cost-effective open alternative

(Saleem et al. 2020a; de Carvalho and Saleem 2019). The grid is evolving rapidly and developing a defense mechanism for an open alternative is a moving target that is challenging and difficult (Liu et al. 2018).

While researching the cyber-secure functionalities that might exist in some common grid-edge devices—such as PV inverters (Khan et al. 2020), electric vehicle charging stations, microgrid controllers, phasor measurement units (PMUs), advanced metering infrastructure, or wind turbines—it was found that:

- Very few vendors use cryptography to secure their devices and communications.
- Some devices lacked basic cybersecurity functionalities, such as a cryptographic checksum (i.e., HMAC) and secure firmware upgrades.
- Many were vulnerable to common attacks such as reconnaissance, MITM, and denial-of-service (DOS).
- Although some devices were not directly susceptible to cyberattacks (i.e., capacitor banks, synchronous condenser), their controllers were vulnerable to cyber threats.
- Online documentation regarding a device's security controls were not commonly available.

To better understand the growing need to secure the dynamic and rapidly evolving energy systems—specifically, DER systems—we scheduled a cybersecurity workshop at NREL's Energy Systems Integration Facility on July 17, 2018. The workshop was attended by 45 people, including 16 personnel from utilities, 8 personnel from component vendors, 15 personnel from national laboratories (including NREL and Sandia), government cybersecurity experts, and personnel from standards development organizations. This workshop provided stakeholders a chance to express their concerns and share ideas about unsecured operational communications on the distribution grid related to DERs and other grid components.

The workshop focused on understanding the challenges of cryptography in real-world applications, the need for cryptography, and the impact and benefits that the electric power industry will receive from a dedicated cryptographic module for DERs. Participants were also consulted on the possible design of the cryptographic module, where on the grid a cryptographic module could be placed, and how to seamlessly integrate and incorporate a cryptographic module without disrupting current grid operations. In addition, attendees discussed that because communications to a DER could come from end users, aggregators, vendors, data analytics, and operation engineers, this creates a range of issues on the ultimate control and protection of the data. Some workshop participants also expressed concerns about the widespread use of the Modbus protocol for DER communications because the communications are in clear text. Based on the suggestions we received in the workshop, the best possible option for Module-OT design came out to be a bump-in-the-wire (BITW) technology that could be employed for authentication and confidentiality.

1.2 Key Features of Module-OT

Module-OT comes as a single BITW solution that offers system owners, electric utilities, and aggregators a better option to secure the critical energy infrastructure with minimal changes. It provides security to the DERs that exist today, especially because DER devices tend to have a long life and have limited built-in security. Following are some key features of Module-OT:

1. **End-to-end encryption**: This module leverages OpenSSL to perform cryptographic operations on all in-flight data. By default, the system uses strong cryptographic algorithms and cipher suites, such as ECDH ECDSA AES 128 CCM TLS 1.3, but it can be configured to use any cipher suite supported by OpenSSL, allowing flexibility or the ability to adapt to new standards. End-to-end encryption uses Transport Layer Security (TLS) to secure legacy protocols and device communications in a DER using Transmission Control Protocol (TCP)/Internet Protocol (IP).
2. **Hardware cryptographic acceleration**: To handle large numbers of devices at a DER site and to reduce overhead from cryptography, the module leverages hardware cryptographic acceleration from Intel's Advanced Encryption Standard (AES) New Instructions (NI). This instruction set allows software packages (such as OpenSSL) to use the processor directly for cryptographic operations over slower software-based approaches. The use of AES-NI demonstrates that using more expensive and faster processors can provide significant speedup in throughput, as demonstrated in reports comparing the results of OpenSSL speed tests across a variety of x86 processors that support AES-NI.
3. **IP whitelisting**: Module-OT uses a preconfigured whitelist to determine authorized hosts. The Ips in this whitelist can be edited by authorized users in a configuration file. If the device sees a connection attempt from an IP address not in the whitelist, it immediately closes the connection and warns the system administrator. This behavior can repeat a preconfigured number of times before more drastic measures are taken, such as using a firewall for blocking. In the test bed used to validate this module, 10 such connection attempts were allowed before the connection was explicitly blocked. After the preconfigured number of times, the connection is blocked from sending any packets to the device using an iptables-based firewall. The application also adds a rule to automatically block connections from the malicious IP. In this manner, Module-OT provides DoS attack protection. This behavior can also be configured to protect the device from distributed DoS attempts. DoS mitigation by default is done only on WAN port, but it is extendable to the local-area network (LAN) as well.
4. **Authentication**: Module-OT has been designed to use certificates for authentication and perform key management. It requires a valid X.509 certificate to connect to other modules using TLS. Communications can be tested by using self-signed certificates, but it is recommended for end users to use their own in a production environment. Certificates and other sensitive data on the module are protected using full disk encryption with tamper protection enforced by a trusted platform module (TPM) to prevent unauthorized access.
5. **Legacy/serial communications support**: One of the most overlooked areas in existing secure-gateway or endpoint solutions is the ability to support legacy grid devices. Technologies on the electric grid are designed to last many years and use legacy serial RS485 connections for communications. Many researchers recommend a BITW solution to address these problems, and one of Module-OT's core functions is to provide this support. To achieve that, the module performs conversion between TCP and serial protocols and relays serial commands to the DERs. It automatically virtualizes a TCP-based device that clients could target for communication with the legacy device.

6. **Role-based user access control**: To allow for remote control and monitoring, Module-OT supports the Secure Shell (SSH) protocol. To limit the potential for abuse of this connection (as well as the device in general), the module can be enabled to allow outside SSH connections only through its least-privileged user using both a key and a password. This user account has read-only access to limited 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 both a pass phrase and key and general hardening of the SSH server, the device aims to be protected from least-privileged violations that lead to unwanted intrusion and alteration of its configuration. Unauthorized access by means of password failures and exploit scanning will ban offenders at the network level and inform administrators through a log or security information and event management system.
7. **Ease of use**: Module-OT's ability to communicate over serial, Ethernet, and wireless and its BITW configuration makes it easy to use in any type of DER system.

1.3 What Makes Module-OT Unique?

Module-OT is unique because it:

- Has low-memory and low-processor footprints
- Is portable to a variety of Linux-based operating systems and architectures
- Is open source, easy to install, and readily available in popular Linux distributions such as Ubuntu and Debian
- Complies with all three protocols supported by the Institute of Electrical and Electronics Engineers (IEEE) 1547-2018 such as IEEE 1815 (DNP3), IEEE 2030.5 (SEP 2.0) and SunSpec Modbus
- Meets *Federal Information Processing Standard (FIPS) 140-2* Level 1 requirements
- Received a Cryptographic Algorithm Validation Program (CAVP) certificate
- Has been tested and validated in a high-fidelity, utility-grade environment—a 500-KW PV-plus-storage site.

1.4 Module-OT Application Overview

Cryptographic modules are supposed to maintain a secure communications channel between the routers. Module-OT uses point-to-point, one-to-many, and many-to-many network communications channels to perform its functionality (e.g., connection authentication, transmission encryption).

- **Point-to-point**: The point-to-point application includes dial-up modem, cellular modem, or fiber-optic modem. Module-OT uses FIPS 140-2-approved cryptographic algorithms to authenticate all data between two end points and is capable of rejecting all session requests if it detects any unauthorized access to either endpoint. Figure 2 shows the generalized point-to-point application connection for Module-OT.

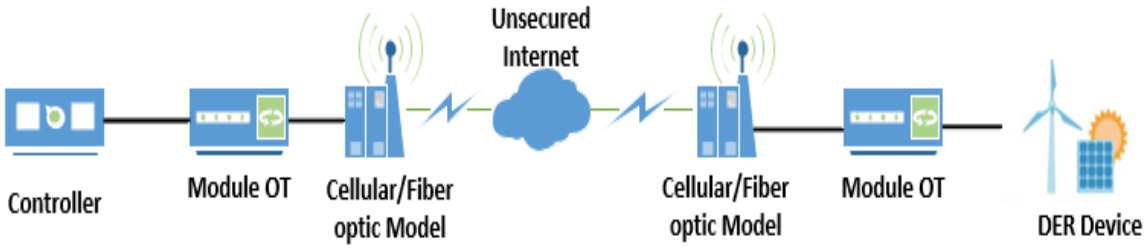


Figure 2. Module-OT point-to-point application

- **One-to-many**: Most field device energy management systems are configured with a one-to-many network architecture, where several DER devices share the same communications channel. Module-OT operates in the one-to-many network architecture, as shown in Figure 3.

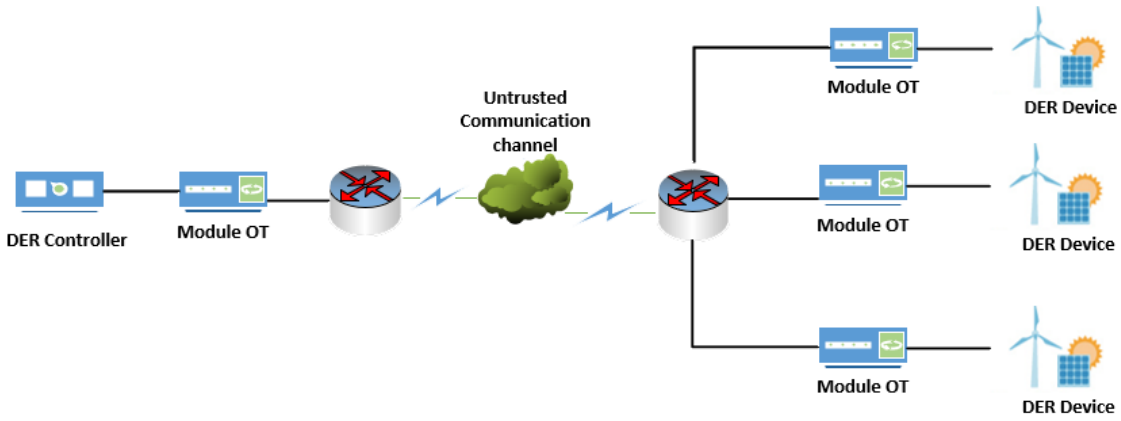


Figure 3. Module-OT one-to-many application

- **Many-to-many**: A many-to-many network is used when there are many endpoints with many users. When a user connects an endpoint device by initiating a session, Module-OT performs like a point-to-point application. Each session initiated by Module-OT is unique to the user in the many-to-many network structure. Figure 4 shows the many-to-many application connection architecture for Module-OT devices.

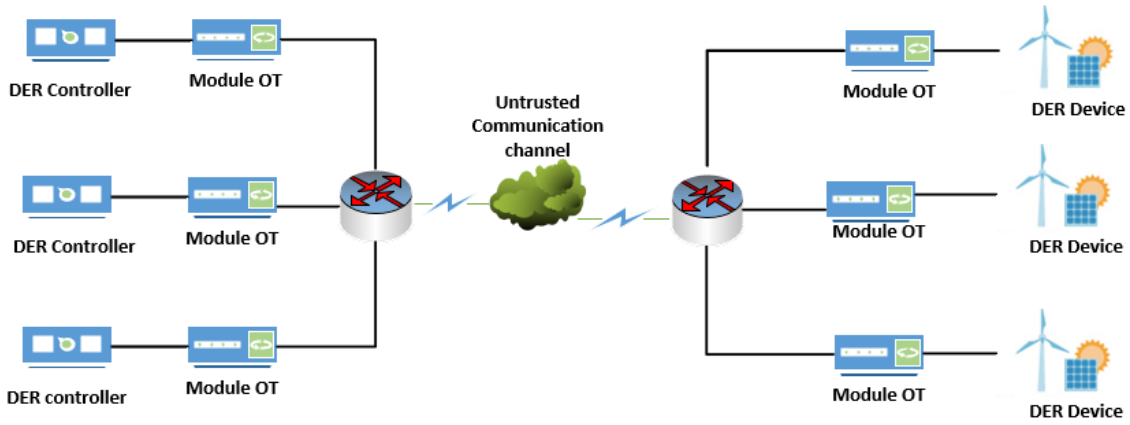


Figure 4. Module-OT many-to-many application

1.5 Module-OT Cryptographic Algorithms

In the cryptographic module, the cryptographic algorithm performs the most important task, such as data encryption, authentication, and digital signature generation, which are all required to comply with FIPS 140-2. FIPS 140-2 maintains a list of encryption-decryption, digital signature, hashing algorithms, etc. These FIPS 140-2 approved algorithms have gone through extensive testing from the security perspective. Following are the approved algorithms mentioned in FIPS 140-2 (NIST 2002):

- Symmetric key—AES-128, AES-192, AES-256, Triple-DES, Escrowed Encryption Standard
- Asymmetric key—DSA, ECDHE-RSA, ECDSA
- Hash standards—SHA-1, SHA-224, SHA-256, SHA-512, SHA-512/224, SHA-512/256
- Message authentication—CCM, GCM, GMAC, HMAC
- Random number generator—deterministic, nondeterministic.

To comply with FIPS 140-2 Security Level 1, at least one of these algorithms should be incorporated into cryptographic module. The algorithm that was agreed upon by the project team for Module-OT is ECDHE_ECDSA_AES_128_CCM_8_SHA-256. Network communications are secured using TLS 1.3.

Compatibility with communications protocols IEEE 1547-2018 provides interoperability requirements; monitoring, control, and information exchange requirements; communications protocol requirements; and communications performance requirements (IEEE 2018a). These requirements help to ensure the interoperability of DERs when they are gets connected to the electric grid. Specifically, the interoperability and grid support functionalities bring value to monitoring and situational awareness of DER systems, and they provide advanced controls, such as integration with DER management tools for aggregation. The potential stakeholders for the communications, control, and monitoring of the information exchange are the area EPS operator, the DER aggregator, the DER operator, the DER owner, and the building/facility manager.

The standard recognizes cybersecurity as a critically important issue for DER deployments that are connected to broader monitoring and control communications networks, but it does not

mandate requirements like it does for interoperability, communications, and information exchange. According to IEEE 1547-2018, all DERs should have the provision of a local DER interface, and this local DER interface should maintain the communications between the wide-area network (WAN) and the DER field devices. This communication interfaces increase the cyberattack surfaces; therefore, they need to be strictly secure and resilient. The communications capabilities between the interfaces are managed by the area EPS operator, the DER aggregator, the DER operator, the DER owner, and the building/facility manager. 2030.5 (SEP 2.0) (IEEE 2018b), IEEE 1815 (Distributed Network Protocol 3 (DNP3)) (IEEE 2012), and SunSpec Modbus are noted by IEEE 1547-2018 (SunSpec Alliance 2019) as the approved DER communications protocols.

Module-OT supports all these communications protocols. Figure 5 shows the Module-OT location in a DER utility communications network.

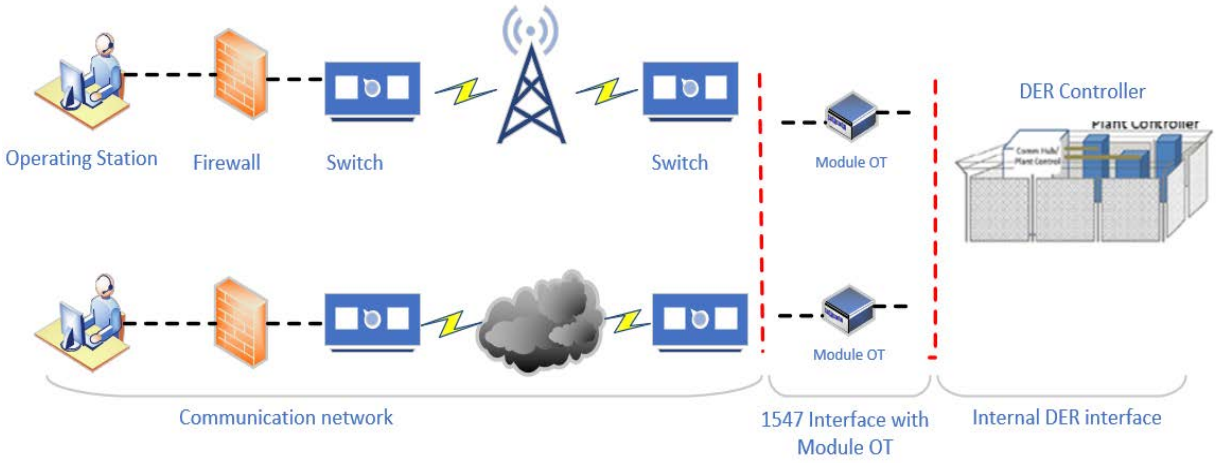


Figure 5. Module-OT location in utility communications network

2 Practical Considerations of Cryptography in Distributed Energy Resource Systems

To understand the general requirements and cryptographic design needs for an encryption module for DER systems, Baker et al. (2018) performed preliminary research to explore the composition of DER systems and relevant cybersecurity concerns. Specifically, the authors explored the interoperability and system requirements for implementing cryptography in DER systems. The results were captured in *General Requirements for Designing and Implementing a Cryptography Module for Distributed Energy Resource (DER) Systems.*" The report presents and discusses different types of cryptography algorithms, including symmetric encryption algorithms with different cypher block operation modes. Additionally, the report assesses the requirements from the SunSpec Common Smart Inverter Profile, California Rule 21, and IEEE 2030.5 for prioritizing functionalities within the Module-OT device (Jacobs et al. 2019; Lai et al. 2019). Machine-to-machine authentication and encryption pertaining to communications with grid-attached power inverters were also studied and are captured in the report *Review of Authentication Strategies and Trends for Distributed Energy Resources (DERs)* (Lai and Cordeiro 2018). This report also provided a detailed review of current cryptography strategies, best practices for DER cryptography, and a summary of challenges and alternatives of using the x.509 standard for public key infrastructure.

2.1 Design Constraints and System Impact of a Distributed Energy Resource Cryptographic Module

The design constraints and system impact of a DER cryptographic module are studied further in *Analysis of Design Constraints and System Impact of DER Cryptographic Module* (Jacobs et al. 2018). This report explores the impact of the additional security on the DER environment and how to ensure that the security principles of confidentiality, integrity, and availability were obtained and/or preserved. The DER system impacts—explored through different implementation scenarios (e.g., protection schemes, grid support functions, customer-owned DERs, and smart devices such as smart inverters) —are studied in terms of types of communications and sensitivity to latency increase. The security considerations for inverter communications are further explored to understand the impact on inverter communications (e.g., DER device registration, operational status, monitoring data) and how considerations can vary depending on the device type. Next, suitable cryptography algorithms are presented, and the AES is identified as a potential direction because of its ease and flexibility of implementation. Last, the report provides device design constraints, including required interfaces and other compatibility concerns, specifically for BITW implementations.

2.2 Security Considerations for Photovoltaic Inverter Communications

To protect the inverter, the security principles of confidentiality, integrity, and availability must be ensured for each type of message that must pass through the module; therefore, it is important to assess the different types of messages and constraints for each communication function in a DER system. Specifically, it is important to consider the specific services and communications used by smart inverters to support the grid support functions as specified by the Common Smart

Inverter Profile and by information models put together for inverter communications by the SunSpec Alliance.

In discussing security requirements for the module and communications, several points are important to consider. These include the security of data at rest, the security of data in motion, the authentication of clients and services, the authorization of requests to ensure that they are valid and come from appropriate sources, and the impact on the communications when each is protected. Because the Module-OT device is a BITW solution, the importance of securing data at rest is mostly ignored. With that said, the module might need to store minimal amounts of data for security purposes (keys) or management of the module itself. These data will be protected from disclosure using the appropriate mechanisms, and because this information is not part of the inverter communications, the performance impact to the DER system will be minimal. Securing data in motion, authentication, and authorization are all security measures that will be examined for the various communication types required by the DER. In addition, the impact of issues that could occur because of improper implementation of this security module must be considered in the design of this security module. Such security system failures could lead to malicious communications being allowed through the module, valid communications being rejected, or excessive overhead on messages that do not require such protections yet are supporting services that are significantly impacted by the additional computational time required to support these additional security measures.

These considerations are further discussed in the full report *Analysis of Design Constraints and System Impact of DER Cryptographic Module*, as referenced in Section 2.1. The report documents the different types of inverter communications, such as DER device registration, DER group management, inverter connect/disconnect, scheduling power values and modes, operational status, monitoring data, nameplate ratings and adjusted settings, alarms, and DER maintenance.

