



Your Partner for Growth

# **ECI LightSOFT, EMS-NPT, NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800 Software Security Target**

Version 1.3

July 26, 2021

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

<u>Rev</u>	<u>Description</u>
1.0	October 16, 2018, Initial release
1.1	October 21, 2018, Incorporated vendor comments
1.2	March 6, 2019, Addressed lab ORs
1.3	July 26, 2021, Updates for final configuration

**TABLE OF CONTENTS**

**1. SECURITY TARGET INTRODUCTION..... 7**

**1.1 Security Target Reference.....7**

**1.2 TOE Reference .....7**

**1.3 Evaluation Assurance Level.....7**

**1.4 TOE Overview.....7**

1.4.1 Usage and Major Security Features ..... 7

1.4.1.1 LightSOFT ..... 7

1.4.1.2 EMS-NPT ..... 9

1.4.1.3 NPTs ..... 9

1.4.2 Required Non-TOE Hardware/Software/Firmware ..... 10

**1.5 TOE Description .....11**

1.5.1 Physical Boundary ..... 12

1.5.2 Logical Boundary..... 13

1.5.2.1 Audit ..... 13

1.5.2.2 Management..... 13

1.5.2.3 I&A ..... 13

1.5.2.4 Information Flow Control..... 13

1.5.3 TOE Data ..... 13

**1.6 Evaluated Configuration .....15**

**1.7 Functionality Excluded from the Evaluation .....16**

**2. CONFORMANCE CLAIMS..... 17**

**2.1 Common Criteria Conformance.....17**

**2.2 Security Requirement Package Conformance .....17**

**2.3 Protection Profile Conformance.....17**

**3. SECURITY PROBLEM DEFINITION ..... 18**

**3.1 Introduction.....18**

**3.2 Assumptions.....18**

**3.3 Threats .....18**

**3.4 Organisational Security Policies.....19**

**4. SECURITY OBJECTIVES..... 20**

**4.1 Security Objectives for the TOE .....20**

**4.2 Security Objectives for the Operational Environment.....20**

**5. EXTENDED COMPONENTS DEFINITION ..... 22**

**5.1 Extended Security Functional Components .....22**

**5.2 Extended Security Assurance Components.....22**

**6. SECURITY REQUIREMENTS..... 23**

**6.1 TOE Security Functional Requirements .....23**

6.1.1 Security Audit (FAU) ..... 23

6.1.1.1 FAU\_GEN.1 Audit Data Generation ..... 23

6.1.1.2 FAU\_SAR.1 Audit Review ..... 24

6.1.1.3 FAU\_SAR.2 Restricted Audit Review ..... 24

6.1.1.4 FAU\_STG.2 Guarantees of Audit Data Availability ..... 25

6.1.2 User Data Protection (FDP)..... 25

6.1.2.1 FDP_IFC.1 Subset Information Flow Control.....	25
6.1.2.2 FDP_IFF.1 Simple Security Attributes.....	25
6.1.3 Identification and Authentication (FIA) .....	26
6.1.3.1 FIA_AFL.1 Authentication Failure Handling.....	26
6.1.3.2 FIA_ATD.1 User Attribute Definition .....	26
6.1.3.3 FIA_UAU.1 Timing of Authentication.....	26
6.1.3.4 FIA_UID.1 Timing of Identification .....	26
6.1.3.5 FIA_UAU.7 Protected Authentication Feedback .....	27
6.1.4 Security Management (FMT) .....	27
6.1.4.1 FMT_MSA.1 Management of Security Attributes .....	27
6.1.4.2 FMT_MSA.3 Static Attribute Initialisation.....	27
6.1.4.3 FMT_MTD.1(1) Management of TSF Data in LightSOFT.....	27
6.1.4.4 FMT_MTD.1(2) Management of TSF Data in EMS-NPT.....	28
6.1.4.5 FMT_SMF.1 Specification of Management Functions .....	29
6.1.4.6 FMT_SMR.1 Security Roles .....	29
<b>6.2 TOE Security Assurance Requirements .....</b>	<b>29</b>
<b>6.3 CC Component Hierarchies and Dependencies .....</b>	<b>30</b>
<b>7. TOE SUMMARY SPECIFICATION.....</b>	<b>31</b>
<b>7.1 FAU_GEN.1, FAU_SAR.1, FAU_SAR.2 .....</b>	<b>31</b>
<b>7.2 FAU_STG.2 .....</b>	<b>31</b>
<b>7.3 FDP_IFC.1, FDP_IFF.1.....</b>	<b>31</b>
<b>7.4 FIA_AFL.1.....</b>	<b>31</b>
<b>7.5 FIA_ATD.1 .....</b>	<b>31</b>
<b>7.6 FIA_UAU.1, FIA_UID.1, FIA_UAU.7 .....</b>	<b>32</b>
<b>7.7 FMT_MSA.1, FMT_MSA.3.....</b>	<b>32</b>
<b>7.8 FMT_MTD.1 .....</b>	<b>32</b>
<b>7.9 FMT_SMF.1 .....</b>	<b>32</b>
<b>7.10 FMT_SMR.1.....</b>	<b>32</b>
<b>8. PROTECTION PROFILE CLAIMS.....</b>	<b>33</b>
<b>9. RATIONALE .....</b>	<b>34</b>
<b>9.1 Rationale for IT Security Objectives.....</b>	<b>34</b>
<b>9.2 Security Requirements Rationale.....</b>	<b>36</b>
9.2.1 Rationale for Security Requirements of the TOE Objectives.....	36
9.2.2 Security Assurance Requirements Rationale.....	37
<b>ANNEX A AVAILABLE UPDATES.....</b>	<b>38</b>

