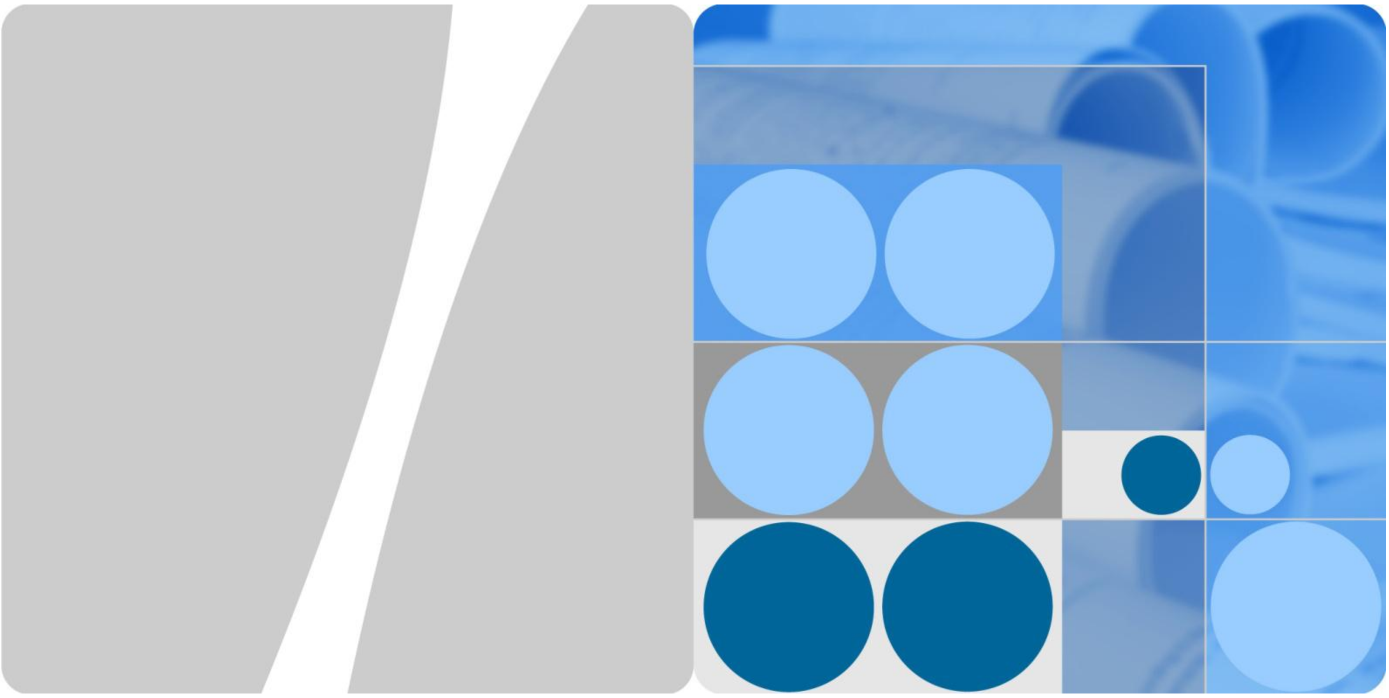


CC Huawei ECC800 V100R021C00SPC100

Security Target

Issue	1.3
Date	2021-03-04

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 Security Target is for the evaluation of ECC800 V100R021C00SPC100 software management component, consisting of application software.

Change History

Changes between document issues are cumulative. The latest document issue contains all the changes made in earlier issues.

Date	Version	Change Description	Author
2019-05-10	1.00	Completed the draft.	Yang Xiaohui, Zhang Zhao, Hu Keshi, Zong Chao, Ye Jiheng
2019-11-10	1.01	Update by review	Hu Wentian, Zhang Zhao
2020-06-04	1.02	Update by review	Zhang Zhao
2020-06-05	1.03	Update by internal review	Zhang Zhao
2020-06-20	1.04	Change section 4.2 “The operational environment shall provide segregation by deploying the management interface in TOE into an independent local network.” to “The operating environment should separate the local network of the TOE from the Internet.”	Zhang Zhao
2020-06-27	1.05	Update by review	Li Chen Zhang Zhao
2020-09-02	1.06	Update by review	Zhang Zhao
2020-11-22	1.07	Update by review	Li Chen Zhang Zhao
2020-12-05	1.08	Update by review	Li Chen Zhang Zhao
2020-12-10	1.1	Update by review	Zhang Zhao

Date	Version	Change Description	Author
2020-12-24	1.2	Update by review	Zhang Zhao
2021-03-04	1.3	Update by review	Zhang Zhao

Contents

Figures

Tables

1 Introduction

This Security Target is for the evaluation of ECC800 V100R021C00SPC100 software management component, consisting of application software. The software is part of ECC800-Pro chassis.

1.1 ST Identification

Title: CC Huawei ECC800 V100R021C00SPC100 Security Target

Version: 1.3

Date: 2021-03-04

Developer: Huawei Technologies Co., Ltd.

1.2 TOE Identification

Name: ECC800 software management component

Version: V100R021C00SPC100

Developer: Huawei Technologies Co., Ltd.