2.3 Impact from Loss of Photovoltaic Generation

To further assess the impact to PV systems with additional latency, an experiment was performed using a simulated 15-bus system with 3 inverters, as shown in Figure 6.

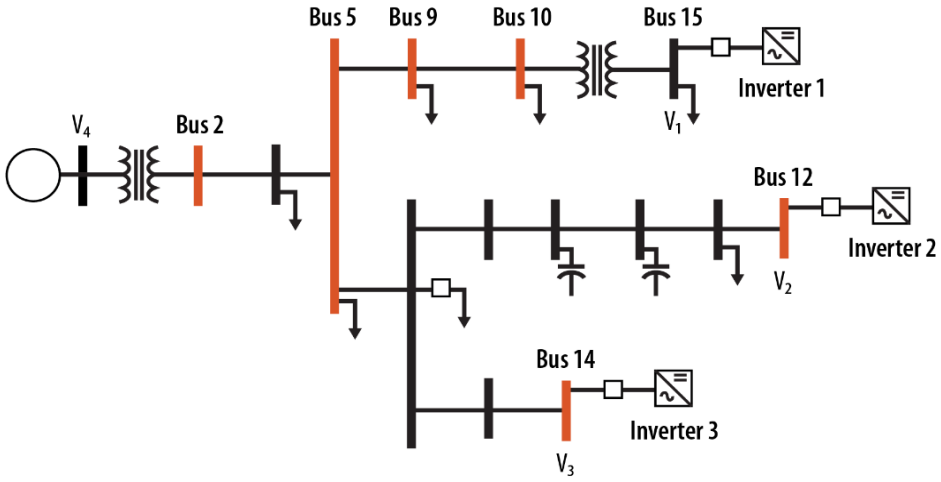


Figure 6. Fifteen-bus system with three inverters

To demonstrate the impact of additional communications and processing times associated with applying security measures to DER communications, this experiment showed the performance of DERs supplying voltage support in a simulation of a distribution feeder. Three additional cases are shown where a disconnect signal is sent to the inverters to demonstrate the impact of an unexpected loss of generation capacity in this distribution feeder. The full details of this experiment and results can be found in the full conference paper, "Analysis of System and Interoperability Impact from Securing Communications for Distributed Energy Resources" (Jacobs et al. 2019). The following conclusions were made from the experiment:

- Adding additional security protections in the communications path can be expected to slow communications because of extra processing and "hops" in the communications path.
- When implementing these delays, it is found that they will impact performance but not significantly, even at high amounts of latency. In other words, the central controller updates at a slow enough rate that even large time delays have little impact. Moreover, additional latency does not affect the local control of the inverters themselves.
- If some PV generation is disabled by a malicious or inadvertent command disabled to disconnect (loss of availability), the overall impact to the system voltage depends on the amount of generation capacity that has been lost.
- The impact to the system voltage is most severe on the buses local to the inverter(s) that have been disabled. This impact is demonstrated in Figure 7.

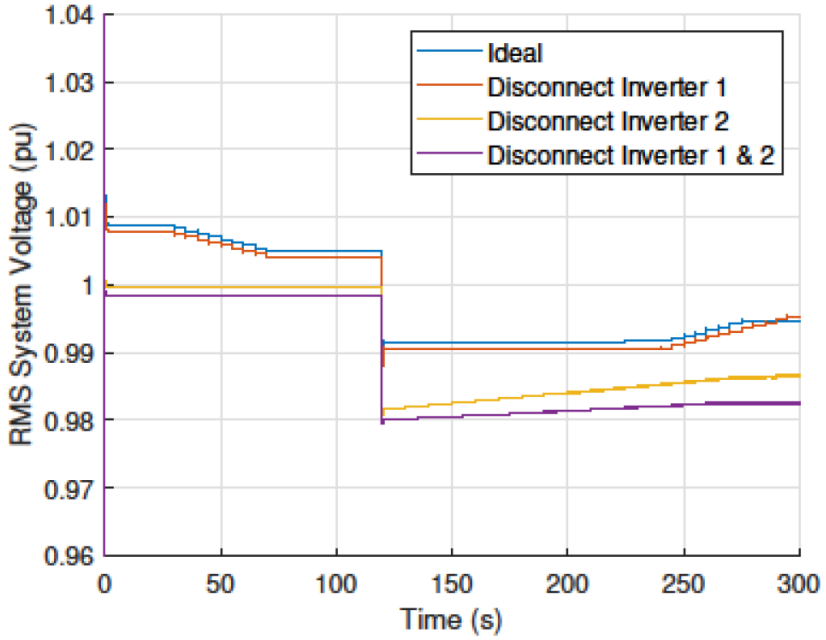


Figure 7. Average system voltage impact as different inverter(s) are disconnected

2.4 Latency Testing

To evaluate the latency that Module-OT could potentially add to DER communications, SCEPTRE was used. SCEPTRE is an application that uses an underlying network emulation and analytics platform (Emulytics) to model, simulate, emulate, test, and validate control system security and process simulations (Sandia 2016). Multiple experiments were run within the SCEPTRE environment, first to simulate PV inverters and then to test the latency of the Modbus over TCP traffic from the SunSpec System Validation Platform (SVP) to each simulated inverter over a secure communication tunnel. The simulated inverters were modeled in the Electric Power Research Institute (EPRI) DER Simulator (EPRI 2018).

The experiment topology involved two primary networks with a total of 14 virtual machines. An application was developed to run on the SVP system in the CORP network that could send Modbus over TCP requests to a given IP and port. This connection was tunneled through an SSH between an SSH server on the CORP network to six individual SSH servers virtually "next" to a respective inverter. There are two virtual routers between the CORP and inverters networks.

Traffic was directed through the SSH server on the CORP network where a particular port number per inverter was used to direct traffic to a specific inverter (e.g., DER-01 is at 192.168.0.101 and port 5510; DER-02 is at 192.168.0.101 and port 5511). The connection to DER-20 was sent direct using Modbus over TCP in the clear to port 5502. DER-01 to DER-06 each had a different SSH server virtually next to them, as shown in Figure 8. Each SSH server has a tunnel connection back to the SSH server on the CORP network and forwards Modbus traffic in the clear from the SSH server to its respective inverter. The Modbus traffic is protected from the SSH server on the CORP network to the SSH server next to each inverter.

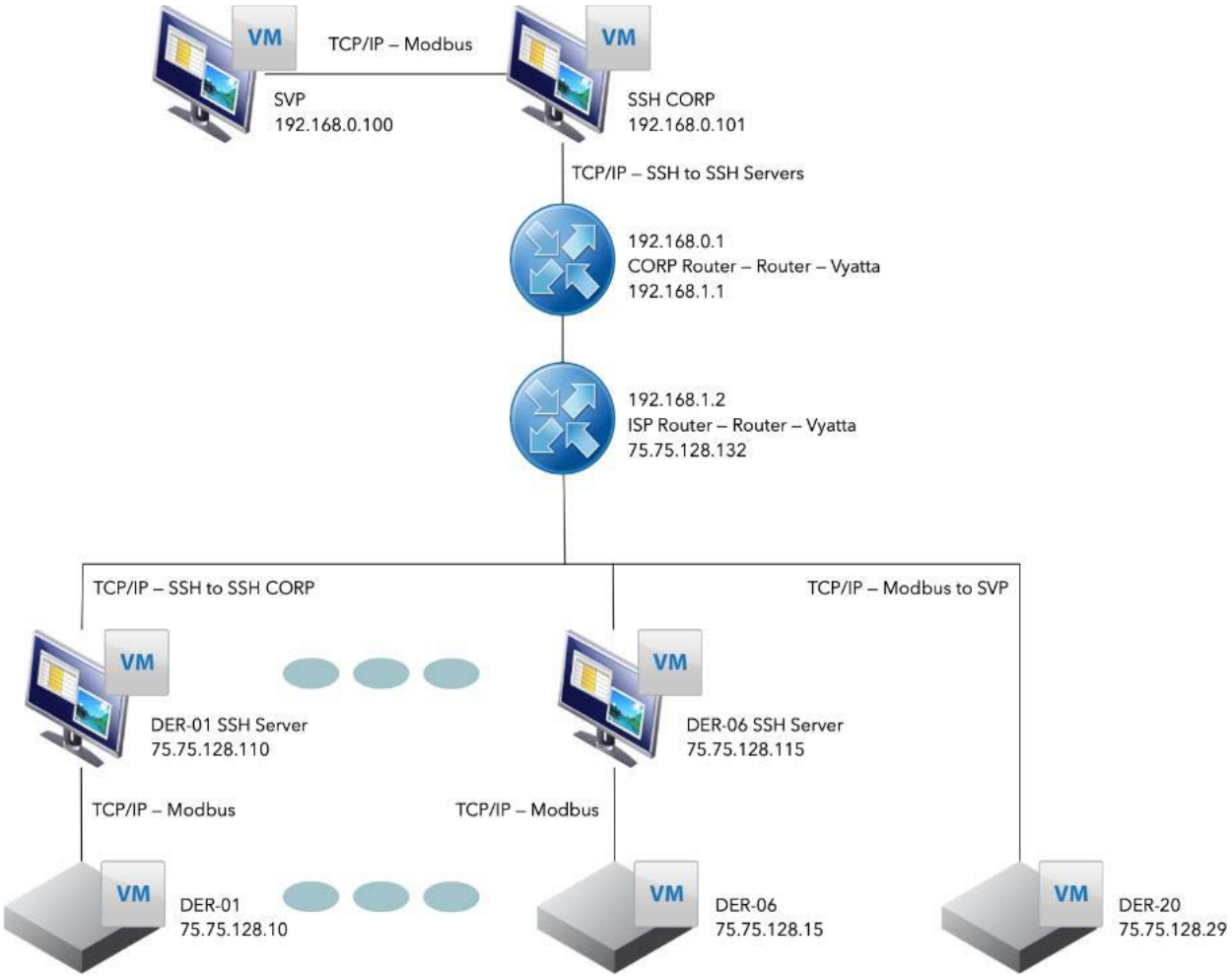


Figure 8. Testing setup to test the latency of the Modbus TCP traffic to multiple simulated inverters

Six SSH ciphers were tested for latency in the Modbus over TCP communications. These six ciphers were selected because they were mutually agreed upon by the project team to be the ones between the SSH server and the SSH clients on the stock virtual machine images. Those six ciphers are as follows:

- DER-01, DER-07, DER-13: aes128-ctr
- DER-02, DER-08, DER-14: aes192-ctr
- DER-03, DER-09, DER-15: aes256-ctr
- DER-04, DER-10, DER-16: aes128-gcm@openssh.com
- DER-05, DER-11, DER-17: aes256-gcm@openssh.com
- DER-06, DER-12, DER-18: chacha20-poly1305@openssh.com
- DER-19, DER-20: none.

The results from this testing are shown in Figure 9.

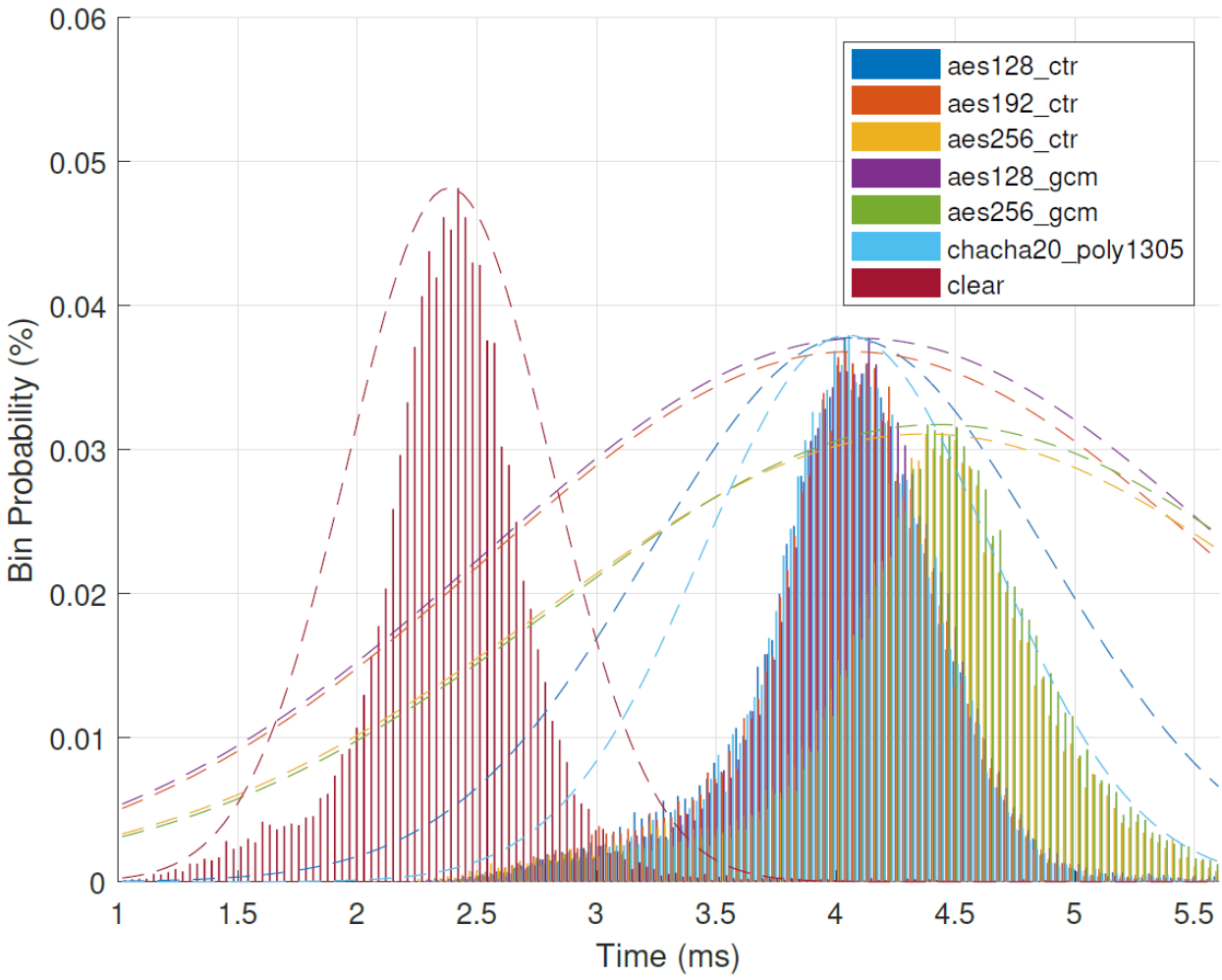


Figure 9. Latency results for various symmetric ciphers

As shown in Figure 9, the plaintext traffic with no encryption is significantly faster than the encrypted traffic. This result should be expected. In this instance with the SCEPTRE configuration described, the cleartext traffic takes approximately 2.4 ms to travel on average. The average latency for the encrypted traffic ranges from 4 ms–4.5 ms, depending on the encryption scheme, meaning that the additional latency from the encryption can be expected to be roughly 2 ms–2.5 ms. Although this value could change drastically for various hardware resources (processors) and implementations, the relative change between the clear traffic and the encrypted traffic shows that a significant impact to latency can be expected and will likely be on the order of milliseconds.

There seems to be a negligible impact or change in travel time between the CTR and GCM modes of operation, however. Also, ChaCha20 is roughly equivalent in terms of additional latency to 128-bit (CTR, GCM) or 192-bit (CTR) AES even though it uses a 256-bit key. Increasing the key length of AES to 256 bits seems to have the largest impact on performance by increasing the communication time to approximately 4.5 ms on average, an increased cost of approximately 0.4 ms more than the latency observed when using shorter length keys for AES; however, the wide distribution of results makes it difficult to discern any definitive relationship on the relative costs of each cipher and cipher mode. Further, although the vast majority of

communication times fall into a nice normal distribution for each set of results, for all the sets there are some outliers that give the distribution a large tail for large communication times, as shown by the large maximum values in Table 2. These are often cases that would be counted as dropped packets and resent, and in this instance, they are rare enough to not impact the distribution by any noticeable amount.

Table 2. Computed Statistics of Latency Results for Various Symmetric Ciphers and Cipher Modes to Secure the Transport Layer for Round-Trip Modbus Communications

Cipher and Cipher Mode	Mean (ms)	Standard Deviation (ms)	Minimum (ms)	Maximum (ms)	Median (ms)
AES128-CTR	4.0526	0.8295	2.0698	81.1382	4.0604
AES192-CTR	4.0662	1.5339	2.1778	206.7507	4.0604
AES256-CTR	4.3728	1.5879	2.0645	206.9327	4.3957
AES128-GCM	4.1056	1.5665	2.2905	205.8982	4.0985
AES256-GCM	4.4290	1.5858	2.2220	205.7683	4.4418
ChaCha20-Poly1305	4.0496	0.6043	2.1506	45.0614	4.0565
Clear	2.3834	0.4236	1.0010	15.1254	2.3847

All in all, from this emulation testing, the Module-OT project selection of AES as the module's encryption algorithm is suitable. The six ciphers have comparable latency impact, which is minimal and on the order of milliseconds. AES is prominent and widely used, which encourages its implementation in the module. Further, the lowest latency requirements for different power system (applicable to DERs) applications is approximately 100 ms, as noted in Table 3 in IEEE 1547-2018 standard (IEEE 2018a). These results indicate a latency impact of a few milliseconds under normal conditions and thus do not violate any application requirements. Although a rare number of packets do take longer than this limit of 100 ms, it is assumed that the packet would be resent within the allotted time frame and that these low error rates will not impact application performance. Nonetheless, field-testing was conducted to validate these results on hardware and to ensure that the relevant application latency requirements are met.

3 Module Design and Prototype

3.1 Design Considerations

Module-OT was developed using the suggestions from stakeholders, current policy, and our understanding of DER system needs. To achieve the design requirements, our hardware platform would need to withstand harsh environments dealing with dust and heat. The logistics to travel to rural energy assets to replace or fix equipment would require the hardware to be low maintenance with minimal moving parts (i.e., fans). This would also need to conform to a small form factor.

3.2 Form Factors

The initial prototype was based on a Raspberry Pi Model B+ because of the form factor and its ability to operate using passive cooling. Although the Module-OT application was able to run on this single-board computer, the lack of additional onboard Ethernet and a hardware security module would not fully fit our requirements. Our current hardware platform was chosen to balance cost and power, which ultimately led to using a Protectli Vault FW4B with an Intel Celeron processor to leverage AES-NI hardware acceleration for our use of the TLS_AES_128_CCM_8_SHA256 ciphers in securing communications, as shown in Figure 10.

Figure 10. Protectli Vault FW4B used in PHIL testing. *Photo by NREL*

This small form factor device contains four port gigabit Ethernet connections for better network throughput and flexibility. The design also contains an onboard high-speed Universal Serial Bus (USB) for legacy serial to USB devices. It was sealed against dust while providing passive cooling to deal with harsh environments (Saleem et al. 2020b). This USB interface was added to provide support and security to the legacy devices; however, it is not a recommended practice to keep unused ports open without evaluating the risk of having no physical security. A future prototype will be custom built using a passively cooled Mini-ITX form with an onboard Trusted Platform Module (TPM).

3.3 Prototype Development

The Module-OT software development used GitLab's continuous integration feature by kicking off tests focusing on security and functional code design and by verifying network operations with each new build. To enhance the physical security and data integrity, an anti-tamper detection mechanism was used along with a TPM. All physical Module-OT deployments include full disk encryption by default. Confidential data and keys used to authenticate internal system services are stored in a secure crypto processor by means of a TPM. Any tampering, such as by brute force or by physically opening the device, are met with immediate destruction of the contents in the TPM, rendering the encrypted hard disk unable to be mounted and read by an adversary.

The functional description with hardware and software requirements, the security policy, and the interfaces of Module-OT are captured in sections 4, 5 and 6.

