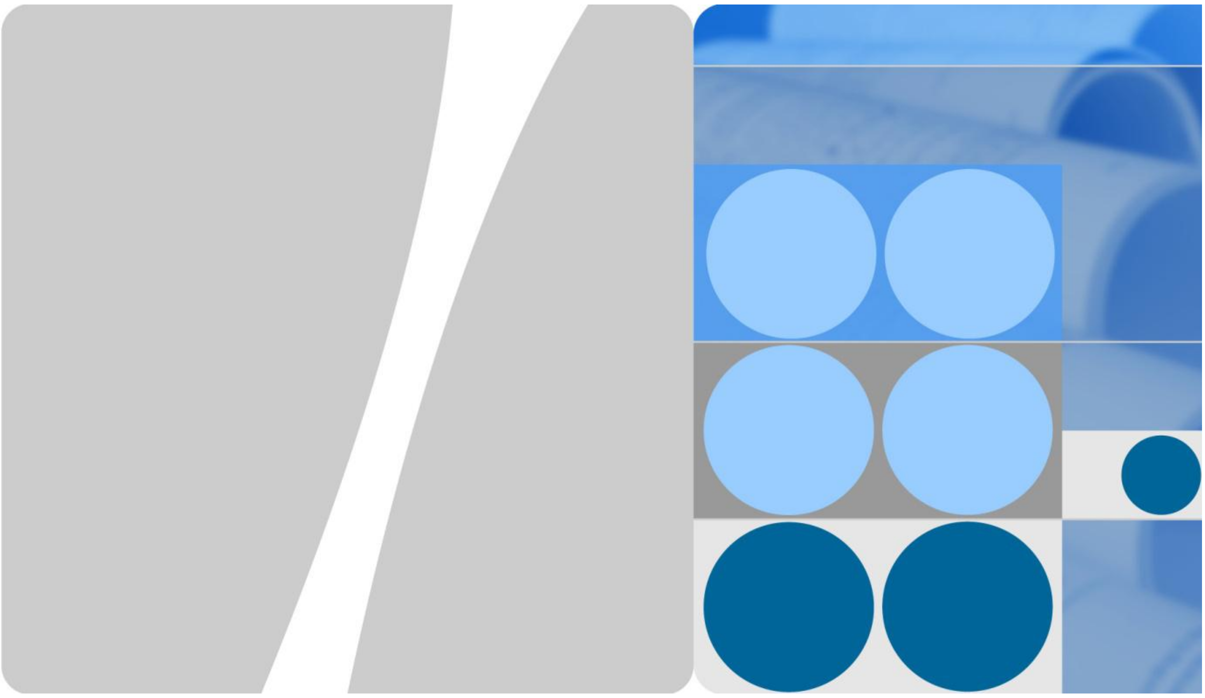


CC Huawei SUN2000HA Software V300R001C00SPC608

Security Target

Issue	1.6
Date	2022-05-11

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

About This Document

Purpose

This document provides description about ST (Security Target).

Change History

Date	Revision Version	Description	Author
2019-05-30	0.1	First Draft	Shenyanbai/00485446
2019-12-10	0.2	Modified based on the first review	Shenyanbai/00485446
2020-01-15	0.3	Modified based on the second review	Shenyanbai/00485446
2020-03-15	0.4	Modified based on the feedback HUA-SUN-OR-009 and HUA-SUN-OR-010	Shenyanbai/00485446
2020-06-24	0.5	Change document name	Shenyanbai/00485446
2020-07-31	0.6	Modified based on the feedback HUA-SUN-OR-001 to HUA-SUN-OR-006 Version1.1 HUA-SUN-OR-013 to HUA-SUN-OR-016 Version1.0	Shenyanbai/00485446
2020-09-10	0.7	Add data filter	Shenyanbai/00485446
2021-03-23	0.8	Modified based on review comments.	Sunwuben/00442792， Chenfei/00532957
2021-03-29	0.9	Change document name. Remove the export/import configuration function from the user role of Special User. Updating the user guides and guidance documents version number	Sunwuben/00442792
2021-04-15	1.0	Modified the audit record related description; Added need role; Corrected some errors.	Sunwuben/00442792
2021-05-08	1.1	Modified based on review comments.	Sunwuben/00442792
2021-07-10	1.2	Modified based on review comments.	Sunwuben/00442792

Date	Revision Version	Description	Author
2021-07-26	1.3	Modified based on review comments.	Sunwuben/00442792
2021-11-02	1.4	Modified based on review comments.	Sunwuben/00442792
2021-12-02	1.5	Modified based on review comments.	Sunwuben/00442792
2022-05-11	1.6	Modified based on CB comments	Sunwuben/00442792

Contents

Figures

Tables

1 Introduction

This CC Security Target is for the evaluation of the Huawei SUN2000HA Software V300R001C00SPC608. The software is part of SUN2000HA inverter chassis.

1.1 ST Identification

Title: CC Huawei SUN2000HA Software V300R001C00SPC608 Security Target

Version: V1.6

Publication Date: 2022-05-11

Developer: Huawei Technologies Co., Ltd.

