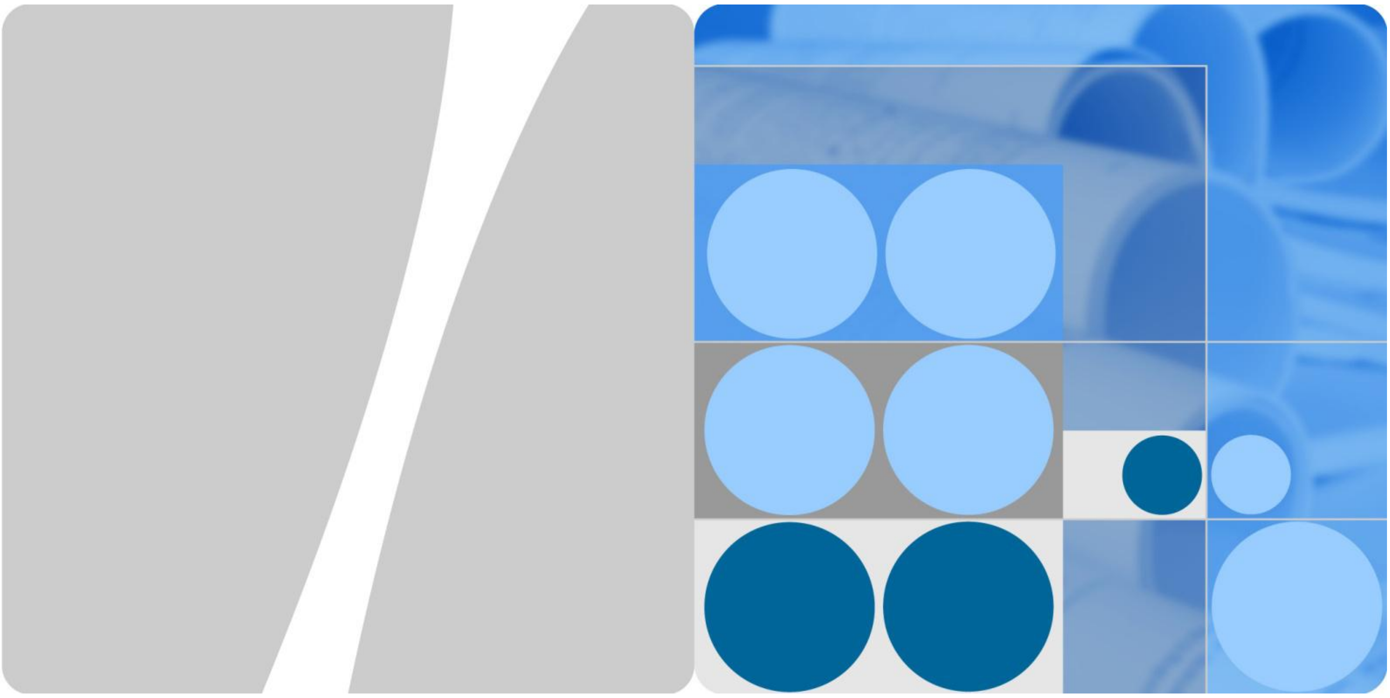


Huawei iSitePower V100R022C00SPC120

Security Target

Issue **1.14**

Date **2022-09-14**

HUAWEI TECHNOLOGIES CO., LTD.

Huawei Technologies Co., Ltd.

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

Website: http://e.huawei.com

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
2019-05-13	1.0	Initial Draft	Yin Guohua
2019-05-18	1.1	Refresh after review	Yuan Man
2020-01-15	1.2	Refresh after review	Yuan Man
2020-03-16	1.3	Delete wifi description	Yuan Man
2020-05-21	1.4	Refresh after review	Chen Hong
2020-07-06	1.5	Refresh after review	Chen Hong
2020-08-18	1.6	Refresh after review	Chen Hong
2021-07-17	1.7	Refresh after review	Chen Hong
2021-07-30	1.8	Refresh after review	Chen Hong
2021-07-30	1.9	Refresh after review	Chen Hong
2021-08-31	1.10	Refresh after review	Chen Hong
2021-09-06	1.11	Refresh after review	Chen Hong
2021-11-16	1.12	Refresh after review	Chen Hong
2022-06-06	1.13	New TOE Name	Chen Hong
2022-09-14	1.14	Patch Update	Chen Hong