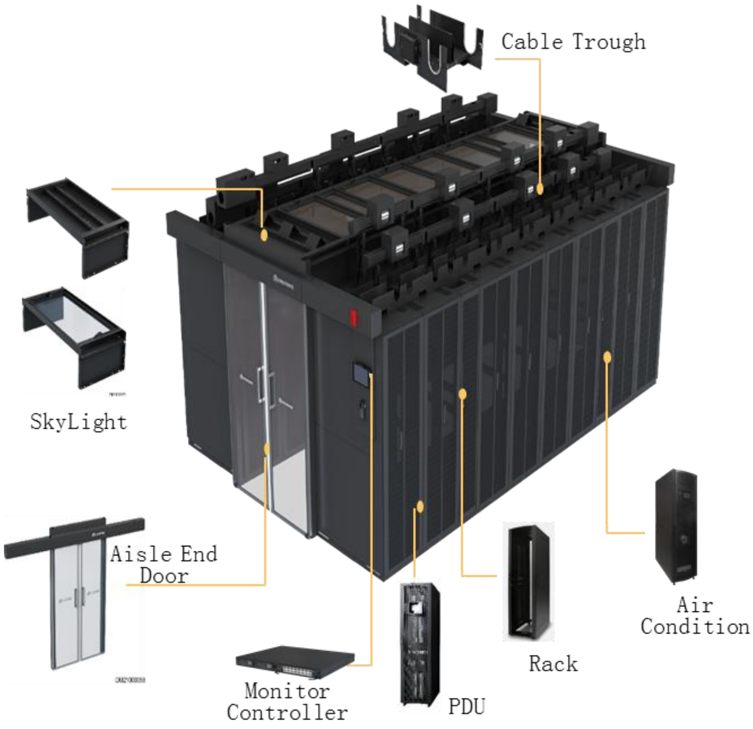
The target of evaluation (TOE) is the ECC800 software which is running on the ECC800-Pro chassis. The TOE only consists of the application software as described in the following chapters and is referred as ECC800 software management component in this ST.

1.3 Product Overview

Data center is a building or portion of a building whose primary function is to house a computer room and its support areas. The smart modular data center is an edge data center solution that is applicable to small and medium data centers.

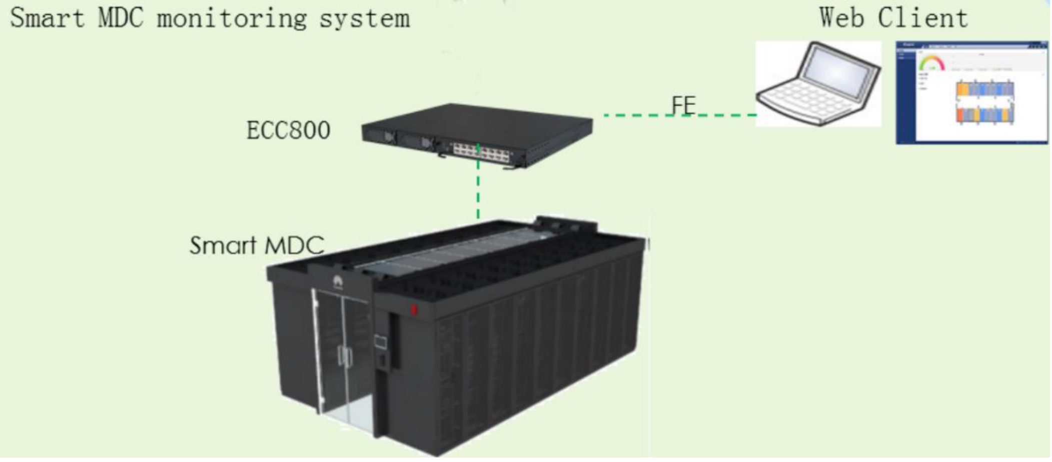
The smart modular data center integrates power supply and distribution, cooling, cabinet aisle, cabling, and monitoring into one module to meet the requirements for fast delivery and on-demand deployment.

Figure 1-1 Smart modular data center overview



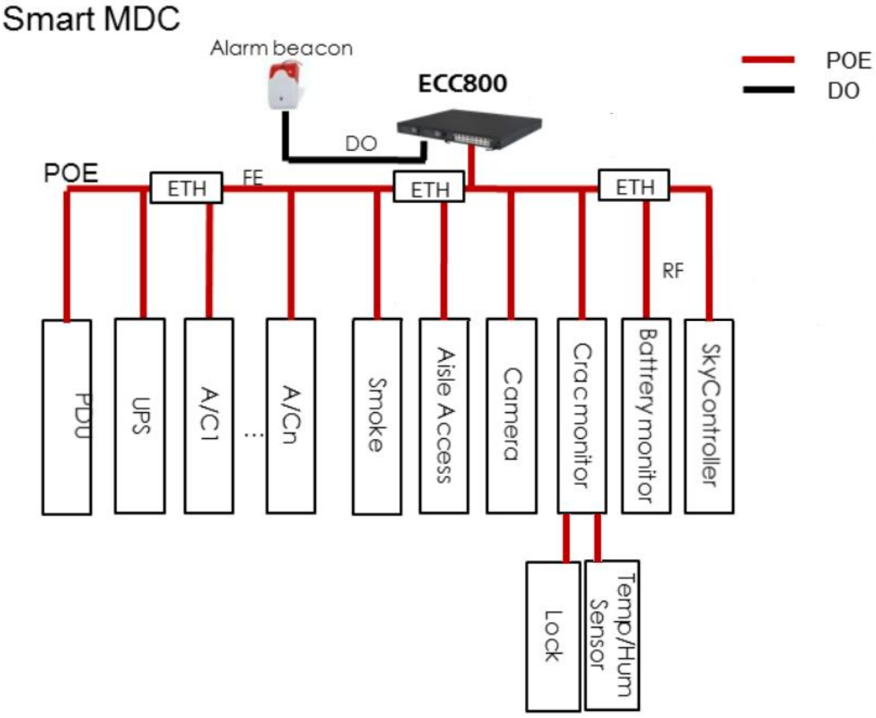
The ECC800-Pro is the monitoring and management unit for the smart modular data center. It centrally monitors the PDUs, air conditioners, environment, and actuators inside the smart module.