1.2 TOE Identification

Name: Huawei SUN2000HA Software

Version: V300R001C00SPC608

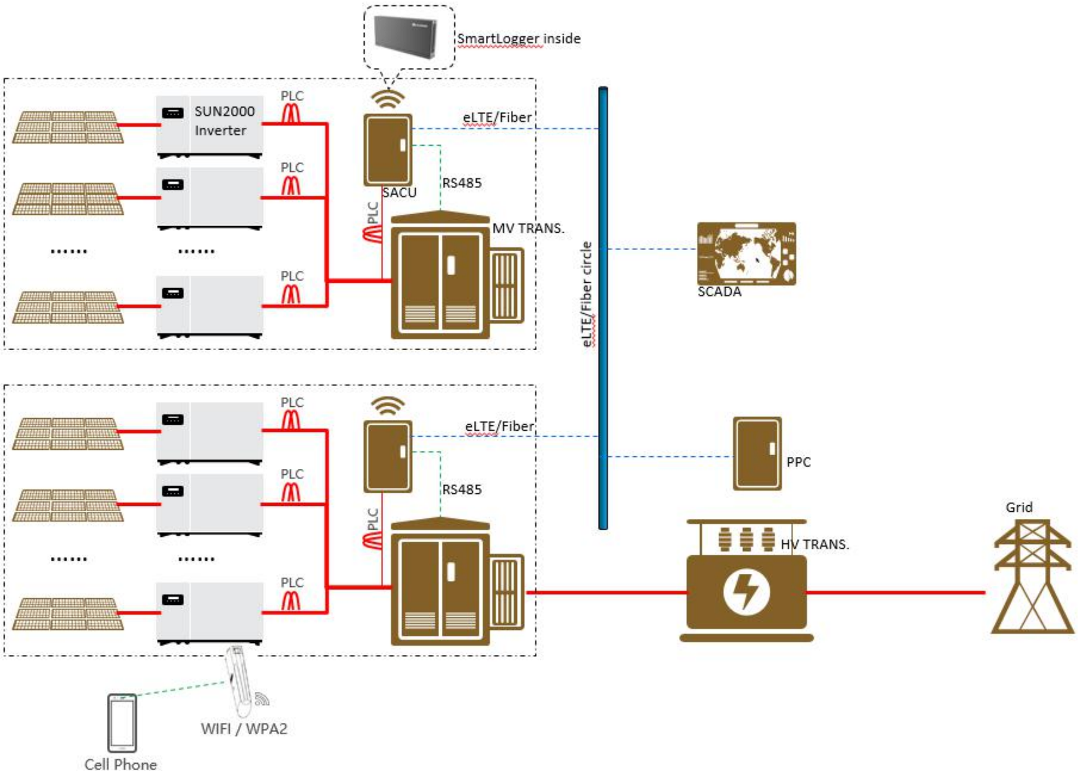
Developer: Huawei Technologies Co., Ltd.

1.3 Product Description

The SUN2000HA inverter is a power generation device used to convert photovoltaics into alternating current. It is generally integrated into the power station as a component of a photovoltaic power plant.

The main function of SUN2000HA inverter is for power generation. It provides power generation status monitoring and inspection service through this communication channel. Additionally， it responds to the dispatch control of the power station or power company. At the same time, it supports the extended USB-WIFI Adapter module for communication with mobile phones. The mobile phone performs as the user interface (UI). Users operate the SUN2000HA inverter can perform user password management, software upgrade, log exports and time settings.

Figure 1-1 Position of the SUN2000HA inverter on the entire PV plant communication network



1.3.1 Architectural overview of SUN2000HA

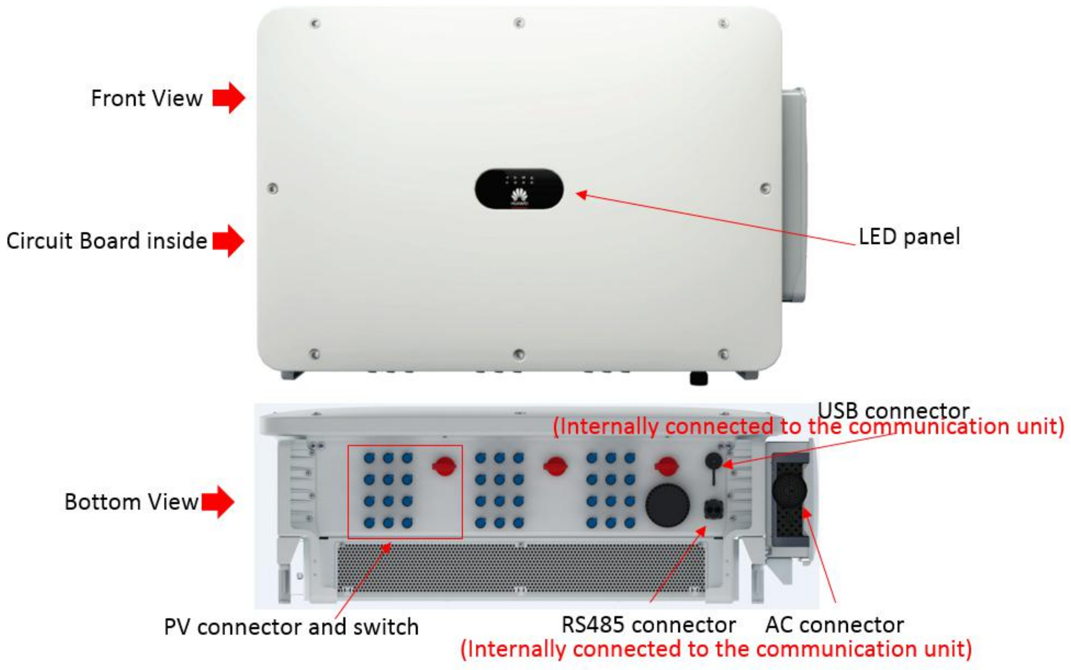
This section will introduce SUN2000HA inverter from a physical architectural point of view and a software architectural point of view.

1.3.1.1 Physical Architecture of SUN2000HA

SUN2000HA inverter consists of the hardware and the software.

The hardware is composed of chassis, circuit boards, LED panel and connectors. The chassis is used to install circuit boards, including power circuit boards and communication boards. The LED panel is used to indicate the operating status of the system. The connectors is used to connect to PV plant, AC Grid, USB-WiFI Adapter stick and USB disk.

Figure 1-2 System architecture of the SUN2000HA



The main service provided by this inverter is to convert the direct current of photovoltaic panels into alternating current that can be feed-in to the grid. The PV terminals are used to connect photovoltaic panels. The AC terminal is used to connect to the grid.

The USB terminal and AC terminal are internally connected to the communication unit. Provide near-end maintenance and communication services.

