Article

Cybersecurity Certification Requirements for Distributed Energy Resources: A Survey of SunSpec Alliance Standards

Sean Tsikteris, Odyssefs Diamantopoulos Pantaleon, and Eirini Eleni Tsiropoulou

Dept. of Electrical and Computer Engineering, University of New Mexico, Albuquerque, NM 87131-0001; stsikteris1@unm.edu; odiamantopoulospanta@unm.edu; eirini@unm.edu
* Correspondence: eirini@unm.edu

Abstract: This survey paper explores the cybersecurity certification requirements defined by the SunSpec Alliance for Distributed Energy Resources (DER) devices, focusing on aspects such as software updates, device communications, authentication mechanisms, device security, logging, and test procedures. The SunSpec Cybersecurity Standards mandate support for remote and automated software updates, secure communication protocols, stringent authentication practices, and robust logging mechanisms to ensure operational integrity. Furthermore, the paper discusses the implementation of the SAE J3072 standard using the IEEE 2030.5 protocol, emphasizing the secure interactions between electric vehicle supply equipment (EVSE) and plug-in electric vehicles (PEVs) for functionalities like vehicle-to-grid (V2G) capabilities. This research also examines the SunSpec Modbus standard, which enhances the interoperability among DER system components, facilitating compliance with grid interconnection standards. The paper also analyzes the existing SunSpec Device Information Models, which standardize data exchange formats for DER systems across communication interfaces. Finally, the paper concludes with a detailed discussion of the energy storage cybersecurity specification and the blockchain cybersecurity requirements as proposed by the SunSpec Alliance.

Keywords: Distributed Energy Resources, SunSpec, Electric Vehicles, Cybersecurity.

Citation: Tsikteris, S.; Diamantopoulos Pantaleon, O. Tsiropoulou, E.E. Cybersecurity Certification Requirements for Distributed Energy Resources: A Survey of SunSpec Alliance Standards. *Energies* **2024**, *1*, 0. https://doi.org/

Received:
Accepted:
Published:

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

1. Introduction

The shift towards digitization and decentralization in the electric power grid is an important step in order to achieve both economic and environmental sustainability [1]. Distributed Energy Resources (DERs), such as rooftop solar panels, battery storage systems, and electric vehicles, are increasingly integrated into the modern power grids, and they provide significant benefits to the power and utility companies by reducing the operational costs, while also giving greater control to the users and the energy aggregators over their energy production and consumption [2]. However, as DERs become more interconnected and interoperable, several cybersecurity concerns arise, especially due to their remote management and control. Additionally, the reliance on communication networks and the wide variety of DER configurations significantly expand the potential attack surface.

In this paper, a detailed survey is presented based on the SunSpec Alliance's proposed best practices related to the DER devices cybersecurity standards. The analysis focuses on the SunSpec cybersecurity certification requirements and their main categorization. Then, a detailed analysis is provided on the SunSpec requirements for the test procedure by identifying the main test cases and analyzing the SAE J3072 system architecture. Then, the SunSpec Modbus functionalities are presented, where the SunSpec Modbus is an open communication standard specifically designed to facilitate interoperability among the DER system components. Additionally, the SunSpec device information models are presented in order to standardize the device data exchange. Moreover, the SunSpec energy storage cybersecurity specifications are discussed along with the SunSpec blockchain cybersecurity requirements. Finally, a detailed gap analysis is performed to identify the main gaps of the

SunSpec Alliance Cybersecurity standards, and solutions are proposed to address these gaps.

1.1. Related Work

DERs play a critical role in the operation of modern smart grid systems [3]. Recently, substantial research work has been focused on the cybersecurity challenges related to the DER devices. A Bayesian deep learning approach is introduced in [4] to enhance the intrusion detection in smart grids consisting of DERs and address the data imbalance and measurement noise challenges in order to improve the cybersecurity levels of the overall system. A new security and resilience framework for smart inverters is analyzed in [5] to address the emerging cyber threats and bridge the gap between the cybersecurity and power-electronics communities. A useful open-source dataset for cybersecurity analysis of Battery Energy Storage Systems (BESS) is provided in [6] to facilitate the risk evaluation and the development of monitoring algorithms for the DER system. A monolithic cybersecurity architecture for power electronic systems is proposed in [7] by integrating the semantic principles into the signal reconstruction in order to enhance the resilience against data attacks and to improve the system performance through a unified, scalable approach validated on real-world and simulated networks. A hybrid multi-model co-simulation infrastructure that integrates software and hardware simulators to effectively test and evaluate DER scenarios is presented in [8] in order to address the challenges related to interoperability, cybersecurity, and data management.

The authors in [9] focus their study on designing a resilient distributed algorithm utilizing homomorphic encryption and an event-triggered mechanism to protect privacy and ensure the convergence of micro-grid energy management systems despite the potential data intrusions and attacks. Focusing on the resilience against cyberattacks, the authors in [10] introduce a distributionally robust recovery resource allocation method using a tri-level defender-attacker-defender model and they ultimately optimize the recovery processes. A comprehensive review of the vulnerabilities, cyberattack defense strategies, and research tools for inverter-based power systems with distributed energy resources is summarized in [11]. An active defense approach that enhances the detection of False Data Injection (FDI) attacks in DER-based microgrids is proposed in [12] by adopting a dynamic system reconfiguration and using distributed energy resources. A thorough review of the current practices, challenges, and future trends in the cyberphysical security of grid-connected battery energy storage systems (BESSs) is provided in [13]. A real-time cybersecurity testbed framework is developed in [14] to evaluate the undetectable false data injection attacks on utility-scale distributed energy resources and state estimators.

A new propulsion energy model for fixed-wing Unmanned Aerial Vehicles (UAVs) is proposed in [15] to jointly optimize the 3D flight trajectories and data collection schedules for secure and energy-efficient data collection under eavesdropping attacks. A non-orthogonal multiple access (NOMA) assisted secure offloading scheme for vehicular edge computing (VEC) networks is designed in [16] by utilizing physical layer security (PLS) and an asynchronous advantage actor-critic (A3C) algorithm to minimize the energy consumption while ensuring offloading security and low computation delay in the presence of malicious eavesdroppers. Also, a deep recurrent reinforcement learning (DRRL)-based energy-efficient cooperative secure transmission scheme for mmWave vehicular networks is presented in [17] aiming at optimizing the beam allocation, cooperative node selection, and transmit power to enhance the secrecy performance while minimizing the energy consumption. The security and functional safety challenges of Artificial Intelligence (AI) in embedded automotive systems are analyzed in [18] and the authors provide recommendations on how machine learning can address these challenges, along with an overview of contemporary engineering practices and the role of AI edge processing. The authors in [19] critically evaluate seven major cybersecurity frameworks and introduce a novel risk management-based evaluation criteria. Also, the authors provide a unified mapping approach to streamline compliance across multiple standards. In [20], the authors compare the NIST Cybersecurity Framework (CSF) v2.0 with a new European Union standard to assess their suitability and identify gaps for achieving a comprehensive cybersecurity coverage in the defense sector, particularly in the Space domain. A comprehensive cyber risk management plan for the ICT unit of the ABC organization is presented in [21] using NIST CSF v1.1, ISO/IEC 27005:2018, and NIST SP 800-53, identifying 105 risks and providing 86 control recommendations.

1.2. Contributions & Outline

This paper provides a comprehensive survey of the cybersecurity certification standards established by the SunSpec Alliance for Distributed Energy Resources (DER) systems. The key contributions of this survey paper are as follows:

- We analyze the SunSpec Cybersecurity Standards, focusing on critical aspects such as secure communication, robust authentication processes, automated software updates, and comprehensive logging protocols to ensure the safety and reliability of DER devices.
- We emphasize the importance of remote and automated software update mechanisms and encrypted communication channels for maintaining the security of DER systems. Our survey highlights the adoption of SAE J3072 in conjunction with the IEEE 2030.5 protocol, and its role in securing communication between electric vehicle supply equipment (EVSE) and plug-in electric vehicles (PEVs), particularly in vehicle-to-grid (V2G) operations.
- We present in detail the SunSpec Modbus standard which aims at enhancing the interoperability between various DER components and supports the compliance with grid integration requirements.
- We evaluate the SunSpec Device Information Models, which offer standardized data structures that facilitate seamless communication across the DER systems. Finally, we provide an in-depth analysis of the SunSpec Alliance's energy storage cybersecurity framework and its proposed blockchain-based security standards.

The remainder of this paper is organized as follows. Section 2 analyzes the SunSpec Cybersecurity Certification requirements and Section 3 discusses the SunSpec Requirements for the test procedure. Section 4 provides a thorough gap analysis and proposes a path to address these gaps. Finally, Section 5 concludes the paper.

2. SunSpec Cybersecurity Certification Requirements

SunSpec Cybersecurity Certification has identified and organized the cybersecurity requirements in the following main categories [22,23]:

1. **Software Updates/Product Support:** The Distributed Energy Resources (DER) devices must (i) support updating mutable security and operational software components, including the operating system, boot loader, applications, libraries, etc.; (ii) provide a mechanism for users to read the current software version.; (iii) support remote updates, communicating with a remote server at least once per day to download and install software updates.; (iv) support automated updates to streamline the update process.; (v) verify the authenticity and integrity of software updates before installing them.; and (vi) meet the same security requirements as remote updates in the case that the DER devices support local updates.
2. **Device Communications:** The DER devices must (i) implement secure communication protocols (TLS 1.2 or higher, IPSec Version 2 or higher, or SSH-2) for all communications accessing the public Internet.; and (ii) reject deprecated security technologies identified by NSA and IETF to prevent vulnerabilities.
3. **Authentication:** Regarding the authentication of the DER devices, the SunSpec Alliance (i) requires each user to have unique security credentials for access levels or accounts; (ii) mandates secure authentication mechanisms for all electronic access, locally or remotely; (iii) requires automatic logout after a period of inactivity; (iv)

