ECI LightSoft, EMS-APT, NPT-1010, NPT-1020/1021 and NPT-1200 Software Security Target

Version 1.8

January 6, 2016

ECI Telecom Ltd.
30 Hasivim Street
Petach Tikvah, 4959388
Israel

DOCUMENT INTRODUCTION

Prepared By:

Common Criteria Consulting LLC
15804 Laughlin Lane
Silver Spring, MD 20906
USA

Prepared For:

ECI Telecom Ltd.
30 Hasivim Street
Petach Tikvah, 4959388
Israel

REVISION HISTORY

Rev	Description
1.0	January 3, 2015, Initial release
1.1	January 25, 2015, Addressed ECI comments
1.2	May 12, 2015, Addressed lab ORs
1.3	June 12, 2015, Updated TOE versions
1.4	August 28, 2015, Additional TOE version updates
1.5	October 31, 2015, Corrections for testing consistency
1.6	December 17, 2015, Clarified the evaluated configuration
1.7	December 21, 2015, Modifications to FMT_MTD.1
1.8	January 6, 2016, Clarified restrictions on LS Client and added installation documentation; modified the supported roles and FMT_MTD.1(1) and (2), and clarified log references

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS LIST

ACL	Access Control List
APT	Access Packet Transport
CDE	Common Desktop Environment
CLI	Command Line Interface
CMIP	Common Management Information Protocol
CORBA	Common Object Request Broker Architecture
DBMS	DataBase Management System
DWDM	Dense Wavelength Division Multiplexing
EAL	Evaluation Assurance Level
EML	Element Management Layer
EMS	Element Management System
GCT	GUI Cut Through
GUI	Graphical User Interface
HTTP	HyperText Transfer Protocol
I&A	Identification & Authentication
MAC	Media Access Control
ME	Managed Element
MPLS	MultiProtocol Label Switching
NE	Network Element
NEL	Network Element Layer
NML	Network Management Layer
NMS	Network Management System
NPT	Native Packet Transport
OSS	Operations Support System
OTN	Optical Transport Network
RDR	Remote Database Replicator
ROADM	Reconfigurable Optical Add-Drop Multiplexer
SAR	Security Assurance Requirement
SDH	Synchronous Digital Hierarchy
SFP	Security Function Policy
SFR	Security Functional Requirement
SML	Service Management Layer
SONET	Synchronous Optical NETworking
SP	Service Provider
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
VNC	Virtual Network Computing

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the ECI LightSoft, EMS-APT, NPT-1010, NPT-1020/1021 and NPT-1200 Software. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4*. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

ECI LightSoft, EMS-APT, NPT-1010, NPT-1020/1021 and NPT-1200 Software Security Target, Version 1.8, dated January 6, 2016.

1.2 TOE Reference

Composite system comprised of ECI LightSoft Software Version 11.2 (build 04113) with fixes NSx1120_4113-100 10, NC1120_4113-100 10; EMS-APT Software Version 4.0 (build 20) with fixes BC0400-01 1, BC0400-02 1, BS0400-01 1, BS0400-02 1; NPT-1010 Software Version 4.0 (build 35); NPT-1020/1021 Software Version 4.0 (build 35); and NPT-1200 Software Version 4.0 (build 35).

Note that the NPT-1021 is simply a special configuration of the NPT-1020, intended for North American markets. In the remainder of this document, "1021" is dropped from the nomenclature for simplicity.

1.3 Evaluation Assurance Level

Assurance claims conform to EAL2 (Evaluation Assurance Level 2) from the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 4.

1.4 TOE Overview

1.4.1 Usage and Major Security Features

The TOE consists of the LightSoft and EMS-APT TOE components providing control and monitoring functions for the NPT-1010, NPT-1020, and NPT-1200 components (executing on supported appliances) that provide packet transport services. These systems are intended for use in Service Provider (SP) environments.

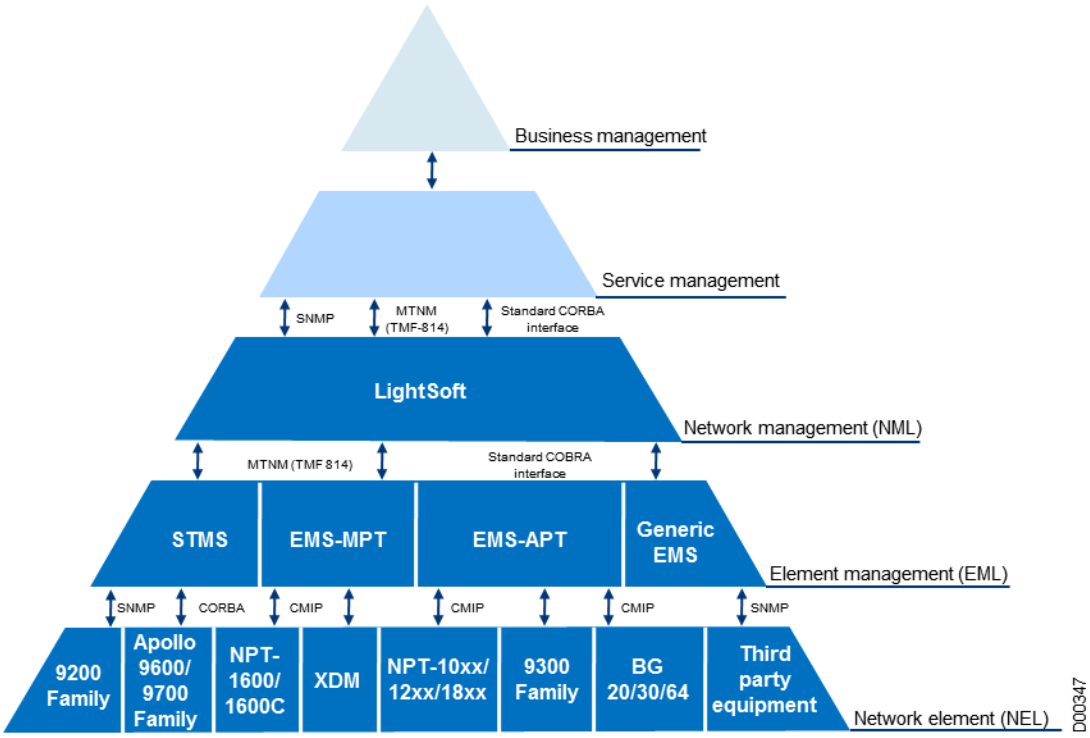
1.4.1.1 LightSoft

LightSoft is a Network Management System (NMS) providing the control and monitoring of all ECI products deployed by an SP. LightSoft, when integrated with an Element Management System (EMS), enables SPs to manage multiple technologies (SDH/SONET, DWDM-based optical, ROADM, Carrier Ethernet, and MPLS) independently of the physical layer. LightSoft simultaneously provisions, monitors, and controls many network layers with multiple transmission technologies. It does this from one application, using the same software platform and database. LightSoft provides an elegantly simple, secure, robust solution to the complexities of network management.