Contents

1 Introduction......6
1.1 ST Reference......6
1.2 TOE Reference......6
1.3 TOE overview......6
1.3.1 TOE Type......6
1.3.2 TOE Usage and major security features......6
1.3.3 Non-TOE Hardware and Software......7
1.4 TOE description......8
1.4.1 Physical Scope......8
1.4.1.1 Evaluated Configuration......8
1.4.2 Logical Scope......9
1.4.2.1 Authentication......9
1.4.2.2 Authorization......9
1.4.2.3 Auditing......9
1.4.2.4 TOE Access......9
1.4.2.5 Security management......10
2 CC Conformance Claim......11
3 Security Problem Definition......12
3.1 Asset......12
3.2 Threats......12
3.3 Organizational Security Policy......13
3.4 Assumptions......13
4 Security Objectives......14
4.1 Security Objectives for the TOE......14
4.2 Security Objectives for the Operational Environment......14
4.3 Rationale for Security Objectives......15
5 Extended Components Definition......17
5.1 FAU_GEN_EXT.3 Simplified audit data generation......17
6 Security Requirements......19
6.1 Conventions......19

6.2 Security Functional Requirements........19
6.2.1 Security Audit (FAU)........19
6.2.2 User Data Protection (FDP)........21
6.2.3 Identification and Authentication (FIA)........21
6.2.4 Security Management (FMT)........23
6.2.5 TOE access (FTA)........24
6.3 Security Functional Requirements Rationale........24
6.3.1 Coverage........24
6.3.2 Sufficiency........25
6.3.3 Security Requirements Dependency Rationale........27
6.4 Security Assurance Requirements........28
6.5 Rationale for Security Assurance Requirements........28
7 TOE Summary Specification........29
7.1 Authentication........29
7.2 Authorization and Security Management........30
7.3 Auditing........31
7.4 TOE Access........32
8 Abbreviations, Terminology and References........34
8.1 Abbreviations........34
8.2 References........34

List of Tables

Table 1 : Non-TOE Hardware and Software components....7

Table 2 : User’s workstation minimum the requirements....7

Table 3 : Description of the assets to be protected....12

Table 4 : Mapping Objectives to threats....15

Table 5 : Mapping objectives for the environment to assumption.... 16

Table 6 : Mapping of the SFRs to the security objectives....25

Table 7 : SFRs sufficiency analysis....26

Table 8 : Dependencies between TOE security functional requirements.... 28

Table 9 : Web Interface user roles rights....30

Table 10 : LCD Panel user roles rights....30

1 Introduction

1.1 ST Reference

ST Title	Huawei iSitePower V100R022C00SPC120 Security Target
ST version	1.14
Date	2022-09-14
Vendor and ST author	Huawei Technologies Co., Ltd

1.2 TOE Reference

TOE Name	iSitePower
TOE software version	V100R022C00SPC120
Developer	Huawei Technology Co., Ltd

1.3 TOE overview

1.3.1 TOE Type

The iSitePower is a software product running on the Linux operating system based on the ARM chip of the Cortex-A8 architecture for monitoring and managing Huawei's box-type and cabinet-type power systems. It can be accessed through an user Web UI and a LCD panel.

1.3.2 TOE Usage and major security features

The TOE is a software that monitors and manages Huawei's box-type and cabinet-type power systems. It provides a web interface (WebUI) and a LCD Panel that allow users to operate with the TOE in order to change values and parameters.

The TOE provides the following key security features:

- **Authentication:** Only authenticated users are allowed to log in to the TOE, query TOE data, and set TOE parameters. The TOE provides different user roles. If a user fails to be authenticated for multiple consecutive times, the user is locked to prevent unauthorized access. Lastly, the TOE provides a password policy.
- **Authorization:** Only authorized users are able to execute certain actions based on their privileges.
- **Auditing:** An operation log records the operations that the TOE user have performed on the system and the result of the operation and is used for tracing and auditing. Depending on the role of the user it is possible to review certain audit logs. The TOE protect the stored audit records in the audit trail from unauthorized deletion and it roll back the oldest records if the audit trail exceeds a certain number of logs.
- **Security Management:** The TOE provides three different user roles (administrator, engineer 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.

