Document #:

Status: Draft

Version: 0.1

SunSpec Cybersecurity Certification

Phase 1 Requirements

Abstract

TBD.

22

License Agreement and Copyright Notice

Prepared by the SunSpec Alliance
4040 Moorpark Avenue, Suite 110
San Jose, CA 95117

Website: sunspec.org
Email: info@sunspec.org

44

About the SunSpec Alliance

The SunSpec Alliance is a trade alliance of developers, manufacturers, operators, and service providers together pursuing open information standards for the distributed energy industry. SunSpec standards address most operational aspects of PV, storage, and other distributed energy power plants on the smart grid, including residential, commercial, and utility-scale systems, thus reducing cost, promoting innovation, and accelerating industry growth.

Over 100 organizations are members of the SunSpec Alliance, including global leaders from Asia, Europe, and North America. Membership is open to corporations, non-profits, and individuals. For more information about the SunSpec Alliance, or to download SunSpec specifications at no charge, visit sunspec.org.

About the SunSpec Specification Process

SunSpec Alliance specifications are initiated by SunSpec members to establish an industry standard for mutual benefit. Any SunSpec member can propose a technical work item. Given sufficient interest and time to participate, and barring significant objections, a workgroup is formed and its charter is approved by the board of directors. The workgroup meets regularly to advance the agenda of the team.

The output of the workgroup is generally in the form of a SunSpec Interoperability Specification. These documents are considered to be normative, meaning that there is a matter of conformance required to support interoperability. The revision and associated process of managing these documents is tightly controlled. Other documents are informative, or make some recommendation with regard to best practices, but are not a matter of conformance. Informative documents can be revised more freely and more frequently to improve the quality and quantity of information provided.

SunSpec Interoperability Specifications follow a lifecycle pattern of: DRAFT, TEST, APPROVED, and SUPERSEDED.

For more information or to download a SunSpec Alliance specification, go to https://sunspec.org/about-sunspec-specifications/.

Revision History

Version	Date	Comments
0.1	22-11-23	Initial draft based on Lumian contribution

Contents

1 Scope

TBD.

2 References

[1] IETF, RFC 2119, “Keys words for use in RFCs to Indicate Requirement Levels”, March 1997. http://www.ietf.org/rfc/rfc2119.txt.

3 Definitions, abbreviations and terminology

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

None

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

DER Distributed energy resource

SWUP Software Updates

3.3 Terminology

The specification lists a series of requirements, either explicitly or within the text, which are mandatory elements for compliant solutions. Recommendations are given, to ensure optimal usage and to provide suitable performance. All recommendations are optional.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are following the notation as described in RFC 2119 1[1].

1. MUST: This word, or the terms "REQUIRED" or "SHALL", means that the definition is an absolute requirement of the specification.
2. MUST NOT: This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification.
3. SHOULD: This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
4. SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
5. MAY: This word, or the adjective "OPTIONAL", means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

4 Requirements

4.1 Software Updates/Product Support

4.1.1 DER/SWUP/REQ-01: Software Updates

Summary

The DER device SHALL support updating mutable security and operational software functions.

Description

The DER device SHALL have the ability to have software components, listed in Table 4-1, updated, if the respective component is installed on the device.

Table 4-1: Updatable Software Components

Component/Functionality	Must be updatable?
Operating system (kernel)	Yes
Operating system (non-kernel)	Yes
Boot loader	Yes
BIOS	No
Applications	Yes
Libraries	Yes
Configuration	Yes
Certificates	Yes

Rationale

The security community is constantly finding new vulnerabilities in software. These new vulnerabilities are reported to the public at least 60 days after they have been found. Adversaries often design attacks around these newly found vulnerabilities. Devices that are not able to be updated will continue to be a target of these adversaries.

4.1.2 DER/SWUP/REQ-02: Remote Updates

Summary

The DER device SHALL have the capability to support remote updates.

Description

A device SHALL communicate with a remote server at least once per day to download and install a software update when available. The device MAY allow a user to turn off remote updates, but remote updates SHALL be active by default (default factory setting).