1.3.1.2 Software Architecture of SUN2000HA

All the software run in the communication and control circuit board. Which is responsible communication, managing and controlling, and security features in SUN2000HA inverter.

In terms of the software, SUN2000HA software architecture consists of three logical planes to support centralized controlling and management and running status sampling.

Plugin plane
Core plane
Sampling and Controlling plane

The **plugin plane** provides external communication services and near-end maintenance services. Processes protocols and signals, configures and maintains the system status, and reports and controls the system status.

The **core plane** is the core of the entire system. It provides user management, alarm management, log management, and software upgrade management, etc.

The **sampling and controlling plane** is used to manage system and sample data.

1.4 TOE Overview

1.4.1 TOE Type

The TOE is the software running in the Operating System that is deployed into communication board inside Huawei SUN2000HA inverter, which is the access node of inverter.

1.4.2 TOE usage and major Security Features

It provides near-end maintenance through:

- Huawei mobile phone APP connected to the SUN2000HA inverter through the USB-WIFI Adapter stick inserted into the USB terminal.
- Smartlogger connected to the SUN2000HA inverter through the MBUS or RS485 with Modbus-RTU protocol (in the TOE evaluated configuration is used the RS485 port).

The TOE provides the following major security features:

- **Authentication and Authorization:** Only authenticated users are allowed to log in to the TOE, query TOE data, and set TOE parameters. Only authorized users are able to execute the previous actions based on their privileges. If a user fails to be authenticated for multiple consecutive times, the user is locked for a period of time to prevent unauthorized access.
- **Auditing:** An operation log records the operation that an administrator has performed on the system and the result of the operation and is used for tracing and auditing.
- **Security Management:** The TOE provides four different user roles (Common user, Advanced user, Special user and Datalogger user). Also, the TOE provides: user password management, software upgrade, log exports and time settings.

1.4.3 Non-TOE Hardware and Software

The environment for TOE comprises the following components:

-User’s mobile phone (user mobile phone must be a Huawei phone), that used by installer or maintainers to connect to USB-WIFI Adapter stick, to communicate with the TOE.
- The USB-WIFI Adapter stick is inserted into the inverter USB connector when working.
-Mobile phone app SUN2000, that can be download from Huawei app store.
-Local SmartLogger connected to SUN2000HA using MBUS or RS485 with Modbus-RTU protocol.

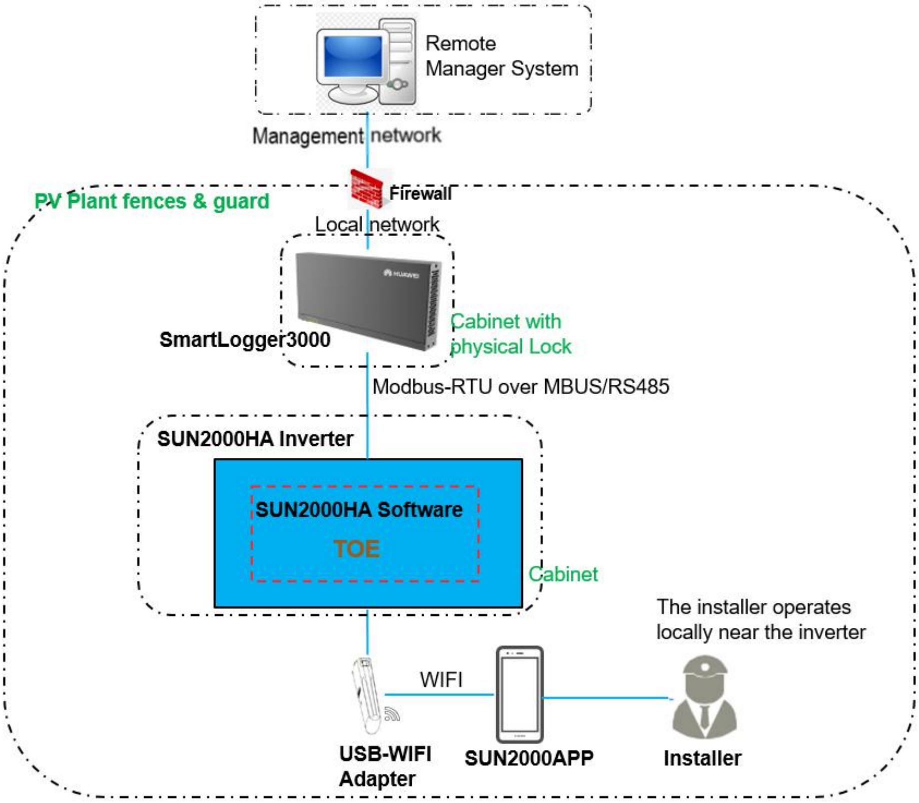
Table below lists the requirement and main information about the Non-TOE hardware and software:

Table 1-1 Lists of Non-TOE requirement

Non-TOE	Item or module type	Requirement
Mobile phone	Huawei Mobile phone	Operating system: android 4.4 or later

Mobile phone app	SUN2000APP	Software version: 3.2.00.016
USB-WIFI Adapter stick	USB-Adapter2000-C	
Remote Manager System PC	Desktop PC	Supported web browsers: Firefox52, Chrome 58 and IE9 or above
Security Firewall	Firewall	
SmartLogger	SmartLogger3000	Software version:V300R001C00SPC605 or greater
SUN2000HA inverter	SUN2000HA 185KTL-H1	Note: SUN2000HA 185KTL-H1, SUN2000HA 175KTL-H0 and SUN2000HA 185KTL-INH0 are the same series inverter.