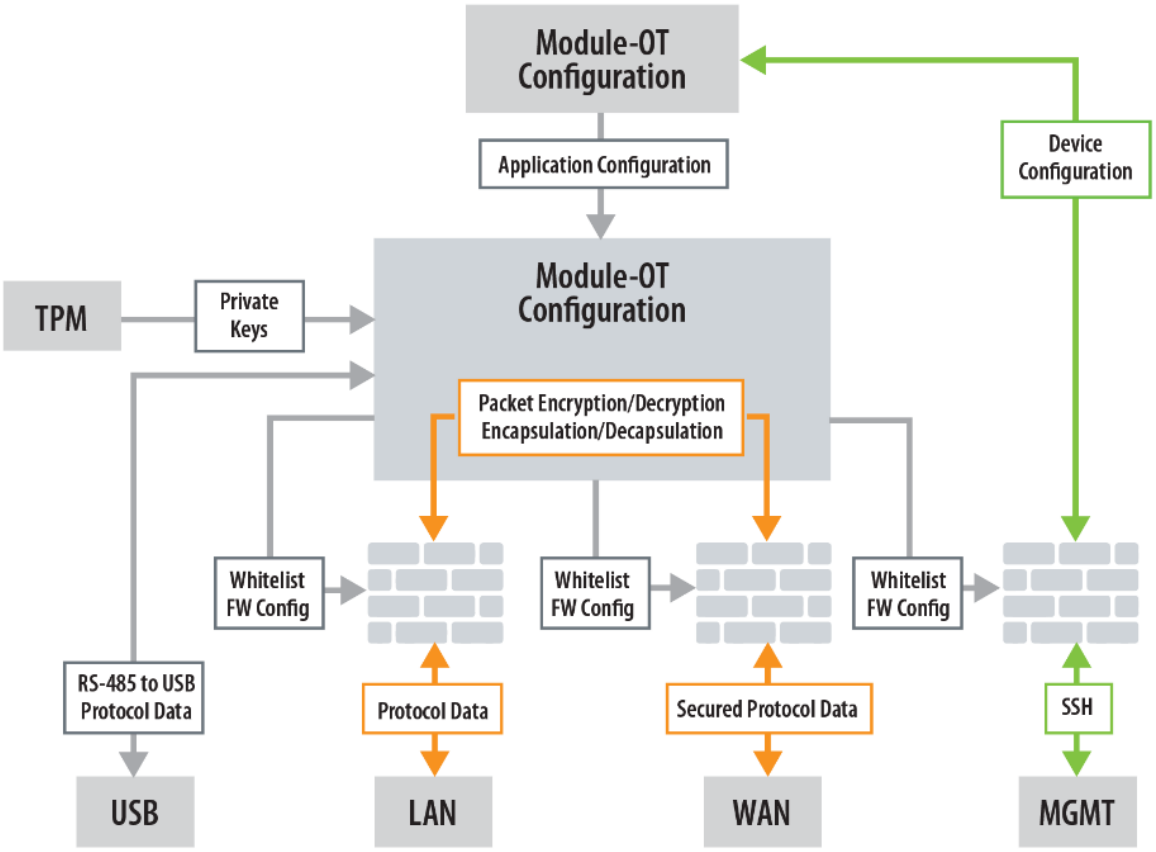


Figure 11. Module-OT interfaces and data flow

4 Functional Description, Interfaces, and Operating System Requirements of Module-OT

4.1 Device Description

The Module-OT platform consists of a physical BITW device that runs a custom-built application built with Go and Python and leverages the AES-NI set available on modern hardware for cryptographic acceleration. By combining these features, Module-OT acts as an all-in-one low-cost solution to enable cryptographically secured communications to any critical remote servers or devices. Because the software was developed using Golang, the source can be easily compiled for different architectures. Official public releases can only be built by NREL and enforced by a signed source. Table 3 describes the design considerations of the Module-OT platform.

Table 3. Design Considerations of the Module-OT Platform

Design Considerations	Solution
Module location in network topology	Gateway for WAN uplink/downlink
Expected communication agents in network	Controller via WAN at one end and LAN controller at another
Communications protocol	Secured TCP/IP communications via SSL
User authentication method	Using X.509 certificates
Required hardware interfaces	RJ45, RS485
Selected cryptographic cipher suite	AES_128_CCM_8
Cryptographic key protocol	ECDHE_ECDSA
Key management method	Certificates managed through a certificate authority selected by the user, installer, or operator
Management software interface	Hardened SSH server
Whitelisting capability	Firewall and security rules implemented on local operating system
Device hardening method	System file encryption and SSH hardening policies
Management interface hardening method	Access logs, user authentication lockout, and user account access control

4.1.1 Hardware Requirements

For AES-128-CCM hardware acceleration to occur, the AES-NI instruction set architecture must be supported on the processor. Most Intel and AMD, x86-64 processors built in the past few years support AES-NI. As rule of thumb, the more memory and processing power the central processing unit has, the more devices can be interconnected. The Module-OT development group does not endorse or support any specific hardware brand. The internal development environment for the current Module-OT version has been deployed and tested on the Protectli firewall micro appliance, model FW4B-0-8-120. Any hardware that has the minimum hardware requirements described in Table 4 should be able to handle multiple devices within the proper latency limits.

To enable serial device support, the module requires an additional USB-serial (RS485) adapter to be available. Any such device can be accessed at */dev/USB0.*

To enable serial device support, the module requires an additional USB-serial (RS485) adapter to be available. Any such device can be accessed at */dev/USB0* on Debian or Ubuntu-based GNU/Linux distributions.

Table 4. Minimum Hardware Requirement

Processor	**2-GHz Dual-core x84, 64-bit, AES-NI**
RAM	DDR3 - 8 GB
Storage	4 GB*

The actual Module-OT application is only 11 MB, but it also requires extra storage for operating system and software dependencies. The remaining unused storage is used for logs and other recorded data.

More experiments will be made in the future to find the minimum hardware requirements for interconnecting larger numbers of devices. The main metric is based on end-to-end wired communication latency. Although Module-OT is capable of supporting built-in wireless interfaces, they should be disabled for security purposes, if unused.

4.1.2 Software Requirements

In addition to the hardware requirement, the Module-OT application has the following application software dependencies when built manually:

- Python—interpreted programming language
- Nmap—network mapping utility
- OpenSSL—TLS/SSL communication handler
- LibSSL—SSL library
- OpenSSH—SSH server handler
- PyModbusTCP—Python-based ModbusTCP-serial relay
- Fail2ban—SSH administration tool
- gufw—iptables frontend for configuration
- net-tools—deprecated network interface configuration
- systemd—Linux framework for services (We do not officially support system-v init, but it is trivial to implement through a manual installation.)

The development of Module-OT also requires the following environment dependencies:

- Go—interpreted programming language
- Pip—Python package installer
- Protobuf—language-neutral, platform-neutral extensible mechanism for serializing structured data
- Spacelog—logging library for go
- Openssl—go-based application programming interface (API) wrapper for openssl

- Golang crypto/sha3—cryptographic functions for go
- Ullaakut/nmap—nmap api wrapper.

4.1.3 Cryptographic Requirements

Internet Protocol Security (IPSec) and TLS are embedded in the Module-OT system to provide sufficient defense-in-depth between a DER and the grid. Module-OT adopts X.509 certificates based on public key infrastructure. For encryption and decryption, Module-OT uses an asymmetric encryption algorithm (Elliptic Curve Digital Signature Algorithm-ECDSA) because this algorithm is capable of providing different sets of private and public keys for encryption and decryption rather than a single shared key. The key length of an asymmetric cipher used in Module-OT is 128 bits. The lifetime of the ephemeral key is set to a default of 10 years, which is also customizable.

4.2 Interfaces of Module-OT

Like other commercially available cryptographic modules, Module-OT also has four logical interfaces: data input, data output, control input, and status output. These logical interfaces are distributed over one or more physical ports.

The data input interface consists of the input parameters—cryptographic keys and Content Security Policies (CSPs), authentication data, and status information from another module—of the Module-OT API functions. The data output interface consists of the output parameters of the API functions. The control input interface consists of the actual API functions. The status output interface includes the return values of the API functions. The ports and interfaces are shown in Table 5.

Table 5. Module-OT Ports and Interfaces

FIPS Interface	Physical Port	Logical Interface
Data input	LAN/WAN	API input parameters
Data output	LAN/WAN	API output parameters and return values
Control input	MGMT	API input parameters
Status output	MGMT	API return values
Power output	Physical port of the tested platform	N/A

4.2.1 Physical interfaces

A basic Module-OT deployment has the following physical interfaces.

- **Ethernet ports**: Each Module-OT endpoint device requires at minimum 2 RJ45 Ethernet ports for the use of TCP/IP. The physical Module-OT device will be acting as a BITW, forwarding traffic across a port from an internal LAN through an upstream port acting as WAN. An optional management port is also available to allow the user to connect to the system using SSH. The SSH server will allow only key-plus-password-based authentication and will automatically blacklist users attempting to probe the service with brute-force attacks

or after too many unsuccessful log-in attempts. Industrial Control System (ICS) protocols and other traffic being sent from the internal LAN across the WAN are encapsulated with sessions actively secured using a Secure Sockets Layer (SSL) through signed certificates. Interfaces are protected by whitelisting through the Linux firewall, iptables. Interfaces by default have all unused ports closed. All traffic is monitored from known enabled ports.

- **USB ports**: Physical USB ports can be used for connecting peripherals and adapters to enable services such as serial over USB and will be secured by controlling physical access as well as through a configurable access control list preventing normal regular users from mounting or accessing the interface. Unused USB ports should be disabled through password-protected Unified Extensible Firmware Interface (UEFI) or Basic Input/Output System (BIOS) configurations to prevent unauthorized boot devices or peripherals.
- **RS-485**: Physical RS-485 for protocols such as Modbus and DNP3 will be provided by a USB-to-RS485 adapter. This will be protected by a configurable access control list preventing normal users from using the interface without appropriate credentials, and it is enabled only by an end user through password protected UEFI or BIOS.

4.2.2 Software Interfaces

The WAN interface corresponds to the communication between the Module-OT client and server. The LAN interface specifies the subnet of the critical resources on the electric grid. MGMT refers to the control subnet.

ModuleOT – Unit 1 loaded configuration (/usr/lib/ssl/config.json)


```
{
   "WANINTERFACE": "enp1s0",
   "WANIP": "10.10.49.45",
   "WANMASK": "24",
   "GATEWAYIP": "10.10.49.49",
   "LANINTERFACE": "enp2s0",
   "LANIP": "172.31.73.1",
   "LANMASK": "24",
   "MANINTERFACE": "enp3s0",
   "MANIP": "192.168.23.1",
   "TLSPORT": "8000",
   "WHITELIST" : ["10.10.49.45","10.10.49.49"],
   "NETWHITELIST":
["172.31.75.1","172.31.75.2","172.31.73.1","172.31.73.2","172.31.74.68","172.31.74.69","172.31.74.67
","172.31.74.64","192.168.2.104","192.168.2.105"],
   "MODBUSIP": "",
   "PASSTHRUIP": ["172.31.74.72","172.31.74.71"],
   "PROTECTEDPORTS": ["502","80","20000","8080"],
   "PASSTHRUPORTS" : ["4712"]
}
```


4.3 Operating System Requirements

Module-OT was developed and optimized to run on i686 or AMD64 Debian-based distributions of Linux. The current version is implemented on Ubuntu 16.04 LTS because it is Common

Criteria certified. The recommended installation of Module-OT requires the use of Advanced Package Tool (APT) to ensure correct dependencies and the optimal secure configuration; however, manual installation and building of binaries and dependencies is possible. The minimal operating environment for the recommended installation of Module-OT requires the following:

- Administrative/root access
- Package management (optional/recommended)
- Systemd support (optional/recommended)
- Capability to set minimum of three logical/physical network interfaces (WAN, LAN, MGMT)
- Logging infrastructure (Linux Log Rotate, systemd, and syslog)
- Dependencies—list out here or point to location in document.

5 Installation and Configuration

Figure 12 shows the basic setup architecture that could be used to set up Module-OT to secure communications between the ICS in the substation network on the right to the utility network's human-machine interface (HMI) on the left over an Internet connection.

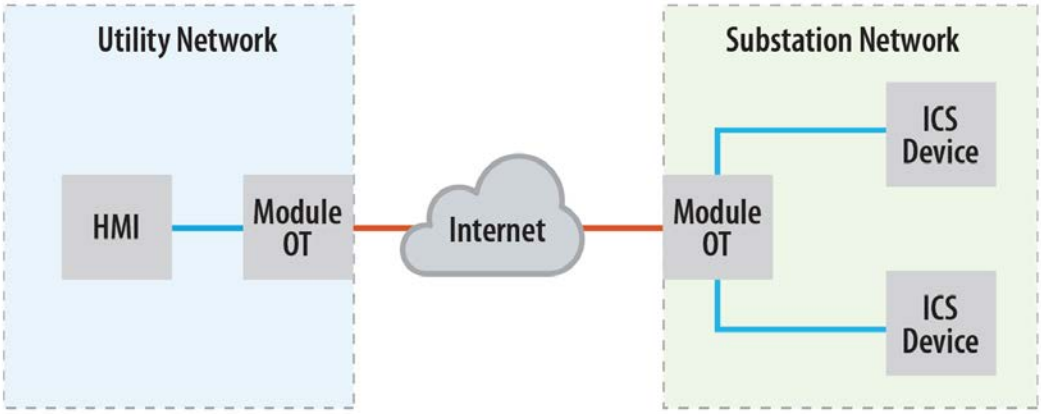


Figure 12. Module-OT basic setup diagram

5.1 Software Installation

To manually install the application software dependencies, follow these steps:

- Install Python: *sudo apt-get install python*
- Install Nmap: *sudo apt-get install nmap*
- Install OpenSSL: *sudo apt-get install openssl*
- Install OpenSSH: *sudo apt-get install openssh-server*
- Configure SSH server: *sudo nano /etc/ssh/sshd_config*
- Install PyModbusTCP: *sudo pip install PyModbusTCP*
- Place the MotApp executable in */usr/bin/*
- Place the moduleot.service file in */etc/services/* and enable the service: *sudo systemctl enable moduleot.service*

Note: These instructions will provide you with a copy of the project up and running on your local machine. To locally compile the source code, you will need to set up Golang on your system and compile the code with the included dependency packages in your *$GOPATH/src* directory.

Additionally, to install the development software dependencies, follow these steps:

- Install Go: *sudo apt-get install golang*-go
- Install Pip: *sudo apt-get install python-pip*
- Install Protobuf: *sudo apt install protobuf-compiler*

The GitHub release of Module-OT also provides an automated script to create the development environment to build and install Module-OT manually. A prebuilt version of Module-OT is also available as an official source released by developers at NREL. An officially packaged source for supported Ubuntu or Debian versions can be installed by adding the Module-OT repository:

/etc/apt/sources.list.d/

The repository will be accessible only once a key is installed via:

1. apt-key add <module-ot.gpg>—This will install the certificate.
2. apt-get install apt-transport-https—This will make apt-get use https.
3. apt-get update—This will update with the new repository.
4. apt-get install module-ot—This will install Module-OT into the device.

5.2 Software Configuration

Once the software installation is complete, configuration files on Module-OT need to be updated. Note that the current version has the same software on both the client and server sides. In both Module-OT devices, you can find the file "*config.json*" on the following path:

/etc/moduleot/config.json

The file has the variables described in the Table 6.

Table 6. Configuration File Summary

Config Variable	Description	Example
WANINTERFACE	Name of the WAN interface	"enp1s0"
WANIP	IP address of the WAN interface	"10.10.25.45"
WANMASK	(0-32) bit-number representation of network mask for the WAN interface	"24"
GATEWAYIP	IP address of gateway	"10.10.49.49"
LANINTERFACE	Name of the LAN interface	"enp2s0"
LANIP	IP address of the LAN interface	"192.168.10.10"
LANMASK	(0-32) bit-number representation of network mask for the LAN interface	"24"
TLS_PORT	Port used for TLS communications	"8000"
WHITELIST	List of IP addresses that can connect to Module-OT servers	["192.168.108.130","192.168.10.20"]
NETWHITELIST	List of TCP clients that can be added to the Module-OT network	["10.10.49.45","10.10.49.49"]
MODBUSIP	IP address for the Modbus SERIAL relay to use	"192.168.10.40"
PASSTHROUGHIP	Allowed IPs for unencrypted data to bypass Module-OT. Useful for PMU data	["172.31.74.72","172.31.74.71"]
PROTECTEDPORTS	List of ports used for encrypted data flow	["502","80","20000","8080"]
PASSTHRUPORTS	Allowed ports for unencrypted data to bypass Module-OT. Useful for PMU data	["4712"]

Following are expanded descriptions of the variables in the configuration file:

- **LAN interface**: This is the physical network connection (usually an Ethernet RJ45 port) that is connected to the "unencrypted side" of the network. This should connect to the trusted internal utility or grid network.
- **WAN interface**: This is the physical network connection (usually an Ethernet RJ45 port) that is connected to the encrypted side of the network. This port should connect to a DMZ or an externally facing network.
- **Subnetwork mask**: A subnetwork mask is a number that defines a range of IP addresses available within a network; it could be for either IPv4 or IPv6, but the current version of Module-OT uses IPv4. A single subnet mask limits the number of valid IPs for a specific network. "/24" is a different representation of the "255.255.255.0" subnetwork mask.
- **Network IP whitelist**: This is a list of IP network addresses that can communicate within the internal LAN network on both the grid and utility sides. This list most likely will be changed to match the IP address of each intelligent electric device that is connected.
- **Pass-through IP and port addresses**: Some applications such as PMUs are very sensitive to network latency and delays. At the moment, this feature allows some applications to bypass the whole Module-OT application. This port and the list of IP addresses needs to match the addresses of the devices that need to bypass the Module-OT application (for instance, PMU devices).
- **Network gateway**: A network gateway is an interconnected device that provides interoperability between outside networks (utility side) and local devices (grid side). This needs to match the IP address of the utility network.
- **Modbus IP address**: Module-OT allows interconnection to legacy Modbus devices through a TCP-to-Modbus adapter. This IP address should match the IP address of the Modbus adapter.
- **TLS port**: Module-OT uses TLS connections in the transport layer. Each application needs to have a network port associated with it. Port "8000" is currently being used to follow the DER standards; however, this could potentially be changed to any other port if needed.

Before using Module-OT for the first time, the configuration file should be modified on each device (client and server) according to the networking addresses of each system. Always remember to restart the Module-OT system service after making modifications in this file.

sudo systemctl restart moduleot.service

The file '/etc/network/interfaces' can be modified to assign static IPs to the LAN and WAN interfaces. Regardless of what is statically assigned, the application will assign the IP provided in the config file. The following LAN configuration must be added to '/etc/network/interfaces'. The WAN interface must also be added following the same formula.

Finally, the *dhcpcd* service must be disabled with:

sudo systemctl disable dhcpcd

For reconfiguration, update the file “config.json” in /etc/moduleot/ and restart the Module-OT service (always):

sudo systemctl restart moduleot.service

The service can also be stopped and started using the systemctl stop and start commands in a similar manner.

6 Module-OT Security Policy

According to FIPS 140-2, a cryptographic module needs to maintain an appropriate level of security for the application and environment where the module is used/installed, and it is the duty of the responsible cryptographic module authority to provide the acceptable level of security. Following is a summary of the different security levels, according to FIPS 140-2:

1. **Security Level 1**: This is the lowest security level, where the cryptographic module maintains the basic security requirements. This security level allows a cryptographic module to be executed in an unevaluated operating environment.
2. **Security Level 2**: This security level adds some additional security features to the cryptographic module. These features not only enhance the physical security mechanism but also provide some authorization capabilities to the cryptographic module. To achieve this security level, FIPS 140-2 makes it mandatory to add tamper-evident coating or a seal in the cryptographic module. Also, Security Level 2 requires role-based authentication in a cryptographic module. Additionally, the cryptographic module must be executed in a trusted operating environment.
3. **Security Level 3**: In addition to Security Level 2 requirements, Security level 3 requires an identity-based authentication mechanism in a cryptographic module. Security Level 3 requires input/output of plaintext CSPs to be performed in an independent port. This port should be logically separated from other interfaces. Security Level 3 also requires that the input/output form of plaintext CSPs should be in encrypted form in the cryptographic module.
4. **Security Level 4**: This security level provides the highest level of security. In this level, the physical security posture is enclaved in an envelope capable of detecting and responding to any unusual attempts at physical access. Security Level 4 is also capable of protecting the cryptographic module against security compromise due to environmental conditions or fluctuations outside of the module's normal operating ranges for voltage and temperature.