**LIST OF FIGURES**

Figure 1 - Management Architecture..... 8  
 Figure 2 - Representative TOE Deployment ..... 12  
 Figure 3 - Physical Boundary ..... 12

**LIST OF TABLES**

Table 1 - LightSOFT/EMS-NPT Server Minimum Requirements ..... 10  
 Table 2 - LightSOFT Client-Side Application Minimum Requirements..... 11  
 Table 3 - TOE Data Descriptions ..... 14  
 Table 4 - Assumptions..... 18  
 Table 5 - Threats..... 18  
 Table 6 - Organisational Security Policies ..... 19  
 Table 7 - Security Objectives for the TOE..... 20  
 Table 8 - Security Objectives of the Operational Environment ..... 20  
 Table 9 - LightSOFT Auditable Events ..... 23  
 Table 10 - EMS-NPT Auditable Events..... 24  
 Table 11 - LightSOFT TSF Data Access Details ..... 27  
 Table 12 - EMS-NPT TSF Data Access Details ..... 28  
 Table 13 - EAL2 Assurance Requirements ..... 29  
 Table 14 - TOE SFR Dependency Rationale ..... 30  
 Table 15 - Security Objectives Mapping..... 34  
 Table 16 - Rationale For Security Objectives Mappings ..... 34  
 Table 17 - SFRs/SARs to Security Objectives Mapping ..... 36  
 Table 18 - Security Objectives to SFR Rationale..... 36

## ACRONYMS LIST

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

## 1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the ECI LightSOFT, EMS-NPT, NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800 Software. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5*. As such, the spelling of terms is presented using the internationally accepted English.

### 1.1 Security Target Reference

ECI LightSOFT, EMS-NPT, NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800 Software Security Target, Version 1.3, dated July 26, 2021.

### 1.2 TOE Reference

Composite system comprised of ECI LightSOFT Software Version 14.91 (build 1307) along with required fixes as mentioned in Annex A; EMS-NPT Software Version 7.6 (build 229) along with required fixes as mentioned in Annex A; NPT-1022 Software Version 7.6 (build 269), NPT-1050 Software Version 7.6 (build 269); NPT-1200 Software Version 7.6 (build 269); NPT-1300 Software Version 7.6 (build 269); and NPT-1800 Software Version 7.6 (build 269).