Rationale

DER devices are located on site and are not easily (or inexpensively) accessible by maintenance crew for local software updates. Even if cost and resources were not a factor, the time required to visit all sites and manually update software is more time then adversaries need to conduct their attacks. Remote updates allow vendors and site managers to trigger software updates remotely in seconds, giving adversaries much less time.

4.1.3 DER/SWUP/REQ-03: Automatic Updates

Summary

The DER device SHALL support automated updates.

Description

No additional explanation

Rationale

Without automated updates a user needs to manually trigger a device to obtain an update. If thousands of devices are in the field, this takes too much time even if the update can be triggered remotely and even if the user acts quickly when an update is available.

4.1.4 DER/SWUP/REQ-04: Secure Updates

Summary

The DER device SHALL verify the authenticity and integrity of software updates, prior to installing it.

Description

The DER device SHALL use a mechanism that verifies that the software update package came from a trusted source, such as the manufacturer. An example of an authentication mechanism is a cryptographic signature. The DER device SHALL verify that the software update package was not modified by a third party. An example of an integrity mechanism is a checksum or hash.

Rationale

Attacking the software update system is commonly used by adversaries, and can allow an adversary to gain complete control over a device. Checking the authenticity (the creator/author) and integrity (the package has not been modified) of a package prevents such attacks.

4.1.5 DER/SWUP/REQ-05: Downgrade Prevention

Summary

The DER device SHALL prevent firmware downgrade attacks, i.e., prevent updates to previous software versions. Vendors SHALL keep the previous software images for rollbacks and package them as new updates when a rollback is needed.

Description

The DER device SHALL reject all software updates that are older than the currently installed software. If a vendor wishes to rollback to a previous version, the previous version software must be re-packaged as the most recent version.

Rationale

If an adversary can install a previous version of software that contains known vulnerabilities, the adversary can successfully attack the device once the device is using the previous version. If a new software update causes more problems for the device than it aims to fix, the manufacturer needs to take a previous version of the software out of archive and re-package it as a newer software update. This will give time for vendors to fix the problematic software update.

4.1.6 DER/SWUP/REQ-06: Local Updates

Summary

If the DER device supports local updates, then this functionality SHALL comply with the same security requirements of the remote update functionality.

Description

No other explanation necessary.

Rationale

Same as the Secure Updates requirement.

4.2 Device Communications

4.2.1 DER/DCOM/REQ-01: Secure Communications

Summary

The DER device SHALL implement at least one of TLS 1.2 (or higher), IPSec Version 2 (or higher), or SSH-2 for all communications that can access the open Internet.

Description

Any DER device functionality that can communicate over the open Internet MUST be secured by the latest versions of either TLS, IPSec, or SSH. This includes not only default functionality but also optional or configurable functionality. For example, if a DER device can communicate to a local device using MODBUS over a serial line, and this communication

functionality can also be configured to communicate MODBUS over an IP network, this functionality MUST be secured.

TLS 1.2 (or higher), IPSec Version 2 (Committee on National Security Systems Policy 15-compliant), and SSH-2 SHALL be the only allowed protocols for securing such communications.

Rationale

Network access to a device is one of the easiest attack vectors for adversaries because an adversary does not need physical access to the device to carry out an attack. Attacks can modify data in transit, spoof communications from a trusted endpoint, and eavesdrop on sensitive data. TLS, IPSec, and SSH are widely used and scrutinized protocols that offer the authentication and encryption capabilities that prevent these attacks, and the required versions are specified because previous versions of these protocols contain vulnerabilities. While there are other protocols that have the same capabilities of TLS, IPSec, and SSH they do not receive the same scrutiny and are therefore considered less trustworthy.

4.2.2 DER/DCOM/REQ-02: Downgrade Prevention

Summary

The DER device SHALL configure the minimum required version of the cryptographic protocol that is used and reject connections and requests to use older protocol versions.

Description

A DER device that is configured to use TLS 1.2 MUST reject requests to use TLS 1.1 or lower. A device configured for IPSEC Version 2 MUST reject requests to use other IPSec versions and configurations. A device configured with SSH-2 MUST reject requests to use previous version of SSH.

Rational

Downgrade attacks can compromise the security properties of TLS since previous protocol versions have known vulnerabilities.