Figure 1-2 Position of the monitor controller on the smart modular data center



Each smart modular data center provides an independent and integral environment and power monitoring interface. This interface constantly monitors devices such as the power supply and distribution equipment, UPS, smart cooling products, temperature and humidity sensors, water sensors, smoke sensors, and video surveillance equipment inside the module.Historical data and alarm events are recorded.

Figure 1-3 Logical networking of the smart modular data center monitoring system



The power distribution units (PDUs), air conditioners, sensors (such as smoke and water sensors) in the smart module are connected to the ECC800-Pro over the FE, RS485, and DI ports. The ECC800-Pro performs centralized management for the smart module. The ECC800-Pro supports the following functions:

- Temperature and humidity monitoring: Detects and collects statistics on the ambient temperature and humidity inside the smart module.
- Smoke monitoring: Detects smoke in the smart module and provides real-time alarm signals.
- Power distribution monitoring:
  a. Detects and collects statistics on the total input phase voltage, current, frequency, power factor, electric energy, active power, apparent power, load rate and cabinet interior busbar temperature for the smart module.
  b. Detects the current, electric energy, switch status, contact temperature, and load rate of the IT and smart cooling product power distribution branches; collects statistics on electric energy by month or year.
- Smart cooling product monitoring:
  a. Monitors the supply and return air temperature and humidity in real time.
  b. Configures the supply air temperature set point in a unified manner, without the need to separately configure it for each smart cooling product.
  c. Monitors and displays the fan speed, and displays the running percentage.
  d. Displays the cooling load rate.
  e. Monitors and displays the compressor running status.
  f. Provides reminders on regular air filter replacement.

g. Displays the real-time running status of the heating and humidifying.

- Video surveillance: Connects to three cameras and provides PoE power supply;

1.4 TOE Overview

1.4.1 TOE Type

The ECC800 software is a software product running on the Linux operating system based on the ARM chip of the Cortex-A7 architecture. In the northbound direction, the ECC800 software provides web-based login for connecting to manage the TOE.

In the southbound direction, the ECC800 controller collects and configures signals, and manages alarms for southbound components.

1.4.2 TOE usage and major security features

The TOE is a software to manage and monitor devices inside the smart module data center (Smart MDC). It provides a web interface (WebUI) that allow users to operate with the TOE in order to change values and parameters.

The TOE provides the following key security features:

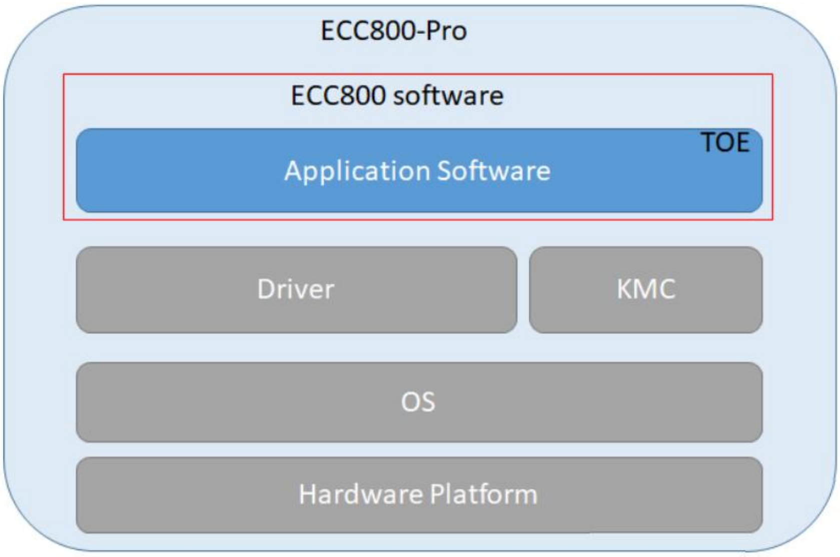
- **Authentication and Authorization:** Only authenticated users are allowed to log in to the TOE, query TOE data, and set TOE parameters. Only authorized users are able to execute the previous actions based on their privileges. If a user fails to be authenticated for multiple consecutive times, the user is locked to prevent unauthorized access.
- **Auditing:** An operation log records the operation that a local administrator has performed on the system and the result of the operation and is used for tracing and auditing. Only authorized local administrators can review and query the records.
- **Management:** The TOE provides two different user roles (administrator and operator). Also, the TOE provides the functionality to manage: time settings, user configuration, updates and logs export.
- **TOE Access:** The TOE is able to manage the concurrent multiple sessions by limiting the number of active sessions per user. The TOE is also able to terminate an interactive session after an inactivity period of time.