Module-OT has been validated to comply with Level 1 of FIPS 140-2. Although Level 1 does not require tamper-detection and role-based access controls, Module-OT has these two additional features, which helps it reach Level 2 compliance. Table 7 provides the level of security validation for Module-OT.

Table 7. Module-OT Security Level

Security Component	FIPS 140-2 Security Level
Cryptographic module specification	1
Cryptographic module ports and interfaces	1
Roles, services, and authentication	1
Finite state model	1
Physical security	N/A
Operational environment	1
Cryptographic key management	N/A
Electromagnetic compatibility/electromagnetic interference	N/A
Self-tests	1
Design assurance	1

6.1 Approved Algorithms

In the cryptographic module, the cryptographic algorithm performs the most important tasks of data encryption, authentication, and digital signature generation. The algorithms implementing these tasks are required to be FIPS 140-2-approved. FIPS 140-2 maintains a list of encryption-decryption, digital signature, and hashing algorithms. To comply with FIPS 140-2 Security Level 1, at least one of the approved algorithms listed in FIPS 140-2 should be incorporated with the cryptographic module. The approved algorithms of Module-OT are described in Table 8. In Module-OT, all the different algorithms perform different functionalities and are supported by TLS 1.3.

Table 8. Approved Algorithms of Module-OT

Security Function	Approved Algorithm
Symmetric key	AES-128
Asymmetric key	ECDHE, ECDHE-RSA
Hash standard	SHA-256
Message authentication	CCM-8

6.2 Finite State Model

The operation of Module-OT and its core dependencies maintains a finite state model, which comprises a set of input events, a set of output events, a set of multiple status, and functions. The capabilities of the finite state model is described as follows:

- Show operational or error state.
- Show transition from one state to another.
- Describe the input event that initiates the transition from one state to another.
- Describe the output event that results in transition from one state to another.

A finite state model can be represented by a finite state diagram. Figure 13 shows the state transition diagram for Module-OT. Each state is described as follows:

- **State 1 power-on state**: The host operating system has loaded the Module-OT software application into the memory in this state. The Module-OT transitions to the power-on state when the application is invoked as a process by the host operating system.
- **State 2 self-test state**: In this state, Module-OT performs self-tests.
- **State 3 error state:** This state initiates when the power-up self-test failed. The Module-OT application terminates when it detects a power-up self-test error.
- **State 4 operational state**: The self-test state executed properly, and cryptographic algorithms can be accessed by the Module-OT application. Module-OT will remain in the operational state until the application is terminated and enters the power-off state.
- **State 5 cryptographic officer state**: In this state, the cryptographic officer service (e.g., initialization) is performed.
- **State 6 user state**: The application is in the user state.
- **State 7 show status state**: The application is performing a show status operation.
- **State 8 key management state**: The application is performing a key management operation.
- **State 9 power-on state**: The host operating system has terminated the application process and released all memory.

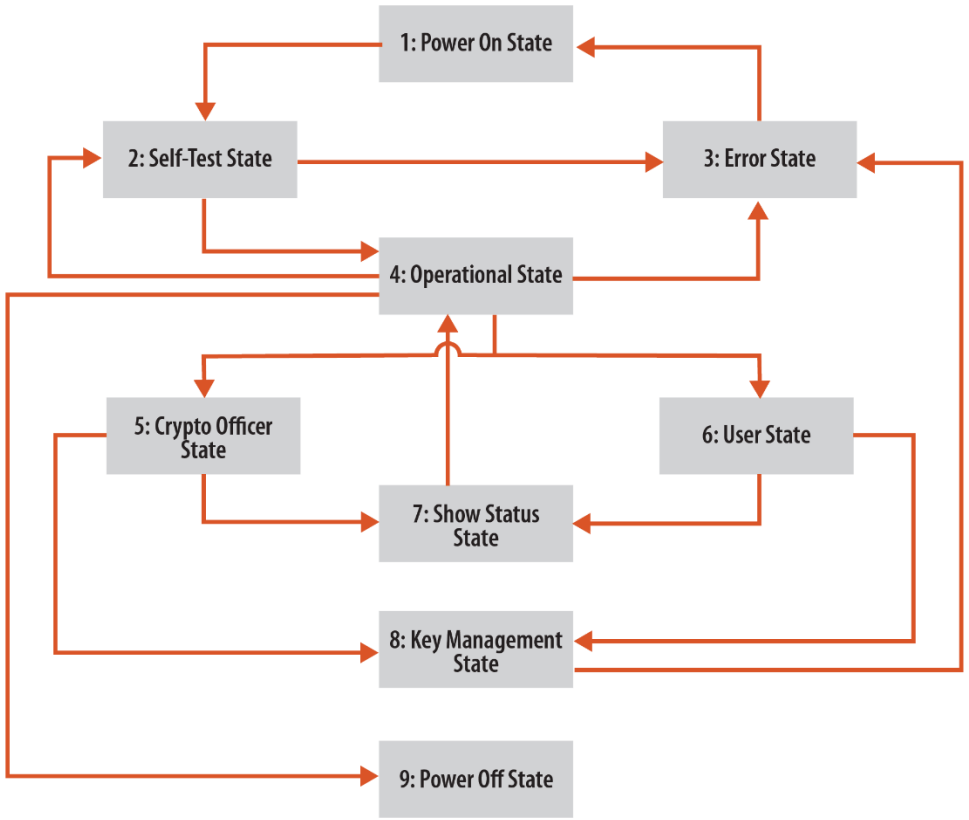


Figure 13. Module-OT finite state transition diagram

6.3 Roles, Services, and Authentication

Module-OT has the capability to support authorized roles for operators and corresponding services within each role. This subsection describes the roles, services, and authentication method of Module-OT according to the FIPS 140-2 requirements.

6.3.1 Roles

Module-OT supports the following authorized role for the Module-OT user, Module-OT administrator, and Module-OT developer. By maintaining the authorized roles, Module-OT completes the requirement policy of FIPS 140-2.

- **User role**: The role of the user in Module-OT is to perform general services, such as cryptographic operations and other security functions. The user in Module-OT is responsible for updating and deleting the key from the private database.
- **Cryptographic officer/Module-OT administrator role**: In Module-OT, the cryptographic officer performs the Module-OT initialization, the input-output of cryptographic keys, and other audit or management functions. The cryptographic officer has control to access the module before and after installation (e.g., execute Module-OT cryptographic code, have physical access to the operating environment).
- **Module-OT developer role**: The Module-OT developer is assigned to change any internal Module-OT configuration setting, if required. This developer group can access the root kernel of Module-OT.

6.3.2 Service

According to the FIPS 140-2 definition, service refers to all the operations, functions, or services performed by a cryptographic module. Module-OT initiates services, operations, or functions by gathering all data and control inputs. Those service inputs will result in some service outputs as a status or data. Following are descriptions of the services provided by Module-OT to the operator:

- **Show status**: Show the current output status of Module-OT.
- **Perform self-test**: Initiate and run the self-test.
- **Perform approved security function**: Perform the approved security function according to Module-OT modes of operation.

Module-OT additionally performs other approved services, such as symmetric encryption/decryption, keyed hashing, hashing, signature generation, and key generations.

6.3.3 Authentication

A cryptographic module is required to authenticate an operator who plans to access the module and to verify that the operator is authorized to assume the requested role and perform services within that role. To maintain Security Level 1, a cryptographic module supports at least one authentication mechanism:

- **Role-based authentication**: The module supports one or more roles that are explicitly or implicitly selected by operators. The cryptographic module does not require authentication of the individual operator's identity.

- **Identity-based authentication:** The module requires authentication of the individual operator's identity. This is done by considering the selection of roles and by the assumption of the selected roles.

Module-OT supports role-based authentication and permits a cryptographic officer to perform all the required service functions within their operating limit. Module-OT also permits an operator to change roles when required. Table 9 describes the approved services supported by Module-OT and the approved security functions, keys, and roles within those services.

Table 9. Module-OT Approved Services and Roles

Service	Approved Security Functions	Keys and/or CPSs	Roles
Module initialization	SHA256 hash check – OpenSSL	Precomputed SHA256 hash on Module-OT build	System
Symmetric encryption/decryption	OpenSSL	Preloaded key/certificates	System
Keyed hashing	OpenSSL	N/A	System
Hashing	OpenSSL	Precomputed SHA256 hash on Module-OT build	System
Random bit generation	OpenSSL DRBG	N/A	System
Signature generation	OpenSSL	N/A	Cryptographic officer
Key transport	OpenSSL/TLS	Preloaded key/certification	System
Key agreement	OpenSSL/TLS	Preloaded key/certification	Cryptographic officer
Key generation	OpenSSL/institution/third party	Preloaded key/certification	Cryptographic officer
Perform self-test	Module-OT, Linux	N/A	System
Zeroization	Linux OS/DD	N/A	System, cryptographic officer
Show status	Linux OS	N/A	User

6.4 Module-OT Modes of Operation

Module-OT, and its libraries, supports approved modes of operation. In this mode, Module-OT approves the security functions mentioned in Table 9 and will prevent access to the approved security functions during a nonapproved state of operation. For example, Module-OT is not able to generate keys in a nonapproved mode of operation, neither could it switch between two modes of operation using previously generated keys for approved services. Note that Module-OT will be in FIPS-approved mode when all power-up self-tests have been completed successfully, and only approved algorithms are invoked.

6.5 Module-OT Cryptographic Boundary

All the hardware, software, and firmware in a cryptographic module are required to be contained within a secure cryptographic boundary. This boundary will protect not only the hardware from physical tampering but also the software and firmware components from cyberattack.

The cryptographic boundary definition from the FIPS 140-2 states: "An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module" (NIST 2001).

6.5.1 Physical/Hardware Boundary

The physical boundary is the platform on which the software/firmware/operating system resides. The Module-OT prototype is built using Protectli Vault FW4B with an Intel Celeron processor to leverage AES-NI hardware acceleration. Figure 14 shows the physical boundary of the Module-OT hardware.

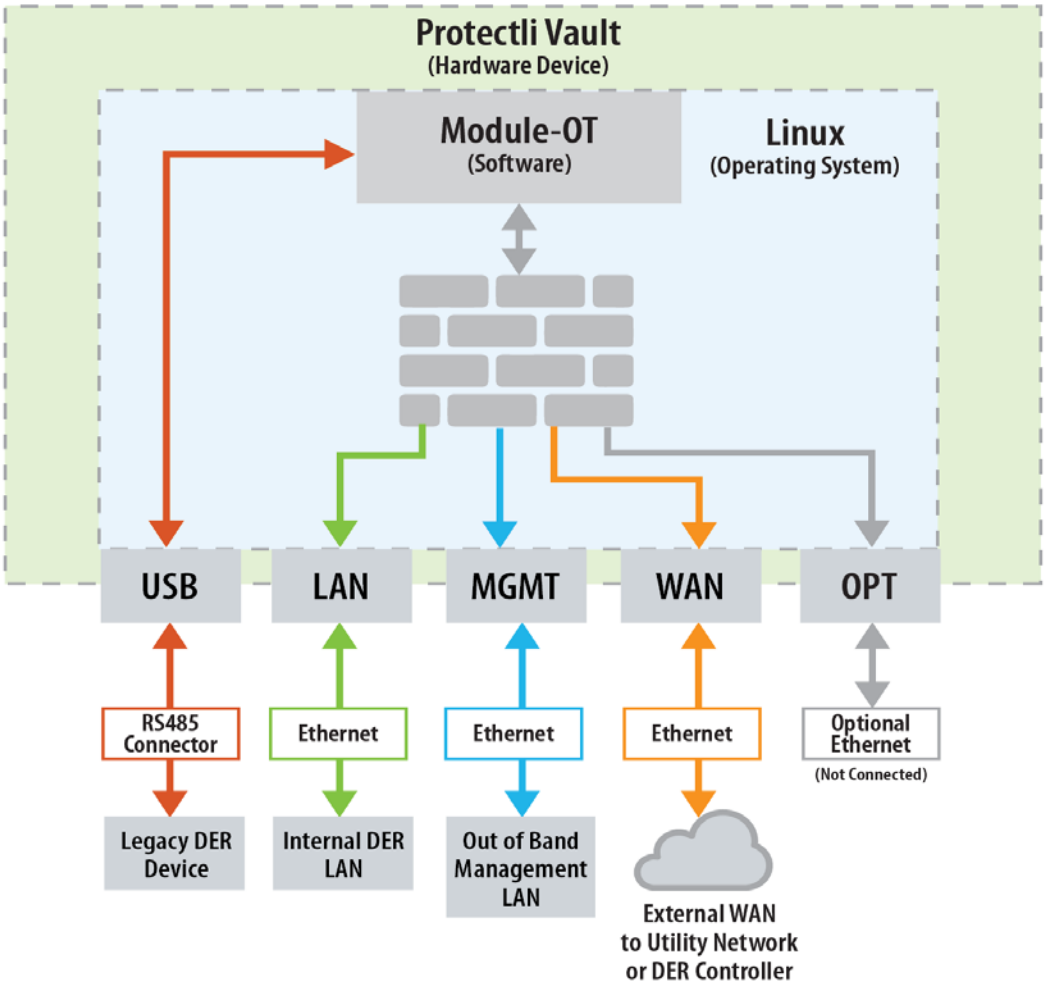


Figure 14. Module-OT physical boundary

6.5.2 Logical Boundary

The logical cryptographic boundary of Module-OT is a single-object file linked to OpenSSL. This Module-OT object file performs the calling application and communicates with the host operating system. The calling function invokes the module services. Note that the logical boundary resides in the physical boundary. Figure 15 shows the logical relationship of the Module-OT application to other software and hardware components residing in the physical boundary.

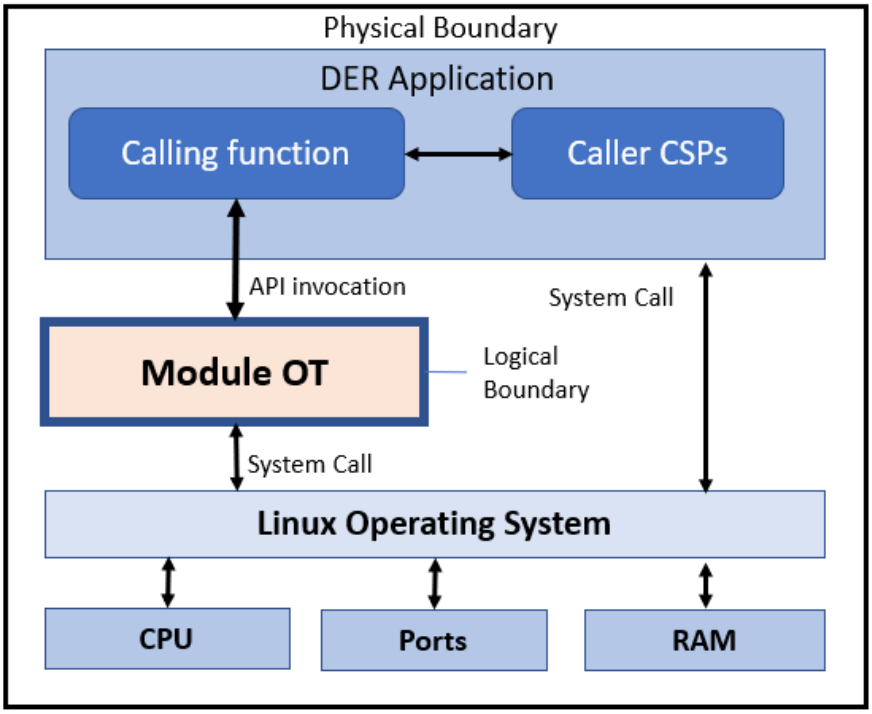


Figure 15. Module-OT logical boundary

6.6 Guidance

Module-OT identifies three different user groups based on their privileges. These include a user group, user administrator/cryptographic officer group, and a system administrator/developer group. The user group can view logs, status information, and settings, and they can change their password. A user administrator/cryptographic officer is responsible and authorized to create, delete, and modify accounts on behalf of a user. The user administrator is assigned to manage a user account, view all information, and analyze events. All the actions performed by a user or a cryptographic officer are logged in a database. The third group is a developer or system administrator group created to change any internal Module-OT configuration setting. This developer group can access core functions for the operating system and Module-OT. Tampered user accounts are disabled automatically. Table 10 describes all the user groups as well as the privileges in detail.

Table 10. User Groups

Username	Password	Privileges
motuser	motpass1	SSH, basic
moduleot	NREL	Sudo
root	NREL	Root

Note: Because of this design, only the motuser account can log in via SSH, and it is necessary to switch to a higher privileged account by running the "su" command.

6.6.1 Cryptographic Officer Guidance

The Module-OT security policy is developed to support its validation against FIPS 140-2 Security Level 1. The package that forms Module-OT can be installed by standard tools available on GNU/Linux distributions such as Ubuntu or Debian. Official builds of Module-OT are signed with a build key, and overall integrity is checked with a SHA-256 signature. This signature is automatically validated for official builds upon running the Module-OT application. Invalid signatures will cause the application to exit. A cryptographic officer is responsible for requesting the new Module-OT installation packages from the responsible system administrator or developer. Additionally, a cryptographic officer should not install Module-OT packages if an integrity error is found in the packages. Note that the main service function of a cryptographic officer is to perform cryptographic initialization and key management. A cryptographic officer can also access Linux system logs and can audit events. This access mechanism of Module-OT is done via journalctl, viewing the contents of /var/log, and running standard tools as an authorized superuser. In Module-OT, a cryptographic officer can also configure the operating system's audit mechanism. Once Module-OT is installed properly, the cryptographic officer should begin configuring Module-OT for the correct FIPS 140-2-approved modes of operation. The proper configuration setting step is mentioned in Section 5.

Module-OT employs tamper-evident mechanisms to ensure that the system has not been physically modified prior to operation. On physical modules, security stickers, and tamper switches are placed near hinge points. Residue from security stickers will alert a cryptographic officer if the device has been opened, and tamper switches will notify and activate security protections upon boot.

In Module-OT, a cryptographic officer is also responsible in performing zeroization of private keys and CSPs. Zeroization is done by removing all sensitive information (i.e., keys, certificates, configurations, user data) from the device. To perform zeroization, a cryptographic officer will properly authenticate to Module-OT and run the system configuration script to return the device to the default factory setting. After performing this function, the cryptographic officer must do a power cycle on Module-OT to clear all material contained in the volatile memory and being used by Module-OT

6.7 Self-Tests

FIPS 140-2 requires a cryptographic module to perform self-tests to ensure the integrity of Module-OT. This self-test functionality also guarantees correct operation of the module during the startup. Additionally, the approved mode function of any cryptographic module requires a

conditional test during normal operation. Module-OT supports a power-on self-test and conditional self-test. The following section describe the Module-OT self-test capabilities.

6.7.1 Power-On Self-Tests

The power-on self-tests are performed during the initialization of Module-OT and do not require a cryptographic officer to run. During the power-on self-test, Module-OT does not provide any output data. If any of the power-on self-tests are not successful, Module-OT will not initialize and will enter an error state where no Module-OT services can be accessed. Table 11 describes the types of power-on self-tests performed by Module-OT.

Table 11. Power on Self-Tests for Module-OT

Type	Test
Integrity test	HMAC-SHA-256, hash check
Known answer test	AES-128, ECDSA-256, RSA-2048, SHA-256 with OpenSSL

Note that Module-OT performs all power-on self-tests automatically when the module is initialized. This test is required before a user access the Module-OT approved mode of operations.

6.7.2 Conditional Self-Tests

Conditional self-tests are performed when new random numbers or asymmetric key pairs are generated during Module-OT operation. The conditional self-tests are done to achieve the PCT and the FLT. Table 12 shows the conditional tests performed by approved algorithms in Module-OT.