1.3.3 Non-TOE Hardware and Software

The TOE environment is composed by following components:

Components	Description
Huawei's box-type and cabinet-type power system.	This device provides power supply to the SMU02C.
SMU02C	Hardware platform where the TOE runs.
Operating system	Linux 4.19.90
OpenSSL	OpenSSL version 1.1.1k

Table 1: Non-TOE Hardware and Software components

The TOE is accessible from the LED Panel sited in the SMU02C and from a web application running in a workstation which must have at least this minimum requirements:

Components	Description
Browser	Firefox 52, Chrome 58, or Internet Explorer 11 or above.
RAM Memory	4GB RAM

Table 2: User’s workstation minimum the requirements

1.4 TOE description

1.4.1 Physical Scope

This section will define the physical scope of the iSitePower:

➢ The **SOFTWARE** part of the TOE is the following:

Delivery Item	Version	Signature File	Sha256sum hash
iSitePower_V100R022C00SPC120_02X.zip	V100R022C00SPC120	iSitePower_V100R022C00SPC120_02X.zip.asc	a1f168414ed953deb29a51638c9a65504cbaf438ed09acbaeb5853d178e2b53d

Huawei will provide privileges to the customer's account that allows a user to log in the official website and download the corresponding software package. The software is available in the following link:

https://support.huawei.com/enterprise/en/site-power-facility/isitepower-pid-250722182/software/257282435/?idAbsPath=fixnode01|9452479|251662535|21781574|22318399|250722182

➢ The **GUIDANCE** part of the TOE is the following:

Name of the evidence	Version	Sha256sum hash
Huawei iSitePower V100R022C00SPC120 AGD_OPE V0.4.pdf	0.4	8c8b1c484d45f14540fe8e701e5e817426fe2ef476eb38d8b8f8b41e1d1e7357
Huawei iSitePower V100R022C00SPC120 AGD_PRE V0.4.pdf	0.4	4a59038ca55b203fbbc8cd6bbd440e063d59e67a6eefaa4a8fa86dd4e053edeb

Huawei sends the previous documentation via an email generated automatically by Huawei File Transfer System (etrans).

1.4.1.1 Evaluated Configuration

The TOE is evaluated using the following physical platform:

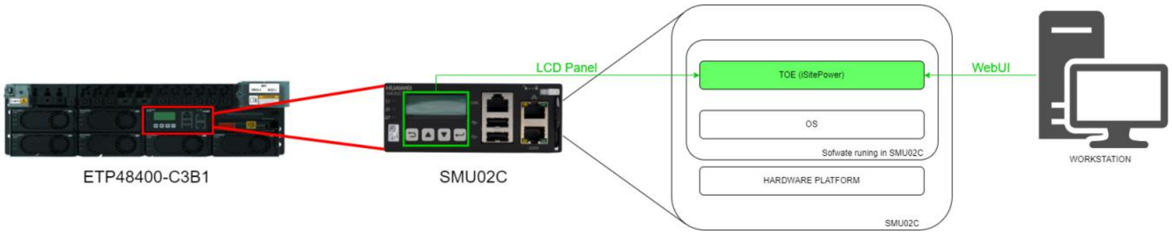


Figure 1: iSitePower evaluated configuration

- **ETP48400-C3B1:** box-type and cabinet-type power system.
- **SMU02C:** Incorporated in the ETP48400-C3B1
- **OS:** Linux stm32mp15x 4.19.90
- **OpenSSL:** OpenSSL version 1.1.1k

1.4.2 Logical Scope

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

1.4.2.1 Authentication

The TOE authenticates users based on usernames and passwords.

The TOE provides the local authentication mode. The usernames and passwords are stored on the local device. During login, the local usernames and passwords stored on the local device are used for authentication. When a user logs in to the web interface the first time and after the password of a user expires, the user is prompted to change the default password. In addition, password brute force defense mechanism, and automatic lock is performed.

The passwords must meet the complexity requirements defined in the password policy.

1.4.2.2 Authorization

The TOE group-based authorization mechanism is used to manage access based on predefined role groups.

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.

1.4.2.3 Auditing

Logs record the routine maintenance events of the TOE. The TOE users are able to see depending on their role certain logs in order 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.

The TOE protect the stored audit records in the audit trail from unauthorized deletion and it roll back the oldest records if the audit trail exceeds a certain number of logs.