The LightSoft management concept is based on a layered architecture in accordance with the ITU-T M.3010 standard for compliant layer architecture. Separate layers make up the management structure. The lowest level, the Network Element Layer (NEL), constitutes the embedded agent software of the NEs. The second layer, the Element Management Layer (EML),

controls many individual NEs, while the third layer, the Network Management Layer (NML), controls the main network management functions. This architecture is illustrated in the following figure.

Figure 1 - Management Architecture



LightSoft functions at the NML, while a variety of different Element Management Systems (EMSs) controlled through the LightSoft umbrella function at the EML. Each EMS (e.g. EMS-APT) is tailored to a specific type of NE. For this evaluation, only the EMS-APT (for the NPTs) is used with LightSoft, and the only NEL types managed are the NPT-1010, NPT-1020, and NPT-1200.

A northbound interface connects either the EMS or LightSoft to the SP's Operations Support System (OSS) at the Service Management Layer (SML). However, this interface is not included in the evaluation. The interface between the EMS and NMS is included in the evaluation.

The user interface to LightSoft is via a GUI provided by a client-side application, which communicates with the centralized server. The client-side application may execute on the same system as the server and be accessed remotely, or it can execute on Solaris or Linux workstations. The client-side application and server communicate via CORBA.

Users of the GUI must successfully complete an Identification & Authorization process to LightSoft. User accounts are defined within LightSoft, and only authorized users are able to utilize the LightSoft functionality. Each user is associated with a profile (role). LightSoft has a default set of profiles providing typical levels of access. Users may also define custom profiles in order to meet specific requirements.

LightSoft permits SPs to partition their networks according to their organizational and logistical needs. User access to EMSs and NEs can be limited by associating a user with a specific partition.

Configuration operations performed by users are audited, and the audit records may be viewed by authorized users.

Configuration information and audit records are stored in an Oracle database running on a separate zone of the Solaris server hosting LightSoft.

1.4.1.2 EMS-APT

The EMS-APT is an advanced EMS designed to manage the Access Packet Transport (APT) products, including the BroadGate (BG) family and the Native Packet Transport (NPT) family of networks. It has an advanced architecture which supports multiple operating systems for integrated management, either standalone or with the NMS. For this evaluation, the EMS-APT is always integrated with the NMS and is only used to manage the NPT family (and specifically the NPT-1010, NPT-1020, and NPT-1200).

The EMS-APT consists of a centralized server system as well as a client-side application. For this evaluation, the server-side of the EMS-APT always executes on the same server as LightSoft, but in a separate logical domain. Multiple instances of the EMS-APT server may be deployed for scalability with extremely large networks; this functionality is not included in the evaluation..

Users access the EMS-APT functions via the LightSoft GUI. LightSoft automatically invokes EMS-APT functionality to perform user-requested operations involving NEs. LightSoft also provides a GUI Cut Through (GCT) capability to enable users to open a direct EMS-APT session.

EMS-APT user accounts are maintained separately from LightSoft user accounts. However, for this evaluation, all user accounts are managed in LightSoft and accounts are automatically uploaded from LightSoft to EMS-APT. Each user is associated with one of the EMS-APT default roles (specified via the LightSoft profile) to limit the functions that may be performed.

Configuration operations performed by users are audited, and the audit records may be viewed by authorized users.

Configuration information and audit records are stored in a MySQL database running in the same zone of the Solaris server hosting EMS-APT.

1.4.1.3 NPTs

The NPT-1010, NPT-1020, and NPT-1200 are NE appliances that provide Native Packet Transport (NPT) services within the SP network. The NPT-1010, NPT-1020, and NPT-1200 software is the software executing on the appliances. The appliances are a family of carrier-class MPLS-based multiservice packet transport platforms for the metro environment. Equipped with a broad mix of Ethernet and TDM interfaces, the NPT family supports delivery of both packet and TDM-based services over a converged packet infrastructure.

The NPT family members included in the evaluation are:

1. NPT-1010 – Designed for CPE environments, providing packet throughput of 5 Gbps.

2. NPT-1020 – Designed for access environments, providing packet throughput ranging from 10 Gbps to 60 Gbps.
3. NPT-1200 – Designed for metro aggregation environments, providing packet throughput ranging from 70 Gbps to 240 Gbps.

The security functionality of all of the family members is identical. The family members differ in their targeted environment, the number and types of interfaces, and aggregate throughput.

The NPTs send Alarm notifications to the EMS-APT for operational conditions that occur. The NPTs also support Access Control Lists (ACLs) that may be configured for Ethernet ports. ACLs enable information flow control via configuration of allowed (white listing) or denied (black listing) of MAC addresses.

For management, the NPTs support a CLI user interface as well as CMIP from LightSoft/EMS-APT. For this evaluation, once installed the appliances are managed solely via LightSoft/EMS-APT.

1.4.2 Required Non-TOE Hardware/Software/Firmware

The TOE consists of LightSoft and EMS-APT software executing on one or more dedicated Solaris servers, (optionally) the LightSoft client-side application executing on Solaris or Linux workstations, and the NPT-1010, NPT-1020, and NPT-1200 software executing on supported appliances. The dependencies for each of the components are described in subsequent paragraphs.

The Solaris server that hosts the server side of the LightSoft NMS and EMS-APT software components of the TOE is supplied by ECI. The following table provides details of the server as supplied. The Oracle DB is in a dedicated zone on the Solaris server.

Table 1 - LightSoft/EMS-APT Server Minimum Requirements

Item	Requirements
Base Hardware	7 virtual CPUs
Memory	64 GB
Hard Disk	85 GB
Operating System	Hardened Solaris x86 11.2 Rev01
Desktop	CDE 5.10, X11 Version 1.0.3
CORBA	Orbix 6.3.6 with fix OR0301-01

The client-side application of LightSoft can be installed on the same system as the server component (in a separate zone) and be accessed remotely by users. The client-side application also may execute on Solaris workstations. In this mode the application establishes remote CORBA connections to the server. The following table provides minimum requirements for workstations hosting the client-side application.