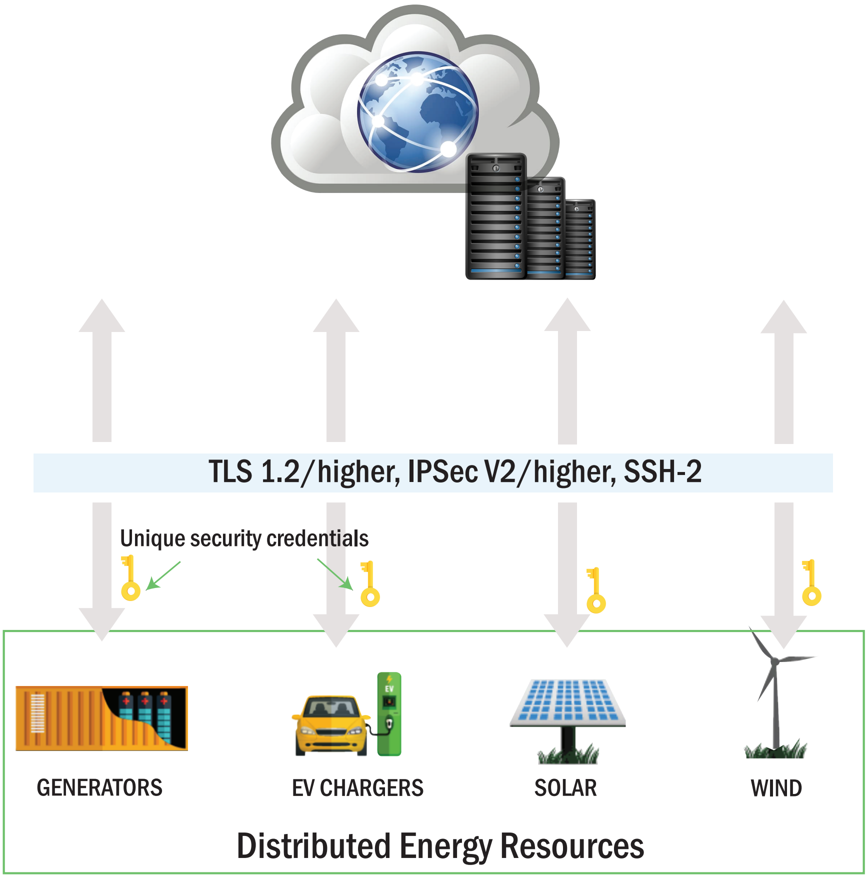

Figure 1. SunSpec Cybersecurity Certification Requirements – An Overview.

allows authorized users to set session timeout periods; (v)) enforces strong password requirements or provides a strength meter; (vi) requires users to create new passwords if defaults are shared or displayed; (vii) implements account lockouts after consecutive failed login attempts; (viii) prevents storage or display of unencrypted passwords; and (ix) supports at least one admin account without brute force prevention.

4. **Device Security:** Regarding the device security, the SunSpec Alliance (i) removes or disables unnecessary interfaces and ports before device transfer; and (ii) supports a "factory reset" option for end-of-life or repurposing.
5. **Logging:** The logging requirements include secure storage, timestamps, resolution, accuracy, configuration, security events, remote logs, incident reporting, power setting logs, power cycle logs, and panel logs.

3. SunSpec Requirements for Test Procedure

The **required equipment and software** to perform tests in accordance with the SunSpec Cybersecurity Certification requirements are [24]: (i) *IUT (Interface Under Test)* (one or two devices, depending on local software update support, running older software images); (ii) *endpoints* (devices to exercise communication capabilities, with documentation for modifying security settings); (iii) *remote log and incident server* (receives and stores log files and incident reports from the DER); (iv) *remote software update server* (sends software updates to the DER); (v) *software images* (current, unauthenticated, modified, and old images provided by the manufacturer); (vi) *documentation* (completed and signed ICS document, product manual, IXIT, and functional specifications); (vii) *network monitoring tools* (traffic monitor, Wi-Fi, Bluetooth, and Ethernet scanners); and (viii) *secrets* (keys, passwords, tokens for authenticating communications).

165 The superset test cases that should be validated, along with their purpose, are listed
166 as follows in Tables 1 and 2.

Test Case	**Purpose**
Software Version	Verify the IUT can read the version of each component
Secure Updates	Ensure the IUT verifies authenticity and integrity before installing updates
Automatic Remote Updates	Verify support for automatic remote updates
Software Downgrade Prevention	Confirm the IUT rejects updates to older software versions
Secure Update Operations	Optional test to ensure manufacturer maintains secure operations for update processes
Support of Secure Communications	Ensure that all communication capabilities accessible by the public are adequately secured
Communication Downgrade Prevention	Ensure prevention of unsecure protocol usage or downgrade
Minimal Interfaces	Confirm absence of unused interfaces or ports
Support of Secure Boot	Ensure implementation of secure boot
Support of Root of Trust Protection	Verify prevention of root of trust data modification
Support for Root of Trust Extension	Ensure secure extension mechanism for root of trust data
Unique Credentials	Confirm requirement of separate credentials for each user account
Authentication	Ensure authentication of all logical connections, including physical panels
Session Timeout	Confirm timeout of authenticated sessions after inactivity

167

Table 1. Superset test cases that should be validated along with their purpose (part 1).

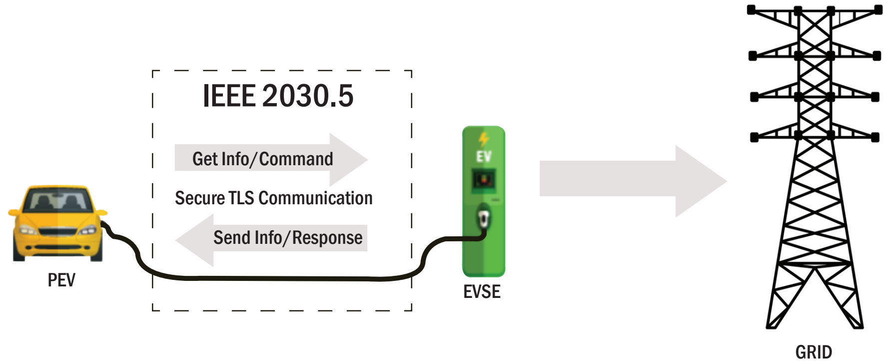

Figure 2. PEV and EVSE Interaction following the IEEE 2030.5 protocol.

Test Case	Purpose
Configurable Timeout	Ensure user-configurable session timeout
Strong Passwords	Aims to ensure that the IUT enforces strong password policies and notifies users when weak passwords are entered
Unique Passwords	Verifies whether the IUT utilizes unique passwords or prompts users to create new passwords upon first login
Brute Force Prevention	Confirms that the IUT effectively prevents brute force password attacks
Admin Login without Brute Force Protection	Ensures that the IUT supports at least one network-accessible admin account that does not utilize brute force prevention
Password Protection	Confirms that the IUT does not reveal passwords at any point, including during login attempts or profile data access
Support for Credential Revocation	Ensures that the IUT rejects authorization credentials that have been revoked or expired
Support of Credential Provenance	Confirms that the IUT's authentication credentials are securely created and protected according to relevant standards

Table 2. Superset test cases that should be validated along with their purpose (part 2).

3.1. SunSpec Requirements SAE J3072 Implementation using the IEEE 2030.5 protocol

This section focuses on the requirements for the implementation of the Society of Automotive Engineers (SAE) J3072 standard using the IEEE 2030.5 protocol. The goal is to support the electric vehicle supply equipment (EVSE) and plug-in electric vehicles (PEVs) manufacturers, and/or operators, and/or system integrators to establish the necessary grid support inverter systems within PEVs connected to electric power systems (EPS) through conductively coupled electric vehicle supply equipment (EVSE). SAE J3072 specifies the necessary technical and performance criteria to ensure safe and effective interaction between the vehicle's inverter system and the power grid in order to enable several functionalities, e.g., vehicle-to-grid (V2G) capabilities, as presented in Fig. 2 [25].

SAE J3072 System Architecture Overview:

- **System Concept:** SAE J3072 defines how the PEVs connect to the EPS via the EVSE using onboard inverter systems. The communication between the PEVs and the EVSEs is managed using the IEEE 2030.5 protocol, which ensures the safe and authorized power discharge from vehicles to the grid.
- **Security Considerations:** The primary security focus is on the communication between PEVs and EVSEs, specifically preventing man-in-the-middle (MITM) attacks. Both the PEV and EVSE must use IEEE 2030.5 compliant certificates and secure HTTPS connections to mitigate these risks. However, due to the point-to-point nature of the physical connection and additional protocols, the likelihood of successful MITM attacks is considered low.
- **Communications Architecture:** The PEV and EVSE communicate over a physical power line communication (PLC) link, utilizing TCP/IP protocols for secure data transfer. Each connection is unique to ensure proper authentication and data integrity.
- **Operations and Compliance:** Upon connection, the PEV identifies and authenticates the EVSE, discovers necessary resources, and exchanges information to receive discharge authorization. This authorization is periodically monitored and managed to ensure the PEV operates within defined limits. If unauthorized activity is detected, the EVSE can revoke discharge permissions and, if necessary, disconnect the PEV.
- **Periodic Operations:** PEVs continuously send operational data to the EVSE, including metrology and status information, ensuring compliance with site-specific limits and discharge authorizations. The communication frequency and data requirements are dynamically managed by the EVSE.
- **Exception Handling:** PEVs operate in a default mode unless explicitly authorized to discharge by the EVSE. Authorization can be withdrawn due to communication failures or other exceptions, prompting the PEV to cease discharging within a specified timeframe. Both PEVs and EVSEs must be capable of handling such scenarios to maintain system integrity.

The main security protocols identified by the SunSpec Alliance in order to implement the SAE J3072 using the IEEE 2030.5 protocol are summarize as follows.

1. **TLS Encryption:** Mutual TLS encryption is mandatory during initial communications to establish a secure connection. Both devices exchange IEEE 2030.5-compliant certificates to authenticate each other.
2. **Device Certificates:** PEV certificates must encode make and model details using Object IDs (OIDs). This information enables the verification of the PEV's authenticity and suitability for connection.
3. **IPv6 Usage:** All communications utilize IPv6, with specific address blocks and stateless address autoconfiguration for secure and unique identification of devices on the network.
4. **Restricted Bridging/Routing:** Initially, the EVSE restricts any bridging or routing of PEV communications to prevent unauthorized network access. Bridging may only be enabled after the successful PEV authorization.
5. **Service Discovery:** Multicast DNS (mDNS) is employed for discovering services on the network, ensuring that devices can locate necessary resources securely without reliance on external DNS servers.