Table 12. Module-OT Conditional Tests

Algorithm	Test
DSA	PCT
ECDSA	PCT, FLT

7 Cryptographic Validation

NREL contracted with Leidos to provide a FIPS 140-2 initial conformance assessment review for the cryptographic implementation used by Module-OT. The primary goal of this review was to identify the effort required to obtain a FIPS 140-2 validation for the cryptographic components that comprise Module-OT. Leidos performed remote gap analysis sessions mainly by reviewing the requirements from the FIPS 140-2 *Derived Test Requirements* document and checking those against Module-OT's functionalities. Following are the findings by Leidos.

- Module is using the OpenSSL v1.1.1d cryptographic library, with some modifications made to the build process for it to operate in the DER environment.
- Module-OT runs on a Linux distribution, which is executed on a Protectli Vault device.
- Module-OT has passed the CAVP (NIST 2021b) testing, as shown in Figure 15 and described in NIST (2021a).
- Module-OT currently implements AES-128, ECDSA and SHA-256 only.
- Module-OT currently implements an HMAC SHA-256 integrity mechanism that meets the FIPS 140-2 requirements.
- Module-OT is still in a developmental state and therefore subject to change.

7.1 Algorithm Implementation

As found by Leidos, Table 13 identifies the approved algorithms (and their configurations) supported for each cryptographic implementation identified in the Module-OT application.

Table 13. FIPS 140-2 Approved Algorithms Implementation in Module-OT Application

Algorithms Supported	Implemented	Algorithm Options
AES	Yes	CCM (128-bit) encrypt and decrypt
DRBG	No	
DSA	No	
ESDSA	Yes	Sign and verify
HMAC	No	
KAS	Yes	EC Diffie-Hellman
KTS	No	
RSA	No	
SHA	Yes	SHA-256
Triple-DES	No	

7.2 Algorithm Testing

The Module-OT application does not directly implement any cryptographic functionality, but instead uses a customized build from the OpenSSL project. Our custom build sourced from the OpenSSL v1.1.1 branch is configured to remove all unused and potentially unsecured cryptographic algorithms and APIs. To ensure correct and secure operation, we contracted with Leidos to certify the build's cryptographic module under the NIST CAVP. The certification process involved testing the implementations of NIST-approved cryptographic algorithms and

individual components. Because by default the core application relied on AES_128_CCM_8, the algorithm capabilities shown in Table 16 were then selected to be validated.

Table 14. Selected Algorithm Capabilities for Validation

AES-CCM	
Key length	128, 192, 256
Tag length	32, 48, 64, 80, 96, 112, 128
IV length	56, 64, 72, 80, 88, 96, 104
Payload length	0-256
AAD length	0-524288

AES-CTR	
Direction	Encrypt
Key length	128, 192, 256
Counter tests performed	

AES-ECB	
Direction	Encrypt
Key length	128, 192, 256

Certification was performed by running individual test vectors generated by Leidos through a test harness developed at NREL. The test vectors each contained precomputed values and parameters that were read by the test harness and then executed through the appropriate cryptographic functions implemented by OpenSSL. The output was then sent to Leidos to verify that a correct value was produced. The custom OpenSSL build used by Module-OT was validated by Leidos on September 29, 2020 (NIST 2021a).

7.3 Recommendations from Leidos to Further Improve Module-OT Cybersecurity Posture

- Leidos recommended developing documentations such as a security policy, evidence for FIPS 140-2 certification, a finite state model, a list of hardware and software components used in the development of Module-OT, and a block diagram showing all the major components and data flows of Module-OT.
    - The project team worked on this recommendation and developed all the necessary documentation that would help users and/or commercialization partners to easily integrate Module-OT within their device or system.
- Leidos also recommended performing specific conditional tests, as required by FIPS 140-2. At the time of this validation, Module-OT did not require any conditional self-tests because it was still under development.
    - The project team worked on this recommendation later to make Module-OT support all types of self-tests, including power-on self-tests and conditional self-tests. Section 6.7 describes Module-OT's updated self-test capabilities. Note that Module-OT performs all power-on self-tests automatically when the module is initialized. This test is required to be performed before the user starts using the Module-OT approved mode of operations.

8 Testing

To evaluate the robustness of the developed module, three different kinds of testing were performed:

1. Laboratory testing at NREL and Sandia
2. Field-testing at a utility site
3. Red team testing by Sandia.

For each testing category, test procedures and experiment plans were developed. The laboratory test procedures sought to conduct various experiments to test Module-OT in a comprehensive manner. The procedures comprised two parts: bench testing and emulation testing. In addition, a series of attack scenarios was performed in a laboratory environment, leveraging hardware-in-the-loop simulation at NREL's Energy Systems Integration Facility, the Information Design Assurance Red Team (IDART) (Sandia 2021) at Sandia, and NIST's *Guide to Industrial Control Systems (ICS) Security* (NIST 2015), and successfully demonstrated Module-OT's ability to withstand such attacks. The red team assessment was also performed by combining the practices from multiple sources, such as NIST's *Guide to Industrial Control Systems (ICS) Security* (NIST 2015), best cybersecurity practices, and the collective project team's expertise regarding functionality of a cryptographic module. Finally, field-testing was performed in which Module-OT was deployed at a 500-kW PV and storage plant, known as the Prosperity site, which is owned and operated by PNM. This was to demonstrate secure communications between the Prosperity site to the utility's control center without any disruption to operations.

8.1 Laboratory Testing Approach

8.1.1 Bench Testing

1. **Information gathering**: Ensure that relevant documentation of the Module-OT device operation and implementation is provided.
2. **Functional testing**: Check that the functional baseline is met, including identifying interfaces, validating functionality against requirements and specifications, and testing that interoperability requirements are met; includes firmware integrity and critical functionality self-tests.
3. **Cryptographic implementation, public key infrastructure, key exchange/ authentication, and encryption (Section 4)**: Validate the implementation of the cryptographic software packages and other implementation details, ensuring that proper key exchange and certificate handling is conducted, and ensuring that successful encryption and decryption are performed; includes cryptographic self-tests derived from FIPS documentation.

8.1.2 Emulation Testing

1. **Implementation testing in emulation environment**: Use the cyber-physical emulation environment to ensure DER system constraints are not violated and that effective encryption/decryption processes are performed.

8.2 Field-Testing Approach—Demonstration at Utility-Owned Photovoltaic Site

For the demonstration and proof of concept, a 500-kW PV-plus-battery storage site was chosen. The site, Prosperity site (Figure 16), is owned and operated by PNM. It features 2,158 panels producing up to 500 kW on a 4.9-acre site in south Albuquerque, New Mexico. The site uses advanced lead-acid batteries with an energy rating of 1 MWh. The goal of the Prosperity project was to learn and address how to safely integrate a variable power source (e.g., solar energy) with a grid designed to handle steady, one-way power flows and make solar power available when the customer most wants it.

Figure 16. Aerial view of Prosperity site. *Photo by PNM*

For the demonstration of Module-OT at the Prosperity site, six use cases with test procedures were developed with the aim to create the testing and evaluation procedure for field demonstration of the device. This primarily included functional and implementation testing at the Prosperity site environment. Specifically, Module-OT was integrated into the Prosperity site system, and the communication traffic was encrypted at several points of interest, such as an inverter, micrologger, and switch. The following six use cases assessed the impact and effectiveness of the capabilities provided by the Module-OT device:

1. Between the PV meter and the switch
2. Between the micrologger and the switch
3. Between the switch and the gateway
4. One device between the micrologger and the switch and the other between the switch and the gateway
5. Between the gateway and the Fiber MUX

6. One device between the gateway and the Fiber MUX and the other at the PNM office.

In each use case, the goal was to (1) collect unencrypted traffic, (2) collect encrypted traffic, and, correspondingly, (3) collect decrypted traffic. In our preliminary testing, we explored each use case to narrow down the case that would be used for the final testing results. Ultimately, we decided to focus on Use Case 2, between the micrologger and the switch, to demonstrate Module-OT's ability to protect inverter communications (a primary goal of the project).

One of the few challenges of the project was to identify the location where we could place Module-OT for testing at the prosperity site. After days of discussions with the project partners, we agreed that the best location for placing the Module-OT is right next to the gateway/router at the distributed PV site and behind the firewall at the control center, as shown in Figure 17.

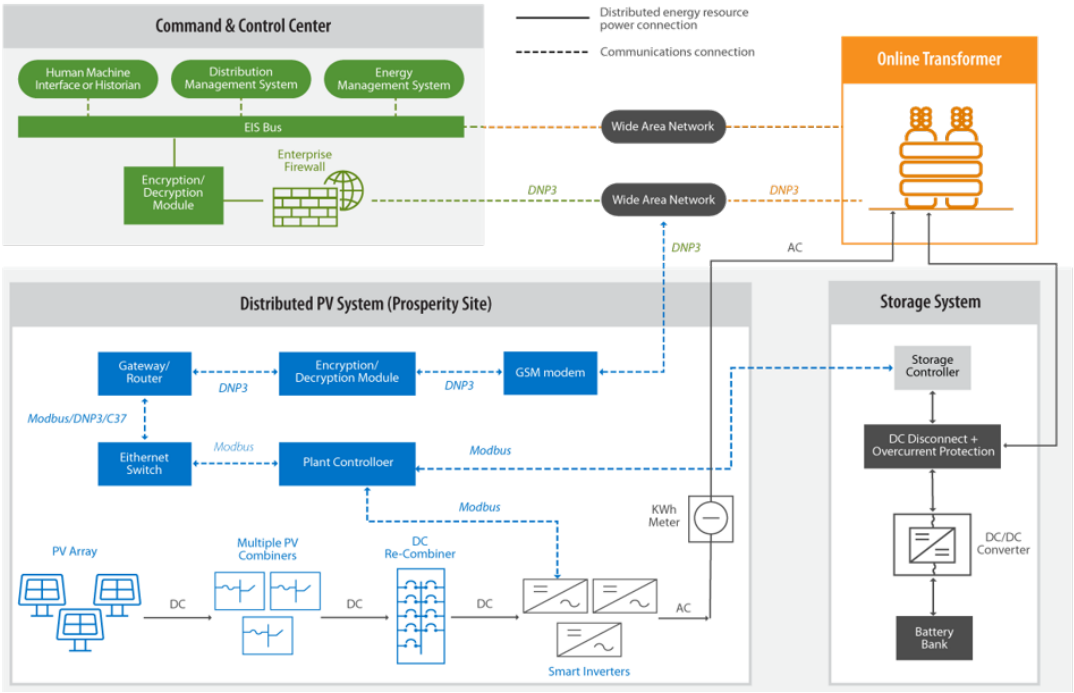


Figure 17. Placement of Module-OT at the Prosperity site

8.3 Red Team Testing Approach

The goal of the read team assessment was to identify Module-OT's weaknesses by demonstrating fragilities of the device to encourage a robust approach to the development and maintenance of the security module. The attacks conducted within this red team exercise spanned reconnaissance, interruption, interception, and cryptanalysis exploration, and the subsequent results and analysis provides important information for improving the security of Module-OT.

Red teaming is defined as an authorized, adversary-based assessment conducted to strengthen defenses through awareness of the system's potential vulnerabilities. The Module-OT devices in consideration comprise server and client applications installed on commercial, off-the-shelf network security hardware. For the red team experiment procedure, the objective was to assess the risks and vulnerabilities posed by system, network, application, and more thorough targeted activities—under controlled conditions—that might be engaged by an adversary. The red team

assessment combined practices from multiple sources: Sandia's Information Design Assurance Red Team, NIST's *Guide to Industrial Control Systems (ICS) Security*, best cybersecurity practices, and collective expertise regarding the functionality of a cryptographic module. These guides were used in defining the experiments that were conducted under controlled conditions to assess and evaluate potential security breaches to the cryptographic devices.

Vulnerability assessment and penetration testing are focused on finding and exploiting flaws to determine the security of systems. Although vulnerability assessment will identify vulnerabilities without exploiting them, penetration testing will find and exploit the vulnerabilities that would lead to device and information compromise. In addition, the experiment ensured that the system properly implements the following properties that affect the ability of a system to operate efficiently: confidentiality, integrity, and availability (CIA). This is known as the CIA triad (Security Ninja 2018), and it forms the basic tenets of information security. Other properties that were encountered and evaluated during the assessment process include accountability, non-repudiation, authorization, audit, and access control.

The red team assessment for the Module-OT server and client applications focused on a frozen version of the software installed, the encrypted communications between the modules, and the communications between the end devices using the application. Device entry points and configurations were also evaluated. These evaluations provided a snapshot of the security profile of the Module-OT cryptographic devices to determine the security of the system when exposed to complex environments.

The attacks for the assessment were conducted with the level of access that a general Internet user would have on either the WAN or LAN. A LAN can be specific to a building, whereas a WAN connects several LANs typically over the public Internet. Module-OT has a LAN network interface for interconnecting several DER devices within a limited area, a WAN network interface for facilitating communications with the LAN network in a different location, and a remote network monitoring interface. Attacks on the Module-OT devices were targeted toward connections on the LAN initiated by the DER devices to the Module-OT application and the encrypted WAN communications between the Module-OT devices in use. This is because points of interconnection leading to data exchange are causes for cybersecurity concerns because when they are manipulated, they can lead to negative system or operational impacts. In addition, flaws in the architectural design of the system—such as weaknesses in protocol implementation, authorization, and authentication strategies—were also examined.

8.3.1 Types of Attacks

There are many different types of vulnerability and penetration tests/experiments. The tests for the assessment are designed to:

- Find security vulnerabilities in the software and hardware.
- Perform network services tests to exploit information from the operating system and network services.
- Manipulate available metadata from the user guide documentation.
- Bypass or break the encryption used by the cryptographic modules.

The tools for vulnerability assessment and penetration testing can be broadly classified using network scanners and network attack tools. Based on these tools, two types of attacks—passive and active attacks—are described as follows.

8.3.1.1 Passive Attack

To gain as much information as possible about the target system of interest, system monitoring and data captures were employed as passive attacks. Passive attacks using network scanner tools involved the following two methods:

- Network reconnaissance, which involves information gathering of the target system.
- Vulnerability scanning, which uses plug-ins to check for flaws to identify known vulnerabilities where threats are categorized as high, medium, and low severity.

8.3.1.2 Active Attack

Active attacks go beyond the mere passive vulnerability scanning explored initially to a tighter coupling of actively exploiting identified vulnerabilities using the relevant penetration testing tools, such as:

- Interruption—the act of rendering the system unavailable to legitimate users. These tests investigate the availability of the Module-OT and DER devices in a communications network under a DoS attack.
- Interception—includes dropping, delaying, or altering data in transit. These tests investigate the confidentiality and integrity of data transfers under a MITM attack.
- Fabrication—includes inserting unauthorized data onto the network. These tests investigate the confidentiality and integrity of data transfers under a MITM attack.
- Privilege escalation—the act of exploiting flaws in design configurations to gain elevated access to unauthorized resources. These tests investigate the confidentiality, integrity, availability, and authorization of data under a privilege escalation attack.
- Cryptographic exploration—the act of exploiting failures and weaknesses to evaluate cryptographic systems. These tests investigate the confidentiality, integrity, availability, and authorization of data specific to cryptographic vulnerabilities.

9 Results

9.1 Laboratory Testing Results

The laboratory testing performed by Sandia focused on both bench and emulation experiments for Module-OT (Cordeiro 2019). These experiments were derived from the needs of DER systems, FIPS 140-2 guidelines for cryptographic devices, and discussions among the project team members. Key takeaways gathered from the testing results are documented as follows:

- A critical test was checking that the added latency from Module-OT did not violate any DER system constraints as specified by IEEE 1547-2018 latency requirements, and this was satisfied by the device (frozen version in December 2019). The emulation test environment, as shown in Figure 18, was stood up using a virtual machine manager technology, minimega (minimega 2021). Virtual machines were deployed to create the network and run the SunSpec SVP and instances of the EPRI DER Simulator. The SVP acts as an aggregator to send control commands to the inverter instances modeled in the EPRI DER Simulator; the SVP also requests information (e.g., voltage) from the inverters.
- Implementation of self-tests on the Module-OT device, both functional and cryptographic, was another recommendation that Sandia provided. It was then addressed with the continued development of the Module-OT device.
- Module-OT features such as whitelisting, firewall implementations, and the support of different communications protocols were also tested and verified; however, recommendations were provided for further flexibility and security.
- Documentation requirements are key for eventual implementation by a user. The Module-OT device now has a security policy document that describes how Module-OT meets the security requirements of FIPS 140-2 Level 1. The information captured in the security policy document will help potential users to easily adopt and implement Module-OT to provide added security to the DER systems. A subset of security policy documents has been added to Section 6 of this report.
- Future integration with IEEE 2030.5 (not currently supported by TLS 1.3) was recommended as a key industry discussion for the commercialization of Module-OT.

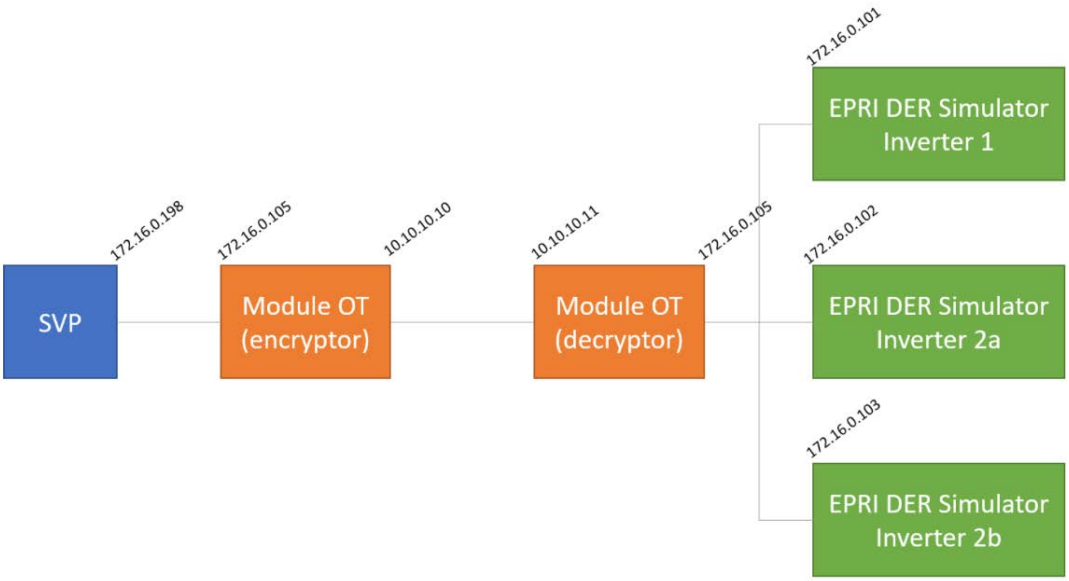


Figure 18. Emulation test environment

9.1.1 Validation of Module-OT Using the Cyber Energy Emulation Platform

To conform with rigorous availability requirements on potentially mission-critical ICS, Module-OT was put through various scenarios with equipment from different manufacturers to evaluate its performance and operation and to determine how it will behave in a real-world environment. A virtual instance of the core Module-OT platform was deployed and tested in our Cyber Energy Emulation Platform (CEEP) at NREL. CEEP is a novel emulation platform developed for achieving real-time visualization of large-scale environments involving cyber-physical devices. It allows for including real, physical hardware along with emulated devices communicating with each other as part of the same system. The CEEP is also capable of streaming, collecting, storing, transporting, and visualizing all data within the emulated environment.

Module-OT was integrated and deployed within CEEP as a series of virtual machines, containers, and hardware-in-the-loop solutions integrated with the ESIF's Power Systems Integration Laboratory (PSIL). Figure 19 demonstrates five different variations of deployments. These deployments captured the broad landscape of how Module-OT can be used in DER systems. The five different deployments depict three main approaches of how Module-OT can be deployed. These include (1) totally virtual through software-defined networking (SDN), (2) totally hardware-in-the-loop, and (3) a hybrid approach. CEEP has also enabled us to make rapid modification, testing, and validation of Module-OT experiment deployments.