Table 2 - LightSoft Client-Side Application Minimum Requirements

Item	Requirements
Base Hardware	.5 virtual CPUs
Memory	1 GB
Hard Disk	2 GB

Item	Requirements
Operating System	Solaris x86 11.2 Rev01
CORBA	Orbix 6.3.6 (installed during client-side application installation)

The NEs managed by LightSoft/EMS-APT may be any combination of the NPT-1010, NPT-1020, and NPT-1200.

The TOE components communicate with one another via a segregated management network to prevent disclosure or modification of the data exchanged between TOE components. It is the responsibility of the operational environment to protect the traffic on the management network from other (non-TOE) devices.

Each of the NPT appliances provides a dedicated network interface for management interactions. The management interface must be connected to the segregated management network.

1.5 TOE Description

The TOE provides network packet transport functionality in metro environments via a family of appliances, as well as management functionality to securely control and monitor those devices. The management functionality provides multiple roles in order to enable multiple levels of access for users. The managed appliances may be divided into different groups within the management platforms, with access to groups restricted on a per-user basis.

The TOE consists of:

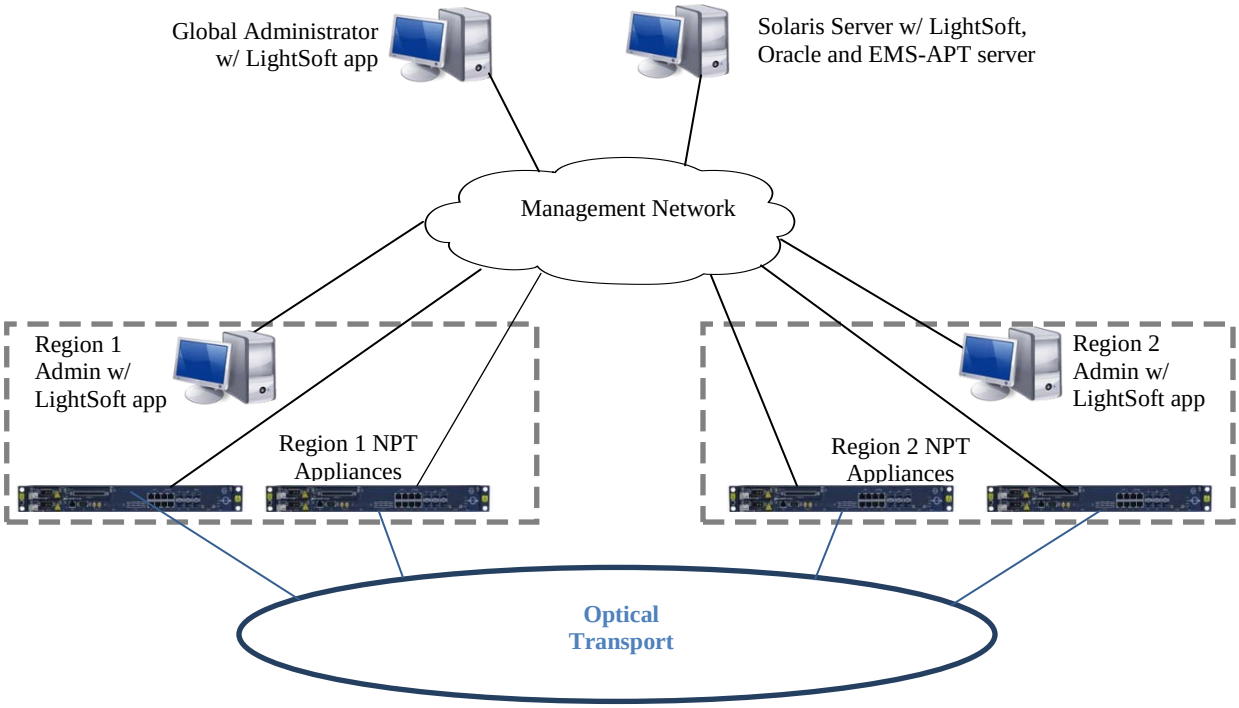
1. One instance of the LightSoft server component executing in one zone on a dedicated Solaris server.
2. One instance of the EMS-APT server component executing on the same server as the LightSoft server. The EMS-APT server uses a separate zone. The MySQL database runs in this zone.
3. One instance of the Oracle database component executing on the same server as the LightSoft server. The Oracle database server uses a separate zone.
4. One or more instances of the LightSoft client-side application. The instances may be installed on the Solaris server (using a separate zone) or on one or more Solaris workstations.
5. One or more instances of NPT-1010, NPT-1020, or NPT-1200 software executing on supported appliances. The software is pre-installed on appliances by ECI. The modular appliances may be populated via any supported combination of modules/cards.

A representative deployment for these components is shown in the following diagram. This diagram illustrates:

- One Solaris Server with the LightSoft server, Oracle database server and EMS-APT server; the managed network includes NEs in two distinct regions
- One administrator with global responsibilities; this user is configured to have access to the NEs in both regions
- One administrator in each of the regions; these users are configured to have access to the NEs in their corresponding region only
- NEs segregated into regional partitions

Note that the regions are logical only – physically the systems can reside in any physical location, and administrator permissions on defined on a per-user basis.

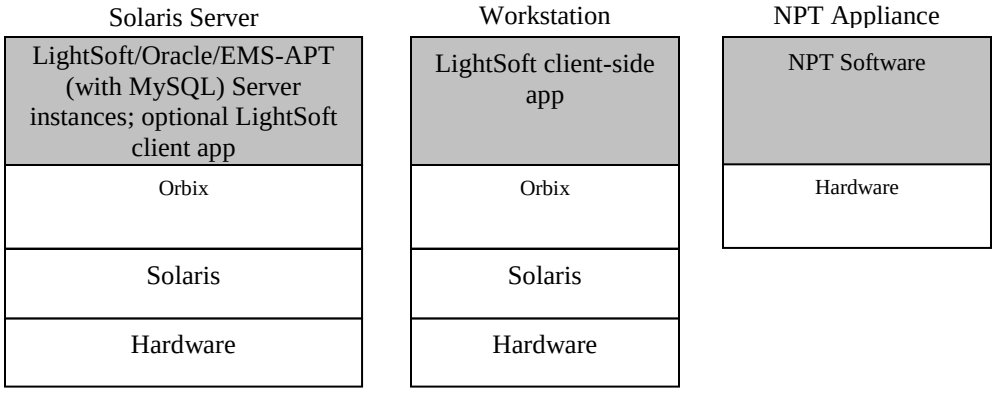
Figure 2 - Representative TOE Deployment



1.5.1 Physical Boundary

The physical boundary of the TOE is depicted in the following diagram (shaded items are within the TOE boundary).