These requirements ensure the secure and authenticated interactions between the EVSE and the PEVs, aiming at securing the data exchange and operational integrity of the electric

vehicle charging systems. It is noted that if communication is lost between the PEV and the EVSE, the PEV sends a heartbeat message every second, and the EVSE monitors for these signals. A failure to receive ten consecutive heartbeats prompts the EVSE to stop the PEV from discharging. Therefore, the reception of three consecutive heartbeats restores the connection. Additionally, the EVSE has a gatekeeper function to cut off power if unauthorized or out-of-limit discharging occurs, and can revoke discharge authorization, which the PEV must comply with within three seconds. The SAE J3072 standard also covers coordinated charging/discharging and sleep/wake functions to ensure secure and efficient operations.
The IEEE 2030.5 messages: (i) facilitate the communication between the PEVs and the EVSE, and (ii) ensure secure interactions, i.e., service discovery and resource retrieval. The following cybersecurity requirements need to be considered throughout the communication between the PEVs and the EVSE:

1. **Service Discovery:** The PEVs and EVSEs use mDNS and DNS-SD for the service discovery, and also they establish a secure TLS connection before retrieving the DeviceCapability resources.
2. **Resource Discovery:** The PEVs have access to a wide range of resources, e.g., DeviceCapability, Time, EndDeviceList, and DERList, in order to ensure the secure data exchange.
3. **PEV Gets Site Limits:** The PEVs retrieve site limits from the EVSEs in order to guarantee their compatibility and secure communication.
4. **PEV Sends Info to EVSE:** The PEVs send information, e.g., Device Information, Power Status, DER Capability, and DER Settings, to the EVSEs in order to guarantee the secure data transmission.
5. **PEV Gets Management Information:** The PEVs retrieve information, e.g., Function Set Assignments, Time, DER Program List, Default DER Control, and DER Control List, in order to guarantee the secure management and operation.
6. **DERControl Responses:** The EVs send responses to the DERControl commands, in order to indicate the status of the control action. These responses are immediately sent upon receiving the control command.
7. **Mirror Usage Point Setup:** The EVs post mirror usage point data, including meter readings such as active power, reactive power, voltage, and frequency. These readings are posted periodically and their update rate is determined by the meter usage point configuration.
8. **Subscriptions and Notifications:** The EVs subscribe to receive notifications about changes in control commands or system configurations. The charging infrastructure sends notifications to EVs when such changes occur.
9. **Periodic Gets of Information:** The EVs periodically query the charging infrastructure for updates on control commands, meter readings, and system configurations. This allows the EVs to stay synchronized with the charging infrastructure and respond to the changes in a timely and synchronized manner.
10. **Sends Periodic Information:** The periodic information sent by the PEVs includes updates on the DERStatus, PowerStatus, DERAvailability, Meter Readings (i.e., Active Power, Reactive Power, Voltage, and Frequency), which serve as the heartbeat messages for the detection of the loss of communication. Additionally, the PEVs interact with the new DERControl, and they adjust the Active Power limits for the site, and also, coordinate the charging and discharging processes through the DERControl responses.

3.2. SunSpec Modbus

The SunSpec Modbus is an open communication standard specifically designed to facilitate interoperability among DER system components. Developed by the SunSpec Alliance, this protocol leverages the widely adopted Modbus framework, which has been a cornerstone in industrial electronic communications since the 1980s. SunSpec Modbus defines standardized parameters and settings for the monitoring and control of DER systems, such as solar inverters, PV modules, meters, and energy storage devices. By providing a common language for these components, SunSpec Modbus ensures seamless integration, reduces implementation costs, and supports compliance with updated grid interconnection standards, such as the IEEE 1547-2018 [26].

IEEE 1547-2018 Standard

- **Revision:** April 2018 by IEEE.
- **Requirement:** Communication interface for DER systems.
- **Interfaces:** SunSpec Modbus or other standard interfaces.
- **Adoption:** Mandatory for all DERs in state and local jurisdictions once adopted.

SunSpec Modbus Interface

◇ Purpose:
  - Defines parameters and settings for DER monitoring and control.
  - Enhances interoperability.
  - Facilitates voltage regulation, power factor setting, and power export limiting.

◇ Development:
  - Based on Modbus protocol (1980s).
  - Created by SunSpec Alliance (2009).
  - Extended to cover solar inverters and other DERs.

◇ Adoption:
  - Integrated into ∽ 80% of DER devices.
  - Simple to add SunSpec Modbus support for IEEE 1547 compliance.

Table 3 summarizes the benefits of the SunSpec Modbus interface.

Benefit	Description
Simple Integration	Short step for manufacturers familiar with Modbus to comply with IEEE 1547-2018
Cost Effective	Low cost due to existing network interfaces in most DER devices
Easy Compliance	Provides royalty-free specs, reference software, and development tools

Table 3. Benefits and Descriptions of Integration

SunSpec Modbus and DER Systems

The main applications of the SunSpec Modbus in DER systems are focused on monitoring, control, operations, maintenance, and custom applications. The main components that are utilized along with their interface are summarized in Table 4 [27].

Component	Interface
Inverter	SunSpec Modbus
PV Module	SunSpec Modbus
Meter	SunSpec Modbus
Tracker	SunSpec Modbus
Storage	SunSpec Modbus
Gateway	SunSpec Modbus

Table 4. Components and their SunSpec Modbus Interfaces

The IEEE 1547-2018 standard mandates DER systems to have a standard communication interface, such as SunSpec Modbus, to ensure interoperability, ease of integration, and cost-effective compliance.

◇ Communication and Interoperability:

- Protocol: Leverages Modbus protocol for DER devices.
- Communication: Between loggers, servers, and DER devices.
- Information Model: Defines data points and functionality.

Table 5 lists standards related to communication and interoperability for DER systems and identifies specific standards and their corresponding interfaces.

Standard	Interface
IEEE 1547-2018	Establishes the communication requirements for DER systems.
IEEE 2030.5	Specifies internet communication protocols used in DER systems.
IEEE 1815	Defines protocols for utility network communication.

Table 5. Communication and Interoperability Standards

◇ SunSpec Information Models

- Device Information Models: Define data points and functionality.
- Encoding: Uses JSON and CSV formats.

Table 6 summarizes the types of SunSpec information models and their purposes.

Model	Description
Common Model	Provides basic identification details about the physical device, such as manufacturer, model, and serial number. This model is always included in a SunSpec-compliant device.
Standard Models	Specify common data points implemented by devices within a given category. These models ensure that devices within the same category share a common set of data points for interoperability.
Vendor Models	Defined by individual device vendors, these models include data points unique to the vendor's specific implementation. Although they must adhere to certain rules, they do not follow the SunSpec Standard Model review process. Each Vendor Model requires an identifier assigned by SunSpec.

Table 6. SunSpec Information Models

Key Aspects of SunSpec Device Information Models	**Description**
Standardization	The models ensure a consistent method for defining and using device data.
Communication Interfaces	They support data exchange via Modbus and JSON, making them versatile for different applications.
Model Structure	The models consist of various elements such as models, points, point groups, symbols, and comments to represent device data comprehensively.

Table 7. Key aspects and descriptions of SunSpec device information models.

◇ Certification and Conformance

Element	Description
Model	Logical grouping of data points with a unique model ID.
Point	Defines a device data point with a value.
Point Group	Groups multiple points or other point groups.
Symbol	Name-value pair representing constant values for points.
Comment	Annotations for documenting elements.

Table 8. Key elements and their descriptions in SunSpec device information models.

Attribute	Description	Model	Point Group	Point	Symbol
ID	Element name, unique within the group	R	R	R	R
Points	Array of point definitions		R		
Groups	Array of point group definitions		O		
Value	Constant value associated with the element				R
Type	Element type		R	R	
Count	Occurrence count of the element		O	O	
Size	Element size, mandatory for strings			O	
Scale Factor	Scale factor point for the element			O	
Units	Units associated with the element			O	
Access	Read or read/write access			O	
Mandatory	Indicates if element is mandatory			O	
Label	Short label for the element	R	R	O	O
Description	Element description	O	O	O	O
Symbols	Name-value pair for enumerated values		O	O	O

Table 9. Description of attributes in the model hierarchy. R, O indicate required and optional attributes, respectively.

  - Process: Vendors declare implementations in a Protocol Implementation Conformance Statement (PICS).
  - Conformance: Verified against SunSpec standards.

3.3. SunSpec Device Information Models to Standardize Device Data Exchange

SunSpec Device Information Models provide a standardized approach for specifying and structuring device data for exchange across communications interfaces. These models facilitate the standardization of device data sets, which can be represented using the Modbus or the JSON encoded messages. The key aspects of the SunSpec Device Information Models are summarized in Table 7 as follows [28].
Toward defining the SunSpec device information models the following elements are adopted (Table 8).
The Device Information Model definitions represent collections of device data points, which can be standardized for interface usage. These models use definition elements to structure and describe device data, as summarized in Table 8. The attributes associated with each

Numeric Types	Floating Point Types	Other Types
int16, int32, int64: Signed integers of 16, 32, and 64 bits respectively.	float32: 32-bit floating-point number.	string: UTF-8 encoded string.
uint16, uint32, uint64: Unsigned integers of 16, 32, and 64 bits respectively.	float64: 64-bit floating-point number.	sunssf: Scale factor for applying multipliers or dividers.
raw16: 16-bit raw value.		pad: 16-bit pad used for alignment.
acc16, acc32, acc64: Unsigned accumulators of 16, 32, and 64 bits respectively.		ipaddr: Unsigned 32-bit IPv4 address.
bitfield16, bitfield32, bitfield64: Bitfields of 16, 32, and 64 bits respectively.		ipv6addr: 16-byte IPv6 address.
enum16, enum32: Enumerations of 16 and 32 bits respectively.		eui48: 48-bit MAC address.

Table 10. Description of various data types

Model Name	Description
DER AC Measurement	Measurement data, status, and alarm information.
DER Capacity	Capacity-related information.
DER Enter Service	Enter service related data.
DER AC Controls	AC control settings and parameters.
DER Volt-Var	Voltage-var control settings and parameters.
DER Volt-Watt	Voltage-watt control settings and parameters.
DER Trip LV	Low voltage trip settings and parameters.
DER Trip HV	High voltage trip settings and parameters.
DER Trip LF	Low frequency trip settings and parameters.
DER Trip HF	High frequency trip settings and parameters.
DER Frequency Droop	Frequency droop settings and parameters.
DER Watt-Var	Watt-var control settings and parameters.
DER Storage Capacity	Storage capacity related information.
DER DC Measurement	DC measurement data and parameters.

Table 11. Description of Model Names

element type are summarized in Table 9. Device Information Models standardize data points for device communication interfaces. Models can be encoded in JSON or CSV for ease of use and implementation. Models can be mapped into a Modbus address space, creating a Modbus map that corresponds to the device's supported data points (i.e., Modbus usage). Models can be represented as JSON objects, facilitating data exchange via RESTful web services or other JSON-based interfaces (i.e., JSON usage). By using standardized Device Information Models, the devices can efficiently exchange data in a consistent and interoperable manner across different communication protocols.

Furthermore, the SunSpec Device Information Model Specification defines a structured approach for modeling and encoding device information, primarily aimed at energy-related devices. The specification defines various types of data representation within the model, ranging from numeric to floating point to other types of data representation, as summarized in Table 10, each with specific attributes that govern their behavior and encoding.