4.2.3 DER/DCOM/REQ-03: Ciphersuites

Summary

A DER device SHALL only use ciphersuites specified in TLS 1.3 (or higher) or IEEE 2030.5-2018 (or higher)

Description

TLS 1.2 contains ciphersuites that have been found to be vulnerable. TLS 1.3 removes these ciphersuites. TLS 1.2 implementations must only use TLS 1.3 ciphersuites. IEEE 2030.5-2018 also defines a ciphersuite that is also allowed (TLS_ECDHE_ECDSA_WITH _AES_128_CCM_8 using elliptic curve secp256r1).

Rationale

TLS 1.3 is not yet widely supported in software libraries. TLS 1.2 is widely supported, and it is straightforward to remove support for ciphersuites that are not specified in TLS 1.3 and IEEE 2030.5-2018.

4.3 Authentication

4.3.1 DER/AUTH/REQ-01: Unique Credentials

Summary

The DER device SHALL require the use of unique security credentials (such as passwords or keys) for each level of privilege and user account available on the Device.

Description

If the DER device has multiple access levels or multiple user accounts, it MUST support unique security credentials for each access level and user account.

Rationale

Sharing credentials among multiple users is generally not a good security practice. A device must allow for different credentials for each security access level and user. However, if a user wants to use the same credentials across access levels and user accounts, the device is allowed to accommodate this desire. In this case the user could use a secure password management application to mitigate the risks of using shared credentials.

4.3.2 DER/AUTH/REQ-02: Authentication

Summary

All electronic access to the device, whether locally through a control panel or diagnostic port, or remotely through communications channels, SHALL be protected with an authentication mechanism that securely identifies a subject with a unique user identification (ID).

Description

This requirement specifies that a device MUST have the ability to differentiate between different users (with an ID) and authenticate them securely. The authentication means is not specified, but MUST be secure. If passwords are used as the authentication mechanism, they MUST comply with the requirements in this document. There are also many passwordless authentication mechanisms such as X.509 certificates, unique login codes sent out-of-band, and use of FIDO compatible devices. See references below for details.

Rationale

Authenticating a user's electronic access to a device prevents installation of malicious code, unauthorized access to data, and control of a device by an adversary. Unique IDs are required for many of these authentication methods, and allow devices to allocate different permissions to different users.

References

NIST Special Publication 800-63B

4.3.3 DER/AUTH/REQ-03: Session Timeout

Summary

All authenticated sessions SHALL have a timeout.

Description

The DER device MUST have a timeout feature that automatically logs out a user who remains logged in after a period of inactivity. Inactivity SHALL be defined as the absence of input from local or remote DER interfaces and endpoints.

Rationale

This requirement addresses sessions wherein the user can be replaced by an adversary. For example, if a user logs into an admin panel (physically on the device or via remote computer) and the user walks away without logging off, an adversary who gains access to the panel can start an attack.

4.3.4 DER/AUTH/REQ-04: Configurable Timeout

Summary

The length of time before a session automatically times out SHALL be settable by an authorized user.

Description

This requirement states that a device MUST give an authorized user the capability to change the session timeout period. Examples of this capability include a configuration screen on a physical panel or a configuration API.

Rationale

The ideal timeout period is dependent on the characteristics of the site where the device is installed. If the device is within a secured perimeter the timeout period can be longer. The timeout for a remote technician can also be longer if the technician's computer has access control. A physical admin panel in a public space MAY require a shorter timeout period.

4.3.5 DER/AUTH/REQ-05: Strong Passwords

Summary

If a DER device uses passwords for authentication, then the DER device SHALL enforce strong passwords and SHALL notify users if they attempt to use a weak password.

Description

Compliance with this requirement SHALL be achieved in one of two ways:

1. Password strength meter: Device implements a password strength meter that follows NIST password recommendations (5.1.1.2 of the NIST Special Publication 800-63B). Only passwords deemed by the strength meter to be “strong” SHALL be allowed.
2. Password MUST meet the following set of rules to be allowed:
    - At least 8 characters in length, and the device MUST allow passwords up to 64 characters in length
    - Case sensitive

Rationale

Passwords are an often-used attack vector for adversaries. Strong passwords prevent basic password attacks. The latest password research has concluded that length and entropy of a password is the best predictor of strength. Requiring numbers and symbols has shown to not increase the strength of a password.