Figure 3 - Physical Boundary



The physical boundary includes the following guidance documentation:

1. *LightSoft Version 11.2 Getting Started & Administration Guide*
2. *LightSoft Version 11.2 User Guide*

3. *LightSoft Version 11.2 Fault Management and Performance Monitoring Guide*
4. *LightSoft V11.x - Installation and Update Procedure*
5. *EMS-APT Version 4.0 Installation Guide (Solaris)*
6. *EMS-APT Version 4.0 User Guide*
7. *EMS-APT Version 4.0 Service Management Guide*
8. *EMS-APT Version 4.0 Performance Management Guide*
9. *EMS-APT Version 4.0 Network Management Guide*
10. *EMS-APT Version 4.0 Supporting Information*
11. *NPT-1010 Version 4.0 Installation and Maintenance Manual*
12. *NPT-1020 Version 4.0 Installation and Maintenance Manual*
13. *NPT-1021 Version 4.0 Installation and Maintenance Manual*
14. *NPT-1200 Version 4.0 Installation and Maintenance Manual*
15. *How to Create a Bootable CF Card for BG-64/BG-30/NPT1020/1200 User Guide*
16. *How to Use the Boot Configuration Tool User Guide*
17. *ECI LightSoft (v11.2), EMS-APT (v4.0), NPT-1010 (v4.0), NPT-1020/1021 (v4.0) and NPT-1200 (v4.0) Software Common Criteria Supplement*
18. *Common Management HW Preparation and Configuration Activities*
19. *Common Phase 11.2 Activities for Preparation, Installation and Upgrade of Management Systems Infrastructure*
20. *ECILoracle v11 - SW Installation and Upgrade Procedure*

1.5.2 Logical Boundary

1.5.2.1 Audit

Audit records are generated for specific actions performed by users. The audit records are saved and may be reviewed by authorized administrators.

1.5.2.2 Management

The TOE provides functionality for administrators to configure and monitor the operation of the TOE via the client-side GUI application. The LightSoft and EMS-APT products support multiple roles to enable different users to be assigned different permissions. Access to the NEs may be restricted on a per-user basis.

1.5.2.3 I&A

The TOE identifies and authenticates users of the client-side GUI application before they are granted access to any TSF functions or data. When valid credentials are presented, security attributes for the user are bound to the session.

1.5.2.4 Information Flow Control

The NPTs enforce ACLs that can be configured for Ethernet ports. An ACL specifies the source and destination MAC addresses that are allowed or denied for a port. Denied packets are silently discarded.

1.5.3 TOE Data

The following table describes the TOE data.

Table 3 - TOE Data Descriptions

TOE Data	Description
EMS-APT Action Log	Contains audit records of configuration actions by users of EMS-APT.
EMS-APT Alarms	Alarms from the NEs or EMS-APT for operational conditions.
EMS-APT Network Elements	Specify the NPT appliances that are managed and their configuration.
EMS-APT Security Log	Contains audit records of logins/logouts for user access.
EMS-APT Services	Defines the configuration of Services within NEs.
EMS-APT User Accounts	Define the authorized users of an EMS-APT instance. Note that user accounts are managed via LightSoft. Attributes include: • Username • Assigned Role
LightSoft Activity Log	Contains audit records of configuration actions by users of LightSoft.
LightSoft Alarm Configurations	Configuration of Alarm generation in TOE components.
LightSoft Alarms	Alarms from the NEs or EMS-APT for operational conditions.
LightSoft Profiles	Define the access permissions (capabilities) to be associated with a user. The capabilities also specify the EMS-APT Role (or none) for associated users.
LightSoft Resource Domains	Define the resource domains the managed elements may be grouped into. Attributes include: • Resource Domain Name • Associated MEs
LightSoft Security Log	Contains audit records of logins/logouts for user access and automated account actions such as disabling idle user accounts.
LightSoft Security Preferences	Define the security parameters that apply to all users. Attributes include: • Minimum Password Length • Default Password Expiration • Password Reuse History • Maximum Unsuccessful Login Attempts • Login Reactivation Time • Default Inactivity Timeout • Inactivity Timeout Action • Strong Password Enforcement • Account Becomes Idle Time • Action Upon Becoming Idle

TOE Data	Description
LightSoft User Accounts	Define the authorized users of LightSoft. Attributes include: • Username • Password • Associated User Group • Account Lock Status • Password Expiration Date • Inactivity Timeout Value • Account Idle Value • Consecutive Unsuccessful Login Count • EMS-APT associated Role (or none)
LightSoft User Groups	Define user groups within LightSoft. Attributes include: • Group name • Associated Users • Associated Profile • Associated Resource Domains

1.6 Evaluated Configuration

The following configuration restrictions apply to the evaluated configuration:

1. The default Profiles in LightSoft are not modified and the associations between those Profiles and pre-defined User Groups are not changed. Additional Profiles and User Groups may be created to provide customized Roles.
2. Only the default Roles are used in EMS-APT, and the permissions for those Roles are not modified.
3. User Accounts are defined in LightSoft and synced between LightSoft and EMS-APT.
4. A single Network Operator is defined in LightSoft. Support for multiple SPs in a single LightSoft instance is not included in this evaluation.
5. All control and monitoring of NEs after they have been installed is performed via LightSoft/EMS-APT only. The CLI available on the NEs is used during installation only.
6. The Inactivity Timeout for all User Accounts is configured as a numeric value (not "Unlimited") to force inactive sessions to be locked or terminated.
7. The LightSoft client supports remote access via Xterminal. Remote Xterminal access can be configured for VNC and/or HTTP (web). In the evaluated configuration, only VNC access is used.
8. The LightSoft client must not be installed in the same Solaris zone as the LightSoft server.
9. The following Solaris user account names are created in multiple of the Solaris zones used with the LightSoft server, LightSoft client, EMS-APT and Oracle DB components: root, enm, nms, ems, stms, bgf, ora, and sshd. The passwords specified for these user accounts must not be common between the zones.
10. Password complexity and usage settings should be consistent with enterprise policy. At minimum, the following settings must be configured:

a. Minimum Password Length: 8
b. Default Password expiration: 45 days
c. Password Reuse History: 5
d. Max Unsuccessful Login Attempts: 3
e. Login Reactivation: 5 minutes
f. Default Inactivity Timeout: 10 minutes
g. Strong Password Enforcement: Enable
h. Becoming Idle If No Login: 6 months
i. Action Upon Becoming Idle: Inhibit & record in log

1.7 Functionality Excluded from the Evaluation

The following functionality or the TOE is excluded from the evaluation:

1. Remote Database Replicator (RDR) option for server redundancy
2. LightSoft interface to a higher-level OSS
3. LightSoft interface to third party EMS instances
4. LightSoft integration with enterprise user authentication servers (Central User Administration)
5. LightSoft support for multiple carriers within a single LightSoft instance (Customer Network Management)

2. Conformance Claims

2.1 Common Criteria Conformance

Common Criteria version: Version 3.1 Revision 4, dated September 2012

Common Criteria conformance: Part 2 extended and Part 3 conformant

2.2 Security Requirement Package Conformance

EAL2

The TOE does not claim conformance to any security functional requirement packages.