### 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 5*.

### 1.4 TOE Overview

#### 1.4.1 Usage and Major Security Features

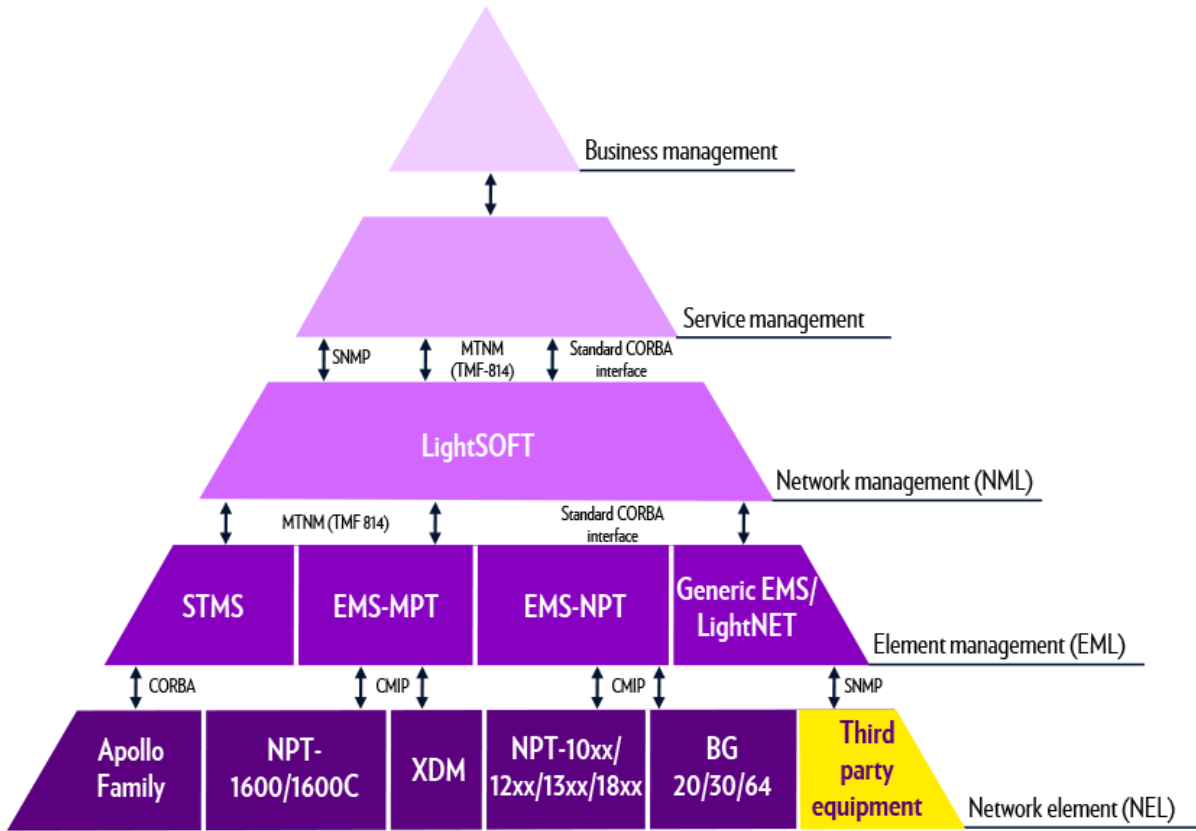
The TOE consists of the LightSOFT and EMS-NPT TOE components providing control and monitoring functions for the NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800 components (executing on supported appliances) that provide packet transport services. These systems are intended for use in Service Provider (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-NPT) is tailored to a specific type of NE. For this evaluation, only the EMS-NPT (for the NPTs) is used with LightSOFT, and the only NEL types managed are the NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800.

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-NPT**

The EMS-NPT is an advanced EMS designed to manage the Native Packet Transport (NPT) products. It has an advanced architecture which supports multiple operating systems for integrated management, either standalone or with the NMS. For this evaluation, the EMS-NPT is always integrated with the NMS and is only used to manage the NPT family (and specifically the NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800).

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

Users access the EMS-NPT functions via the LightSOFT GUI. LightSOFT automatically invokes EMS-NPT 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-NPT session.

EMS-NPT 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-NPT. Each user is associated with one of the EMS-NPT 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-NPT.

#### **1.4.1.3 NPTs**

The NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800 are NE appliances that provide Native Packet Transport (NPT) services within the SP network. The NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800 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-1022 - Designed for access environments, providing packet throughput ranging from 10 Gbps to 60 Gbps.

2. NPT-1050 – MPLS-based multiservice packet optical transport platform optimized for the metro access aggregation and access nodes, providing packet throughput ranging from 72 Gbps to 120 Gbps.
3. NPT-1200 – Designed for metro aggregation environments, providing packet throughput ranging from 70 Gbps to 240 Gbps.
4. NPT-1300 – MPLS-based multiservice packet transport platform, optimized for high-capacity metro aggregation applications, providing packet throughput up to 920 Gbps.
5. NPT-1800 – MPLS-based multiservice packet transport platform, optimized for high-capacity metro-core nodes, providing packet throughput up to 2 Tbps.