Each element in the model can have several attributes that define its characteristics: (i) Count: Specifies the number of occurrences of the element.; (ii) Size: Maximum length of the element in 16-bit words.; (iii) Scale Factor (sf): Applies a signed scale factor to numeric values.; (iv) Units: Specifies the units associated with the element.; (v) Access: Specifies if the element is read-only, i.e., R, or read/write, i.e, RW.; (vi) Mandatory: Specifies whether the element is mandatory, i.e., M, or optional, i.e., O.; (vii) Label: Short label associated with the element.; and (viii) Description: Provides a brief description of the

Symbol	Description	Access
Ena	Enables or disables the function.	Read/Write
AdptCrvReq	Selects a new curve setting.	Read/Write
AdptCrvRslt	Result of the AdptCrvReq operation.	Read-Only
NPt	Number of possible curve points.	Read-Only
NCrv	Number of curve instances.	Read-Only
ActPt	Number of active points in the curve.	Read/Write

Table 12. Curve Management Points

Region	DER Behavior	Precedence Hierarchy
Trip	DER trips when region is entered.	1 (highest)
May Trip	DER may continue operating or trip.	3
Momentary Cessation	DER ceases energizing but does not trip.	2

Table 13. Voltage Trip/Momentary Cessation Points

element. The primary encoding format for defining SunSpec Device Information Models is JSON, providing a structured and human-readable representation. CSV encoding is also supported for convenience, allowing models to be created and inspected using spreadsheet applications. Finally, for integration with the Modbus, SunSpec models are mapped into Modbus registers, specifying address locations, supported function codes (Read Holding Registers, Write Multiple Registers), and error handling procedures.

3.4. SunSpec DER Information Model Specification

The SunSpec DER Information Model Specification outlines a detailed and thorough framework for defining data exchange standards between DERs and different interfacing systems. The specification defines standard SunSpec Device Information Models for DERs, enabling reliable information exchange between DERs and control systems. It supports various DER management functions through specific models like DER AC Measurement, Capacity, Frequency Droop, and more. The DER information models as introduced by SunSpec are summarized in Table 11 [29].
Several important management points related to curves within the SunSpec DER Information Model Specification have been identified for managing and adjusting curve settings in DERs, as summarized in Table 12.
SunSpec has also defined the behavior of DERs related to voltage trip and momentary cessation within specified regions. Three main types of voltage trip have been identified: immediate trip, i.e., where the DER must trip immediately upon entering the region, momentary cessation, i.e., where the DER ceases energizing but does not trip, and conditional behavior, i.e., where the DER may or may not trip based on specific conditions. This hierarchical structure and categorization (Table 13) help to clarify which behavior takes precedence when multiple conditions are active at the same time, ensuring consistent and reliable DER operation in varying grid conditions.

Moreover, focusing on the *DER Capacity information model*, this model provides a structured approach to manage ratings and settings for DERs and includes read-only ratings and configurable settings that override default values for operational parameters. Based on the DER Capacity information model, different DER capacity points are characterized by RW access, i.e., indicating whether the point is Read-Write (RW), Read-Only (-), or Write-Only (-), they can be mandatory for the model (M) or optional (-), and static (S) or dynamic (-) in

Group/Point Name	Label	Data Type	RW Access	Mandatory (M)	Static (S)
DERCapacity	DER Capacity group ID	uint16	-	M	S
L	DER Capacity Model Length	uint16	-	M	S
WMaxRtg	Active Power Max Rating	uint16	-	-	S
WOvrExtRtg	Active Power (Over-Excited) Rating	uint16	-	-	S
WUndExtRtg	Active Power (Under-Excited) Rating	uint16	-	-	S
VAMaxRtg	Apparent Power Max Rating	uint16	-	-	S
VarMaxInjRtg	Reactive Power Injected Rating	uint16	-	-	S
WChaRteMaxR	Charge Rate Max Rating	uint16	-	-	S
VNomRtg	AC Voltage Nominal Rating	uint16	-	-	S
AMaxRtg	AC Current Max Rating	uint16	-	-	S

Table 14. DER Capacity Points

nature, as summarized in Table 14. A similar approach is followed for the DER capacity settings, as presented in Table 15.[1]

3.5. *SunSpec Energy Storage Cybersecurity Specifications*

The SunSpec Alliance Interoperability Specification outlines detailed data models (please also refer to the previous section) and MODBUS register mappings tailored for standalone Energy Storage Systems (ESS). Initially focused on lithium-ion and redox flow batteries, SunSpec accommodates diverse storage technologies, such as advanced lead-acid and vanadium redox flow batteries. The SunSpec ESS Models specification aligns closely with cybersecurity standards and protocols to ensure robust communication interfaces across devices. The models are designed to integrate seamlessly with IEC 61850-7-420, maintaining consistency in naming conventions, units, and behaviors, while some concepts in this specification currently lack direct equivalents in IEC 61850-7-420. An overview of the SunSpec ESS Models is provided in Table 16 [30].
SunSpec ESS Models specification introduces support for flow batteries, addresses feedback from industry stakeholders, and enhances the robustness and comprehensiveness of the models, making them suitable for deployment in production systems. In commercial and industrial setups, Lithium-ion Battery Strings are used to provide backup power and peak power limiting capabilities. These are structured into strings composed of modules, each monitored through specific models. Manufacturers must manage the Modbus register limits (i.e., avoid exceeding the 65,535 register limit) when implementing multiple models. Flow batteries, unlike Lithium-ion, typically operate as a single string and provide significant energy capacity. The Battery Base Model and Flow Battery String Model are core components for communication. The foundational model providing essential information like nameplate values, state of charge management, depth of discharge, and health metrics applicable across different battery technologies.

Focusing on the battery type and alarm information, the SunSpec ESS models outline the following descriptive standards regarding each aspect of the ESS (either hardware or

[1] Please note that the most representative and important DER capacity points and capacity settings are summarized in Table 14 and Table 15, respectively.

Group/Point Name	Label	Data Type	RW Access	Mandatory (M)	Static (S)
WMax	Active Power Max Setting	uint16	RW	-	-
WOvrExtPF	Specified Over-Excited PF	uint16	RW	-	-
WMaxUndExt	Active Power (Under-Excited) Setting	uint16	RW	-	-
VAMax	Apparent Power Max Setting	uint16	RW	-	-
VarMaxInj	Reactive Power Injected Setting	uint16	RW	-	-
VNom	Nominal AC Voltage Setting	uint16	RW	-	-
AMax	AC Current Max Setting	uint16	RW	-	-

Table 15. DER Capacity Settings

software or operation-oriented aspect) for communicating with and managing the battery systems.

3.6. SunSpec Blockchain Cybersecurity Requirements

The SunSpec Blockchain Work Group proposes a blockchain-based key registry for DER devices to enhance cybersecurity by providing accessible and integrity-protected information about cryptographic keys. This set of cybersecurity standards addresses the current shortcomings in security practices for DERs and ensures their robust protection against cyber threats [31].
A permissioned blockchain architecture is proposed using Byzantine Fault Tolerant (BFT) consensus, with governance structures designed to mitigate security risks, including nation-state threats and coercion. The main components of this architecture include a high-level data model and an API for managing and querying key security information. The main actors involved in the DER service security based on this standard are summarized in Table 18, while different use case scenarios where this standard can find applications are presented in Table 19.
The proposed standard organizes and secures the key management practices across the energy grid. The primary use case involves the secure management of private/public key pairs for Distributed Energy Resources (DER) devices, facilitated by blockchain technology. The main interactions that take place, include:

- **Authorized Assessor Audit:**
  - An authorized assessor conducts security audits on key generation, key storage within DER Clients, and key exposure in the manufacturing supply chain.
  - Audit results are stored on the blockchain for transparency and integrity.
- **Key Generation and Provisioning:**
  - The Key Generator creates and provisions private/public key pairs into DER Clients, ensuring adherence to audited processes.

Model #	Name	Summary	Availability
802	Battery Base Model	Key monitoring and control points for all batteries	TEST
803	Lithium-ion Battery Bank	Monitoring and control for lithium-ion battery banks	TEST
804	Lithium-ion Battery String	Monitoring and control for lithium-ion battery strings	TEST
805	Lithium-ion Battery Module	Monitoring and control for lithium-ion battery modules	TEST
806	Flow Battery Bank	Monitoring and control for flow battery banks	N/A
807	Flow Battery String	Monitoring and control for flow battery strings	TEST
808	Flow Battery Module	Monitoring and control for flow battery modules	N/A
809	Flow Battery Stack	Monitoring and control for flow battery stacks	N/A

Table 16. Overview of SunSpec Energy Storage Systems Models

  - Keys can be provisioned during manufacturing or installation, with mechanisms to securely store and control access to the private key.
- **Manufacturer Responsibilities:**
  - Manufacturers produce DER Clients, ensuring compliance with audited processes for key handling and provisioning.
  - Manufacturers register each device's key on the blockchain, linking it to audited processes and device information.
- **Certificate Authority (CA) Issuance:**
  - CAs issue certificates based on blockchain-verified information, ensuring secure mapping between public keys and device attributes.
  - Certificates are essential for secure TLS sessions between DER Clients and DER Servers, facilitating mutual authentication.
- **DER Server Validation:**
  - DER Servers validate DER Client certificates during TLS handshakes using blockchain data, ensuring the trustworthiness of private key management meets minimum security requirements.

The proposed cybersecurity standard also integrates traditional certificate authority (CA) mechanisms with Blockchain for enhanced security and lifecycle management of DER Clients. To realize the latter, the following main points need to be ensured:
Certificate Creation and Validation:

- A CA issues X.509 certificates containing DER Client public keys and policy parameters.
- Certificates are used for authentication during communication with DER Servers.

Table 17. Battery Aspects

Aspect	Description
Battery Type Enumeration (Typ)	Enumerates the type of battery connected, aiding Modbus masters in identification.
Battery Alarms and Warnings (Evt1)	Bitfield for managing alarms and warnings; includes standard and custom alarm capabilities.
Alarm Reset (AlmRst)	Resets latched alarms upon receiving a value of 1; updates Evt1 to reflect alarm reset status.
External Battery Measurements	Registers: V (External Battery Voltage), A (Total DC Current), W (Total Power)
Max/Min Cell Voltage (CellVMax/CellVMin)	Provides maximum and minimum voltages across all cells; essential for monitoring cell performance.
Optional Location Data	Registers: CellVMaxStr, CellVMaxMod, CellVMinStr, CellVMinMod; specify location of extreme voltages.
Dynamic Limits	Registers: AChaMax (Max Charge Current), ADisChaMax (Max Discharge Current), VMax (Max Voltage), VMin (Min Voltage)
Operational Boundaries	Communicates maximum and minimum operational limits for current and voltage; ensures safe operations.
Battery States (State)	Enumerates operational states (Disconnected, Initializing, Connected, Fault)
State Transitions	Managed via SetOp commands; reflect state changes such as connect/disconnect operations.
Inverter State (SetInvState)	Indicates current state of connected inverter to coordinate battery operations.
Temperature Monitoring	Registers: ModTmpMax (Max Module Temperature), ModTmpMin (Min Module Temperature)
Location-Specific Data	Registers: ModTmpMaxStr, ModTmpMaxMod, ModTmpMinStr, ModTmpMinMod; provide temperature location.
String-Level Metrics	Registers: StrVMax, StrVMin (Voltage); StrAMax, StrAMin (Current); StrSoC, StrSoH (State/Health)
Operational Details	String state (StrSt), fault reasons (StrDisRsn), and health metrics at string level.