2.3 Protection Profile Conformance

No conformance to any registered protection profile is claimed.

3. Security Problem Definition

3.1 Introduction

This chapter defines the nature and scope of the security needs to be addressed by the TOE. Specifically this chapter identifies:

A) assumptions about the environment,

B) threats to the Devices and

C) organisational security policies.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.2 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the Operational Environment.

Table 4 - Assumptions

A.Type	Description
A.ECI	Administrators perform installation of the TOE in conjunction with ECI personnel.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.MGMTNETWORK	The TOE components will be interconnected by a segregated management network that protects the intra-TOE traffic from disclosure to or modification by untrusted systems or users, and limits traffic from entering the management network.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.NOTRST	The TOE can only be accessed by authorized users.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

3.3 Threats

The threats identified in the following table are addressed by the TOE and the Operational Environment.

Table 5 - Threats

T.Type	Description
T.COMINT	An unauthorized person may attempt to compromise the integrity of TOE data by bypassing a security mechanism.
T.INVSRC	Network systems communicating via the TOE may attempt to access unauthorized remote network systems by transmitting packets through the TOE with misleading source MAC addresses.
T.LOSSOF	An unauthorized person may attempt to remove or destroy data from the TOE.

T.Type	Description
T.NOHALT	An unauthorized person may attempt to compromise the continuity of the TOE's functionality by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.UNAUTHDST	Network systems communicating via the TOE may gain unauthorized access to remote network systems by transmitting packets through the TOE to unauthorized destination MAC addresses.

3.4 Organisational Security Policies

The Organisational Security Policies identified in the following table are addressed by the TOE and the Operational Environment.

Table 6 - Organisational Security Policies

P.Type	Description
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE.
P.MANAGE	The TOE shall only be managed by authorized users.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of activities.

4. Security Objectives

This section identifies the security objectives of the TOE and the TOE's Operational Environment. The security objectives identify the responsibilities of the TOE and the TOE's Operational Environment in meeting the security needs. Objectives of the TOE are identified as *O.objective*. Objectives that apply to the operational environment are designated as *OE.objective*.

4.1 Security Objectives for the TOE

The TOE must satisfy the following objectives.

Table 7 - Security Objectives for the TOE

O.Type	Description
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.AUDITS	The TOE must record audit records for data accesses and use of the TOE functions.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.
O.INFFLW	The TOE must be able to restrict traffic flows via Ethernet ports according to configured source and destination MAC addresses.
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.

4.2 Security Objectives for the Operational Environment

The TOE's operational environment must satisfy the following objectives.

Table 8 - Security Objectives of the Operational Environment

OE.Type	Description
OE.ECI	Administrators perform installation of the TOE in conjunction with ECI personnel.
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
OE.MGMTNETWORK	The operational environment will provide a segregated management network interconnecting the TOE components that protects the intra-TOE traffic from disclosure to or modification by untrusted systems or users, and limits external traffic from entering the management network.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE.
OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.TIME	The IT Environment will provide reliable timestamps to the TOE.

5. Extended Components Definition

5.1 Extended Security Functional Components

None

5.2 Extended Security Assurance Components

None

6. Security Requirements

This section contains the functional requirements that are provided by the TOE. These requirements consist of functional components from Part 2 of the CC.

The CC defines operations on security requirements. The font conventions listed below state the conventions used in this ST to identify the operations.

Assignment: indicated in italics

Selection: indicated in underlined text

Assignments within selections: indicated in italics and underlined text

Refinement: indicated with bold text

Iterations of security functional requirements may be included. If so, iterations are specified at the component level and all elements of the component are repeated. Iterations are identified by numbers in parentheses following the component or element (e.g., FAU_ARP.1(1)).

6.1 TOE Security Functional Requirements

The functional requirements are described in detail in the following subsections. Additionally, these requirements are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation* with the exception of completed operations.

6.1.1 Security Audit (FAU)

6.1.1.1 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) *The events in the following tables*.

Application Note: The LightSoft server and each EMS-APT server instance maintains separate audit trails and the audit functionality is always active. The following tables identify the types of audit records generated for each server type.

Application Note: The servers maintain Activity/Action Logs and Security Logs. In the following tables, the audit record description is preceded by "A:" or "S:" to identify which log the audit record is stored in. The audit records for startup of the audit function are stored in the NMSGF.log file.

Table 9 - LightSoft Auditable Events

Event	Audit Record Event	Details
Successful login	S: Login	
Failed login due to invalid user name	S: Invalid user name	Supplied user name
Failed login due to invalid password	S: Invalid password	
User Account locked due to repeated failed login attempts	S: Password is blocked	
Logout	S: Logout	
User Account disabled due to idle period expiration	S: Idle user disabled	User Account

Event	Audit Record Event	Details
User Account automatically re-enabled	S: User password reopened	User Account
User Account created	A: Create User '*username*'	User Account
User Account deleted	A: Delete User '*username*'	User Account
User Account modified	A: Edit User '*username*'	User Account
Security Preferences modified	A: Edit Security Rules	
Data item created	A: Create *item type "item name'*	Item name
Data item deleted	A: Create *item type "item name'*	Item name
Data item created	A: Create *item type "item name'*	Item name

Table 10 - EMS-APT Auditable Events

Event	Audit Record Event + Result	Details
NE (or NE component) created, deleted, or modified	A: *action* - Successful	NE or component identifier, type of item, all configuration parameter values for the item
Service created, deleted, or modified	A: *action* - Successful	Service or component identifier, type of item, all configuration parameter values for the item

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *the hostname/IP address of the client-side application*.

6.1.1.2 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide *authorized users with the Admin or Security Administrator Role (Profile)* with the capability to read *all Security Log and Activity/Action Log 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.