1.4.2.4 TOE Access

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

1.4.2.5 Security management

The TOE provides the functionality to manage user configuration, updates and logs export depending on the user role. Accounts are managed by group. Each group represents specific rights assigned to accounts in the group. The WebUI of the TOE contains three different groups of roles (administrator, engineer and operator) and the LCD Panel contains two groups (administrator and engineer). For example, the accounts in the administrator group have rights to perform all security management and advanced settings operations. Unauthorized operations are not allowed.

2 CC Conformance Claim

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:

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.

Table 3: Description of the assets to be protected

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 un-authenticated 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 ETP48400-C3B1 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 and the LCD Panel.
- **A.Security:** The system where the TOE is installed is able to provide secure encryption for the external logical interfaces accessible for attackers.
- **A.NoEvil:** The TOE users of both the LCD Panel and web management interface 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 (SMU02C and ETP48400-C3B1), 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 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. Access control management, including the association of users and corresponding privileged functionalities.

4.2 Security Objectives for the Operational Environment

- **OE.PhysicalProtection:** It is assumed that the TOE and the TOE environment (the ETP48400-C3B1 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 are 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 and the LCD Panel.
- **OE.Security:** The system where the TOE is installed is able to provide secure encryption for the external logical interfaces accessible for attackers.
- **OE.NoEvil:** The administrators and the engineers users of both the LCD Panel and web management interface are not hostile, and will follow and abide by the instructions provided by the TOE documentation.
- **OE.Hardware:** The underlying hardware of SMU02C and ETP48400-C3B1 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.

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 interface are logged. **(O.Audit)**
P.AccessControl	**O.Authorization** **O.SecurityManagement**	Only authorized users can perform certain management operations.**(O.Authorization)** The user authorization is provided and can be managed by the TOE. **(O.SecurityManagement)**

Table 4: Mapping Objectives to threats

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.

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

Environmental Objective	**Assumption**
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

Table 5: Mapping objectives for the environment to assumption

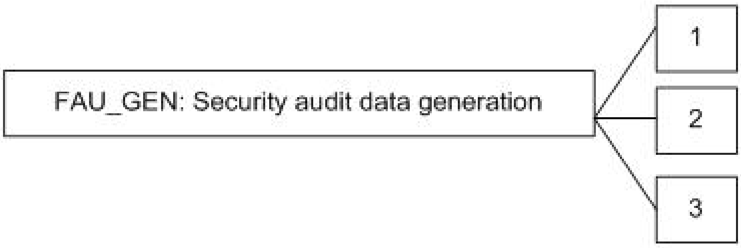
5 Extended Components Definition

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

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]** (between brackets) indicates the completion of an assignment.
- ***Italicised and bold text*** indicates the completion of a selection.
- Iteration/N indicates an element of the iteration, where N is the iteration element name.

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: **[**

- **Login and logout**
- **Adding and deleting users**
- **Changing user accounts**
- **Changing user passwords**
- **Locking and unlocking user accounts**
- **Changing user role groups**
- **Changing the system security configuration**
- **Modifying system configuration parameters**
- **Restarting the system**
- **Restoring factory settings**
- **Upgrading software**

]

FAU_GEN_EXT.3.2 The TSF shall record within each audit record: Date and time of the event, **user name, operation source and parameter**.

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 role, Engineer role and Operator role of the WebUI]** with the capability to read **[**

- **Administrators: all the information**
- **Engineers: information regarding its user role and below**
- **Operator: information regarding its user role**

] 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 **Operation Log** tab of the web interface . 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 **Operation Log** tab of the web interface . The 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 **Operation Log** tab of the web interface . The audit review 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 **[3000 event logs].**

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 **Operation Log** tab of the web interface . The audit review 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 or menus of the LCD Panel**
- **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 or LCD Panel menus information attributes:

- **There are no security attributes of the web interface windows information or of the LCD Panel menus 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 or menu 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/menu 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 related to **[user logging in]**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been ***met***, the TSF shall **[lock the account for 10 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: **[**

- **User name**
- **User role**
- **Password**
- **Password validity period**
- **the inactivity time which an account is automatically logged out**
- **Status of the account (locked/unlocked)**
- **Lock Time (Minute) and Allowable Illegal Access Times**

]

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 (Add, Modify and Delete)**
- **Restoring factory settings**
- **Modifying system settings:**
  - ➢ **IP Whitelist (Add, Delete, Activate All)**
  - ➢ **Refresh the key manually**

]

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.