Figure 1-3 The TOE in its operational environment



1.5 TOE Description

1.5.1 Physical scope

The TOE is a 'software only'. TOE consists of the software running on the Operating System of the SUN2000HA inverter chassis, but not the hardware. The software is pre-burned on the factory production state using an old version of the TOE. Therefore, the final user shall update the TOE with the software defined in the table below to reach the evaluated version.The TOE, the signature file and the associated documentation (CC Huawei SUN2000HA Software V300R001C00SPC608 AGD_OPE V1.1, CC Huawei SUN2000HA Software V300R001C00SPC608 AGD_PRE V1.1, SUN2000HA V300R001C00 Communication Matrix 02 and SUN2000-(175KTL-H0, 185KTL-INH0, 185KTL-H1) MODBUS Interface 03) can be downloaded from the Huawei's support website:

https://support.huawei.com/enterprise/en/digital-power/sun2000ha-pid-21785801/software/254406651?idAbsPath=fixnode01%7C9452479%7C21439560%7C7921563%7C21102414%7C21785801

To download the software, you need to have a Huawei account of the support website first, and please register an account role with download permission. To obtain a register account, you have to contact Huawei Customer Service via email (e.support@huawei.com)

The associated Guidance documentation can be downloaded from Huawei's support website :

- SUN2000-(175KTL-H0, 185KTL-INH0, 185KTL-H1) Series User Manual 13 [UM]: https://support.huawei.com/enterprise/en/doc/EDOC1100226116?idPath=9452479%7C21439560%7C7921563%7C21102414%7C21571652

- FusionSolar App and SUN2000 App User Manual 02 [APP]: https://support.huawei.com/enterprise/en/doc/EDOC1100096889?idPath=9452479%7C21439560%7C7921563%7C21102414%7C21571652

Note: Although the SUN2000HA V300R001C00 Open_Source_Software_Notice is delivered in the package; it is not part of the TOE scope. This document is delivered because of internal obligations from Huawei.

Table 1-2 List of Delivery Items

Type	Delivery Item	Version	Format	SHA256
Software	SUN2000HAV300R001C00SPC608_package.zip	V300R001C00SPC608	.zip	74ccda90f7a5632a5441119da9ee5a99f341d220c6fac92eabcee87b925f8be5
Software Signature File	SUN2000HAV300R001C00SPC608_package.zip.asc	-	.asc	NA
Guidance	SUN2000-(175KTL-H0, 185KTL-INH0, 185KTL-H1) Series User Manual.pdf	13	pdf	1a700bd3d2f279960414e861d2f5f1b0a8335cf3e0f471a24ba0e

				6175d05b90c
Guidance	FusionSolar App and SUN2000 App User Manual	02	pdf	09190b4b27db2ee653863d5dc49c3b3f8283e6f27aeea7a6e30d6915e37dbd58
Document	CC Huawei SUN2000HA Software V300R001C00SPC608 AGD_OPE	1.1	pdf	1f740fafd3155714ae0e29ca676878782219886f8db3ca0c9c6f3bf0352b309d
Document	CC Huawei SUN2000HA Software V300R001C00SPC608 AGD_PRE	1.1	pdf	6acc9312d0d92fef359c9b9ba1931d3517a92bc52f3a86dc55232c8c081d4301
Document	SUN2000-(175KTL-H0, 185KTL-INH0, 185KTL-H1) MODBUS Interface Definitions	03	.pdf	a4a26a0535d4f11f3c3cff9d818f94f7864d3f22a426c225ac87e6722b9bad14
Document	SUN2000HA V300R001C00 Communication Matrix	02	.xls	28c28057f9d678e702cc2a9fb969b3eec8f50a800b5c2b4c1d81a5da23747302

1.5.2 Logical scope

The TOE boundary from a security functionality point of view is:

1.5.2.1 Authentication

The TOE authenticates users by user name and password though the MODBUS TCP protocol. The TOE identifies users based on user role and enforces their authentication before granting them access to any TSF functionality. The TOE supports local authentication login which compares the input of the password in the login form of the SUN2000APP with the one stored in the flash memory of the TOE.

The Identification is performed by two means:

The machine to machine interface (MB) works on the RS485 or MBUS port (in the TOE evaluated configuration is used the RS485 port). The communication is performed over the MODBUS-RTU protocol which works in the form of slave/master. When the TOE and the Smartlogger are connected between each other, the identification is performed and the Smartlogger is considered as master and TOE as slave.

In the other way, the identification performed through the SUN2000APP, the user introduces the password of the user role and sent it to the TOE to compare it. If the password are equals, the set of options for such user role is returned. Three user roles can be identified through this interface: Common user, Advanced user and Special user.

1.5.2.2 Authorization

Authorization indicates that devices assign operation authorities to accounts according to their validity.

The TOE controls access by the group-based authorization framework with predefined role groups for management. Four hierarchical access groups (roles) are offered and can be assigned to individual user accounts.

Only authenticated users can set or configure the TOE.

An account is authorized to perform certain operations and is not allowed to perform unauthorized operations. If an account attempts to perform any unauthorized operation, an error message is returned.

1.5.2.3 Auditing

Logs record routine maintenance events of the TOE. Advanced user, special User and Datalogger user can find security vulnerabilities and risks by checking logs. Considering security, the TOE provides logs to record security events and operation events.

Security logs record operation events related to user activities in the management plane (e.g. modification of passwords and login or logout) and all operation instructions in the management plane.

1.5.2.4 Security management

The TOE provides four access roles: three different user roles (Common user, Advanced user and Special user) accessed by the SUN2000 APP and one machine to machine interface role DataLogger user. This security configuration includes: user password management, software upgrade, log exports and time settings.

1.5.3 Evaluated Configuration

The TOE (Huawei SUN2000HA Software V300R001C00SPC608) only has one mode of operation and therefore, there is only one TOE configuration.

The environment for TOE comprises the following components:

-User’s mobile phone (user mobile phone must be Huawei phone), that used by installer or maintainers to connect to USB external USB-WIFI Adapter stick, to communicate with the TOE.
- The USB-WIFI Adapter stick is inserted into the inverter USB connector when working.
-Mobile phone app SUN2000, that can be download from Huawei app store.
-Local SmartLogger connected to SUN2000HA using MBUS or RS485 with Modbus-RTU protocol.