6.1.1.3 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 that have been granted explicit read-access.

6.1.1.4 FAU_STG.2 Guarantees of Audit Data Availability

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.2.2 The TSF shall be able to prevent unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that *all of the most recent, except for a sufficient number of the oldest records to create space to store the current record,* stored audit records will be maintained when the following conditions occur: audit storage exhaustion.

Application Note: When a new audit record is generated and storage space for it is exhausted, a sufficient number of the oldest audit records are deleted to make room for the current audit record. Typically just one record (the oldest) is deleted.

6.1.2 User Data Protection (FDP)

6.1.2.1 FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the *Ethernet Traffic Filtering SFP* on

a) Subjects: Remote network systems sending Ethernet packets through an Ethernet port on the NPTs;

b) Information: Ethernet packets; and

c) *Operation: Forwarding of received Ethernet packets.*

6.1.2.2 FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the *Ethernet Traffic Filtering SFP* based on the following types of subject and information security attributes:

a) Subject attributes: Receiving port, configured ACL;

b) Information attributes: Presumed source and destination MAC addresses.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

a) If an ACL is configured for the receiving port and it specifies permitted traffic, the packet is forwarded if the presumed source or destination MAC address is explicitly included in the ACL.

b) If an ACL is configured for the receiving port and it specifies denied traffic, the packet is forwarded if the presumed source or destination MAC address is not explicitly included in the ACL.

Application Note: ACLs may specify either source or destination addresses, but not both.

FDP_IFF.1.3 The TSF shall enforce the *no additional information flow control SFP rules.*

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules:

a) If no ACL is configured for the receiving port.

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: *no rules, based on security attributes, that explicitly deny information flows*.

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when an administrator configurable positive integer within *the range 1-5* unsuccessful authentication attempts occur related to *consecutive login failure attempts of an individual User Account*.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall *lock the User Account for an administrator configured amount of time*.

6.1.3.2 FIA_ATD.1 User Attribute Definition

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

a) User name;

b) Password;

c) Associated User Group (which specifies the LightSoft capabilities and EMS-APT Role);

d) Account Lock Status;

e) Password Expiration Value;

f) Inactivity Timer Value;

g) Account Idle Value;

h) Consecutive Unsuccessful Login Count.

6.1.3.3 FIA_UAU.1 Timing of Authentication

FIA_UAU.1.1 The TSF shall allow *no actions* on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.4 FIA_UID.1 Timing of Identification

FIA_UID.1.1 The TSF shall allow *no actions* on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.5 FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only *one dot for each supplied character* to the user while the authentication is in progress.

6.1.4 Security Management (FMT)

6.1.4.1 FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the *Ethernet Traffic Filtering SFP* to restrict the ability to query, modify the security attributes *ACLs assigned to Ethernet ports on NEs* to EMS-APT users with the Roles of *Admin, Configuration, Provisioning, or Maintenance (query only).*

6.1.4.2 FMT_MSA.3 Static Attribute Initialisation

FMT_MSA.3.1 The TSF shall enforce the *Ethernet Traffic Filtering SFP* to provide permissive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the *no roles* to specify alternative initial values to override the default values when an object or information is created.

6.1.4.3 FMT_MTD.1(1) Management of TSF Data in LightSoft

FMT_MTD.1.1(1) The TSF shall restrict the ability to query, modify, delete, *create* the *TSF data in LightSoft identified in the following table* to *the authorised roles identified in the following table*.

Application Note: To conserve space, the following abbreviations are used for the allowed operations: Query = Q, Modify = M, Delete = D, and Create = C.

Application Note: Customized Profiles may be configured as well to create customized Roles.

Table 11 - LightSoft TSF Data Access Details

TSF Data	Admin	Security	Config.	Provis.	Maint.	Obser.	Level 1	Level 2	Ex Admin	Ex Provis	Ex Monitor	NBSP *
Alarms (M:Acknowledge Alarms)	Q,M	Q	Q,M	Q,M	Q	Q	Q	Q	Q,M	Q,M	Q	Q,M
Alarm Counters	Q,M,D,C	Q,M,D,C	Q	Q	Q	Q	Q	Q	Q,M,D,C	Q	Q	Q,M,D,C
Alarm Indicators	Q,M,D,C	Q,M,D,C	Q	Q	Q	Q	Q	Q	Q,M,D,C	Q	Q	Q,M,D,C
Fault Mgmt Administration – Event Log Configuration	Q,M,C	Q,M,C										Q,M,C
Fault Mgmt Administration – Alarm Forwarder Configuration	Q,M,D,C	Q,M,D,C										Q,M,D,C
Activity Log	Q	Q										

TSF Data	Admin	Security	Config.	Provis.	Maint.	Obser.	Level 1	Level 2	Ex Admin	Ex Provis	Ex Monitor	NBSP *
Security Administration	Q,M,D,C	Q,M,D,C	Q	Q	Q				Q	Q		Q,M,D,C
Security Log	Q	Q										
Active Users* (M: force logout operation)	Q,M	Q,M	Q	Q	Q				Q	Q		Q,M

Application Note: All users may change their own password, which is one element of the User Account.

*Application Note *: NBSP is the northbound session profile, which is solely intended to be used by an OSS at the service management and/or business management layer as shown in Figure 1. A user with this profile is allowed to use the northbound CORBA interface of LightSoft to communicate with an OSS. The credentials need to be configured in an OSS for users who intend to exchange Security/Traffic/Fault management information. When a user is connected from an OSS, interactive login via the LightSoft GUI for that user is not allowed. Since an OSS (when in use) is typically continuously connected to LightSoft, any GUI login attempt will be denied for the OSS users.*

*Application Note **: Modify/Delete/Create operations are allowed for Trail management via import of XML files only.*

6.1.4.4 FMT_MTD.1(2) Management of TSF Data in EMS-APT

FMT_MTD.1.1(2) The TSF shall restrict the ability to query, modify, delete, *create* the *TSF data in EMS-APT identified in the following table* to *the authorised roles identified in the following table*.