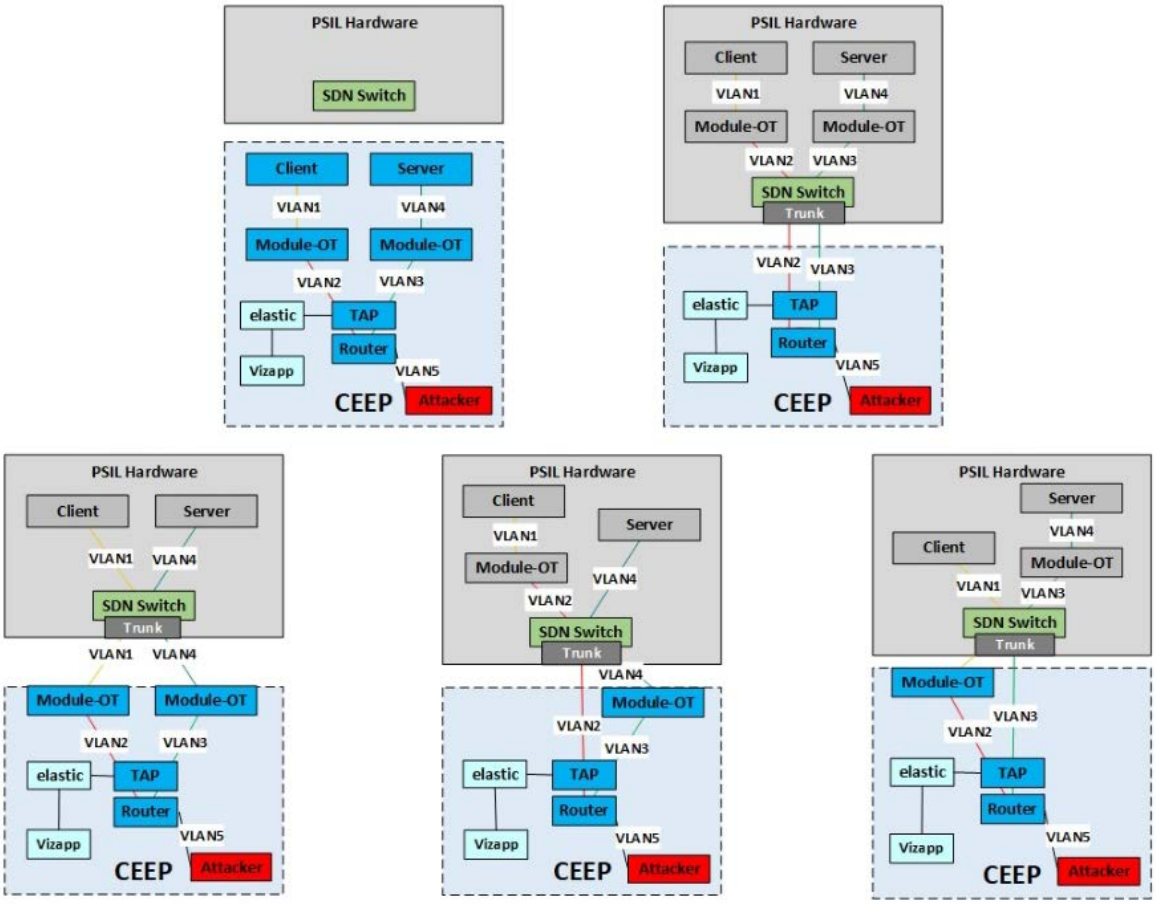


Figure 19. Various deployments of Module-OT within CEEP

Deployment 1: As a proof of concept, Module-OT was explored as a virtualized deployment linked to an automation, orchestration, continuous integration (CI), and continuous delivery (CD) workflow process. The experiment framework—which enabled the rapid deployment of Module-OT as virtual machine within a software defined network—was established for the experimentation of Module-OT within a virtualized and SDN context. Figure 20 demonstrates the deployment of Module-OT as an experiment leveraging CEEP's services.

Module-OT was deployed as a virtual system running as a kernel-based virtual machine and SDN leveraging minimega. This kernel virtualization, minimega, runs on top of a Docker container within a Kubernetes pod that links to the CI/CD pipeline. This enables rapid prototyping of the experiment system and networking architectures as well as CI/CD for modifications to code and/or experiment deployment. This deployment has allowed Module-OT to be explored as a virtual machine distribution that can be deployed to scale across SDNs through automation and orchestration methodologies.

Deployment 2: Module-OT was deployed as virtual systems running as kernel-based virtual machines within an SDN. The goal of this deployment variation was to integrate it with PSIL assets, such as the microgrid controller and PV inverters. This deployment variation allowed Module-OT to be explored as a virtual machine deployment within an SDN in conjunction with hardware-in-the-loop assets. An SDN hardware-in-the-loop integration framework was

established by the project team, allowing for communications among a series of virtual LANs, enabling trunking and virtual LAN tagging to occur between the series of virtual switches that extend communications from the experiment to the physical interface of the server and communicate through a series of SDN switches between the ESIF's data center and PSIL devices. Figure 21 demonstrates the deployment of Module-OT virtual machine deployment within an SDNN.

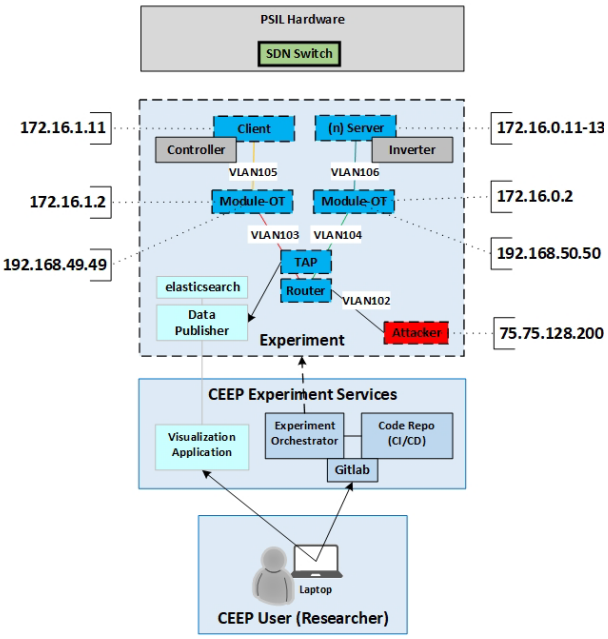


Figure 20. Module-OT deployment 1 within CEEP

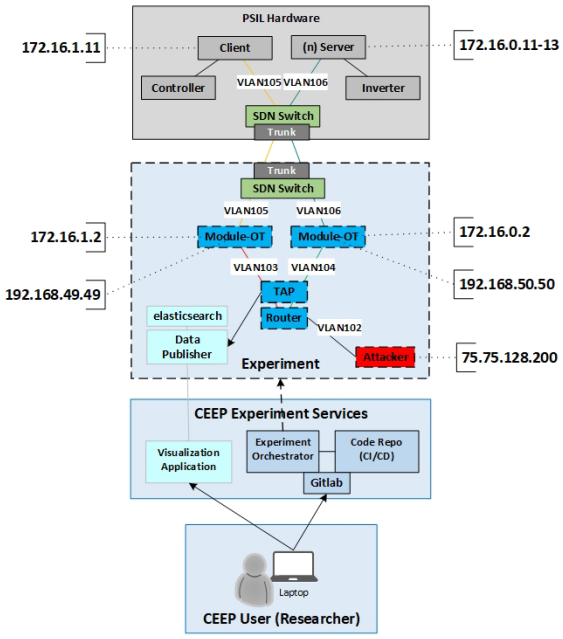


Figure 21. Module-OT deployment 2 within CEEP

9.1.2 Validation of Module-OT through Power-Hardware-in-the-Loop

After successfully testing Module-OT in various virtual configurations, the next step was to validate operation in a physical environment using power-hardware-in-the-loop. Testing was performed at NREL's PSIL to create a microgrid comprising both residential and commercial hardware. The microgrid was configured to simulate a remote PV energy generation site for a utility, as shown in Figure 25.

Residential PV generation was simulated by a 10-kW TerraSAS DC power supply programmed to follow a PV power generation curve typically seen on a sunny day. The DC power from the power supply was then connected to a 10-kW Fronius Primo (Figure 22a), where it was then fed into a variable load programmed to simulate energy usage from a residential consumer.

Commercial PV generation was simulated using two 250-kW Magna DC power supplies programmed to follow a PV power generation curve typically seen on a sunny day. The DC power from the supplies were each connected to inverters used in commercial applications, a 125-kW SMA high-power inverter (Figure 22b), and a 100-kW AE100TX inverter (Figure 22c). The power from the inverters was also fed into a variable load programmed to simulate energy usage from a commercial consumer.

Figure 22. (a) Fronius Primo 10-kW residential inverter, (b) SMA high-power 125-kW commercial inverter, (c) AE100TX 100-kW commercial inverter, and (d) SEL-3555 RTAC. *Photos by NREL*

Module-OT for both the residential and commercial PV generation was configured to secure communications between the devices at the PV site and the utility. During testing, we were able to send DNP3 and Modbus protocol data from each inverter across the WAN securely to a SEL-3555 RTAC (Figure 22d) acting as a utility HMI (Figure 23) seen at the utility.

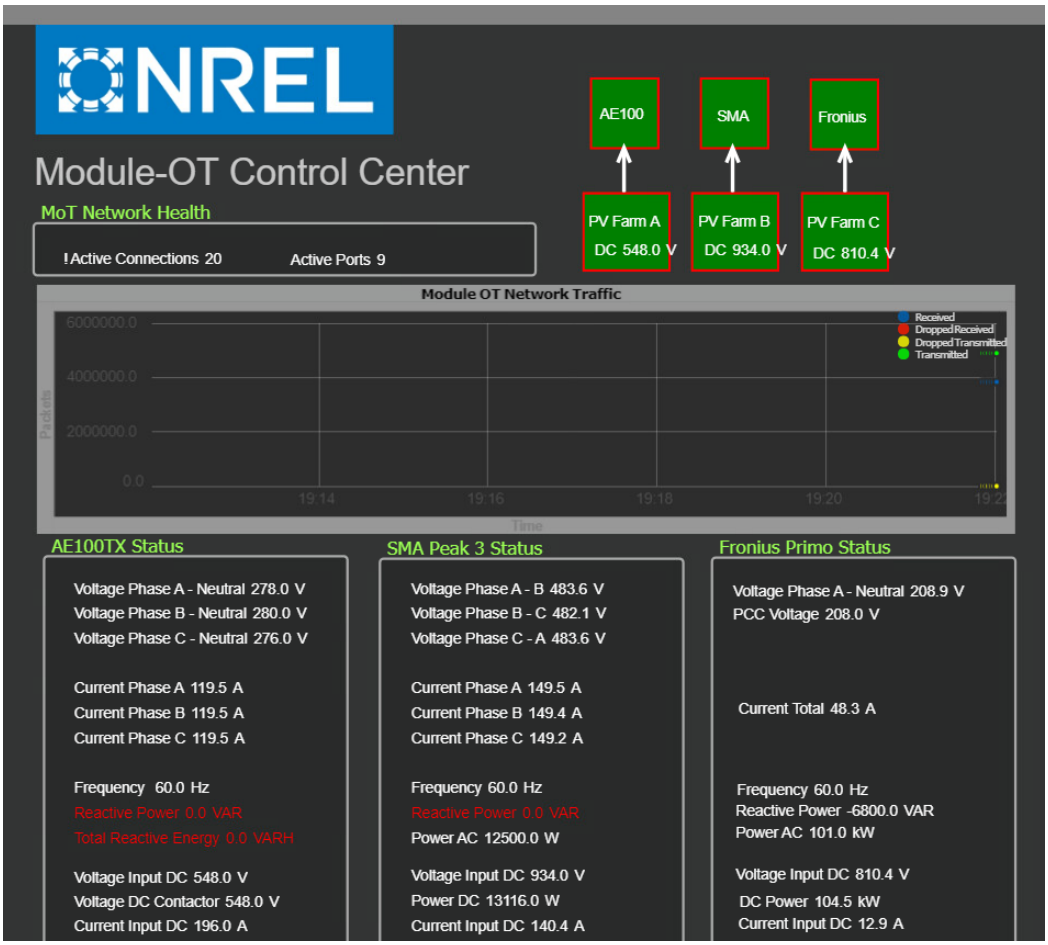


Figure 23. HMI implemented by the SEL-3555 RTAC

Network data were actively captured with Wireshark across the Module-OT WAN using a physical Ethernet terminal access point (Figure 24) to analyze TCP/IP sessions and ensure they were secure. Similarly, we captured data at the LAN for each Module-OT device and verified that no unauthorized sessions were able to communicate.

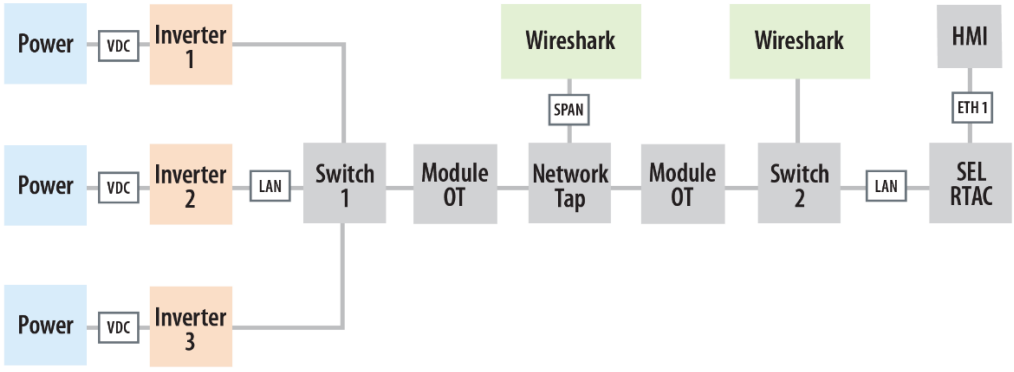


Figure 24. Physical LAN tap location

Once the protocol communications between each inverter at the simulated remote PV site and the HMI at the control center were established across Module-OT, we began testing overall resilience. During this phase, we physically disconnected the inverters to prevent them from talking to the HMI to understand the effects on the communications session in Module-OT. After a few rounds, we found that Module-OT was able to rapidly restore communications, and in most instances, it was able to buffer protocol data, ensuring nothing was lost.

Our final test considered protocol latency and how well Module-OT would perform during general faults. For this scenario, we generated faults and alarms at the HMI by randomly shutting down PV generation. Our results concluded that Module-OT was able to communicate critical events rapidly and even buffer them in the event of a loss of connectivity.

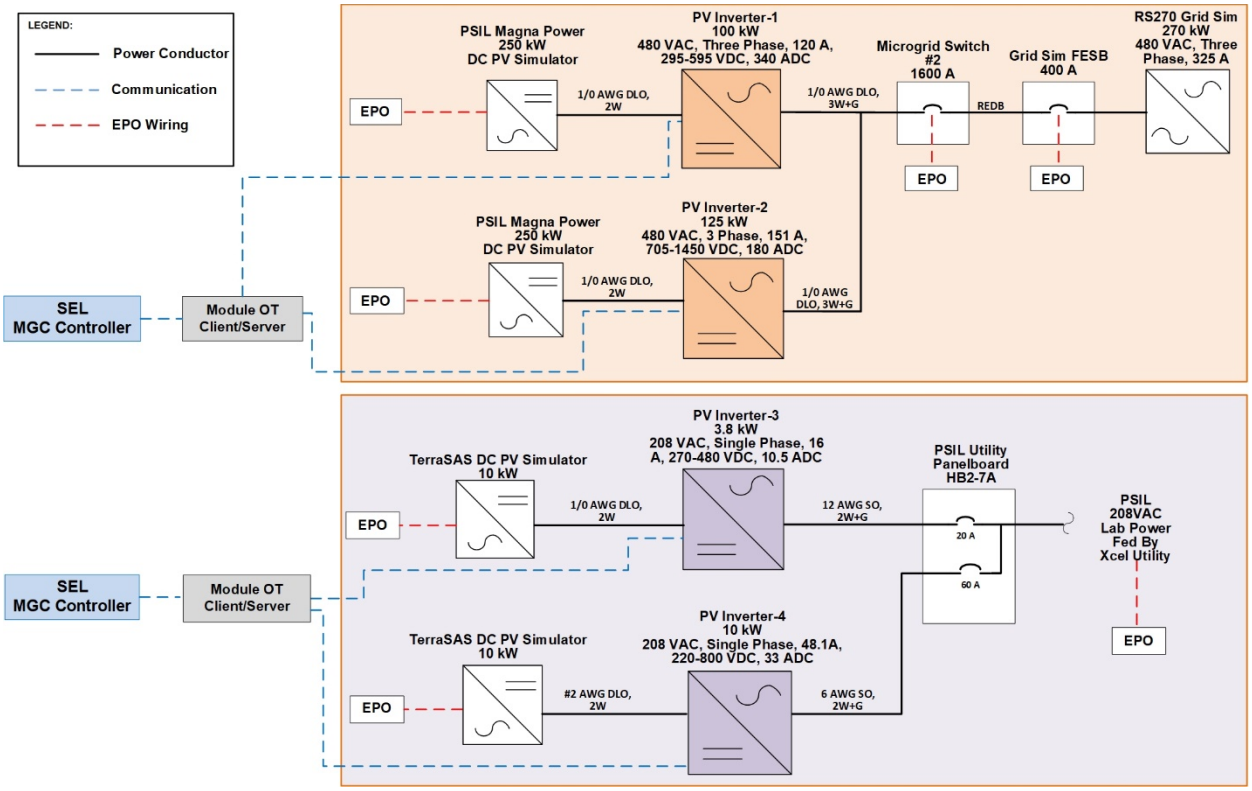


Figure 25. Power-hardware-in-the-loop testing setup with residential and commercial hardware

9.2 Field-Test Results

The field-testing experiments that were performed at the Prosperity site were also derived from the needs of DER systems, FIPS 140-2 guidelines for cryptographic devices, and discussions among the project team members. The main objective of the field-testing was to study the impact of the Module-OT devices on the PV system communications and to ensure that no power system disruptions were caused; by accessing the site's PV meter data, we were able to determine that the modules caused no added disruptions to the PV system operation by examining the output power, frequency, and voltage data. An example of the PV voltage data collected on November 26, 2019, is shown in Figure 26. The voltage variation remained within limits (~3 V), as confirmed by PNM, even with the Module-OT devices integrated.

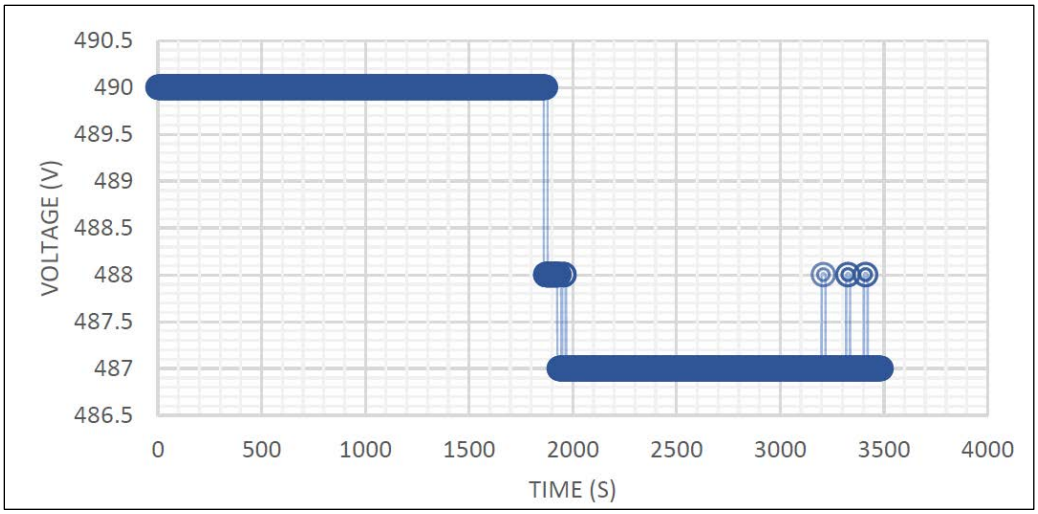


Figure 26. PV meter voltage data

As mentioned in Section 8.2, the project team drafted six use cases for the testing. The preliminary testing of Use Case 1 was successful, but it did not provide the same interest as Use Case 2 because only PV meter data were encrypted. Use Case 2 provided the scenario in which Module-OT was specifically encrypting and decrypting inverter communications. For Use case 3, although the communications traffic was expected to be collected, we were unable to see any targeted traffic—i.e., Modbus and DNP3. The same thing happened for Use Case 4, where the decryptor is placed at the same location. The lack of traffic flow was likely caused by the connectivity disruption between the data servers and clients caused by adding and removing test equipment and network cables multiple times. Use Case 5 and use Case 6 were of original interest to demonstrate post-gateway and offsite communications encryption/decryption; however, we again found that inserting equipment disabled communications between the DER devices and the data client polling them. Additionally, traffic in this network segment had a higher speed connection, and the hubs that were inserted in the network to allow verification of unencrypted, encrypted, and decrypted data were inadequate for this use case. For Use Case 6, PNM was ultimately unable to make the planned connections in their corporate network at the Aztec offices; further approvals are required, and PNM is investigating the process. Thus, Use Case 2 was selected as the primary use case for performing the final testing of Module-OT and for demonstrating its ability to protect inverter communications (via micrologger) at a utility PV site with a utility-commissioned inverter. Figure 27 shows the placement of the Module-OT devices for Use Case 2 within the green triangles, where E indicates encryption, and D indicates decryption.