Table below lists the requirement and main information about the TOE evaluated configuration:

Table 1-3 List of items in the evaluated configuration

Item	Module type	Requirement
TOE	SW	Huawei SUN2000HA Software V300R001C00SPC608
SUN2000HA inverter	SUN2000HA 185KTL-H1	Note: SUN2000HA 185KTL-H1, SUN2000HA 175KTL-H0 and SUN2000HA 185KTL-INH0 are the same series inverter.
Mobile phone	Huawei Mobile phone	Operating system: android 10.
Mobile phone app	SUN2000APP	Software version: 3.2.00.016
USB-WIFI Adapter stick	USB-Adapter2000- C	
Remote Manager System PC	Desktop PC	Web browser: Firefox 78.14.0esr
Security Firewall	Firewall	
SmartLogger	SmartLogger3000	Software version:V300R001C00SPC605

The TOE in its operational environment diagram please refer to the diagram in section 1.4.3 .

2 CC Conformance Claims

2.1 CC Conformance Claim

The version of CC is 3.1R5.

This ST is CC Part 2 conformant and CC Part 3 conformant.

This ST is EAL3 conformance as defined in CC Part 3, with the assurance level of EAL3 Augmented with ALC_FLR.2.

No conformance to a Protection Profile is claimed.

3 Security Problem Definition

3.1 Asset

The assets to be protected are the information stored, processed or generated by the TOE. Including below:

Table 3-1 Description of asset

Asset	Description
A1.Stored configuration data	The integrity and confidentiality of the stored configuration data should be protected. Configuration data includes the security related parameters under the control of the TOE (user account information and passwords, audit records, software package).
A2. In transit configuration data	The integrity and confidentiality of the configuration data when travelling in the WIFI network.
A3. Wired transit configuration data	The integrity and confidentiality of the configuration data when travelling in the management network.

3.2 Threats Agent

This section describes the threats agent from expertise, resources, opportunity and motivation aspects.

Table 3-2 List of threats agent

Agent	Description
Wifi Network attacker	An unauthorized agent who is connected to the Wireless network.
Management Network attacker	An unauthorized agent who is connected to the Management network.

3.3 Threats

This section specifies the threats that are addressed by the TOE and the TOE environment.

As a result, the following threats have been identified:

a) Threats from network attacker

Table 3-3 Threat: T1.UnauthenticatedAccess

Threat: T1.UnauthenticatedAccess	
Adverse Action	An attacker bypass the login authentication and gain access to the TOE in order to read and modify TOE configuration data.
Asset	A1.Stored configuration data
Threat Agent	Wifi Network Attacker Management Network attacker

Table 3-4 Threat: T2. CommunicationTampering

Threat: T2. CommunicationTampering	
Adverse Action	An attacker in the network gains access to the WiFi communication network between the TOE and SUN2000 mobile application, violating the confidentiality and integrity.
Asset	A2. In transit configuration data
Threat Agent	Wifi Network attacker

Table 3-5 Threat: T3. ManagementNetworkTampering

Threat: T3. ManagementNetworkTampering	
Adverse Action	An attacker in the management network gains access to the wired management network through the communication between the SmartLogger and Remote Manager System PC, violating the confidentiality and integrity.
Asset	A3. Wired transit configuration data
Threat Agent	Management Network attacker

3.4 Organizational Security Policy

P.AccessControl

The TOE is able to provide user roles with different set of privileges in order to control and restrict the user accessible functions.

3.5 Assumptions

This section specifies the assumptions on the TOE environment that are necessary for the TOE to meet its security objectives.

A.PhysicalProtection It is assumed that the TOE and the TOE environment all items defined in the section 1.4.3 Non-TOE Hardware and Software) are located in the PV plant which is protected against unauthorized physical access. The remote manager system is also located in other secure access facility connected through a network (that is non-protected by the environment) labelled as management network. The management and Wifi networks are accessible from outside the secure access facilities. The SUN2000APP mobile application can only connect via local wifi network. The wifi network scope is not limited to the extension of the secure access facility. Only authorized and trusted users are allowed to enter inside both facilities.

A.Communication It is assumed that the operating system of SUN2000HA inverter (where the TOE is installed) is able to provide secure encryption for the external accessible interfaces. The operating system of SmartLogger device is able to provide secure encryption for the external accessible interfaces.

A.Hardware It is assumed that the underlying hardware of SUN2000HA inverter, which is outside the scope of the TOE, works correctly.

A.TrustworthyUsers The users in charge during the preparative procedures phase, users of the operational environment, the users of the TOE and the user in charge of the remote manager system are not hostile and will follow and abide by the instructions provided by the TOE documentation.

A.Time It is assumed that the underlying OS provides the reliable timestamps to the TOE.

4 Security Objectives

4.1 Security Objectives for the TOE

The following objectives must be met by the TOE:

- **O.Authorization** The TOE shall implement different authorization role that can be assigned to users in order to restrict the functionality that is available to individual users.
- **O.Authentication** The TOE must authenticate users for access. The TOE shall support the authentication of users by local username and password. The authentication mechanisms shall allow identifying users.
- **O.Audit** The TOE shall provide functionality to generate audit records for security-relevant events.
- **O.Security_Management** The TOE shall provide functionality to securely manage security functions provided by the TOE. This includes: user password management**,** software upgrade, log exports and time settings.

4.2 Security Objectives for the Operational Environment

- **OE.PhysicalProtection** The TOE and the TOE environment (all items defined in the section 1.4.3 Non-TOE Hardware and Software) are located in the PV plant which is protected against unauthorized physical access. The remote manager system is also located in a different secure access facility connected through a network (that is non-protected by the environment) labelled as management network (therefore, there are two different secure access facilities). The management and Wifi networks are accessible from outside the secure access facilities. The SUN2000APP mobile application can only connect via local wifi network. The wifi network scope is not limited to the extension of the secure access facility. Only authorized and trusted users are allowed to enter inside both facilities.
- **OE.Communication** The operating system of SUN2000HA inverter (where the TOE is installed) is able to provide secure encryption for the external accessible interfaces. The operating system of SmartLogger device is able to provide secure encryption for the external accessible interfaces.
- **OE.Hardware** The underlying hardware of SUN2000HA inverter shall work correctly.
- **OE.TrustworthyUsers** Those responsible for the installation and operation of the TOE and its operational environment (preparative procedures phase) the users of the TOE and the users in charge of the remote manager system are trustworthy, and well-trained such that they are capable of securely managing the TOE and following the provided guidance.
- **OE.Time** The underlying OS provides the reliable timestamps to the TOE.