Table 12 - EMS-APT TSF Data Access Details

TSF Data	Admin	Config.	Provis.	Maint.	Observer	Level 1	Level 2
EMS-APT Action Log	Query	n/a	n/a	n/a	n/a	n/a	n/a
EMS-APT Alarms	Query Modify* Delete	Query Modify* Delete	Query Modify* Delete	Query Modify* Delete	Query	Query	Query
EMS-APT Network Elements	Query, Modify, Delete, Create	Query Modify Delete, Create	Query Modify** Delete	Query	Query	Query	Query
EMS-APT Security Log	Query	n/a	n/a	n/a	n/a	n/a	n/a
EMS-APT Services	Query, Modify, Delete, Create	Query, Modify, Delete, Create	Query, Modify, Delete, Create	Query	Query	Query	Query
EMS-APT User Accounts	Managed via LightSoft						

Application Note: NMS user accounts with the Admin and Security profile have the same EMS access permissions (Admin in the table above). The EMS-APT Security role is only relevant when the EMS-APT is accessed independently from LightSoft. Since the EMS-APT is only accessed via LightSoft GCT functionality in the evaluated configuration, the EMSA-APT Security role is not relevant.

Application Note: NMS user accounts with the Exclusive Admin, Exclusive Provisioning and Exclusive Monitoring profiles are not assigned any EMS-APT Role, and LightSoft users with these Profiles do not have corresponding user accounts created in EMS-APT. Therefore, these LightSoft Roles have no EMS-APT access.

*Application Note *: The Modify operation for EMS-APT Alarms refers to acknowledging the Alarms.*

*Application Note **: The only modification allowed for NEs by these roles is renaming the NEs.*

6.1.4.5 FMT_SMF.1 Specification of Management Functions

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

a) Security configuration (including User Accounts) management;

b) Log management;

c) NE management;

d) Service management;

e) Alarms management.

6.1.4.6 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles *Admin, Security Administrator, Configuration, Provisioning, Maintenance, Observer, Level 1, Level 2, Exclusive Admin, Exclusive Provisioning, Exclusive Monitoring, NBSP, and (for LightSoft only) user-defined roles specifying combinations of capabilities.*

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

Application Note: In LightSoft, Roles are assigned to users via User Group association, which in turn have associated Profiles which define the capabilities for users. The Profiles also specify the EMS-APT Role associated with users.

6.2 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL2. These requirements are summarised in the following table.

Table 13 - EAL2 Assurance Requirements

Assurance Class	Component ID	Component Title
Security Target	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance

Assurance Class	Component ID	Component Title
	AGD_PRE.1	Preparative procedures
Life-Cycle Support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

6.3 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 14 - TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FAU_GEN.1	No other components.	FPT_STM.1	Satisfied by the operational environment (OE.TIME).
FAU_SAR.1	No other components.	FAU_GEN.1	Satisfied
FAU_SAR.2	No other components.	FAU_SAR.1	Satisfied
FAU_SAR.3	No other components.	FAU_SAR.1	Satisfied
FAU_SEL.1	No other components.	FAU_GEN.1, FMT_MTD.1	Satisfied Satisfied
FAU_STG.2	FAU_STG.1	FAU_GEN.1	Satisfied
FDP_IFC.1	No other components.	FDP_IFF.1	Satisfied
FDP_IFF.1	No other components.	FDP_IFC.1, FMT_MSA.3	Satisfied, Satisfied
FIA_AFL.1	No other components.	FIA_UAU.1	Satisfied
FIA_ATD.1	No other components.	None	n/a
FIA_UAU.1	No other components.	FIA_UID.1	Satisfied
FIA_UAU.7	No other components.	FIA_UAU.1	Satisfied
FIA_UID.1	No other components.	None	n/a
FMT_MSA.1	No other components.	[FDP_ACC.1 or FDP_IFC.1], FMT_SMF.1 FMT_SMR.1	 Satisfied, Satisfied, Satisfied
FMT_MSA.3	No other components.	FMT_MSA.1, FMT_SMR.1	Satisfied, Satisfied
FMT_MTD.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	No other components.	None	n/a
FMT_SMR.1	No other components.	FIA_UID.1	Satisfied

7. TOE Summary Specification

7.1 FAU_GEN.1, FAU_SAR.1, FAU_SAR.2

Audit records for the events specified in the tables included with the FAU_GEN.1 are generated. The LightSoft and EMS-APT servers generate audit records for actions taken by their users and maintain a separate audit trail. The audit trail consists of Security Logs and Activity/Action Logs; audit records for startup of the audit function are stored in the NMSGF.log file in the /sdh_home/nms/logs directory. The contents of the audit records are described in FAU_GEN.1.

The client-side GUI application provide authorized users with the LightSoft Role of Admin or Security Administrator with the ability to review audit records in a human readable form in LightSoft. Users with the EMS Role of Admin or Security Admin may review audit records in a human readable form in LightSoft. Users that do not have those capabilities or roles do not have access to any audit record information.

7.2 FAU_STG.2

Separate audit trails are maintained for LightSoft and EMS-APT.

The user access functionality of the TOE does not provide any mechanism to modify audit records. If no space is available in the database when the TOE attempts to insert a new audit record, the oldest audit record is deleted and the new record is inserted.

Users with the Security Administration capability in LightSoft, or the Admin or Security Admin role in EMS-APT, may delete audit records via archiving.

7.3 FDP_IFC.1, FDP_IFF.1

ACLs may be configured for Ethernet ports of the NPTs. Each ACL specifies a list of source and destination MAC addresses that may be permitted or denied through the interface. If the flow is permitted, received packets are forwarded; if denied, received packets are silently dropped. If no ACL is associated with a port, all packets are forwarded.

7.4 FIA_AFL.1

Consecutive login failures for each defined user account are tracked. If the administrator configured number of consecutive failures is met for a user account, that user account is automatically locked. After an administrator configured number of minutes, the account is automatically unlocked. Administrators may manually unlock the account as well.

7.5 FIA_ATD.1

The TOE maintains the following information for each LightSoft user account:

- User name
- Password
- Associated User Group (which specifies the Role)
- Account Lock Status
- Password Expiration Value
- Inactivity Timer Value
- Account Idle Value
- Consecutive Unsuccessful Login Count

The TOE maintains the following information for each EMS-APT user account:

- User name
- Associated Role

7.6 FIA_UAU.1, FIA_UID.1, FIA_UAU.7

The TOE requires all users of the client-side GUI application to successfully identify and authenticate themselves before access is granted to any TSF data or functions. User credentials are collected via the GUI and validated by the TOE. When a password is supplied, the TOE echoes a single dot for each supplied character to obscure the user input. If an invalid password is supplied, the count of unsuccessful login attempts for the User Account is incremented. If the supplied password is valid, the count is reset to 0.

7.7 FMT_MSA.1, FMT_MSA.3

ACLs for the information flow control function may be configured in the EMS-APT by users with the roles of Admin, Configuration, or Provisioning. The Maintenance role may view the ACLs. By default no ACL is associated with a port.