References

NIST Special Publication 800-63B

4.3.6 DER/AUTH/REQ-06: Unique Passwords

Summary

If pre-installed passwords are used, then the DER device SHALL require users to create a new password when they first login.

Description

If a DER device manufacturer loads the same password on multiple devices, then the DER device MUST require the user to create a different password when the device is first accessed by the user.

Rationale

Default common passwords are one of the most commonly used attack vectors into devices. Many jurisdictions around the world have outlawed the practice of using default common passwords.

4.3.7 DER/AUTH/REQ-07: Brute Force Prevention

Summary

The DER device SHALL support blocking authentication requests, either temporarily or permanently, from an account or user after at most 10 failed password login attempts.

Description

After a maximum of 10 consecutive failed password login attempts to a unique user account, the device MUST lock out the user for at least 5 minutes. The maximum number of consecutive failed password login attempts is 10 before lock out occurs.

Rationale

Brute force password attacks can break even strong passwords given enough time. Temporary lockouts make brute force attacks infeasible by dramatically increasing the amount of time necessary to guess the correct password.

4.3.8 DER/AUTH/REQ-08: Password Protection

Summary

The DER device SHALL prevent storage or display of unencrypted passwords.

Description

The DER device MUST NOT display stored plain text passwords on screens, including the local display panel, configuration software (local or remote; offline or online), web browser, and terminal access. A device MUST NOT store plain text passwords in audit trails, the memory area or files, or other records and configuration files. A DER device MAY display the password a user enters for authentication.

Rationale

Passwords stored in plain text can be copied and distributed to adversaries. Adversaries that gain access to the device through a lower clearance security channel could copy passwords of users with much higher clearance.

4.4 Device Security

4.4.1 DER/DSEC/REQ-01: Minimal Interfaces

Summary

The DER device SHALL have any unneeded logical interfaces and ports removed (or disabled if removal is not possible) prior to transfer of device custody.

Description

A device manufacturer MUST list (in PICS) all logical interfaces and ports used by the device, as well as the use. Any logical interfaces and ports not on this list SHOULD be removed or disabed before the device is transferred from the manufacturer's custody. The manufacturer must not rely on a customer or installer to remove or disable unused logical interfaces and ports. Examples of logical interfaces and ports include: USB ports, memory card slots, serial ports, ethernet ports, and TCP ports (e.g.- port 5590).

Rationale

Many operating systems default to opening multiple ports (port 21, port 53, port 80, port 110, port 23, port 139 etc.). If these ports are not used, they become targets for adversaries especially if they are not secured properly. USB ports are another common attack vector. Stuxnet took advantage of a USB port on a computer at a centrifuge facility.

4.4.2 DER/DSEC/REQ-01: Factory Reset

Summary

The DER device SHALL support a "factory reset" option for end-of-life or repurposing the device.

Description

A factory reset option allows the owner of the device to wipe data from the device and return it to the “factory setting”, which is the state the device was in when it was first manufactured, before giving up ownership. Software update files need not be wiped as they do not contain sensitive data and fix device vulnerabilities..

Rationale

Over a device’s lifetime in service it MAY collect and store sensitive data such as logs, encrypted passwords, and configuration files. These files MAY be utilized by an adversary to initiate an attack on the original owner's existing assets.

4.5 Logging

4.5.1 DER/LOG/REQ-01: Logging

Summary

The DER device SHALL store logs that are readable by the highest level of access control.

Description

No further explanation needed.

Rationale

Logs are required to analyze and stop security breaches.

4.5.2 DER/LOG/REQ-02: Log Storage

Summary

The DER device SHALL store logs locally in persistent memory.

Description

No further explanation needed.

Rationale

Logs need to survive power loss.

4.5.3 DER/LOG/REQ-03: Timestamp Logs

Summary

The DER device SHALL log events with a timestamp.

Description

No further explanation needed.

Rationale

Logging events with a timestamp is required for security forensics.

4.5.4 DER/LOG/REQ-04: Timestamp Resolution

Summary

The DER device SHALL timestamp logs with a resolution of at least 1 millisecond.

Description

No additional explanation necessary.

Rationale

In order to record the order of network events a resolution of at least 1 millisecond is required.