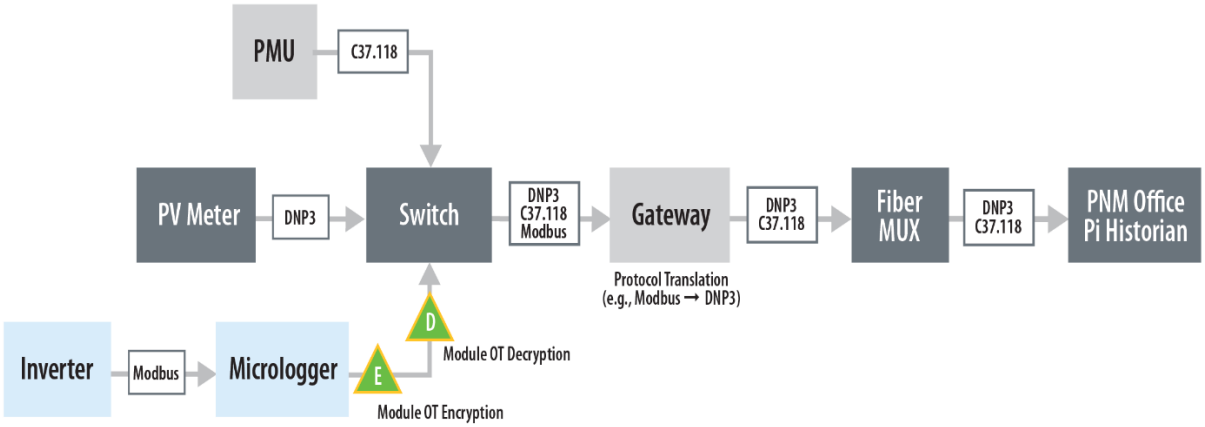


Figure 27. Location of Module-OT for Use Case 2

There were many challenges in testing the various use cases because of the lack of situational awareness regarding the PNM Prosperity site—primarily because it is a research site that is not actively used for any experiments and, thus, some diagrams and knowledge were outdated; however, PNM was very helpful with investigating these issues and finding available information.

Key takeaways gathered from the testing results are documented as follows:

- Module-OT was able to encrypt/decrypt traffic, perform module-to-module authentication, and whitelist IP addresses and ports for Modbus traffic between the micrologger and switch.
- Module-OT was also able to support both Modbus and DNP3 traffic, but the challenge of handling mixed traffic was identified (e.g., such as C37.118). This challenge was later addressed by NREL by creating a nonencrypted tunned for C37.118 traffic.
- Permissions and accessibility of certain PNM resources became an issue, specifically concerning the placement of a decryption module at their data center. This can be overcome, but it might require excessive time and paperwork. For future testing opportunities, it would be useful and realistic to test other use cases, such as encrypting traffic between the gateway and Fiber MUX.

Overall, for the use case of protecting inverter communications, the Module-OT devices were successful in their integration at the PNM PV Prosperity site both for cryptographic processes and environmental impacts. This showed promise for future applications to other DER systems.

9.3 Red Team Testing Results

The laboratory test environment for the red team experiments is shown in Figure 29. The testing environment initially comprised physical devices and later transitioned into a virtual implementation using virtual machines. The experiments were conducted on an isolated and controlled network environment. The network was created with two cryptographic modules for encrypting DER communications, DER server and client devices, network hubs for connecting multiple devices, and a computer with Kali Linux software for penetration testing and security auditing, as shown in Figure 28. The cryptographic modules being examined had three network interfaces: for (1) the encrypted WAN network that represents the network connection between

two remote sites, (2) the unencrypted LAN network connecting devices within a specific area, and (3) remote network monitoring management. Following are the lesson learned from the red team exercise.

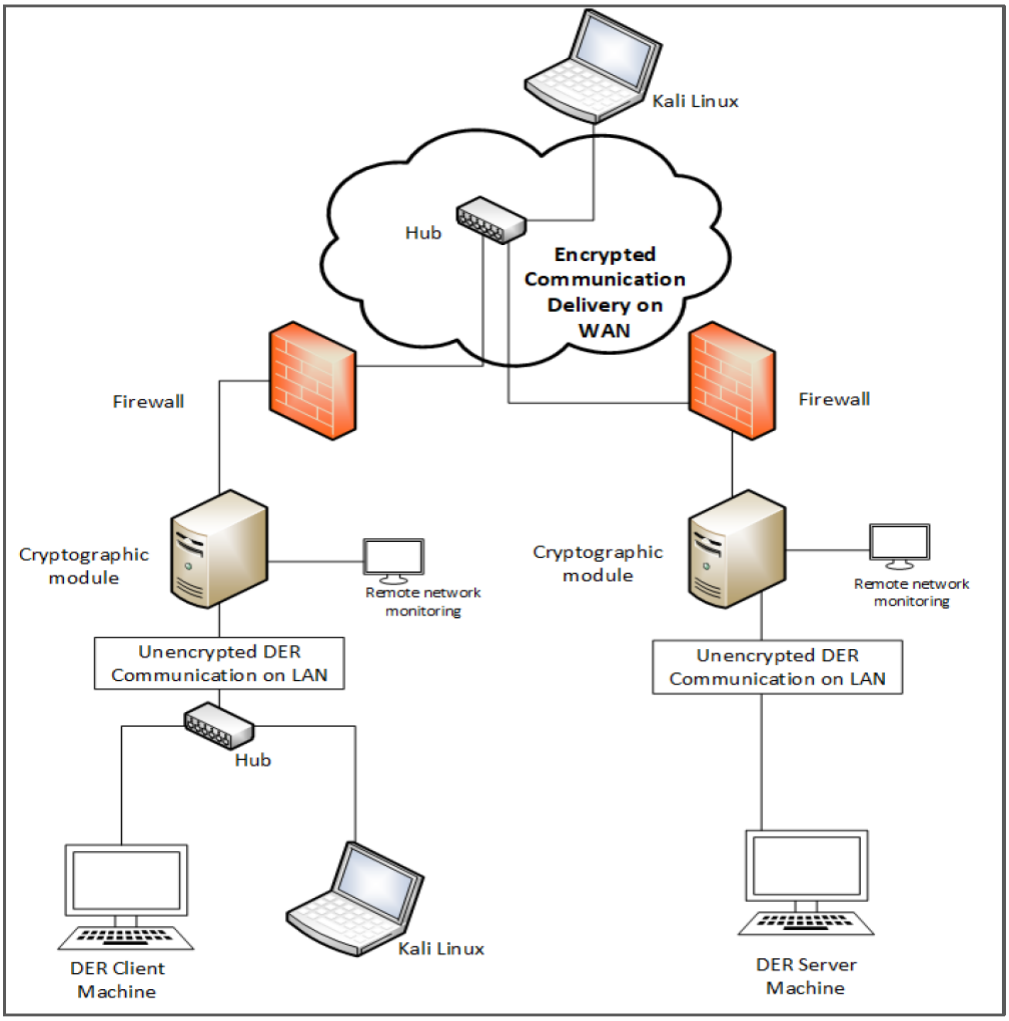


Figure 28. Physical test bed for red team assessment

9.3.1 Recommendations for Planning and Designing Cryptographic Module

Based on the red team exercise, we were able to understand what could be done better next time. Following are the general recommendations for system planning, design and configuration management that should be considered before and while designing a cryptographic module.

- Begin with the end goal in mind, with considerations such as, "what will it take to develop a cryptographic module for the DER community that is FIPS certified for the desired level of information protection while also and removing the barrier for entry for industry providing new or retrofitted communication-based controls for a more secure and interoperable DER?"
- Create control documents for the design.
- Create design specifications, including interface controls.

- Determine system specifications before selecting hardware/software, for example for TLS implementation.
- Review Common Vulnerabilities and Exposures (CVE) (NIST 2021c) for all incorporated services.
- Create decision points for design modifications if reduction in functionality becomes necessary.
- Consider partnering with professional product developers.
- Denial of service is difficult to prevent; in addition to firewall whitelisting already being implemented, setting limits on number of active connections to SSH service is recommended.
- Perform regular upgrades, updates, and patches on the system.
- Given the difficulty in collecting and analyzing logging information, it is best to integrate a centralized logging platform such as Splunk, Syslog-NG, or other application to manage the logs for easier network monitoring and to allow SEIM integration.

Following are the recommendation specifically targeted towards the software application development.

- If the application is using an open-source operating system and open-source cryptographic libraries, and other system libraries, ensure that the system management maintains software modules up to date.
- To reduce the attack surface, consider using a scaled back operating system version or a bare metal implementation of the security application running on hardware without an operating system.
- Software based encryption or virtual TPMs reduce the level of layered defenses provided by a discrete physical device, while only giving the appearance of the associated confidence and respect of a TPM. Therefore, consider implementing a physical TPM, instead of virtual TPM.
- Perform thorough code analysis of the source code and the binary to ensure that the code, or the overall application, is not calling functions that have not been verified. Also ensure that the cryptographic libraries called by the application, and all the data flows must be verified to be secure and traceable.
- As the DER industry moves toward widespread adoption of IEEE 2030.5, the incompatibility between TLS 1.3 and IEEE 2030.5 needs to be addressed (IEEE 2030.5 is not supported as a "constrained device" cipher suite)

10 Conclusion

This project delivered a cryptographically secure module, compliant with FIPS 140-2, that enables electric utilities, DER asset owners, and aggregators to seamlessly integrate or retrofit DER devices. Embedding cryptographic services, as well as authentication and device authorization, on top of preexisting equipment also allows for customization, such as selective encryption based on a preestablished threshold for sensitivity or low-latency application, as well as module replacement without retiring equipment.

The research on DER cryptosystems should focus on making efficient and secure decisions on protocol implementation. Minimizing the attack surface and achieving the separation of processes in communications-enabled DERs are two important stances for improving security. Because security research continually discovers new vulnerabilities, the best practice beyond using vetted solutions might be to allocate sufficient resources during the planning, design, implementation, and life of the product to defend against changing threats. As cryptographer and security reporter Bruce Schneier says, when you look at security, "The question to ask is not whether this makes us safer, but whether [it's] worth the trade-off" (Briand 2019).

10.1 Future Work and Commercialization Plan

Module-OT garnered immense interest from industry after the virtual meeting of industry stakeholders was convened to discuss the potential commercialization path and determine the interested parties. Of the many interested parties, Operant Networks, Yaskawa Solectria Solar, and Idaho Scientific were the top three candidates. NREL plans to work with these interested parties to conduct further research related to Module-OT's optimization and integration with DERs. NREL also plans to help the interested parties to better understand the Module-OT code and to collaborate with them for designing intrinsically secure DER devices.

Future releases of Module-OT will officially migrate to the Ubuntu 18.04 Server, which has been Common Criteria Certified as of December 2020. Debian Stretch will also be supported for development purposes.

References

Baker, James, Patricia Cordeiro, Tom Doepke, Shamina Hossain-McKenzie, Christopher Howerter, Nicholas Jacobs, Deepu Jose, Christine Lai, and Jeffery Zhao. 2018. *General Requirements for Designing and Implementing a Cryptography Module for Distributed Energy Resource (DER) Systems* (SAND2018-9407R). Albuquerque, NM: Sandia National Laboratories. https://www.osti.gov/servlets/purl/1467978.

Bodini, Nicola, Dino Zardi, and Julie K. Lundquist. 2017. "Three-Dimensional Structure of Wind Turbine Wakes as Measured by Scanning Lidar." *Atmospheric Measurement Techniques* 10: 2881–96. https://doi.org/10.5194/amt-10-2881-2017.

Briand, Xavier. 2019. "TED Talk notes: The Security Mirage—Bruce Schneier." *Medium.com,* February 5, 2019. https://medium.com/getting-into-infosec/ted-talk-notes-the-security-mirage-bruce-schneier-b81464ad51a7.

Cordeiro, Patricia, lfeoma Onunkwo, Nicholas Jacobs, Deepu Jose, Brian Wright, and Shamina Hossain-McKenzie. 2019. *Module-OT Laboratory Test Procedure* (SAND2019-15249). Albuquerque, NM: Sandia National Laboratories. https://www.osti.gov/servlets/purl/1592860.

de Carvalho, R. S., and D. Saleem. 2019. "Recommended Functionalities for Improving Cybersecurity of Distributed Energy Resources." Presented at the 2019 Resilience Week (RWS) Symposium, 226–231. https://doi.org/10.1109/RWS47064.2019.8972000.

Electric Power Research Institute (EPRI). 2018. "Overview of EPRI's DER Simulation Tool for Emulating Smart Solar Inverters and Energy Storage Systems on Communication Networks: An Overview of EPRI's Distributed Energy Resource Simulator." Power Delivery and Utilization. https://www.epri.com/research/products/000000003002013622.

Hupp, W. A. Hasandka, R. S. de Carvalho, and D. Saleem. 2020. "Module-OT: A Hardware Security Module for Operational Technology." Presented at the 2020 IEEE Texas Power and Energy Conference (TPEC), 2020, pp. 1–6. https://doi.org/10.1109/TPEC48276.2020.9042540.

Institute of Electrical and Electronics Engineers (IEEE). 2012. *IEEE 1815-2012 – IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)*. Piscataway, NJ.

———. 2018a. *IEEE 1547 – IEEE Standard for Interconnecting Distributed Resources with Electric Power Systems*. Piscataway, NJ.

———. 2018b. *IEEE 2030.5-2018 – IEEE Standard for Smart Energy Profile Application Protocol*. Piscataway, NJ.

Jacobs, Nicholas, Deepu Jose, Shamina Hossain-McKenzie, and Chris Howerter. 2018. *Analysis of Design Constraints and System Impact of DER Cryptographic Module* (SAND2018-11089R). Albuquerque, NM: Sandia National Laboratories. https://www.osti.gov/servlets/purl/1530169.

Jacobs, Nicholas, Shamina Hossain-McKenzie, Deepu Jose, Danish Saleem, Christine Lai, Patricia Cordeiro, Adarsh Hasandka, Maurice Martin, and Christopher Howerter. 2019. "Analysis of System and Interoperability Impact from Securing Communications for Distributed Energy Resources." Presented at the 2019 IEEE Power and Energy Conference at Illinois (PECI), 2019, pp. 1–8. https://doi.org/10.1109/PECI.2019.8698915.

Khan, A., M. Hosseinzadehtaher, M. B. Shadmand, D. Saleem, and H. Abu-Rub. 2020. "Intrusion Detection for Cybersecurity of Power Electronics Dominated Grids: Inverters PQ Set-Points Manipulation." Presented at 2020 IEEE CyberPELS (CyberPELS), 1–8. https://doi.org/10.1109/CyberPELS49534.2020.9311538.

Lai, C., et al. 2019. "Cryptography Considerations for Distributed Energy Resource Systems." Presented at the 2019 IEEE Power and Energy Conference at Illinois (PECI), 2019, pp. 1–7. https://doi.org10.1109/PECI.2019.8698907.

Lai, Christine, and Patricia Cordeiro. 2018. *Review of Authentication Strategies and Trends for Distributed Energy Resources (DERs)* (SAND2018-11778R). Albuquerque, NM: Sandia National Laboratories. https://www.osti.gov/biblio/1481592.

Liu, B., H. Wu, A. Pahwa, F. Ding, E. Ibrahim, and T. Liu. 2018. "Hidden Moving Target Defense against False Data Injection in Distribution Network Reconfiguration." Presented at the 2018 IEEE Power & Energy Society General Meeting (PESGM), 1–5. https://doi.org/10.1109/PESGM.2018.8586470.

minimega. 2021. "What is minimega?" minimega.org.

National Institute of Standards and Technology (NIST). 2001. *Federal Information Processing Standard (FIPS) (FP 140-2)*. Gaithersburg, MD.

———. 2002. *FIPS 140-2: Security Requirements for Cryptographic Modules*. Washington D.C.

———. 2021a. "Cryptographic Algorithm Validation Program." Computer Security Resource Center. https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?validation=33325.

———. 2021b. "Cryptographic Algorithm Validation Program." Project Overview. Computer Security Resource Center. https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program.

———. 2021c. National Vulnerability Database. https://nvd.nist.gov/.

Saleem, D., A. Sundararajan, A. Sanghvi, J. Rivera, A. I. Sarwat, and B. Kroposki. 2020a. "A Multidimensional Holistic Framework for the Security of Distributed Energy and Control Systems." *IEEE Systems Journal* 14 (1): 17–27. https://doi.org/10.1109/JSYST.2019.2919464.

Saleem, Danish, Adarsh Hasandka, Christine Lai, Deepu Jose, and Christopher Howerter. 2020b. "Design Considerations of a Cryptographic Module for Distributed Energy Resources." Presented at the 2020 International Conference on Consumer Electronics 2020. https://www.researchgate.net/publication/338459608_Design_Considerations_of_a_Cryptographic_Module_for_Distributed_Energy_Resources.

Sandia National Laboratories. 2016. "SCEPTRE: SCEPTRE provides a cyber-physical environment to analyze how cyber-initiated events affect the physical world" (SAND2016-8095C). Albuquerque, NM. https://www.osti.gov/servlets/purl/1376989.

———. 2021. "Cooperative Adversarial Security Assessments (CASA)." https://idart.sandia.gov/.

Security Ninja. 2018. "CIA Triad." InfoSec Institute. https://resources.infosecinstitute.com/cia-triad/#gref

Stouffer, Keith, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn. 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.

SunSpec Alliance. 2019. "SunSpec Modbus 700 series."

Zhu, Lei, Jacob Holden, Eric Wood, and Jeffrey Gender. 2017. "Green Routing Fuel Saving Opportunity Assessment: A Case Study Using Large-Scale Real-World Travel Data." Presented at the 2017 IEEE Intelligent Vehicles Symposium (IV), Los Angeles, California, June 11–14. https://doi.org/10.1109/IVS.2017.7995882.

Appendix A: Testing and Troubleshooting

This section provides guidance for testing and troubleshooting Module-OT. This testing and troubleshooting procedure verify the communications of Module-OT and ensures that it meets the FIPS 140-2 security requirement for the intended cryptographic service applications detailed in Section 1.