7.8 FMT_MTD.1

The GUI grants access to TSF data according to the Roles specified in the table included with FMT_MTD.1(1) and the Roles specified in the table included with FMT_MTD.1(2). Access is further limited by the Resource Domains associated with the User Account. Access to TSF data other than that specified in the table is prevented.

7.9 FMT_SMF.1

LightSoft and EMS-APT provide functionality for authorized users to manage the following items:

- Security configuration (including User Accounts)
- Log management
- NEs
- Services
- Alarms

7.10 FMT_SMR.1

All interactive users of the client-side GUI applications are required to successfully complete I&A, at which time the role configured for the user account is associated with the user session. For LightSoft, the Role is determined by the capabilities configured in the user's associated Profile (which is associated with the user account via the User Group). LightSoft provides default Roles, and customized Roles may also be configured (via customized Profiles and User Groups). The EMS-APT Role is also configured via the capabilities. For EMS-APT, only the default Roles are supported.

8. Protection Profile Claims

No conformance to any registered protection profile is claimed.

9. Rationale

This chapter provides the rationale for the selection of the IT security requirements, objectives, assumptions and threats. It shows that the IT security requirements are suitable to meet the security objectives, Security Requirements, and TOE security functional.

9.1 Rationale for IT Security Objectives

This section of the ST demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat and assumption is addressed by a security objective.

The following table identifies for each organizational security policy, threat and assumption, the security objective(s) that address it.

Table 15 - Security Objectives Mapping

	O.ACCESS	O.AUDITS	O.EADMIN	O.IDAUTH	O.INFFLW	O.PROTCT	OE.ECI	OE.CREDEN	OE.INSTAL	OE.MGMTNETWORK	OE.PERSON	OE.PHYCAL	OE.TIME
A.ECI							X						
A.LOCATE												X	
A.MANAGE											X		
A.MGMTNETWORK										X			
A.NOEVIL								X	X			X	
A.NOTRST								X				X	
A.PROTCT												X	
T.COMINT	X			X		X							
T.INVSRC					X								
T.LOSSOF	X			X		X							
T.NOHALT	X			X									
T.PRIVIL	X			X									
T.UNAUTHDST					X								
P.ACCACT		X		X									X
P.MANAGE	X		X	X		X		X	X		X		
P.PROTCT												X	

The following table describes the rationale for the security objectives mappings.

Table 16 - Rationale For Security Objectives Mappings

*.TYPE	Security Objectives Rationale
A.ECI	The OE.ECI objective requires that ECI personnel participate in TOE installation.
A.LOCATE	The OE.PHYCAL provides for the physical protection of the TOE.
A.MANAGE	The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.

*.TYPE	Security Objectives Rationale
A.MGMTNETWORK	The OE.MGMTNETWORK objective ensures that a segregated network will protect the intra-TOE traffic and limit the traffic entering the segregated network from the general enterprise network.
A.NOEVIL	The OE.INSTAL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.NOTRST	The OE.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.PROTCT	The OE.PHYCAL provides for the physical protection of the TOE hardware and software.
T.COMINT	The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.INVSRC	The O.INFFLW objective states that the TOE must be able to filter traffic based on a configured set of source MAC addresses.
T.LOSSOF	The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.NOHALT	The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
T.PRIVIL	The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
T.UNAUTHDST	The O.INFFLW objective states that the TOE must be able to filter traffic based on a configured set of destination MAC addresses.
P.ACCACT	The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated. OE.TIME will provided a time stamp for each audit.
P.MANAGE	The OE.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The OE.INSTAL objective supports the OE.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective provides for TOE self-protection.
P.PROTCT	The OE.PHYCAL objective protects the TOE from unauthorized physical modifications.

9.2 Security Requirements Rationale

9.2.1 Rationale for Security Requirements of the TOE Objectives

This section provides rationale for the Security Functional Requirements and/or Security Assurance Requirements demonstrating that the SFRs/SARs are suitable to address the security objectives.

The following table identifies for each TOE security objective, the SFR(s) and/or SAR(s) that address it.

Table 17 - SFRs/SARs to Security Objectives Mapping

	O.ACCESS	O.AUDITS	O.EADMIN	O.IDAUTH	O.INVFLW	O.PROTCT
FAU_GEN.1		X				
FAU_SAR.1			X			
FAU_SAR.2	X			X		
FAU_STG.2	X			X		X
FDP_IFC.1					X	
FDP_IFF.1					X	
FIA_AFL.1	X			X		
FIA_ATD.1				X		
FIA_UAU.1	X			X		
FIA_UAU.7	X			X		
FIA_UID.1	X			X		
FMT_MSA.1	X					
FMT_MSA.3					X	
FMT_MTD.1	X			X		X
FMT_SMF.1			X			
FMT_SMR.1				X		

The following table provides the detail of TOE security objective(s).

Table 18 - Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.ACCESS	The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. Users authorized to access the TOE are validated using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. This process is supported by defined actions when repeated invalid credentials are supplied [FIA_AFL.1]. The I&A process is also supported by protecting the supplied password from view [FIA_UAU.7]. Only authorized

Security Objective	SFR and Rationale
	administrators of the TOE may access TSF data and functions, and only according to their permissions [FMT_MTD.1]. The ability to configure ACLs is provided, and access is limited to specified roles [FMT_MSA.1].
O.AUDITS	Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1].
O.EADMIN	The TOE must provide the ability to review the audit trail [FAU_SAR.1]. The TOE must provide the ability for authorized administrators to effectively manage the TOE [FMT_SMF.1].
O.IDAUTH	The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The TOE is required to protect the stored audit records from unauthorized deletion [FAU_STG.2]. Security attributes of subjects use to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are validated using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The process includes defined actions when repeated invalid credentials are supplied [FIA_AFL.1]. The I&A process is also supported by protecting the supplied password from view [FIA_UAU.7]. Only authorized administrators may access TSF data and functions, and only according to their permissions [FMT_MTD.1]. The TOE must be able to recognize the different roles that exist for the TOE [FMT_SMR.1].
O.INFFLW	The TOE restricts Ethernet traffic flows per configured ACLs [FDP_IFC.1, FDP_IFF.1]. By default, no ACLs are associated with Ethernet ports and all traffic is permitted to flow [FMT_MSA.3].
O.PROTCT	The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. Only authorized administrators may access TSF data and functions, and only according to their permissions [FMT_MTD.1].

9.2.2 Security Assurance Requirements Rationale

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

A) Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 from part 3 of the Common Criteria.