4.3 Rationale for Security Objectives

The following table provides a mapping of TOE objectives to threats, showing that each objective is at least covered by one threat.

a) Maps for threats and security objectives

Table 4-1 Maps for threats and security objectives

	T1.UnauthenticatedAccess	*T2. CommunicationTampering*	*T3. ManagementNetworkTampering*	*P.AccessControl*	*A.PhysicalProtection*	*A.Communication*	*A.Hardware*	*A.TrustworthyUsers*	*A.Time*
O.Authorization				X					
O.Authentication	X								
O.Audit	X								
O.Security_Management	X								
OE.Communication	X	X	X			X			
OE.PhysicalProtection	X				X				
OE.Hardware							X		
OE.TrustworthyUsers								X	
OE.Time									X

b) Rationale for security objectives and threats

Table 4-2 Rationale for security objectives and threats

Threat /OSP	**Security Objectives**	**Rationale for Security Objectives**
T1.UnauthenticatedAccess	O.Authentication O.Audit O.Security_Management OE.Communication OE.PhysicalProtection	O.Authentication ensures that only successfully authenticated users can access the TOE. O.Audit ensures that any authentication attempt and any query or modifying of the configuration data is recorded in the audit log. O.Security_Management ensures that the security functions (user password management, software upgrade,.log exports and time settings) are securely managed. OE.Communication ensures that

Threat /OSP	Security Objectives	Rationale for Security Objectives
		the SmartLogger device only provides well-known cryptographic protocols such as TLS v1.2 and v1.3 and ciphersuites are used to protect the management network OE.PhysicalProtection ensures that the TOE and its environment (included the remote management system) are located in the PV plant which is protected against unauthorized physical access.
T2. CommunicationTampering	OE.Communication	OE.Communication ensures that the WiFi network is encrypted ensuring that only uses a WPA2 encryption and a CCMP cipher. The only manner to connect to the WiFi is using a PSK (Pre-Shared Key)
T3. UnwantedNetworkTraffic	OE.Communication	OE.Communication ensures that the SmartLogger device only provides well-known cryptographic protocols such as TLS v1.2 and v1.3 and ciphersuites are used to protect the management network
P.AccessControl	O.Authorization	O.Authorization ensures that different permissions are assigned to different users to restrict the available functionality.

c) Rationale for security objectives and assumptions

Table 4-3 Rationale for security objectives and assumptions

Assumption	Security Objectives	Rationale for Security Objectives
A.PhysicalProtection	OE.PhysicalProtection	OE.PhysicalProtection ensures that the TOE and its environment (included the remote management system) are located in the PV plant which is protected against unauthorized physical access.
A.Communication	OE.Communication	OE.Communication ensure that the OS of the SmartLogger and the OS running in the SUN2000HA inverter

Assumption	Security Objectives	Rationale for Security Objectives
		provide strong encryption.
A.Hardware	OE.Hardware	OE.Hardware ensures that the underlying hardware of SUN2000HA inverter is working correctly.
A.TrustworthyUsers	OE.TrustworthyUsers	OE. TrustworthyUsers ensures that those responsible for the operation of the TOE and its operational environment are trustworthy, and well-trained
A.Time	OE.Time	OE.Time ensures that the underlying OS provides the reliable timestamps

5 Extended Components Definition

This ST defines no extended security functional components. All security functional requirements stated for the TOE are stated in [CC2].

6 Security Requirements for the TOE

6.1 Conventions

The following conventions are used for the completion of operations:

~~Strikethrough~~ indicates text removed as a refinement

(underlined text in parentheses) indicates additional text provided as a refinement.

[Bold text] indicates the completion of an assignment.

[*Italicised and bold text*] indicates the completion of a selection.
Iteration/Identifier indicates an element of the iteration, where Identifier distinguishes the different iterations.

[*Italicised and bold text*] indicates an assignment within a selection

6.2 Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [***not specified***] level of audit; and

c) [Operation logs should cover the following activities in the management plane, including:

(1) Login and logout

(2) Changing user attributes (passwords)

(3) Locking user accounts

(4) Modifying system configuration parameters

(5) Restoring settings of the system

(6) Upgrading software]

Application Note: The start-up and shutdown of the audit functions do not generate an audit record.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

1. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
2. For each audit event type, the following information is included based on the auditable event definitions of the functional components included in the PP/ST, [**source port**].

6.2.1.2 FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to **[*prevent*]** unauthorized modifications to the stored audit records in the audit trail.

6.2.1.3 FAU_STG.3 Action in Case of Possible Audit Data Loss

FAU_STG.3.1 The TSF shall [**roll back the oldest records**] if the audit trail exceeds [**200 records in the operation logs].**

6.2.2 Identification and Authentication (FIA)

6.2.2.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when **[*five*]** unsuccessful authentication attempts occur related to **[user logging in]**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **[*met*],** the TSF shall **[**

1. **the User Identification is locked**
2. **record into audit log]**

Application note: The user name and password must be verified during login. If the verification fails consecutively for five times, and if the interval between each attempt is shorter than 2 minutes,this the user account will be locked for 10 minutes.

6.2.2.2 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: **[**

1. **user role,**
2. **password**
3. **Lock Testing Time Allowable Illegal Access Times]**

6.2.2.3 FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.2.4 FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application note: The user is identified by his user name if he is able to successfully authenticate in the TOE.