Application note: Authentication is possible by user name and password. The user is identified by his user name if he is able to successfully authenticate with his user name and corresponding password.

6.2.3.6 FIA_SOS.1 Verification of Secrets

FIA_SOS.1 The TSF shall provide a mechanism to verify that secrets meet **[**

- **The password minimum length of 8 to 20 characters.**
- **The password contain at least two types of the following characters: ‘a– z’, ‘A–Z’, ‘0–9’ or ‘!@*-_?{}=’**
- **Different from the user name or its reverse.**

]

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 **[Administrators of the WebUI]**.

6.2.4.2 FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 Management of Security Attributes. The TSF shall enforce the **[User Group SFP]** to restrict the ability to ***query, modify*** the security attributes **[user role]** to **[users of the Administrator groups]**.

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 **[Administrators of the WebUI]** 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: **[**

- **User Management: add, delete, lock and unlock users.**
- **Modify users' passwords**
- **Modify users' roles.**
- **Read all operation logs**
- **Set Reauthentication Pre-Shared Key**
- **Delete Features**
- **Service Management**

]

6.2.4.5 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles **[**

For WebUI:

- **Administrator**
- **Engineer**
- **Operator**

For LCD panel:

- **Administrator**
- **Engineer**

]

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.

6.2.5.2 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after [**10 minutes of inactivity**].

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 [**two or more connections of the same IP address, the number of online users and the attribute user: Status of the account (locked/unlocked)**].

Application note:

- After an administrator locks a non-administrator user on the WebUI, the user is not allowed to log in to the system.
- After the 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:

- 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.

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.

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
FIA_SOS.1	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

Table 6: Mapping of the SFRs to the security objectives

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:

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. The passwords must meet the complexity requirements defined in the password policy defined in FIA_SOS.1.
O.Authorization	The requirement for access control is spelled out in FDP_ACC.1, and the access control policies are modelled in FDP_ACF.1.
O.SecurityManagement	The management functionality for the security functions of the TOE is defined in FMT_SMF.1. The TOE restricts the ability to determine the behavior of all the functions defined in FMT_SMF.1 to Administrators of the WebUI (FMT_MOF.1). The WebUI of the TOE contains three different groups of roles (administrator, engineer and operator) and the LCD Panel contains two groups (administrator and engineer) . (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.

Table 7: SFRs sufficiency analysis

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.

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_SAR.1 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_STG.1 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
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_ACC.1

	FDP_IFC.1] FMT_SMR.1 FMT_SMF.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

Table 8: Dependencies between TOE security functional requirements

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 Rationale for Security Assurance Requirements

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 management portal, a username and password are requested to verify his identity before the access is given.

The TOE web interface supports maximum attempts for authentication failures within certain period of time. After 5 consecutive fail attempts logins within 5 minutes, the account is locked for 10 minutes (**FIA_AFL.1**). Additionally, when the login reach 3 fail attempts, the TOE will show a captcha image.

The TOE web interface supports for user individual attributes including the user name, user role, password, password validity period, the inactivity time which an account is automatically logged out (10 minutes), lock time and allowable illegal access times (which means that if the user is automatically locked due to failed authentication attempts, the TOE will not allow the user to enter before this period of time finishes) and status of the account (locked/unlocked) (**FIA_ATD.1**).

The TOE enforces that every user needs to successfully authenticate himself by username 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 interface and LCD panel (**FIA_UAU.2**).

The TOE enforces that every user in the web interface and in the LCD panel is successfully identified by username when providing user name and password for authentication before he can use any TOE security function other than the identification and authentication function (**FIA_UID.2**).

Support re-authentication when the user performs important operations in the TOE web interface for the user management (**FIA_UAU.6**).

The TSF provides the following password policy in he TOE web interface (**FIA_SOS.1**):

- The password minimum length of 8 to 20 characters.
- The password contain at least two types of the following characters: ‘a– z’, ‘A–Z’, ‘0–9’ or ‘!@*-_?{}=’
- Different from the user name or its reverse.

7.2 Authorization and Security Management

The TOE enforces an access control by supporting following functions:

There are three hierarchical user groups in the web interface (from low to high): operator, engineer & administrator.