Blockchain Integration:

- DER Servers query the Blockchain using extracted key identifiers from certificates.
- Blockchain provides additional cybersecurity information beyond traditional mechanisms like OCSP and CRL.

Key Lifecycle Tracking:

- Lifecycle stages include manufacturing, distribution, installation, and decommissioning.
- Blockchain records ownership transfers, end-of-life events, and key revocations.

Supply Chain Security:

- Involves multiple actors (manufacturers, distributors, installers) ensuring secure key provisioning and ownership transfer.
- Different scenarios (component integration, service provision) affect Blockchain recording requirements.

Actor	Description
Manufacturer	Responsible for device manufacturing and key registration on the blockchain.
Authorized Assessor	Independent evaluator of key creation and provisioning processes, auditing device security.
Key Generator	Entity creating and provisioning cryptographic keys into DER devices.
Certificate Authority	Issues digital certificates based on blockchain information to validate DER device identities.
Governing Body	Oversees the blockchain governance, establishing rules and security protocols.
DER Client	Equipment in the DER space using registered keys for secure communications.
DER Server	Web server endpoint managing communications with DER Clients based on key security levels.

Table 18. Main Actors Involved in DER Device Security with Different Colors.

Use Case Description	Key Features
Manufacturer registers private/public key pairs on blockchain for DER devices.	Secure key creation and provisioning processes.
Authorized Assessor audits and stores evaluation reports on blockchain.	Independent verification of device security measures.
Certificate Authority validates device identities using blockchain information for TLS sessions.	Issuance of digital certificates based on verified device keys.
DER Server makes trust decisions based on blockchain data regarding device security properties.	Secure communication with DER Clients based on certified key security levels.

Table 19. Main Use Case Scenarios.

4. Gap Analysis on SunSpec Alliance Standards

In this section, based on the detailed survey performed on the SunSpec Alliance Standards, a thorough gap analysis is performed following the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The NIST CSF was initiated by the Department of Energy (DOE) in the United States of America and the Electric Power Research Institute (EPRI) to improve organizational cybersecurity risk management strategies. In our gap analysis, we adopted the version 2.0 of the NIST CSF [32] to analyze the gaps in the SunSpec Cybersecurity standards, given that it provides a structured approach for businesses, government agencies, and other entities to address cybersecurity risks. The version of the NIST CSF offers a broad framework of key cybersecurity goals that organizations of any size, sector, or level of maturity can use to assess, prioritize, and enhance their cybersecurity strategies.

The NIST CSF's core gap analysis is organized into three main components, i.e., Functions, Categories, and Subcategories, with each Category representing a subset of the overarching Functions, and the Subcategories being a breakdown of the Categories. The NIST CSF's core structure is presented in Fig. 3. The detailed gap analysis is presented in Appendix A. The summary of the gap analysis is provided below.

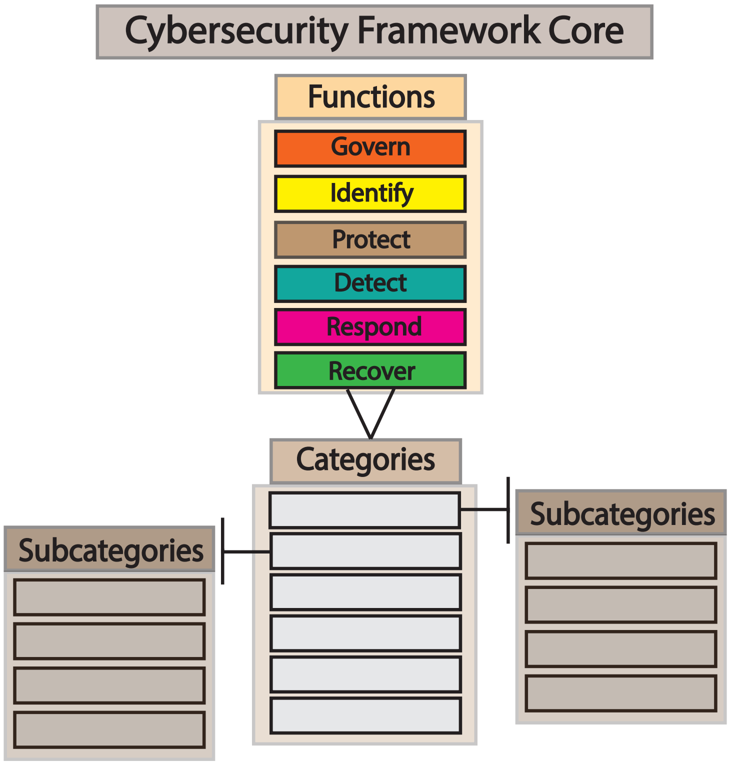

Figure 3. National Institute of Standards and Technology Cybersecurity Framework: Core Structure.

4.1. Gap Analysis

The **SunSpec Cybersecurity Certification** program mainly covers the secure communication among the different DER devices, authentication, software updates, and continuous monitoring of the DER devices. Specifically, SunSpec requires the use of protocols like TLS and IPSec in order to protect the data in transit and it mandates secure methods in order to manage the authentication credentials and ensure that only authorized access is possible. Moreover, SunSpec address the need for regular software updates and provides guidelines in order to prevent the unauthorized software installations. Additionally, SunSpec includes aspects of continuous monitoring and secure communication among the DER devices. On the other hand, topics related to organizational relevant cyber security requirements are not covered by SunSpec. Specifically, SunSpec does not cover organizational security measures, cybersecurity training of personnel, data security specifically in terms of data-in-transit and data-in-use, platform security and infrastructure, and the incident management. Specifically, SunSpec does not cover identity management and access control policies beyond the ones described at the DERs device level as well as broader organizational security practices. SunSpec does not provide requirements for training programs for personnel and for data backup for recovery from data loss or corruption. Additionally, SunSpec does not discuss configuration management practices, technology infrastructure resilience, hardware maintenance and life cycle management of the hardware. The device level cyber security standards provided by SunSpec cover all the critical aspects related to the communication, authentication, autorization, software updates, and monitoring of the devices which is one of the main goals of this project. Organizational related cyber security standards can be addressed, if needed, by other standards listed in this survey analysis. Thus, from the performed analysis it is concluded that SunSpec covers all the most critical aspects of the device-level security which becomes critical for securing the electric vehicles' infrastructure both of the front-end and at the back-end. Table 20 summarizes the main findings of the gap analysis based on the NIST CSF for the SunSpec cybersecurity standards.

	SunSpec
Organizational Context (GV.OC)	Insufficiently Addressed: The SunSpec documentation provides an overview of interoperability processes and standards for Distributed Energy Resource (DER) systems, including the SunSpec Alliance's specification process, information models, and conformance and certification requirements. However, it falls short in addressing critical aspects such as the organizational mission, stakeholder expectations, and legal, regulatory, and contractual requirements related to cybersecurity risk management decisions. Additionally, the documentation lacks identification of specific internal or external stakeholders and does not adequately cover the cybersecurity-related expectations of DERs beyond what is discussed in the specifications. It also fails to address the communication of organizational objectives and services, as the focus remains primarily on the technical cybersecurity requirements for the devices.
Risk Management Strategy (GV.RM)	Insufficiently Addressed: The SunSpec framework insufficiently addresses organizational-level risk management strategies, priorities, constraints, risk tolerance, and objectives. Its focus is primarily on technical specifications and requirements for device cybersecurity, such as software updates, secure communications, and authentication mechanisms. Overall, it lacks comprehensive organizational recommendations or a broader perspective on risk management strategies.
Roles, Responsibilities, and Authorities (GV.RR)	Insufficiently Addressed: The coverage of accountability and responsibility in the SunSpec framework is insufficiently addressed in several key areas. SunSpec emphasizes the device-level certification and specifies the manufacturer requirements to ensure device security and integrity, however, it only indirectly fosters organizational accountability. The framework partially outlines the responsibilities regarding the software updates, communication security, and authentication but lacks a comprehensive discussion on cybersecurity roles beyond these device-specific mandates. Additionally, SunSpec addresses the resource allocation for compliance with cybersecurity standards, however, it does not consider the broader implications of resource management for the overall cybersecurity efforts. Furthermore, there is no mention of human resources practices.
Policy (GV.PO)	Addressed
Oversight (GV.OV)	Insufficiently Addressed: SunSpec does not address organizational-level risk management strategy review and adjustment. It primarily focuses on the technical requirements for device cybersecurity.
Cybersecurity Supply Chain Risk Management (GV.SC)	Not Addressed: SunSpec does not explicitly address roles and responsibilities beyond the device manufacturer and certifying bodies. It focuses solely on the device-level cybersecurity requirements.
Asset Management (ID.AM)	Insufficiently Addressed: The SunSpec certification focuses on individual device type testing rather than comprehensive organizational hardware inventories. It ensures devices are certified individually but doesn't mandate comprehensive organizational inventory management.

	SunSpec
Risk Assessment (ID.RA)	Not Addressed: SunSpec focuses on type testing for individual devices, not organizational vulnerabilities.
Improvement (ID.IM)	Insufficiently Addressed: The SunSpec certification focuses primarily on device-specific cybersecurity requirements and type testing. Evaluations for organizational improvements, such as cybersecurity risk assessments across all functions, are not within the scope.
Identity Management, Authentication, and Access Control (PR.AA)	Insufficiently Addressed: SunSpec specifies requirements for managing authentication credentials securely (e.g., DER/AUTH/REQ-01, DER/AUTH/REQ-06). However, it focuses more on device-specific credentials rather than organizational management of identities across all authorized entities.
Awareness and Training (PR.AT)	Not Addressed: The SunSpec Cybersecurity Certification document primarily focuses on device-level cybersecurity requirements for DER devices. It does not address organizational training and awareness programs for personnel, which are outside the scope of device certification.
Data Security (PR.DS)	Insufficiently Addressed:SunSpec does not explicitly specify requirements for protecting data-at-rest explicitly. It primarily focuses on device-level security and software updates.
Platform Security (PR.PS)	Insufficiently Addressed: SunSpec does not explicitly discuss configuration management practices.
Technology Infrastructure Resilience (PR.IR)	Insufficiently Addressed: The SunSpec documentation does not address protection from environmental threats such as physical damage, natural disasters, or other non-cyber-related environmental risks. The scope is limited to cybersecurity requirements for devices.
Continuous Monitoring (DE.CM)	Insufficiently Addressed: SunSpec focuses on device type testing rather than network monitoring. It ensures that devices communicate securely but does not specify continuous monitoring of networks themselves.
Adverse Event Analysis (DE.AE)	Not Addressed
Incident Management (RS.MA)	Not Addressed
Incident Analysis (RS.AN)	Insufficiently Addressed: The SunSpec documentation primarily focuses on device-level cybersecurity requirements, such as secure software updates, secure communications, and authentication mechanisms. SunSpec emphasizes the importance of security measures and incident prevention (like software update integrity and secure communications), it does not explicitly detail procedures for incident analysis and root cause determination.
Incident Response Reporting and Communication (RS.CO)	Not Addressed
Incident Mitigation (RS.MI)	Not Addressed
Incident Recovery Plan Execution (RC.RP)	Not Addressed
Incident Recovery Communication (RC.CO)	Not Addressed

Table 20. Gap Analysis Summary for SunSpec Cybersecurity Standards

4.2. Addressing Gaps in SunSpec Standards

Based on the performed analysis of the existing SunSpec cybersecurity standards and the discussion regarding the identified gaps, we conclude to the outcome that it is important to extend the focus of the cybersecurity standards beyond the device level security and incorporate organizational levels cybersecurity measures, as identified by the NIST CSF. Based on the above discussion, it is evident that the SunSpec cybersecurity standards mainly emphasize on securing the communication among the distributed energy resource devices, the authentication processes, and the software updates. However, we identified that the SunSpec cybersecurity standards lack coverage in areas such as organizational security policies, personnel training, and incident management protocols. One solution to address this gap is to introduce an additional framework that supplements the SunSpec cybersecurity standards by establishing clear guidelines for organizational practices and include policies for cybersecurity awareness training, data management, and recovery procedures in order to ensure that the organizations not only secure the DER devices but also they buils a robust security culture across all personnel and systems. Another way to address the organizational policies is the extension of the SunSpec cybersecurity standards in order to include broader security management practices, for example identity and access control management at an organizational level.