6.2.3 User Data Protection (FDP)

6.2.3.1 FDP_ACC.1 Subset Access Control

FDP_ACC.1.1 The TSF shall enforce the **[Access Control SFP]** on

[Subject: Common user, Advanced user, Special user and Datalogger user;

Objects: accessible functionality and information through the screens of the SUN2000 APP menus and the SmartLogger menus

Operation: read and modify]

6.2.3.2 FDP_ACF.1 Security Attribute Access Control

FDP_ACF.1.1 The TSF shall enforce the **[Access Control SFP]** to objects based on the following:

[Subjects:

Common user,

Advanced user,

Special user,

Datalogger user

Subjects Attributes: role

Object Attributes:

There are no security attributes of the SUN2000 APP menus and the SmartLogger menus governing the operations]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[if a menu is accessed by a user, he will be able to, depending on the privileges described in the user guidance, read and modify the presented configuration.

If not, the user will not be able to read and modify the screen information.]

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**none**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**none**].

6.2.4 Security Management (FMT)

6.2.4.1 FMT_MOF.1 Management of Security Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to [***determine the behavior of***] the functions **[defined in the column Functions of the table 6-1]** to **[the roles defined in the column User Role of the table 6-1]**.

Table 6-1 Management of security functions

User Role	User Name	Functions
Common user	operator	user password management, time settings
Advanced user	engineer	user password management, software upgrade, log exports, time settings
Special user	admin	user password management, software upgrade, log exports
Datalogger user	Datalogger user	software upgrade, log exports

6.2.4.2 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles **[Common user, Advanced user, Special user and Datalogger user].**

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.2.4.3 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: **[user password management, software upgrade, log exports and time settings]**

6.3 Security Functional Requirements Rationale

6.3.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

Table 6-2 Mapping SFRs to objectives

	O.Authorization	O.Authentication	O.Audit	O.Security_Management
FAU_GEN.1			x	
FAU_STG.1			x	
FAU_STG.3			x	
FIA_AFL.1		x		
FIA_ATD.1		x		
FIA_UAU.2		x		
FIA_UID.2		x		
FDP_ACC.1	x			
FDP_ACF.1	x			
FMT_MOF.1	x			x
FMT_SMR.1	x			x
FMT_SMF.1				x

6.3.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives:

Table 6-3 SFR sufficiency analysis

Security objectives	Rationale
O.Authorization	The requirement for access control is spelled out in FDP_ACC.1, and the access control policies are modeled in FDP_ACF.1. Access control is based on the definition of roles as subject and functions as object as defined in FMT_SMR.1 and FMT_MOF.1. There are four user roles: Common user, Advanced user, Special user and Datalogger user.
O.Authentication	User authentication is implemented by FIA_UAU.2, supported by individual user identification in FIA_UID.2. The requirements on necessary user attributes (passwords) are addressed in FIA_ATD.1. The authentication mechanism supports authentication failure handling as addressed in FIA_AFL.1.

O.Audit	The generation of audit records is implemented by FAU_GEN.1. The protection of the stored audit records against unauthorized modification is implemented in FAU_STG.1. If the audit trail exceeds the size of the storage device The TSF shall roll back the oldest records as required by FAU_STG.3.
O.Security_Management	The management functionality for the security functions of the TOE is defined in FMT_SMF.1. The connected user (Common user, Advanced user, Special user and Datalogger user) has access to the security functions described in FMT_SMF.1, which are only accessible to the authorized user (FMT_MOF.1). There are four user roles: Common user, Advanced user, Special user and Datalogger user (FMT_SMR.1)

6.3.3 Security Requirements Dependency Rationale

Dependencies within the EAL3 package selected for the security assurance requirements have been considered by the authors of CC Part 3 and are not analyzed here again.

The security functional requirements in this Security Target do not introduce dependencies on any security assurance requirement; neither do the security assurance requirements in this Security Target introduce dependencies on any security functional requirement.

The following table demonstrates the dependencies of SFRs modeled in CC Part 2 and how the SFRs for the TOE resolve those dependencies.

Table 6-4 Dependencies between TOE security functional requirements

Security Functional Requirement	Dependency	Resolution
FAU_GEN.1	FPT_STM.1	The dependency is covered by the security environmental objective OE.TIME since the necessary timestamps are provided by the OS.
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.1
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_ATD.1	No Dependencies	None
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	No Dependencies	None
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 The TOE does not support the creation of new users. However, the TOE offers an

Security Functional Requirement	Dependency	Resolution
		access control policy for the predefined users and, therefore, the dependency with FMT_MSA.3 is justified.
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	No Dependencies	None
FMT_SMR.1	FIA_UID.1	FIA_UID.2

6.4 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 3 components augmented with ALC_FLR.2, as specified in [CC3]. No operations are applied to the assurance components.

Table 6-5 Security Assurance Requirements

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level
Development	ADV_ARC	1
	ADV_FSP	3
	ADV_TDS	2
Guidance documents	AGD_OPE	1
	AGD_PRE	1
Life-cycle support	ALC_CMC	3
	ALC_CMS	3
	ALC_DEL	1
	ALC_DVS	1
	ALC_FLR	2
	ALC_LCD	1
Security Target evaluation	ASE_CCL	1
	ASE_ECD	1
	ASE_INT	1
	ASE_OBJ	2
	ASE_REQ	2

	ASE_SPD	1
	ASE_TSS	1
Tests	ATE_COV	2
	ATE_DPT	1
	ATE_FUN	1
	ATE_IND	2
Vulnerability assessment	AVA_VAN	2

6.5 Security Assurance Requirements Rationale

The evaluation assurance level 3 augmented with ALC_FLR.2 has been chosen commensurate with the threat environment that is experienced by typical consumers of the TOE.

Dependencies within the EAL package selected (EAL3) for the security assurance requirements have been considered by the authors of CC Part 3 and are therefore not analyzed here.

7 TOE Specification Summary

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

7.1 Authentication

The following SFR are covered by this security functionality: FIA_AFL.1, FIA_ATD.1, FIA_UAU.2, FIA_UID.2

The TOE authenticates users by user name and password though the MODBUS TCP protocol. The TOE identifies users based on user role and enforces their authentication before granting them access to any TSF functionality. The TOE supports local authentication login which compares the input of the password in the login form of the SUN2000APP with the one stored in the flash memory of the TOE.