1.4.3 Non-TOE Hardware and Software

The TOE environment consists of the following components:

- The TOE runs on the hardware chassis ECC800-Pro with the appropriate TOE environment software:

Figure 1-4 TOE constitution

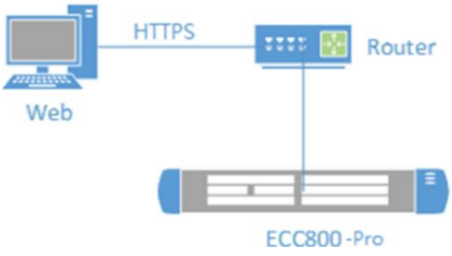


- The OS is: Linux version 4.19.90.
- OpenSSL: installed in the OS, OpenSSL provides encryption functionality for secure channels.
- The KMC is Encryption and decryption security component provided by Huawei.

  The Key Management CBB (KMC) is an independent key management component that provides secure encryption for internal data and certificate maintenance.
- The administrator uses a remote PC to connect to the TOE through the Hypertext Transfer Protocol Secure (HTTPS) secure channel to access the web interface.

  Supported web browsers: Firefox 52, Chrome 58 and IE9 or above.

Figure 1-5 The TOE in its operational environment



1.5 TOE Description

1.5.1 Evaluated Configuration

The TOE was evaluated using the following physical platform:

- Hardware: ECC800-Pro version
- OS: RTOS based on Linux 4.19.90

- KMC version 3.0.0.5.2.
- OpenSSL version 1.1.1f

Other software:

- The web browser version depends on the PC. For better user experience, you are advised to use Firefox 52, Chrome 58, or Internet Explorer 11

1.5.2 Physical scope

The TOE is a 'software only', TOE consists of the application software, but not the underlying OS and hardware, which the application software is running on.

The software package (along with its signature file) and the guidance documentation are delivered in the support website https://support.huawei.com/carrier/ under the path “Carrier Software >> Data Center Integration Solution >> Data Center Facility >> ECC800”.

To TOE documentation is public and can be downloaded once a user has created a Huawei account in the webpage. The steps required to download the TOE software are described in the TOE documentation.

Table 1-1 Physical scope

Type	Delivery Item	Version	Format	SHA256
Software	The package downloaded from the website is: ECC800V100R021C00SPC100.zip The TOE is a software included within the mentioned package and named as: ECC800V100R021C00SPC100.tar.gz	V100R021C00SPC100	Package: zip TOE: tar.gz	ECC800V100R021C00SPC100.zip: eaf076a0e9f8b9ae7bc39bdb3bfa5133beba062d3d4648b6d392d06966d7f41a ECC800V100R021C00SPC100.tar.gz: 12fa92e9cbeb1c1f2d13651b3d7070eb7b6a7032180a52591e8a8f420623bd50
Software Signature File	ECC800V100R021C00SPC100.zip.asc	-	.asc	-
Product Guidance	ECC800 Data Center Controller V100R021C00 User Manual (for ECC800-Pro).pdf	0.2	PDF	75b8ae894dab955d4e5a4da1652792f636b5cddd062f85ab80d8469438e1fae6
	CC Huawei ECC800 V100R021C00SPC100–AGD_OPE V1.8	1.8	PDF	06469a8bcf85f3c0b0328badfbfd4fe6fdf6a00a5cdd4285f1f908e1bbaed622
	CC Huawei ECC800 V100R021C00SPC100–AGD_PRE V1.7	1.7	PDF	2fc6d311b1e259eaba695e8364b011d0629b5d2011693af1d936baca16ddb19b

1.5.3 Logical scope

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

1.5.3.1 Authentication

The TOE authenticates users based on user names and passwords.

The TOE provides the local authentication mode. The user names and passwords are stored on the local device. During login, the local user names and passwords stored on the local device are used for authentication. When a user logs in to the web interface, the user is prompted to change the default password. In addition, password brute force defense mechanism, and automatic logout upon timeout are supported.

1.5.3.2 Authorization

The TOE group-based authorization mechanism is used to manage access based on predefined role groups. The TOE provides two levels of user groups that can be assigned to user accounts.

Only authenticated users can perform TOE command operations supported by the users' rights. Only one user group level can be assigned to a user account. Therefore, the user group level of the user is clear at any time.

Accounts are managed by group. Each group represents specific rights assigned to accounts in the group. Table 1-2 lists the groups and their definitions. For example, the accounts in the administrator group have rights to perform all security management and advanced settings operations. Unauthorized operations are not allowed.

Table 1-2 Groups of accounts

Group	Rights
Operator	The accounts of this group are primarily authorized to query the system information.
Administrator	The accounts of this group are used for security management and are authorized to perform all query and configuration operations.

1.5.3.3 Auditing

Logs record the routine maintenance events of the TOE. The administrator can view logs to find security vulnerabilities and risks.

Logs record operation events related to account management and system configuration, such as changing a password, adding an account, changing a device IP addresses, and other configuration operations.

1.5.3.4 TOE Access

The TOE uses the following mechanisms to protect devices against network attacks. A maximum of three users can log in to the web page concurrently. Also the TOE is able to terminate interactive sessions and present appropriate warnings

1.5.3.5 Security management

The TOE provides the functionality to manage user configuration, time settings, updates and logs export. The TOE provides two different user roles (administrator and operator). Only the administrator is able to manage most of the TOE functions, for instance, add and delete user accounts. However, the operators can modify some of their own attributes and also time settings.