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-NPT 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-NPT. For this evaluation, once installed the appliances are managed solely via LightSOFT/EMS-NPT.

#### 1.4.2 Required Non-TOE Hardware/Software/Firmware

The TOE consists of LightSOFT and EMS-NPT software executing on one or more dedicated Solaris servers, (optionally) the LightSOFT client-side application executing on Solaris or Linux workstations, and the NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800 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-NPT 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-NPT Server Minimum Requirements**

Item	Requirements
Base Hardware	7 virtual CPUs
Memory	48 GB
Hard Disk	85 GB
Operating System	Hardened Solaris x86 11.3 Rev 10
Desktop	CDE 5.10, X11 Version 1.0.3
CORBA	Orbix 6.3.7

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
Operating System	Solaris x86 11.3 Rev 10
CORBA	Orbix 6.3.7

The NEs managed by LightSOFT/EMS-NPT may be any combination of the NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800.

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 TOE consists of:

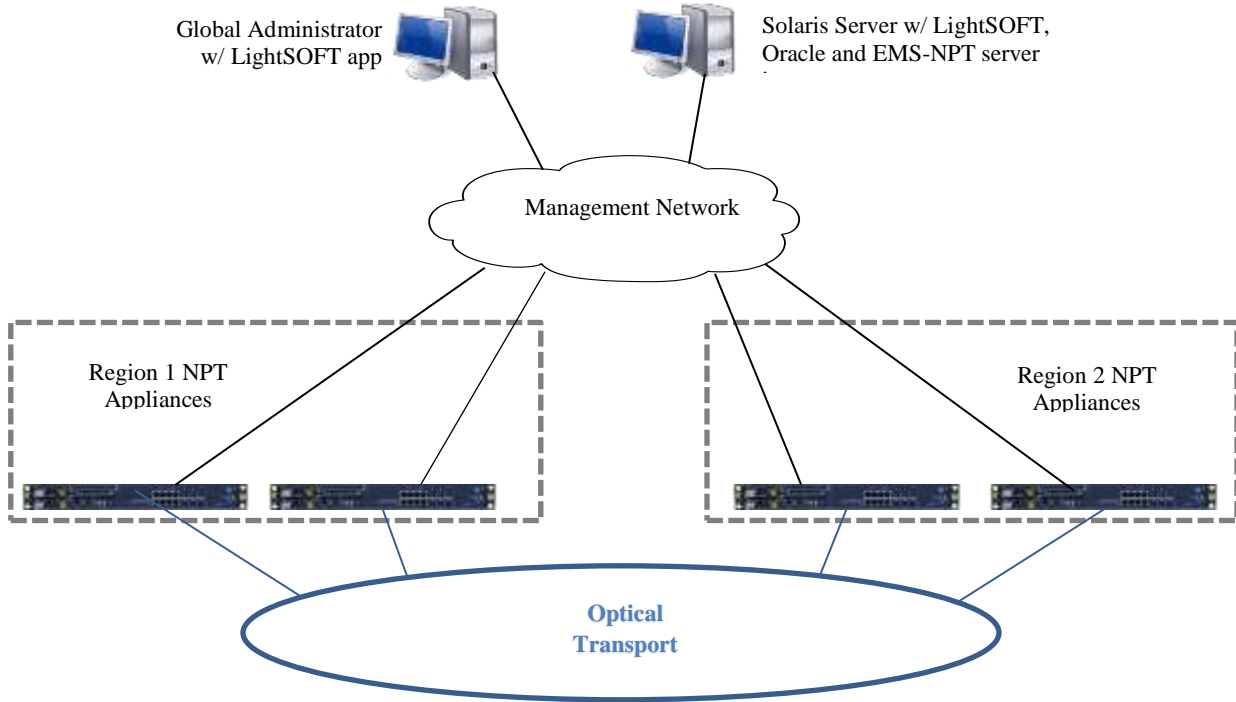
1. One instance of the LightSOFT server component executing in one zone on a dedicated Solaris server with Solaris OS.
2. One instance of the EMS-NPT server component executing on the same server as the LightSOFT server. The EMS-NPT server uses a separate zone. The MySQL database runs in this zone.
3. 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 executing on Solaris workstation or server with Solaris OS.
5. One or more instances of NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800 software executing on supported appliances.