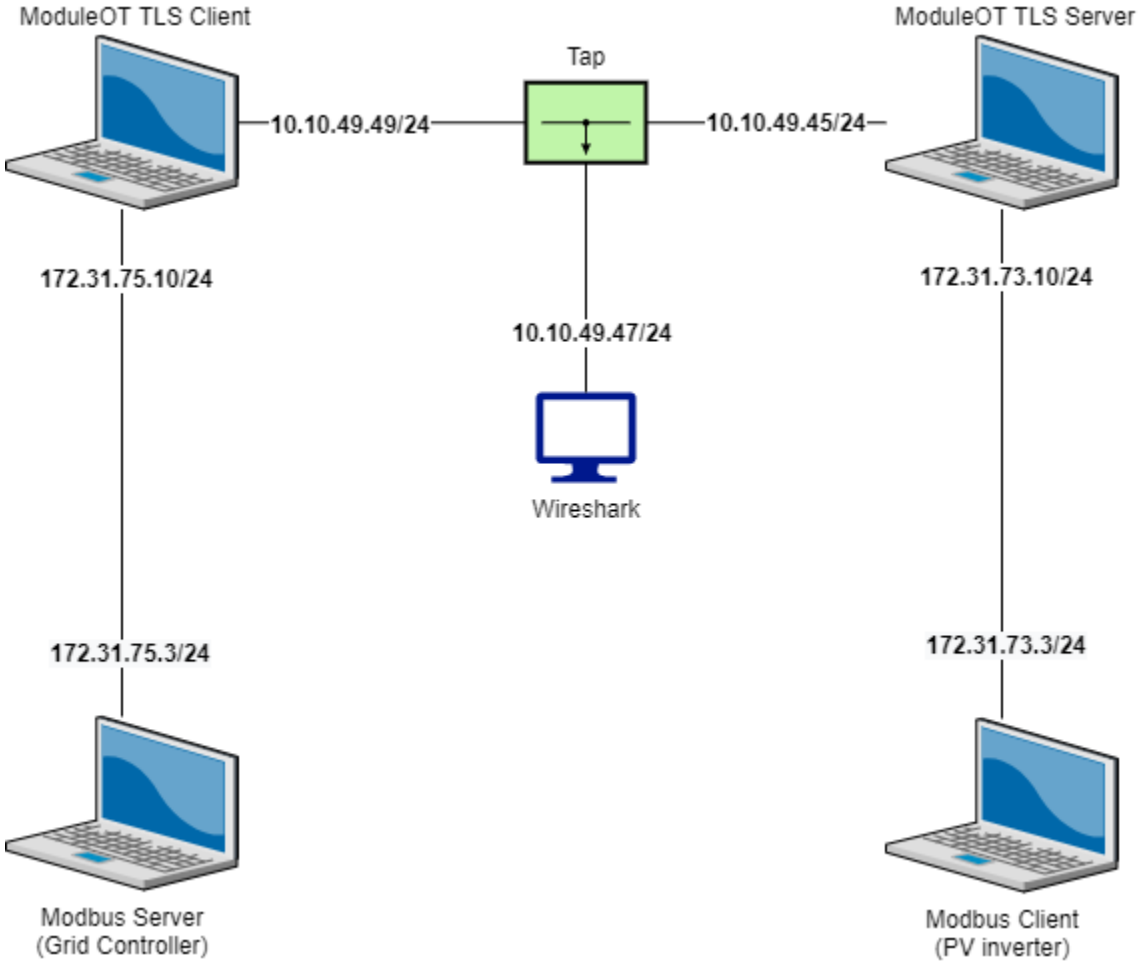


Figure A-1. Module-OT test setup

Testing Procedure

NREL developers performed detailed testing on Module-OT. Figure A-1 shows the Module-OT test setup diagram. The testing procedure will help users to ensure that the Module-OT settings are correct. To check whether Module-OT is operating properly, users should follow these steps:

1. Connect the MOT server and client module on their main Ethernet interfaces over the default network, 10.10.49.0/24. They may be connected directly or through a LAN/WAN. Any changes to the default IP configuration must be made in the config.json file, and the device must be rebooted.

2. Connect the devices to the MOT server. If the devices are available, they should be connected to the required LAN network. If the devices must be emulated, a virtual interface must be set up for each emulated device.
3. Connect the clients to the MOT client device. Any client may connect to the device over the LAN interface. They may freely communicate with the server devices with virtual relay servers hosted on the MOT client for each target server.
4. Start the TCP clients and TCP server devices.
5. Start the OpenSSL server.

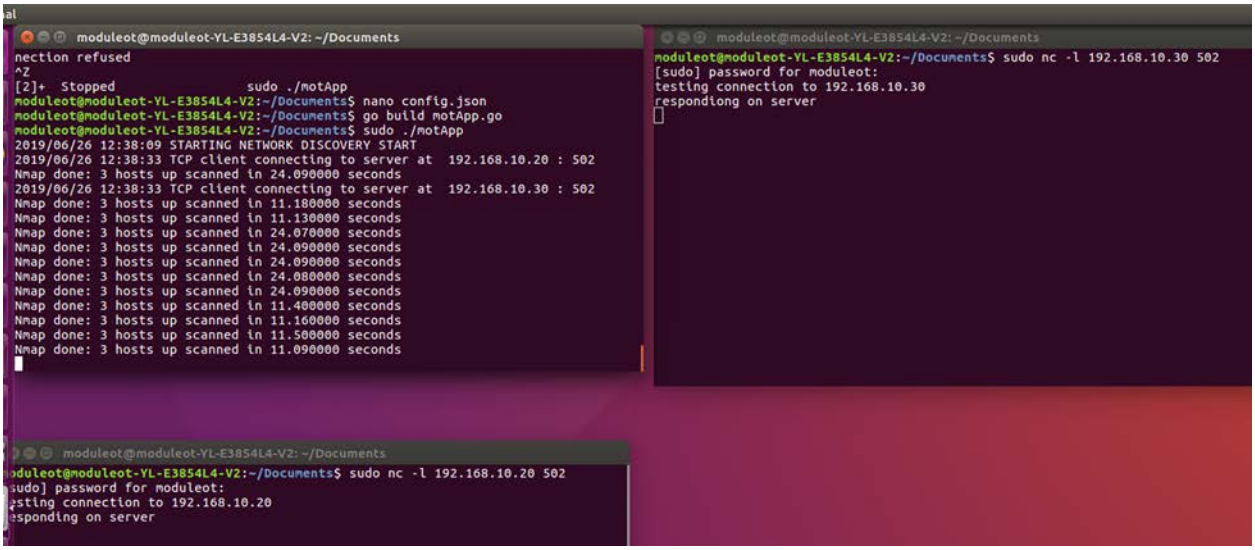


Figure A-2. Start the OpenSSL client.

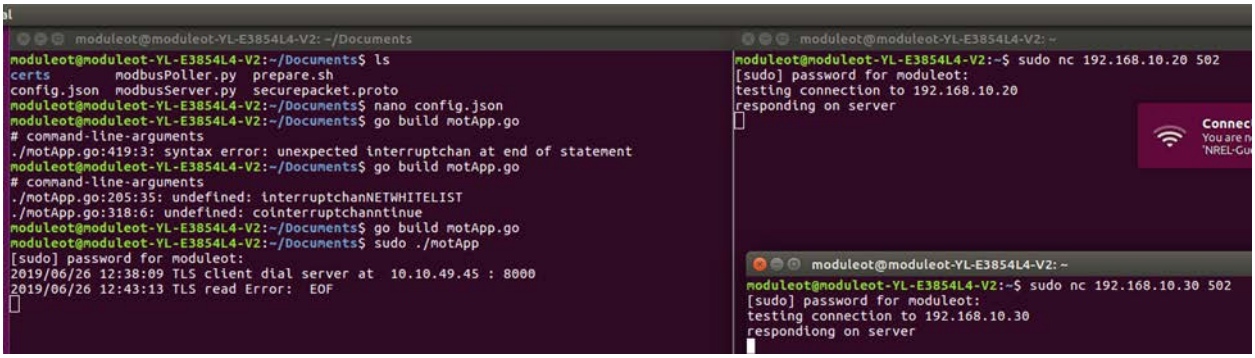


Figure A-3. Start communicating once the server discovers a whitelisted TCP client open IP/Por.

Dropping the connection

1. Repeat the same setup as the basic test.
2. Disconnect the TCP client from the OpenSSL server. The TCP client is dropped from the OpenSSL server.

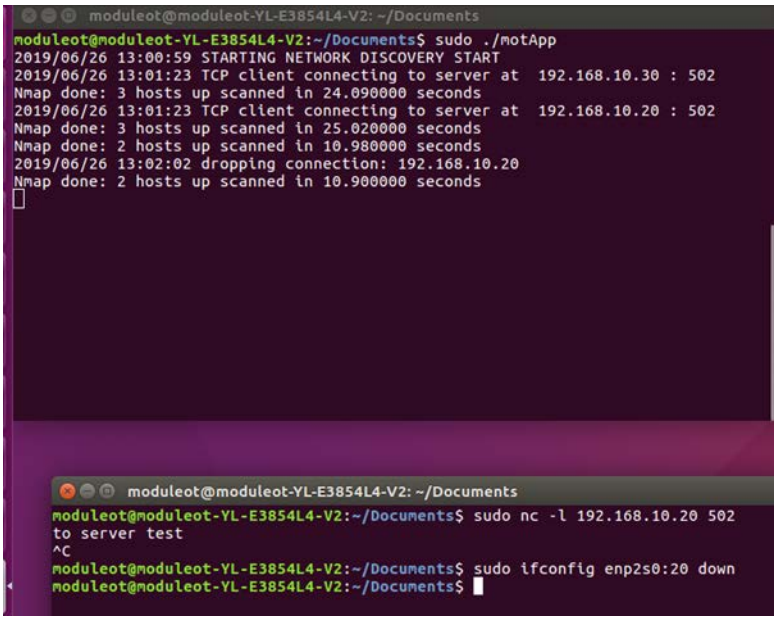
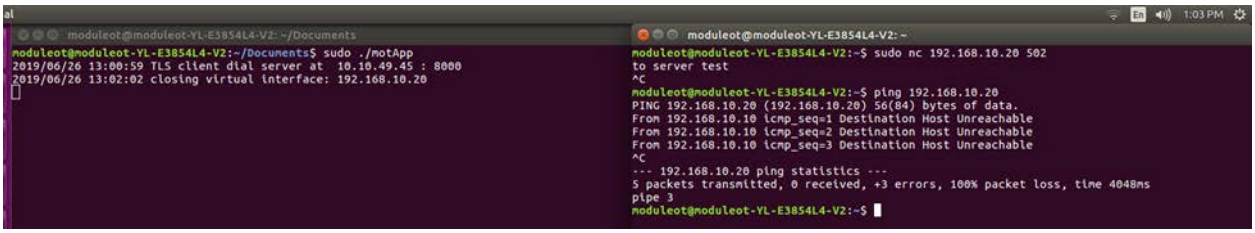


Figure A-4. The OpenSSL client is no longer able to connect to the TCP client.



Appendix B: Workshops and Webinars

Webinar

On December 1, 2020, the project team convened an online meeting of stakeholders interested in securing communications to distributed energy resources (DERs) and other grid-edge devices. These stakeholders included utilities, equipment vendors, nonprofits/utility service organizations, government agencies, and academics. Approximately 30 individuals attended the meeting in addition to the representatives from the three project team partners.

The primary goal of the meeting was to solicit feedback from the stakeholders regarding the Module-OT project and topics related to possible future commercialization. The level of attendance was encouraging but not high enough to draw statistically significant, industry-wide conclusions about DER trends or concerns. Following is a summary of observations from the survey responses:

1. Half of utility attendees maintain communications connections to the DERs on their systems.
2. Utility attendees claim to have a high level of understanding of the security state of their DERs.
3. Utility attendees claim to have a moderate to high level of concern regarding the security state of their DERs.
4. Cost and complexity are moderate- to high-level barriers to securing DERs.
5. Staff time is a moderate- to low-level barrier to securing DERs.
6. Staff knowledge is a high-level barrier to securing DERs.

Although the results are limited by the sample size of the responders, they seem to suggest that the security module developed by the Module-OT project is addressing a legitimate industry need. Among the goals of Module-OT was to make DER security simpler to implement (addressing items 4 and 6 above) and less expensive (addressing item 4 above).

The organizations represented by these individuals included the following:

- **Utilities**:
    - Duke Energy
    - Holy Cross Energy
    - Kootenai Electric Cooperative
    - Los Angeles Department of Water and Power
    - Mountain View Electric Association, Inc.
    - Omaha Public Power District
    - Tri-State.
- **Nonprofit/service organizations**:
    - American Public Power Association
    - National Association of State Energy Officials

    - National Association of Regulatory Utility Commissioners
    - National Rural Electric Cooperative Association
    - Northwest Public Power Association.

- **Vendors**:
    - Eaton Corporation
    - Kitu Systems
    - Operant Networks
    - Schweitzer Engineering Laboratories
    - Yaskawa Solectria Solar.

Government agencies:

    - National Institute of Standards and Technology
    - State Corporation Commission (Virginia).

- **Academic institutions**:
    - Texas A&M University
    - University of Arkansas
    - University of Denver.

Workshop

On July 17, 2018, right after the start of the project, the project team hosted an in-person workshop at the National Renewable Energy Laboratory (NREL). The workshop was divided into two breakout sessions. Each session included a set of questions that revolved around the need for cryptography and the impact and benefits that the electric power industry will receive from a dedicated cryptographic module for DERs. The workshop was attended by 45 people, including personnel from utilities, vendors, national laboratories, government cybersecurity experts, and from standards development organizations.

The goals of this workshop were to solicit the feedback of the stakeholders regarding the form factors and design features of the module and to provide them with a chance to express their concerns and share ideas about unsecured operational communications on the distribution grid related to DERs and other grid components.

Questions in the first breakout session highlighted the need to define where in the grid the module would be situated and subsequently the amount of effort needed to incorporate the module without disrupting current grid operations. Questions in the second breakout session were more focused on the requirements for the design and development of the cryptographic module. In addition to the topics discussed in the two breakout sessions, it was also discussed that because communications to DERs could come from end users, aggregators, vendors, data analytics, and operation engineers, it creates a range of issues on the ultimate control and protection of data. The two breakout sessions in the workshop involved posing questions and facilitating discussions among participants. The following questions were asked during the workshop.

1. Currently, what are the major economic or technical barriers to using cryptography?

2. What level of effort is currently required to incorporate cryptography-based security?
3. Do you feel your staff needs to be trained to use currently available cryptographic products?
4. Does cryptography present problems for interoperability, reliability, intrusion detection systems/intrusion prevention systems, etc.? (Does the inclusion of cryptography break some applications or functions?)
5. Does cryptography introduce latency that presents a problem for real-time equipment operation?
6. What do you want to protect, and how do you justify the value of cryptography?
7. What protocols/standards are you currently using that would benefit from additional security?
8. Which stakeholders might need to communicate with distributed energy resource (DER) devices?
9. What are the categories of devices in which Module-OT should operate (microgrid controllers, inverters, etc.)?
10. Who should be responsible for key management and incident response? Should it be managed in a centralized or a decentralized architecture?
11. Would you like to see a Module-OT solution that helps secure legacy equipment?
12. What should be the principal form factor and performance requirements for Module-OT?
13. What alert/alarm features should be included in Module-OT?

Following is the summary of observations from the breakout sessions.

- One main concern from participants in the workshop was where the cryptographic module would be located. This is very reasonable because the location of the module has much to do with the characteristics of the traffic it would be responsible for encrypting.
    - The project team addressed this concern by checking with the project's industry partners Public Service Company of New Mexico and Yaskawa Solectria Solar to identify the optimal location for placing Module-OT. Based on their suggestions, the team agreed to place Module-OT right next to the gateway/router on the distributed photovoltaic (PV) site and behind the firewall on the control center side, as shown in Figure 17.
- Another concern from the workshop participants was that it is not realistic for utilities to control DERs or devices associated with it. The reason is that currently most DERs are user owned, and utilities do not have communications going to those DERs. Utilities have communications only to the DERs they own, and those are very small in number. Third parties, vendors, and aggregators typically control the larger amounts of DERs on the grid.
    - The project team addressed this concern by conducting a market survey. The number of utilities that own, operate, and manage their own DER systems has significantly increased in the past 5 years, and this number will only continue to

increase moving forward. This can also be validated by the first observation noted in the webinar section, in which we found that half of utility attendees maintain communications connections to the DERs on their systems.

- Participants were concerned that the widespread use of the Modbus protocol for DER communications is a problem because the communications can often be in clear text, which suggests the need for bump-in-the-wire (BITW) technology to be employed for authentication and confidentiality.
    - Although there are not many cybersecurity requirements for SunSpec Modbus, it does provide the option of encrypting the communications traffic by wrapping the communications packets in a Transport Layer Security tunnel; however, for reliability and to avoid network configuration changes, users sometimes opt out of using this option. This is another reason to include Module-OT in DER systems, either as a BITW or an embedded solution that does not require big configuration changes but provides a much-needed security posture to the DER system.
- The interoperability and overall control of the cryptography module were also concerns from workshop participants.
    - The project team addressed this concern by testing Module-OT in the laboratory and at the Prosperity site. The results of this testing are captured in Section 9.
- Finally, a general suggestion raised by multiple participants was that utilities need to include cryptography in their specifications when negotiating with vendors and vendors need to ensure that their products have the latest capabilities.
    - The project team fully agrees with this suggestion. As captured in Section 10.1 on future work, NREL plans to help interested parties better understand the Module-OT code by collaborating with electric utilities to define the set of requirements that could be included in the request for proposals and to collaborate with manufacturers and vendors for designing intrinsically secure DER devices.

Lessons Learned That Informed Module-OT Requirements

The workshop attendees expressed their interest in a wide variety of needs and use cases. The project team realized that it would be impossible to satisfy all the needs; however, PV inverters emerged as a specific application that have wide interest and applicability, and thus the team settled on them as the first use case for the Module-OT project.

Based on the discussions in the workshop and on the lessons learned from the questions and concerns by the workshop attendees, the project team agreed to move forward with the following assumptions and form factors for the module.

1. PV inverters were considered as DERs in this project, and the module will be placed directly in front of the gateway/router (also shown in Figure 17).
2. While thinking about the category of DER system, we assumed that the DER system is owned and operated by a utility, and the other end of the module will be at the control center of that utility (also shown in Figure 17).

3. We agreed to use the Advanced Encryption Standard to provide encryption to the data between two modules.
4. We assumed that the physical security is already in place and is adequate for the device to which the module is attached. In other words, physical security was considered outside the scope of this project.
5. We agreed to develop a built-in whitelist in Module-OT that would allow access only to the Internet Protocol addresses, devices, and personnel that are already identified as legitimate.
6. We agreed to develop a Web interface through which utilities can manage the module. This was meant to be the secure link from which the utility can directly access the module.
7. We also planned to include the utility's Web interface in the whitelist, so the module knows it is an authentic connection.
8. We agreed to have data logging capability in Module-OT that could capture changes in configuration, changes in default settings, and log-in/log-out information, etc.
9. We agreed not to restrict Module-OT to any specific communications protocols, such as Modbus RTU and Modbus Transmission Control Protocol (TCP), Distributed Network Protocol 3, and SEP 2.0.
10. We agreed to enable Module-OT to perform the authentication and integrity checks of the data traffic between DERs and the command-and-control center.

The project team also agreed to create the prototype module as a BITW device. We discussed that the vendors that would eventually decide to commercialize Module-OT could either build a commercial BITW module or adopt its design and embed it into the device itself. Table 17 describes other form factors that were discussed before building a BITW prototype.

Table A-1. Form Factors of Module-OT

	General Solution	Comments	Final Remarks
1	Bolt on	This solution requires additional computing resources, which DERs (inverters) usually do not have; hence, it is not recommended.	Not recommended
2	Embedded	This solution is like a Trusted Platform Module (TPM). TPMs are typically used in high-end servers that have large computing capacity; usually, DERs (inverters) do not have that. In addition, different inverters (from different vendors) have different ways in which they operate; therefore, if this route had been chosen, the module would need to be customized for each inverter, which would be nearly impossible. Thus, this is not a feasible solution, and it is not recommended.	Not recommended
3	BITW	This is the most feasible solution because: There is no need to have additional computing resources in the DERs. There is no need to worry about different architectures of different inverters and no need to worry about how inverters operate. In the workshop, we realized that industry wants a flexible solution, and BITW fits that. We agreed to develop a framework for DER security using selective encryption and to let future users of Module-OT decide how they would like to implement it.	Recommended

We also agreed to include the following hardware and software interfaces:

- Serial port (RS-485): Modbus RTU
- Ethernet port: Modbus TCP
- One fiber port (optional).
- One management interface that will be the secure link from the utility directly to the module.
- One data interface.