Based on the performed gap analysis, we concluded that the SunSpec cybersecurity standards cover authentication between the devices, however, the standards do not specify how the organizations should manage the overall lifecycle of their identities, for example the employee credentials and the multifactor authentication. One solution to address this gap is the extension of the SunSpec cybersecurity standards or complementing them with existing or new standards in order for the organizations to implement a centralized identity management system which will ensure the secure access across all the devices and personnel regardless of their role. This solution will mitigate the risks that are associated with the unauthorized access, as well as the insider threats and the danger of identity misuse.

Based on the performed gap analysis, we also concluded that the SunSpec cybersecurity standards do not include the concept of platform security especially when this is related to the data-in-use or the data-in-transit. Therefore, a way to strengthen the data security is to integrate additional protocols into the existing SunSpec cybersecurity standards and provide explicit guidance in terms of how the data will be secured at all the stages of their life cycle. This solution can include data segmentation techniques that minimize the exposure of sensitive information complementary to existing encryption methods. Also, another solution could be the adoption of standards that cover incident management and data backup procedures to complement the SunSpec cybersecurity standards in order to ensure that the organizations can swiftly respond to data breaches or system failures and ultimately minimize their downtime but also prevent data corruption or loss. Towards addressing the hardware life cycle management which is absent in the SunSpec cybersecurity standards, a solution could be the periodic hardware audits and the establishment of maintenance protocols. Specifically, the organizations can adopt a continuous monitoring approach for the hardware and document specific procedures in order to manage the replacement, upgrade, or the commissioning of the devices. By incorporating such an approach within the existing SunSpec cybersecurity standards, the hardware vulnerabilities can quickly be identified and resolved, thus the risk of exploitation due to outdated or compromised equipment will be reduced. Additionally, by adopting the lifecycle management protocols, the resilience of the overall system will be improved in addition to securing the DER devices.

Concluding this analysis, the goal of this survey is to guide the application of the corresponding techniques to highlight the relationship between the identified gaps in the SunSpec Alliance Standards and the relevant frameworks for addressing these gaps. The gap analysis that is performed above, has identified the critical areas where the SunSpec standards fall short, particularly in organizational cybersecurity measures, such as training protocols, incident management, and comprehensive identity and access management.

By utilizing the NIST Cybersecurity Framework (CSF), the organizations can effectively apply its core functions, i.e., Identify, Protect, Detect, Respond, and Recover—to these gaps. This structured approach provides a roadmap for the organizations to enhance their cybersecurity strategies, and to ensure that both device-level security and broader organizational practices are integrated into their operations. Furthermore, the implementation of additional standards alongside the SunSpec cybersecurity standards can further strengthen an organization's cybersecurity posture. For instance, adopting protocols for incident response and data management can fill the gaps identified in the SunSpec analysis. By providing explicit guidance on how organizations can implement and manage these protocols, this survey emphasizes the importance of a holistic approach to cybersecurity that not only secures the DERs but also fosters a robust security culture across all personnel and systems.

5. Conclusion

In this paper, a detailed survey is presented related to the cybersecurity certification requirements as they have been identified by the SunSpec Alliance for the Distributed Energy Resources devices. The survey is mainly focused on the software updates, the device communications, the authentication mechanisms, the device security, logging, and test procedures as they have been identified by the SunSpec Alliance. The provided discussion also focuses on the remote and automated software updates, the authentication practices, the secure communication protocols, and the logging mechanisms that are adopted based on the SunSpec cybersecurity standards in order to ensure the operational integrity of both the DER devices and the overall system. Focusing on the vehicle-to-grid capabilities, the survey analyzes the secure interactions between the electric vehicle supply equipment and the plug-in electric vehicles as they are derived from the implementation of the SAE J3072 standard that utilizes the IEEE 2030.5 protocol. Additionally, their SunSpec modbus standard is discussed aiming at the enhancing the interoperability among the DER system components and facilitating its compliance with the grid interconnection standards. Moreover, the survey covers existing SunSpec device information models in order to standardize the data exchange formats for the DER systems across different communication interfaces. Finally, a detailed gap analysis is presented in order to identify the gaps that exist within the SunSpec cybersecurity standards and we introduce potential paths that can be followed in order to address these gaps.

Author Contributions: Conceptualization and writing, Sean Tsikteris and Odyssefs Diamantopoulos Pantaleon; methodology, supervision, Eirini Eleni Tsiropoulou. All authors have read and agreed to the published version of the manuscript.

Funding: Funding for this project was provided by the U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Function	Category	Subcategory	Implementation Examples

GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored	Organizational Context (GV.OC): The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood		
		GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	The SunSpec documentation primarily describes the processes and standards for interoperability in Distributed Energy Resource (DER) systems, including information on the SunSpec Alliance, its specification process, information models, and conformance and certification requirements. It does not specifically address the organizational mission, stakeholder expectations, or legal, regulatory, and contractual requirements surrounding cybersecurity risk management decisions.
		GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	Neither internal nor external specific stakeholders have been identified. The cybersecurity-related expectations of the DERs have been discussed in the specifications documents.
		GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed	Not covered.
		GV.OC-04: Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are understood and communicated	The SunSpec documentation does not directly address this function, which involves mainly the understanding and communicating critical organizational objectives and services. The SunSpec Alliance mainly focuses on the technical cybersecurity requirements for the devices.
		GV.OC-05: Outcomes, capabilities, and services that the organization depends on are understood and communicated	Not covered.
	Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions		

		GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders	Not covered. SunSpec does not address organizational-level risk management strategies, priorities, constraints, risk tolerance, and objectives directly. Instead, it focuses on technical specifications and requirements for device cybersecurity, such as software updates, secure communications, and authentication mechanisms.
		GV.RM-02: Risk appetite and risk tolerance statements are established, communicated, and maintained	Not directly covered.
		GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes	It does not address organizational recommendations or risk management strategies.
		GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated	Not directly covered. SunSpec does not address the broader organizational risk management strategies.
		GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	Not directly covered. SunSpec does not address the broader organizational risk management strategies.
		GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	Not directly covered. SunSpec does not address the broader organizational risk management strategies.
		GV.RM-07: Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions	Not directly covered. SunSpec does not address the broader organizational risk management strategies.
	Roles, Responsibilities, and Authorities (GV.RR): Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated		
		GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving	Indirectly covered. SunSpec focuses on the device-level certification, and it implicitly discusses the organizational accountability by specifying the requirements that the manufacturers must meet to ensure the security and integrity of their devices. This indirectly supports a culture of accountability and responsibility within organizations.

		GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	Partially covered. SunSpec specifies mainly the requirements for the manufacturers to adhere to in terms of software updates, communications security, and authentication. However, it does not cover the aspects of organizational cybersecurity roles beyond the main focus of the device-specific mandates.
		GV.RR-03: Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies	Partially covered. SunSpec addresses the resource allocation in terms of ensuring that the devices comply with cybersecurity standards and protocols, i.e., it mandates certain technical capabilities (e.g., secure software updates, secure communications) that would require resources for implementation and maintenance.
		GV.RR-04: Cybersecurity is included in human resources practices	Not covered. There is no discussion related to the human resources practices.
	Policy (GV.PO): Organizational cybersecurity policy is established, communicated, and enforced		
		GV.PO-01: Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	Partially covered.
		GV.PO-02: Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission	Partially covered, as SunSpec periodically reviews and updates the cybersecurity policy.
	Oversight (GV.OV): Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy		
		GV.OV-01: Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction	Partially covered.
		GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks	Not covered. SunSpec does not address organizational-level risk management strategy review and adjustment. It primarily focuses on the technical requirements for device cybersecurity.
		GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed	Not covered.

	Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders		
		GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders	Partially covered.
		GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally	Not covered. SunSpec does not explicitly address roles and responsibilities beyond the device manufacturer and certifying bodies. It focuses solely on the device-level cybersecurity requirements.
		GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes	Not covered. SunSpec does not extend to enterprise-wide risk management processes but rather focuses on specific technical requirements for device certification.
		GV.SC-04: Suppliers are known and prioritized by criticality	Not covered. SunSpec does not mandate the identification and prioritization of suppliers based on criticality but focuses on the device-level cybersecurity requirements.
		GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties	Not covered. SunSpec does not require integration of cybersecurity risk requirements into contracts with suppliers, but it focuses on technical requirements for device certification.
		GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships	Not covered. SunSpec does not address planning and due diligence activities related to supplier relationships, but it focuses on technical device-level cybersecurity requirements.
		GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship	Not covered. SunSpec does not include requirements for ongoing risk assessment and management of supplier relationships.
		GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	Not covered. Incident planning, response, and recovery activities involving suppliers are not addressed by SunSpec documentation.

		GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle	Not covered. SunSpec does not extend to enterprise-wide risk management or lifecycle monitoring of supply chain security practices.
		GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement	Not covered. SunSpec does not mandate provisions for post-partnership or service agreement activities in supply chain risk management.
IDENTIFY (ID): The organization's current cybersecurity risks are understood	Asset Management (ID.AM): Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy		
		ID.AM-01: Inventories of hardware managed by the organization are maintained	Partially covered. The SunSpec certification focuses on individual device type testing rather than comprehensive organizational hardware inventories. It ensures devices are certified individually but doesn't mandate comprehensive organizational inventory management.
		ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained	Not covered. The certification program focuses on software updates for devices but does not address organizational-level inventory management of software, services, and systems.
		ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained	Partially covered. The requirement for secure communications (DER/DCOM/REQ-01) addresses some aspects of network communication security but not comprehensive representations of network flows.
		ID.AM-04: Inventories of services provided by suppliers are maintained	Not covered. The certification focuses on device-level security and updates rather than supplier inventory management.
		ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission	Not covered. Prioritization of assets based on various factors is not addressed in the SunSpec documentation.
		ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained	Not covered. The certification does not mandate data inventory management at an organizational level.

		ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles	Partially covered. Requirements for software updates (DER/SWUP) address lifecycle management for software components on devices but not comprehensive lifecycle management of all organizational systems and assets.
	Risk Assessment (ID.RA): The cybersecurity risk to the organization, assets, and individuals is understood by the organization		
		ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded	Partially covered. SunSpec focuses on type testing for individual devices, not organizational vulnerabilities.
		ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources	Not covered. SunSpec does not address organizational practices like threat intelligence.
		ID.RA-03: Internal and external threats to the organization are identified and recorded	Not covered. This requirement pertains to organizational threat identification, which is beyond SunSpec's scope.
		ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	Not covered. Similar to the previous points, impact assessment related to organizational risks is not within SunSpec's scope.
		ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization	Not covered. SunSpec does not cover risk assessment and response planning at the organizational level.
		ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated	Not covered. This requirement involves organizational risk management processes, not addressed by the SunSpec documentation.
		ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked	Not covered. SunSpec does not include provisions for managing changes and exceptions at the organizational level.
		ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability disclosures are established	Not covered. This pertains to organizational vulnerability management practices, not within the SunSpec scope.
		ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use	Partially covered. SunSpec mandates secure software updates and provenance, but it focuses on devices rather than comprehensive authenticity assessments for all hardware and software.
		ID.RA-10: Critical suppliers are assessed prior to acquisition	Not covered. Supplier assessment is an organizational practice not covered by SunSpec.
	Improvement (ID.IM): Improvements to organizational cybersecurity risk management processes, procedures, and activities are identified across all CSF Functions		

		ID.IM-01: Improvements are identified from evaluations	Not directly covered. The SunSpec certification focuses primarily on device-specific cybersecurity requirements and type testing. Evaluations for organizational improvements, such as cybersecurity risk assessments across all functions, are not within the scope.
		ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties	Partially covered. The certification includes requirements for security tests and exercises related to device communications (DER/DCOM/REQ-01) and updates (DER/SWUP/REQ-05), but it does not explicitly mandate coordination with suppliers or third parties for broader security improvements.
		ID.IM-03: Improvements are identified from execution of operational processes, procedures, and activities	Not covered. The certification focuses on device-specific operational requirements like software updates (DER/SWUP/REQ-01 to REQ-08) but does not extend to organizational processes and procedures.
		ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	Partially covered. The certification requires secure update mechanisms (DER/SWUP/REQ-05 to REQ-08), however, incident response plans specific to organizational operations are not explicitly mandated.
PROTECT (PR): Safeguards to manage the organization's cybersecurity risks are used	Identity Management, Authentication, and Access Control (PR.AA): Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access		
		PR.AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization	Partially covered. SunSpec specifies requirements for managing authentication credentials securely (e.g., DER/AUTH/REQ-01, DER/AUTH/REQ-06). However, it focuses more on device-specific credentials rather than organizational management of identities across all authorized entities.
		PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions	Not covered. SunSpec does not explicitly address proofing identities based on context. It primarily focuses on the technical aspects of authentication (e.g., DER/AUTH/REQ-02) rather than the contextual binding of identities.
		PR.AA-03: Users, services, and hardware are authenticated	Covered. This is covered under DER/AUTH/REQ-02, which mandates authentication mechanisms for electronic access to devices.
		PR.AA-04: Identity assertions are protected, conveyed, and verified	Partially covered. SunSpec addresses the protection of credentials and secure communications (e.g., DER/DCOM/REQ-01), which indirectly contributes to protecting identity assertions during communication.

		PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	Not covered. SunSpec does not explicitly address access permissions, entitlements, or policy management across organizational or user levels, but it primarily focuses on device-specific security measures.
		PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk	Partially covered. SunSpec focuses on cybersecurity measures related to device communication and software updates but does not deal with the physical access management.
	Awareness and Training (PR.AT): The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks		
		PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind	Not covered. The SunSpec Cybersecurity Certification document primarily focuses on device-level cybersecurity requirements for DER devices. It does not address organizational training and awareness programs for personnel, which are outside the scope of device certification.
		PR.AT-02: Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind	Not covered. SunSpec does not specify or require specialized training for roles within organizations using these devices. It focuses solely on the technical security requirements related to device communication, software updates, authentication, etc.
	Data Security (PR.DS): Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information		
		PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected	Partially covered. SunSpec does not explicitly specify requirements for protecting data-at-rest explicitly. It primarily focuses on device-level security and software updates.
		PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected	Covered. The requirement for secure communications using TLS, DTLS, IPSec, or SSH covers the protection of data-in-transit, ensuring confidentiality, integrity, and availability during transmission.
		PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected	Not Covered. SunSpec does not address specific protections for data-in-use, such as runtime data processing security.
		PR.DS-11: Backups of data are created, protected, maintained, and tested	Not Covered. Although there are requirements for software updates and authenticity checks, specific requirements for data backups are not outlined in the SunSpec documentation.

	Platform Security (PR.PS): The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability		
		PR.PS-01: Configuration management practices are established and applied	Not Covered. SunSpec does not explicitly discuss configuration management practices as required by PR.PS-01.
		PR.PS-02: Software is maintained, replaced, and removed commensurate with risk	Covered. Requirements for maintaining, replacing, and updating software components are detailed under the DER/SWUP, addressing the need for regular updates (DER/SWUP/REQ-01, DER/SWUP/REQ-03).
		PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk	Partially Covered. SunSpec addresses hardware maintenance in terms of updates and security implications (DER/SWUP/REQ-01), but does not comprehensively cover hardware-specific aspects such as lifecycle management.
		PR.PS-04: Log records are generated and made available for continuous monitoring	Partially Covered. Log records are mentioned for continuous monitoring (DER/SWUP/REQ-05), however, specific requirements for log generation and retention are not fully described.
		PR.PS-05: Installation and execution of unauthorized software are prevented	Covered. The requirement to prevent unauthorized software installation is addressed under DER/SWUP/REQ-01 and DER/SWUP/REQ-03, ensuring software integrity and authenticity.
		PR.PS-06: Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle	Not Covered. Although secure software updates are emphasized (DER/SWUP/REQ-05), specific practices related to secure software development throughout the lifecycle are not explicitly discussed in the SunSpec documentation.
	Technology Infrastructure Resilience (PR.IR): Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience		
		PR.IR-01: Networks and environments are protected from unauthorized logical access and usage	Covered. The SunSpec Cybersecurity Certification Program requires secure communications (DER/DCOM/REQ-01) and unique credentials (DER/AUTH/REQ-01), which help in protecting networks and environments from unauthorized access. The focus on secure communication protocols and unique user authentication aligns with preventing unauthorized logical access.

		PR.IR-02: The organization's technology assets are protected from environmental threats	Not Covered. The SunSpec documentation does not address protection from environmental threats such as physical damage, natural disasters, or other non-cyber-related environmental risks. The scope is limited to cybersecurity requirements for devices.
		PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	Partially Covered. The SunSpec documentation does focus on ensuring that the devices have secure and updated software (DER/SWUP/REQ-01 to DER/SWUP/REQ-08), which contributes to operational resilience, however, it does not explicitly mention mechanisms for resilience in adverse situations beyond cybersecurity threats.
		PR.IR-04: Adequate resource capacity to ensure availability is maintained	Not Covered. The SunSpec document does not address resource capacity or availability in the broader sense. It focuses on device security, software updates, and secure communications, without specific provisions for maintaining resource capacity to ensure availability.
DETECT (DE): Possible cybersecurity attacks and compromises are found and analyzed	Continuous Monitoring (DE.CM): Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events		
		DE.CM-01: Networks and network services are monitored to find potentially adverse events	Covered. SunSpec focuses on device type testing rather than network monitoring. It ensures that devices communicate securely but does not specify continuous monitoring of networks themselves.
		DE.CM-02: The physical environment is monitored to find potentially adverse events	Not Covered. SunSpec does not address the physical environment monitoring for potentially adverse events. It focuses on device security and software updates rather than physical security aspects.
		DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events	Not Covered. Monitoring personnel activity and technology usage is outside the scope of device type testing covered by the SunSpec documentation.
		DE.CM-06: External service provider activities and services are monitored to find potentially adverse events	Not Covered. Monitoring external service provider activities is not within the scope of the SunSpec documentation.
		DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	Covered. The SunSpec documentation covers aspects related to software updates and some aspects of software security (e.g., authentication, secure communications).
	Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents		
		DE.AE-02: Potentially adverse events are analyzed to better understand associated activities	Not explicitly covered.

		DE.AE-03: Information is correlated from multiple sources	Not explicitly covered.
		DE.AE-04: The estimated impact and scope of adverse events are understood	Not explicitly covered.
		DE.AE-06: Information on adverse events is provided to authorized staff and tools	Not explicitly covered.
		DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis	Not explicitly covered.
		DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria	Not explicitly covered.
RESPOND (RS): Actions regarding a detected cybersecurity incident are taken	Incident Management (RS.MA): Responses to detected cybersecurity incidents are managed		
		RS.MA-01: The incident response plan is executed in coordination with relevant third parties once an incident is declared	Not explicitly covered.
		RS.MA-02: Incident reports are triaged and validated	Not explicitly covered.
		RS.MA-03: Incidents are categorized and prioritized	Not explicitly covered.
		RS.MA-04: Incidents are escalated or elevated as needed	Not explicitly covered.
		RS.MA-05: The criteria for initiating incident recovery are applied	Not explicitly covered.
	Incident Analysis (RS.AN): Investigations are conducted to ensure effective response and support forensics and recovery activities		
		RS.AN-03: Analysis is performed to establish what has taken place during an incident and the root cause of the incident	Partially covered. The SunSpec documentation primarily focuses on device-level cybersecurity requirements, such as secure software updates, secure communications, and authentication mechanisms. SunSpec emphasizes the importance of security measures and incident prevention (like software update integrity and secure communications), it does not explicitly detail procedures for incident analysis and root cause determination.
		RS.AN-06: Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved	Partially covered. The SunSpec documentation stresses the integrity and authenticity of software updates and credential provenance. These requirements indirectly support maintaining the integrity and provenance of records related to software and credentials but do not specifically address recording actions during an investigation.