4.5.5 DER/LOG/REQ-05: Timestamp Accuracy

Summary

The DER device SHALL maintain time accuracy within +/- 1 min of Coordinated Universal Time (UTC) for all logging timestamps.

Description

This requires devices to synchronize with a remote reliable information source such as a cellphone service, Internet server, or GPS signal.

Rationale

Monitoring logs across multiple devices requires timestamps to be consistent.

4.5.6 DER/LOG/REQ-06: Configuration Logs

Summary

The DER device SHALL log any changes in security-related configurations.

Description

If interfaces and ports listed in the Minimal Interfaces requirement have modifiable security settings, any change to these settings MUST be logged. Security configurations (firewalls settings, etc.) MUST be logged as well.

Rationale

When a security-related configuration is changed the device SHOULD log this change so if there is a breach remediation efforts can analyze such changes.

4.5.7 DER/LOG/REQ-07: Network Logs

Summary

The DER device SHALL log network traffic.

Description

The DER device SHALL log the following network traffic information for all interfaces and ports listed in Minimal Interfaces requirement:

- Device initiated communications, including the endpoint address
- Incoming network requests, including endpoint address and request type
- Authentication messages
- Session starts, stops, and timeouts.

Rationale

Many adversaries launch their attacks over the network because it doesn't require physical access. If an adversary successfully penetrates a device, cybersecurity remediation efforts need network logs to determine the cause and effect of the breach.

4.5.8 DER/LOG/REQ-08: Security Logs

Summary

The DER device SHALL log security events.

Description

Security events MUST include: (a) successful and unsuccessful login attempts, (b) detected failure of event logging, (c) software updates and changes, (d) changes to access controls or accounts.

Rationale

This information is also needed for breach remediation.

4.5.9 DER/LOG/REQ-09: Remote Logs

Summary

If the DER device has communication capabilities, then it SHALL send logs to a remote central repository with an upload frequency of at least once per day.

Description

More explanation is not necessary.

Rationale

Centrally-stored logs allow monitoring solutions to detect threats over a large number of devices. It also reduces the storage needs of devices and allows logs to be kept for a longer period of time. Last, it provides log redundancy because if a hacker accesses a device and modifies or deletes the logs on the device the remote repository still has the original logs. An upload frequency of once per day strikes a balance between keeping logs safe and minimizing the network load.

4.5.10 DER/LOG/REQ-10: Log Retention

Summary

The DER device SHALL store (locally or on a remote central repository) network traffic logs for 7 days and all other logs for 90 days.

Description

It is important to note that a manufacturer has the ability to purge log files from a device every day given the Remote Logs requirement. The remote server can maintain compliance with this requirement while the device can minimize its memory storage size.

Rationale

Some security breaches are not discovered until long after the attack was started. The Solar Winds breach started months before it was discovered, but since logs were kept for a long time researchers were able to understand the attack from its inception. This knowledge can be used to prevent the attack from being successful in the future.

4.5.11 DER/LOG/REQ-11: Incident Reporting

Summary

The DER device SHALL upload security incidents to a remote central repository within one minute of the incident.

Description

Security incidents include the following events:

- Failed authentication attempts
- Network activity that deviates from the normal range of activity
- Attempted access to protected data such as private keys

Rationale

If security incidents are uploaded to a remote repository, a central monitoring service can detect patterns across a wide range of devices.

4.5.12 DER/LOG/REQ-12: Power System Logs

Summary

The DER devices SHALL store power system event logs.

Description

Power system event logs include at minimum: (a) when a function is enabled or disabled (b) when there is a change to adjustable settings of the device, (c) when a device is power-cycled.

Rationale

The purpose of a DER device is to manage the behavior of a DER. If an adversary has control of the device, the adversary can attack the power grid by manipulating the power control settings. Logging such manipulations can help detect or analyze unauthorized manipulations. Logging device power cycles can also detect nefarious activity.

4.5.13 DER/LOG/REQ-13: Panel Logs

Summary

If the DER device has an admin panel, then it must log login activity in a manner consistent with the above logging requirements.

Description

This requirement gives more clarity to how physical access logs are to be handled.

Rationale

Physical access must also be monitored, especially if the device is protecting a high-value target.