2 CC Conformance Claims

2.1 CC Conformance Claims

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

The CC version of [CC] is Version 3.1, Revision 5.

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 by the TOE are the following one:

Table 3-1 Description of asset

Asset	Description
A1.Audit data	Audit records composed of the TOE management and user operations
A2.System data	The internal data stored by the TOE (other than security events) including configuration parameters.

3.2 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:

T. Information Disclosure

Threat agent: Non-TOE user

Asset: integrity of A1. Confidentiality and integrity of A2

Adverse action: TOE data is read or modified by unauthenticated personnel.

T. Concurrency

Threat agent: TOE user with administration privileges

Asset: integrity of A2.

Adverse action: several TOE users with administrative privileges managing the TOE at the same time could lead in configuration errors.

T. Undetected

Threat agent: Non-TOE user

Asset: integrity of A2.

Adverse action: external agents cause configuration errors that are not detected or recorded in the operation log.

3.3 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.

3.4 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 (the ECC800-Pro chassis and all the devices of the monitored data center) are protected against unauthorized physical access. Only the management network is physically accessible from outside the secure access facility. Only authorized and trusted personnel is allowed to enter inside the facility.

A.LogicalProtection

It is assumed that the TOE is prepared and configured in order to restrict the access to all its logical interfaces during the operation except for the web management interface.

A.Security

The system where the TOE is installed is able to provide secure encryption for the external interfaces accessible for attackers.

A.NoEvil
The users in charge of the preparative procedures and the user of the TOE are not hostile and will follow and abide by the instructions provided by the TOE documentation.

A.Hardware
It is assumed that the underlying hardware of ECC800-Pro, which is outside the scope of the TOE, works correctly.

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 their functionality.
- **O.Authentication**
  The TOE must authenticate users for access.
- **O.Audit**
  The TOE shall provide functionality to generate audit records for security-relevant administrator actions.
- **O.TOEAccess**

  The TOE shall provide functionality to control the user session establishment.
- **O.SecurityManagement**
  The TOE shall provide functionality to securely manage security functions provided by the TOE. This includes:
  1. User management, including the user name and passwords.
  2. Back ups and updates
  3. Logs export
  4. Time settings

4.2 Security Objectives for the Operational Environment

- **OE.PhysicalProtection**
  It is assumed that the TOE and the TOE environment (the ECC800-Pro chassis and all the devices of the monitored data center) are protected against unauthorized physical access. Only the management network is physically accessible from outside the secure access facility. Only authorized and trusted users is allowed to enter inside the facility.
- **OE.LogicalProtection**

  It is assumed that the TOE is prepared and configured in order to restrict the access to all its logical interfaces during the operation except for the web management interface.

- **OE.Security**

  The system where the TOE is installed is able to provide secure encryption for the external interfaces accessible for attackers.
- **OE.NoEvil**
  The users in charge of the preparative procedures and the TOE users are not hostile, and will follow and abide by the instructions provided by the TOE documentation.
- **OE.Hardware**
  The underlying hardware of ECC800-Pro shall work correctly.
- **OE.Time**

  It is assumed that 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 and environmental objectives to threats and organizational security policies, showing that each threat or OSP is at least covered by one objective.

Table 4-1 Mapping objectives to threats

Threat	Security Objectives	Rationale for Security Objectives
T. Information disclosure	**O.Authentication** **O.SecurityManagement** **O.Audit** **OE.Security**	Only authenticated and identified users can access the TOE. **O.Authentication** The user authentication data can be managed by the TOE **O.SecurityManagement** Login and logout attempts are recorded in the TOE Logs. **O.Audit** The management interface where the assets are transmitted is securely encrypted. **OE.Security**
T. Concurrency	**O.TOEAccess** **O.SecurityManagement** **O.Audit**	The TOE provides countermeasures in order to avoid uncontrolled user session establishment leading in concurrency issues **O.TOEAccess** The administrator can configure the timeout duration when an unused interactive session is terminated. **O.SecurityManagement** Management security events are recorded in the TOE logs. **O.Audit**
T. Undetected	**O.Audit**	The security event on the management

Threat	Security Objectives	Rationale for Security Objectives
	O.SecurityManagement	interface are logged. **O.Audit** Time settings management is provided by the TOE **O.SecurityManagement**
P.AccessControl	**O.Authorization** **O.SecurityManagement**	Only authorized users can access perform some management operations. **O.Authorization** The user authorization is provided and can be managed by the TOE. **O.SecurityManagement**

The following table provides a mapping of the objectives for the operational environment to assumptions showing that each assumption is at least covered by one objective.