Identification

The Identification is performed by two means:

The machine to machine interface (MB) works on the RS485 or MBUS port (in the TOE evaluated configuration is used the RS485 port). The communication is performed over the MODBUS-RTU protocol which works in the form of slave/master. When the TOE and the Smartlogger are connected between each other, the identification is performed and the Smartlogger is considered as master and TOE as slave.

In the other way, the identification performed through the SUN2000APP, the user introduces the password of the user role and sent it to the TOE to compare it. If the password are equals, the set of options for such user role is returned. Three user roles can be identified through this interface: Common user, Advanced user and Special user.

7.2 Authorization

The TOE enforces an access control by supporting following functions:

- Support four user roles.
- There are four user roles, including Common user, Advanced user, Special user and Datalogger user. An account is authorized to perform certain operations and is not allowed to perform unauthorized operations. If an account is used to attempt any unauthorized operation, an error message is displayed. The authority of each user is specified in the following table.

Table 7-1 User level and authorized functions

User Role	User Name	Rights
Common user	operator	The accounts of this role are authorized to perform operations, include user password management and time settings.
Advanced user	engineer	The accounts of this role are authorized to perform operations, include user password management, software upgrade, log exports and time settings.
Special user	admin	The accounts of this role are used for security management and are authorized to perform operations, include user password management, software upgrade and log exports.
Datalogger user	Datalogger user	The accounts of this role are used for security management and are authorized to perform operations, include software upgrade and log exports.

The following SFR are covered by this security functionality: FDP_ACC.1, FDP_ACF.1, FMT_MOF.1, FMT_SMR.1.

7.3 Security Management

The following SFR are covered by this security functionality: FMT_MOF.1, FMT_SMF.1, FMT_SMR.1.

7.3.1 User password management

There are four user roles in the TOE: Common user, Advanced user, Special user and Datalogger user.

User password is forced to change when the user login for the first time. Each user’s password (except the Datalogger user) can be changed, and the user can only change its own password.

7.3.2 Software upgrade

Only Advanced user, Special User and Datalogger user are permitted to perform the software upgrade operation.

The software upgrade is performed through the mobile phone application SUN2000 as the role of Advanced user and Special User. User shall obtain the correct upgrade package first and copy it to the desired path of mobile phone. Then start the SUN2000 application and login as the role of Advanced user or Special user, choose menu Maintenance - > Upgrade Device to perform the software upgrade.

In addition, the software upgrade can be performed through the Smartlogger (Datalogger User). The user shall obtain the correct upgrade package first and copy it to a temporal folder in the remote manager system.

Then, in the Smartlogger web, perform a login and choose Maintenance -> Software Upgrade. Later, select the TOE device, upload the software package and click on ‘upload’. Finally, click on software upgrade at the bottom to perform the upgrade.

7.3.3 Log exports

Only Advanced user, Special User and Datalogger user are permitted to perform the Log exports operation.

Start the SUN2000 application and login as the role of Advanced user or Special user, choose menu Maintenance - > Log management to export the logs.

In addition, the logs export can be performed through the Smartlogger (Datalogger User). Log in the Smartlogger web and click on the Maintenance menu. Then, click on ‘Device Log' submenu, Click on the checkbox to select the TOE and click on Export Log. Wait until the export is completed and then click on Log archiving to download the file on the remote manager system.

7.3.4 Time setting

Only Advanced user and Common User are permitted to perform the time setting operation.

Start the SUN2000 application and login as the role of Advanced user or Common user, choose menu Settings - > Time setting to perform time setting operation.

7.4 Auditing

The TOE can provide auditing by means of operation logs (operation logs is the inverter log):

- Auditing is activated automatically at the start of the TOE and cannot be deactivated.
- Auditing shutdown is done automatically when the TOE is powered off (there is no possibility to stop the auditing).
- Support recording security-related configuration operations in the operation logs, including user management, security settings. The security logs provide the information about the user name, source port, timestamp, event type and operation result.
- Common user, Advanced user, Special user are identified in the operation logs as operator, engineer and admin, respectively.
- Datalogger users are identified in the operation logs using the Source port value.
- The operation logs allow no manual changes.
- The operation logs keep records in time sequence. After the memory is exhausted, the oldest stored records will be overwritten by the new records.

The following SFR are covered by this security functionality FAU_GEN.1, FAU_STG.1, FAU_STG.3

8 Abbreviations and References

8.1 Abbreviations

CBC	Cipher-Block Chaining
CC	Common Criteria
CCMP	Counter Mode CBC-MAC Protocol
EMS	Element Management System
EDR	Enhanced Data Rate
LCT	Local Craft Terminal
LE	Low Energy
LED	Light-Emitting Diode
LMT	Local Maintenance Terminal
NMS	Network Management System
MAC	Message Authentication Code
MPPT	Maximum Power Point Tracking
PP	Protection Profile
PPC	Plant Power Controller
PSK	Pre-Shared Key
PV	PhotoVoltaic
RMT	Remote Maintenance Terminal
SACU	Smart Array Controller Unit
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
RSA	Rivest Shamir Adleman
RADIUS	Remote Authentication Dial-In User Service
SCADA	Supervisory Control And Data Acquisition

SFTP	Secure File Transfer Protocol
SSH	Secure Shell
TLS	Transport Layer Security
MSTP	Multi-Service Transmission Platform
SDH	Synchronous Digital Hierarchy
WDM	Wavelength Division Multiplexing
OTN	Optical Transport Network
OSN	Optical Switch Node
SFP	Security Function Policy
UI	User Interface
WPA2	Wifi Protected Access 2

8.2 References

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1, Version 3.1 Revision 5, September 2017

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2, Version 3.1 Revision 5, September 2017

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3, Version 3.1 Revision 5, September 2017

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1 Revision 5, September 2017