Role	Rights
Administrator	The administrator has the rights for setting, software upgrade, query, export maintenance information, user management, import configuration file and password modification
Engineer	The Engineer has the rights for setting (excluding IP Added to Ban List), software upgrade, query, export maintenance information, import configuration file and password modification
Operator	The operator has rights for setting (excluding IP Added to Ban List), query and password modification.

Table 9: Web Interface user roles rights.

On the other hand, the LCD panel provides by default two different users (admin and engineer) with the roles (administrator and engineer) respectively. Depending on the password the user introduces, the user will log in the LCD panel as a different user role with its specific role.

There are two hierarchical user groups in the LCD Panel (from low to high): engineer & administrator.

Role	Rights
Administrator	The administrator has full access to the functions available in the LCD panel: setting, software upgrade, query, export maintenance information, user management, import configuration file and password modification
Engineer	The Engineer has the rights for setting (excluding IP Added to Ban List), software upgrade, query, export maintenance information, import configuration files.

Table 10: LCD Panel user roles rights.

The administrator and the engineer roles of the two interfaces available do not have the same rights. The user can distinguish the two roles in the the Operation Log tab by the column “Operation Source”.

An 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.

In order to prevent possible privilege escalations, users can change user attributes (esp. their own attributes) only for users up to their own user level and cannot increase the user group attribute beyond their own user group. (**FDP_ACC.1, FMT_SMR.1, FDP_ACF.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3**).

The users are capable of performing the following management functions in both the LCD Panel and the WebUI (**FMT_SMF.1**):

Management Function	LCD Panel	WebUI
User Management: add, delete, lock and unlock users.	NO	YES
Modify users' passwords	YES	YES
Modify users' roles.	NO	YES
Read all operation logs	NO	YES
Set Reauthentication Pre-Shared Key	NO	YES
Log Synchronization	NO	YES
Delete Features	NO	YES
Serial Port Debug	NO	YES
Service Management	NO	YES

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
- Date and time
- Operation Source
- Parameter (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 operation logs of the TOE can be exported to a local directory for auditing.

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. When a log reaches the 3000th position in the log trail, a rollback is performed to store the last logs generated by the actions performed in the WebUI or in the LCD panel. (**FAU_STG.3**).

The TOE records operations that the TOE user have performed on the system and the result of the operation in the operation log, including the operation type, operation object, access IP address, date and time, and each record is associated to the username.(**FAU_GEN_EXT.3, FAU_GEN.2**).

Logs are just accessible via WebUI, they cannot be modified or deleted. (**FAU_STG.1**).

The following operations will be audited:

Management Function	**LCD Panel**	**WebUI**
Login and logout	YES	YES
Adding and deleting users	N/A	YES
Changing user accounts	N/A	YES
Changing user passwords	YES	YES
Locking and unlocking user accounts	N/A	YES
Changing user role groups	N/A	YES
Changing the system security configuration	YES	YES
Modifying system configuration parameters	YES	YES
Restarting the system	YES	NO
Restoring factory settings	YES	YES
Upgrading software	YES	YES

Administrators, engineers and operator can query operation logs in the web interface of their privilege and below. 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. Engineers can see operation logs related to engineer role and operator role. And finally, operators can see operation logs related to operator role. (**FAU_SAR.1, FAU_SAR.2**).

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 web interface is able to deny a session depending on: (**FTA_TSE.1**)

- Two different user authentications with the same IP address.
- Number of users connected.
- The status of the account (if the status is locked, the user cannot login).

Both in the WebUI and the LCD Panel, the TOE supports 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.3**).

In the WebUI, the session ends when you close the web browser or when you click Logout. (**FTA_SSL.4**)

The TOE provides a manually logout session functionality. All users can access to" User Management > User Logout" menu in order to terminate their own session (**FTA_SSL.4**)

When an administrator locks a non-administrator user on the WebUI, the session of the non-administrator user is terminated immediately.

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_TAB.1**)

The TSF shall restrict the maximum number of concurrent sessions that belong to the same user to 1 both in the WebUI and the LCD. The LCD only allows 1 session per user because physically it can only be accessed by one person at a time. (**FTA_MCS.1**)

8 Abbreviations, Terminology and References

8.1 Abbreviations

CC	Common Criteria
SMU	Site Monitoring Unit
ST	Security Target
TOE	Target Of Evaluation
HTTPS	Hypertext Transfer Protocol Secure
UI	User Interface
LCD	Liquid Crystal Display

8.2 References

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

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