Table 4-2 Mapping objectives for the environment to assumptions

Environmental Objective	Assumption
OE.PhysicalProtection	OE.PhysicalProtection directly upholds assumption A.PhysicalProtection.
OE.LogicalProtection	OE.LogicalProtection directly upholds assumption A.LogicalProtection
OE.Security	OE.Security directly upholds assumption A.Security
OE.NoEvil	OE.NoEvil directly upholds assumption A.NoEvil
OE.Hardware	OE.Hardware directly upholds assumption A.Hardware
OE.Time	OE.Time directly upholds assumption A.Time

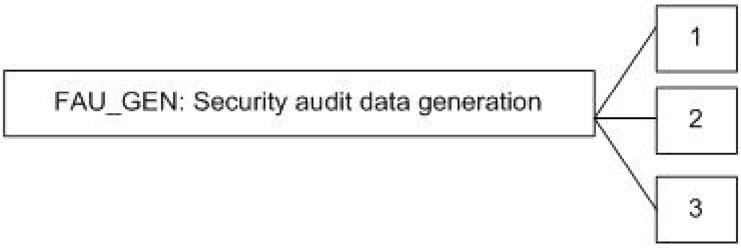
5 Extended Components Definition

5.1 FAU_GEN_EXT.3 Simplified audit data generation

Family behaviour

This Security Target introduces one extended component: FAU_GEN_EXT.3 Simplified audit data generation. This component is a simplified version of FAU_GEN.1 and is therefore a suitable member of the FAU_GEN family. It was added to remove the need to log start and stop of auditing and to simplify the requirement.

Component levelling



FAU_GEN.1 Audit data generation defines the level of auditable events, and specifies the list of data that shall be recorded in each record.

FAU_GEN.2 User identity association, the TSF shall associate auditable events to individual user identities.

FAU_GEN_EXT.3 Audit data generation defines the level of auditable events, and specifies the list of data that shall be recorded in each record but it does not require to log start and stop of auditing.

Management: FAU_GEN.1, FAU_GEN.2, FAU_GEN_EXT.3

There are no management activities foreseen.

Audit: FAU_GEN.1, FAU_GEN.2, FAU_GEN_EXT.3

There are no auditable events foreseen.

FAU_GEN_EXT.3 Simplified audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN_EXT.3.1 The TSF shall be able to generate an audit record of the following auditable events: [assignment: defined auditable events].

FAU_GEN_EXT.3.2 The TSF shall record within each audit record: Date and time of the event, [assignment: other information about the event].

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.

6.2 Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN_EXT.3 Simplified Audit Data Generation

FAU_GEN_EXT.3.1 The TSF shall be able to generate an audit record of the following auditable events:

(1) **Login and logout**

(2) **Adding and deleting users, and changing user attributes (roles and passwords)**

(3) **Locking and unlocking user accounts by administrators**

(4) **Changing user role groups**

(5) **Changing the system security configuration:**

  a) **Timeout duration until an interactive session is terminated**

  b) **Exporting Operationg Logs**

  c) **Disabling upgrade package signature verification**

(6) **Restoring of the system**

FAU_GEN_EXT.3.2 The TSF shall record within each audit record: Date and time of the event, **event type, name of the accessed resource, user name**.

6.2.1.2 FAU_GEN.2 User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that causes the event.

6.2.1.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide **users of the Administrator group** with the capability to read **all information** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Application note: the TOE provides different logs where the events are recorded. All the events generated by FAU_GEN_EXT.3 are recorded in the log "operation log". The audit review only applies to the operation log.

6.2.1.4 FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users who have been granted explicit read-access.

Application note: the TOE provides different logs where the events are recorded. All the events generated by FAU_GEN_EXT.3 are recorded in the log "operation log". The restricted audit review only applies to the operation log.

6.2.1.5 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.

Application note: the TOE provides different logs where the events are recorded. All the events generated by FAU_GEN_EXT.3 are recorded in the log "operation log". The protection of the audit trail storage only applies to the operation log.

6.2.1.6 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 **20000.**

Application note: the TOE provides different logs where the events are recorded. All the events generated by FAU_GEN_EXT.3 are recorded in the log "operation log". The action in case of possible audit data loss only applies to the operation log.

6.2.2 User Data Protection (FDP)

6.2.2.1 FDP_ACC.1 Subset Access Control

FDP_ACC.1.1 The TSF shall enforce the **User Group SFP** on

Subject: users;

Objects: accessible functionality and information through the windows of the Web interface

Operation: read, delete, add and modify

6.2.2.2 FDP_ACF.1 Security Attribute based Access Control

FDP_ACF.1.1 The TSF shall enforce the **User Group SFP** to objects based on the following:

Users security attributes

- **user role**

Web interface windows information attributes:

- **There are no security attributes of the web interface windows information 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 web window is accessed by a user, he will be able to, depending on the privileges described in the user guidance, read/delete/add/modify the presented configuration. If not, the user will not be able to read, delete, add or modify the window 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**.

6.2.3 Identification and Authentication (FIA)

6.2.3.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when ***five*** unsuccessful authentication attempts occur (and the interval between two attempts is shorter than five minutes) related to **user logging in**.

1. FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been ***met***, the TSF shall **Lock user identification for 5 minutes.**

6.2.3.2 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 name**
2. **account validity period**
3. **access right**
4. **password**
5. **password validity period**
6. **the inactivity time which an account is automatically logged out (timeout internal).**
7. **online status of the account (locked/unlocked)**

6.2.3.3 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.

6.2.3.4 FIA_UAU.6 Re-authentication

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions **for some important operations, which are listed as follows:**

User management

Restoring factory settings

Setting the system type

Monitor reset

6.2.3.5 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.

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*** all the functions **defined in FMT_SMF.1** to **users of the Administrator group**.

Application note: except for the "Timeout duration until a interactive session is terminated" and "Time settings". Each user (operator or administrator) can determine the behavior of the time settings and its own timeout duration.

6.2.4.2 FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the **User Group SFP** to restrict the ability to ***query, modify*** the security attributes **user role** to the **users of the Administrator group**.