		RS.AN-07: Incident data and metadata are collected, and their integrity and provenance are preserved	Partially covered. The SunSpec documentation ensures the integrity and provenance of certain data types, particularly software updates and credentials. However, it does not explicitly address the collection and preservation of incident-specific data and metadata.
		RS.AN-08: An incident's magnitude is estimated and validated	Not covered. SunSpec does not cover the estimation and validation of an incident's magnitude. Its primary focus is on preventive measures and ensuring the security and integrity of devices, rather than on post-incident analysis or magnitude estimation.
	Incident Response Reporting and Communication (RS.CO): Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies		
		RS.CO-02: Internal and external stakeholders are notified of incidents	Not explicitly covered.
		RS.CO-03: Information is shared with designated internal and external stakeholders	Not explicitly covered.
	Incident Mitigation (RS.MI): Activities are performed to prevent expansion of an event and mitigate its effects		
		RS.MI-01: Incidents are contained	Not explicitly covered.
		RS.MI-02: Incidents are eradicated	Not explicitly covered.
RECOVER (RC): Assets and operations affected by a cybersecurity incident are restored	Incident Recovery Plan Execution (RC.RP): Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents		
		RC.RP-01: The recovery portion of the incident response plan is executed once initiated from the incident response process	Not explicitly covered.
		RC.RP-02: Recovery actions are selected, scoped, prioritized, and performed	Not explicitly covered.
		RC.RP-03: The integrity of backups and other restoration assets is verified before using them for restoration	Not explicitly covered.
		RC.RP-04: Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms	Not explicitly covered.
		RC.RP-05: The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed	Not explicitly covered.

		RC.RP-06: The end of incident recovery is declared based on criteria, and incident-related documentation is completed	Not explicitly covered.
	Incident Recovery Communication (RC.CO): Restoration activities are coordinated with internal and external parties		
		RC.CO-03: Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders	Not explicitly covered.
		RC.CO-04: Public updates on incident recovery are shared using approved methods and messaging	Not explicitly covered.

References

1. Zografopoulos, I.; Hatziargyriou, N.D.; Konstantinou, C. Distributed Energy Resources Cybersecurity Outlook: Vulnerabilities, Attacks, Impacts, and Mitigations. *IEEE Systems Journal* **2023**, *17*, 6695–6709. doi:10.1109/JSYST.2023.3305757.
2. Sangoleye, F.; Jao, J.; Faris, K.; Tsiropoulou, E.E.; Papavassiliou, S. Reinforcement Learning-Based Demand Response Management in Smart Grid Systems With Prosumers. *IEEE Systems Journal* **2023**, *17*, 1797–1807. doi:10.1109/JSYST.2023.3248320.
3. Patrizi, N.; LaTouf, S.K.; Tsiropoulou, E.E.; Papavassiliou, S. Prosumer-Centric Self-Sustained Smart Grid Systems. *IEEE Systems Journal* **2022**, *16*, 6042–6053. doi:10.1109/JSYST.2022.3156877.
4. Xie, J.; Rahman, A.; Sun, W. Bayesian GAN-Based False Data Injection Attack Detection in Active Distribution Grids With DERs. *IEEE Transactions on Smart Grid* **2024**, *15*, 3223–3234. doi:10.1109/TSG.2023.3337340.
5. Ahn, B.; Kim, T.; Ahmad, S.; Mazumder, S.K.; Johnson, J.; Mantooth, H.A.; Farnell, C. An Overview of Cyber-Resilient Smart Inverters Based on Practical Attack Models. *IEEE Transactions on Power Electronics* **2024**, *39*, 4657–4673. doi:10.1109/TPEL.2023.3342842.
6. Battista Gaggero, G.; Armellin, A.; Ferro, G.; Robba, M.; Girdinio, P.; Marchese, M. BESS-Set: A Dataset for Cybersecurity Monitoring in a Battery Energy Storage System. *IEEE Open Access Journal of Power and Energy* **2024**, *11*, 362–372. doi:10.1109/OAJPE.2024.3439856.
7. Gupta, K.; Sahoo, S.; Panigrahi, B.K. A Monolithic Cybersecurity Architecture for Power Electronic Systems. *IEEE Transactions on Smart Grid* **2024**, *15*, 4217–4227. doi:10.1109/TSG.2024.3368277.
8. Barbierato, L.; Salvatore Schiera, D.; Orlando, M.; Lanzini, A.; Pons, E.; Bottaccioli, L.; Patti, E. Facilitating Smart Grids Integration Through a Hybrid Multi-Model Co-Simulation Framework. *IEEE Access* **2024**, *12*, 104878–104897. doi:10.1109/ACCESS.2024.3435336.
9. Zhang, H.; Yu, C.; Zeng, M.; Ye, T.; Yue, D.; Dou, C.; Xie, X.; Hancke, G.P. Homomorphic Encryption-Based Resilient Distributed Energy Management Under Cyber-Attack of Micro-Grid With Event-Triggered Mechanism. *IEEE Transactions on Smart Grid* **2024**, *15*, 5115–5126. doi:10.1109/TSG.2024.3390108.
10. Liu, Z.; Wang, L. A Distributionally Robust Defender-Attacker-Defender Model for Resilience Enhancement of Power Systems Against Malicious Cyberattacks. *IEEE Transactions on Power Systems* **2023**, *38*, 4986–4997. doi:10.1109/TPWRS.2022.3222309.
11. Tuyen, N.D.; Quan, N.S.; Linh, V.B.; Van Tuyen, V.; Fujita, G. A Comprehensive Review of Cybersecurity in Inverter-Based Smart Power System Amid the Boom of Renewable Energy. *IEEE Access* **2022**, *10*, 35846–35875. doi:10.1109/ACCESS.2022.3163551.
12. Callenes, J.; Poshtan, M. Dynamic Reconfiguration for Resilient State Estimation Against Cyber Attacks. *IEEE Transactions on Emerging Topics in Computing* **2024**, *12*, 559–571. doi:10.1109/TETC.2023.3266303.
13. Trevizan, R.D.; Obert, J.; De Angelis, V.; Nguyen, T.A.; Rao, V.S.; Chalamala, B.R. Cyberphysical Security of Grid Battery Energy Storage Systems. *IEEE Access* **2022**, *10*, 59675–59722. doi:10.1109/ACCESS.2022.3178987.
14. Albunashee, H.M.; Farnell, C.; Suchanek, A.; Haulmark, K.; McCann, R.A.; Di, J.; Mantooth, A. A Test Bed for Detecting False Data Injection Attacks in Systems With Distributed Energy Resources. *IEEE Journal of Emerging and Selected Topics in Power Electronics* **2022**, *10*, 1303–1315. doi:10.1109/JESTPE.2019.2948216.
15. Xiong, X.; Sun, C.; Ni, W.; Wang, X. Three-Dimensional Trajectory Design for Unmanned Aerial Vehicle-Based Secure and Energy-Efficient Data Collection. *IEEE Transactions on Vehicular Technology* **2023**, *72*, 664–678. doi:10.1109/TVT.2022.3203714.
16. Ju, Y.; Cao, Z.; Chen, Y.; Liu, L.; Pei, Q.; Mumtaz, S.; Dong, M.; Guizani, M. NOMA-Assisted Secure Offloading for Vehicular Edge Computing Networks With Asynchronous Deep Reinforcement Learning. *IEEE Transactions on Intelligent Transportation Systems* **2024**, *25*, 2627–2640. doi:10.1109/TITS.2023.3320861.

17. Ju, Y.; Gao, Z.; Wang, H.; Liu, L.; Pei, Q.; Dong, M.; Mumtaz, S.; Leung, V.C.M. Energy-Efficient Cooperative Secure Communications in mmWave Vehicular Networks Using Deep Recurrent Reinforcement Learning. *IEEE Transactions on Intelligent Transportation Systems* **2024**, pp. 1–16. doi:10.1109/TITS.2024.3394130.
18. Wang, Y.; Xiao, J.; Wei, Z.; Zheng, Y.; Tang, K.T.; Chang, C.H. Security and Functional Safety for AI in Embedded Automotive System—A Tutorial. *IEEE Transactions on Circuits and Systems II: Express Briefs* **2024**, *71*, 1701–1707. doi:10.1109/TCSII.2023.3334273.
19. Wang, W.; Sadjadi, S.M.; Rishe, N. A Survey of Major Cybersecurity Compliance Frameworks. 2024 IEEE 10th Conference on Big Data Security on Cloud (BigDataSecurity), 2024, pp. 23–34. doi:10.1109/BigDataSecurity62737.2024.00013.
20. Parmar, M.; Miles, A. Cyber Security Frameworks (CSFs): An Assessment Between the NIST CSF v2.0 and EU Standards. 2024 Security for Space Systems (3S), 2024, pp. 1–7. doi:10.23919/3S60530.2024.10592293.
21. Safitri, E.H.N.; Kabetta, H. Cyber-Risk Management Planning Using NIST CSF V1.1, ISO/IEC 27005:2018, and NIST SP 800-53 Revision 5 (A Study Case to ABC Organization). 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs), 2023, pp. 332–338. doi:10.1109/ICoCICs58778.2023.10277652.
22. Randle, B.; Nunneley, J.; Fox, B.; Cox, C.; Madianos, G.; Blair, J.; Daharsh, J.; Hong, S.; Beran, M.; Lydic, B.; et al. SunSpec Alliance Interoperability Specification-Inverter Controls Model, 2013.
23. SunSpec. Cybersecurity Certification. https://sunspec.org/wp-content/uploads/2024/03/SunSpec-Cybersecurity-Certification-Requirements-Release-2024-v2-clean.pdf.
24. SunSpec. Cybersecurity Certification Release 2024 Test Procedure. https://sunspec.org/wp-content/uploads/2024/03/SunSpec-Cybersecurity-Certification-Test-Procedure-Release-2024-240319-clean.pdf.
25. SunSpec. IEEE 2030.5 V2G-AC Profile Implementation Guide for SAE J3072. https://sunspec.org/wp-content/uploads/2022/06/SunSpec-IEEE-2030.5-V2G-AC-Profile-TEST-1.0.pdf.
26. SunSpec. MODBUS INTERFACE. https://sunspec.org/wp-content/uploads/2019/09/SunSpec-Modbus-FactSheet-RevA-2019-07-web.pdf.
27. SunSpec. Technology Overview. https://sunspec.org/wp-content/uploads/2022/05/SunSpec-Technology-Overview-20220301.pdf.
28. SunSpec. Device Information Model Specification. https://sunspec.org/wp-content/uploads/2022/05/SunSpec-Device-Information-Model-Specificiation-V1-1-final.pdf.
29. SunSpec. DER Information Model Specification. https://sunspec.org/wp-content/uploads/2021/04/SunSpec-DER-Information-Model-Specification-V1-0.pdf.
30. SunSpec. Energy Storage Models. https://sunspec.org/wp-content/uploads/2019/08/SunSpec-Alliance-Specification-Energy-Storage-ModelsD4rev0.pdf.
31. SunSpec. Blockchain to Record Private Key Properties in DER Equipment. https://sunspec.org/wp-content/uploads/2021/03/SunSpecAlliance_BlockchainWG_Specification_BlockchainTo\RecordPrivateKeyProperties_29032021.pdf.
32. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf. [Accessed 08-09-2024].