6.2.4.3 FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the **User Group SFP** to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow **users of the Administrator group** to specify alternative initial values to override the default values when an object or information is created.

6.2.4.4 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

1. **User management: add, delete, lock and unlock users. Modify user passwords and roles.**
2. **Timeout duration until a interactive session is terminated.**
3. **Exporting Operation Logs**
4. **Disabling Upgrade Package Signature Verification**
5. **Time and date settings**

6.2.4.5 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles **Administrator and Operator**.
FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.2.5 TOE access (FTA)

6.2.5.1 FTA_MCS.1 Limitation on multiple concurrent sessions

FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of **1** sessions per user.

Application note: Concurrently, each user can keep only one valid session.

6.2.5.2 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after **10 minute period of inactivity or a 300000 minute maximum session period has been reached**.

Application note:

A user of the Administrator group can set the timeout duration of 10–300000 minutes on the WebUI (10 minutes by default).

6.2.5.3 FTA_SSL.4 User-initiated Termination

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own session.

6.2.5.4 FTA_TSE.1 TOE session establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on **the number of locked users and the number of online users**.

Application note:

1. After an administrator locks a non-administrator user on the WebUI, the user is not allowed to log in to the system.
2. After the maximum number of online users reaches 3 on the WebUI, the login is rejected.

6.2.5.5 FTA_TAB.1 Default TOE Access Banners

FTA_TAB.1.1 Before establishing a user session, the TSF shall display a warning message regarding use of the TOE.

Application note:

1. When a user logs in to the WebUI for the first time, the system prompts the user to change the password immediately.
2. After the password of a user expires on the WebUI, the user is forced to change the password after login.

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 6-1 Mapping SFRs to objectives

Security Functional Requirements	Objectives
FAU_GEN_EXT.3	O.Audit
FAU_GEN.2	O.Audit
FAU_SAR.1	O.Audit
FAU_SAR.2	O.Audit
FAU_STG.1	O.Audit
FAU_STG.3	O.Audit
FDP_ACC.1	O.Authorization
FDP_ACF.1	O.Authorization
FIA_AFL.1	O.Authentication
FIA_ATD.1	O.Authentication
FIA_UAU.2	O.Authentication
FIA_UAU.6	O.Authentication
FIA_UID.2	O.Authentication
FMT_MOF.1	O.SecurityManagement
FMT_MSA.1	O.SecurityManagement
FMT_MSA.3	O.SecurityManagement
FMT_SMF.1	O.SecurityManagement
FMT_SMR.1	O.SecurityManagement
FTA_MCS.1	O.TOEAccess
FTA_SSL.3	O.TOEAccess
FTA_SSL.4	O.TOEAccess
FTA_TSE.1	O.TOEAccess
FTA_TAB.1	O.TOEAccess

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 6-2 SFR sufficiency analysis

Security objectives	Rationale
O.Audit	The generation of audit records is implemented by FAU_GEN_EXT.3. Audit records are supposed to include user identities as defined in FAU_GEN.2 where applicable. Requirements on reading audit records are defined in FAU_SAR.1 and FAU_SAR.2. 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.Authentication	User authentication is implemented by FIA_UAU.2, and re-authentication is implemented by FIA_UAU.6, 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.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 two hierarchical user groups (from low to high): operator, administrator.
O.SecurityManagement	The management functionality for the security functions of the TOE is defined in FMT_SMF.1. The administrator user and operators have the security functions described in FMT_SMF.1 and some of them are invisible to the operator user (FMT_MOF.1) There are two hierarchical user groups (from low to high): operator, administrator (FMT_SMR.1) Requirements on the management functionality for the definition of access control policies are provided in FMT_MSA.1 and FMT_MSA.3.
O.TOEAccess	Multiple concurrent sessions are limited by FTA_MCS.1. The TSF is able to terminate suspended interactive sessions in FTA_SSL.3, also users can terminate their own sessions in FTA_SSL.4. The TOE is able to display warning messages in FTA_TAB.1. Based on the number of locked users and online users the TOE is able to deny session establishment in FTA_TSE.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 6-3 Dependencies between TOE security functional requirements

Security Functional Requirement	Dependency	Resolution
FAU_GEN_EXT.3	FPT_STM.1	The dependency is covered by the security environmental objective OE.TIME since the necessary timestamps are provided by the OS.
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN_EXT.3 The requirements of FAU_GEN.2 apply to the event logs generated in FAU_GEN_EXT.3 FIA_UID.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN_EXT.3 The requirements of FAU_GEN.2 apply to the event logs generated in FAU_GEN_EXT.3
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN_EXT.3 The requirements of FAU_GEN.2 apply to the event logs generated in FAU_GEN_EXT.3
FAU_STG.3	FAU_STG.1	FAU_STG.1
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_ATD.1	No Dependencies	None

Security Functional Requirement	Dependency	Resolution
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UAU.6	No Dependencies	None
FIA_UID.2	No Dependencies	None
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FMT_SMF.1	No Dependencies	None
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FTA_MCS.1	FIA_UID.1	FIA_UID.2
FTA_SSL.3	No Dependencies	None
FTA_SSL.4	No Dependencies	None
FTA_TSE.1	No Dependencies	None
FTA_TAB.1	No Dependencies	None

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 [CC] Part 3. No operations are applied to the assurance components.

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.

7 TOE Summary Specification

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

7.1 Authentication

When a local user logs in to the TOE web page, a user name and password are requested to verify his identity before the access is given.

Table 7-1 SFR to TSF mapping

SFR	TSF
FIA_AFL.1	Support maximum attempts for authentication failures within certain period of time. After 5 consecutive login attempts using one account fail and 5 minutes, the account is locked.
FIA_UAU.6	Support re-authentication when the user performs important operations, such as user management, restoring factory settings, setting the system type and monitor reset.
FIA_ATD.1	Support for user individual attributes including the user name, account validity period, user role (access right), password, password validity period, the inactivity time which an account is automatically logged out (timeout internal) and online status of the account (locked/unlocked).
FIA_UAU.2	The TOE enforces that every user needs to successfully authenticate himself by user name and password before he can use any TOE security function other than the identification and authentication function. The TOE provides one session establishment mechanisms requiring identification and authentication of users: via WEB.
FIA_UID.2	The TOE enforces that every user is successfully identified by user name when providing user name and password for authentication before he can use any TOE security function

SFR	TSF
	other than the identification and authentication function.

7.2 Authorization and Security Management

Role	Rights
Administrator	The administrator has all rights, including the rights for user management, browsing and modifying all parameters in the system, software upgrade, and data import and export.
Operator	The operator has limited rights for user management and system setting and has no rights for version upgrade, running parameters, smart module plan view editing, and internal fault information export.

The TOE enforces an access control by supporting following functions:

- There are two hierarchical user groups (from low to high): operator, administrator.
- A user group is assigned to each account.
- Accounts are managed in groups. When an account is created, it is authorized to perform certain operations and is not allowed to perform unauthorized operations.
- Administrators have the privilege to create other administrator or operator accounts.

Table 7-2 SFR to TSF mapping

SFR	TSF
FDP_ACC.1 FMT_SMR.1	There are two hierarchical user groups (from low to high): operator, administrator. Accounts are managed in groups. When an account is created, it is authorized to perform certain operations and is not allowed to perform unauthorized operations. In order to prevent possible privilege escalations, only administrator can manage the only for users up to their own user group and cannot increase the user group attribute beyond their own user group.
FDP_ACF.1 FMT_MOF.1 FMT_MSA.1 FMT_MSA.3 FMT_SMF.1	There are two hierarchical user groups (from low to high): operator, administrator. A user group is assigned to each account. Accounts are managed in groups. In order to prevent possible privilege escalations, only administrator can manage the security attributes (user groups) of other accounts. Administrator are able to manage some security features: ● Administrators have the privilege to create other

SFR	TSF
	administrator or operator accounts.

7.3 Auditing

The operation log record events related to security configuration, user management, user login and logout.

Fields contained in an operation log include:

- User name (if applicable)
- Date and time
- Name of the accessed resource
- Event type

The TOE allows local administrator to query operation logs by specifying search criteria. The search criteria can be any field contained in an operation log, except Level, Details and Failure Cause.

The TOE checks the number of operation logs when recording operation logs. If the number of logs exceeds 20000, the TOE shall roll back the oldest records.

Table 7-3 SFR to TSF mapping

SFR	TSF
FAU_GEN_EXT.3 FAU_GEN.2	Support recording operations in the operation logs, including twith associated information like event type or date and time of the event.
FAU_SAR.1 FAU_SAR.2	Only Administrators can query operation logs. So only the Administrators can know that whoever accesses and logins the system and any operation on the system according to the content of the operation log.
FAU_STG.1	The operation logs allow no manual changes.
FAU_STG.3	The operation logs and security logs keep records in time sequence. After the memory is exhausted, the oldest records of the logs are overwritten by the latest records. Once the memory is exhausted, an alarm is reported.

7.4 TOE Access

The TOE implements access control at the service layer.

The TOE controls the maximum number of access users and the maximum number of sessions to control the establishment of web client connections.

The TOE is also able to terminate an interactive session after an inactivity period of time.

Table 7-4 SFR to TSF mapping

SFR	TSF
FTA_TSE.1	The TOE is also able to terminate an interactive session after an inactivity period of time.
FTA_SSL.3	Support logout when no operation is performed on the user session within a specified interval. If an account that has logged in does not exchange information with the TOE within the specified interval (10 minutes by default), it will be automatically logged out. The account needs to be authenticated again for a new login.
FTA_SSL.4	The session ends when you close the web browser. The session ends when you click Logout. When an administrator locks a non-administrator user on the WebUI, the session of the non-administrator user is terminated immediately.
FTA_TAB.1	When a user logs in to the WebUI for the first time, the system prompts the user to change the password immediately. After the password of a user expires on the WebUI, the user is forced to change the password after login.
FTA_MCS.1	Each user can keep only one valid HTTPS session.

8 Abbreviations, Terminology and References

8.1 Abbreviations

Table 8-1 Abbreviations

AI/DI	Analog or Digital Input
CC	Common Criteria
ECC	Energy Control Center
ETH	Ethernet
FE	Fast Ethernet
GE	Gigabit Ethernet
HTTPS	Hypertext Transfer Protocol Secure
PDU	Power Distribution Unit
POE	Power Over Ethernet

8.2 References

[CC] Common Criteria for Information Technology Security Evaluation. Part 1-3. September 2012. Version 3.1 Revision 5.

[CEM] Common Methodology for Information Technology Security Evaluation. September 2012. Version 3.1 Revision 5.