Software installation by ECI personnel is included in the purchase of these products. ECI personnel deliver binary images of LightSOFT, EMS-NPT and NPT software to the customer during the installation process.

The software is 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.

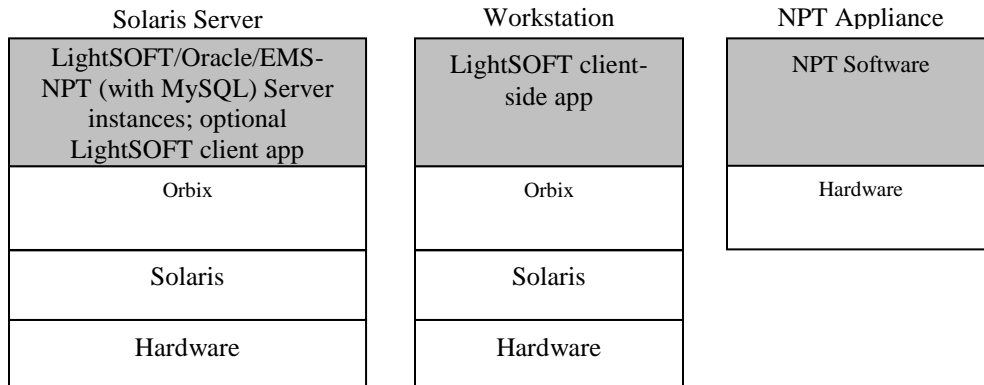
**Figure 2 - Representative TOE Deployment**



**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 14.91 Getting Started & Administration Guide*
2. *LightSOFT Version 14.91 Fault Management and Performance Monitoring Guide*
3. *LightSOFT V14.91 – SW Installation, Update and Configuration Procedure*

4. *EMS-NPT Version 7.6 Installation Guide (Solaris)*
5. *EMS-NPT Version 7.6 User Guide*
6. *EMS-NPT Version 7.6 Service Management Guide*
7. *EMS-NPT Version 7.6 Performance Management Guide*
8. *EMS-NPT Version 7.6 Network Management Guide*
9. *EMS-NPT Version 7.6 Supporting Information*
10. *Neptune (Packet) Version 7.6 Reference Manual*
11. *ECI LightSOFT, EMS-NPT, NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800 Software Common Criteria Supplement*
12. *Common Phase 11.3 Activities for Preparation, Installation and Upgrade of Management Systems Infrastructure*
13. *Common Management HW Preparation and Configuration Activities*
14. *ECILoracle v12 – SW Installation and Upgrade Procedure*

All TOE documentation is provided as PDF files that are downloaded from ECI's Customer Portal.

## **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-NPT 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-NPT Action Log	Contains audit records of configuration actions by users of EMS-NPT.
EMS-NPT Alarms	Alarms from the NEs or EMS-NPT for operational conditions.
EMS-NPT Network Elements	Specify the NPT appliances that are managed and their configuration.
EMS-NPT Security Log	Contains audit records of logins/logouts for user access.
EMS-NPT Services	Defines the configuration of Services within NEs.
EMS-NPT User Accounts	Define the authorized users of an EMS-NPT instance. Note that user accounts are managed via LightSOFT. Attributes include: <ul style="list-style-type: none"> <li>• Username</li> <li>• Assigned Role</li> </ul>
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-NPT for operational conditions.
LightSOFT Profiles	Define the access permissions (capabilities) to be associated with a user. The capabilities also specify the EMS-NPT Role (or none) for associated users.
LightSOFT Resource Domains	Define the resource domains the managed elements may be grouped into. Attributes include: <ul style="list-style-type: none"> <li>• Resource Domain Name</li> <li>• Associated MEs</li> </ul>
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: <ul style="list-style-type: none"> <li>• Minimum Password Length</li> <li>• Default Password Expiration</li> <li>• Password Reuse History</li> <li>• Maximum Unsuccessful Login Attempts</li> <li>• Login Reactivation Time</li> <li>• Default Inactivity Timeout</li> <li>• Inactivity Timeout Action</li> <li>• Strong Password Enforcement</li> <li>• Account Becomes Idle Time</li> <li>• Action Upon Becoming Idle</li> </ul>
LightSOFT User Accounts	Define the authorized users of LightSOFT. Attributes include: <ul style="list-style-type: none"> <li>• Username</li> <li>• Password</li> <li>• Associated User Group</li> <li>• Account Lock Status</li> <li>• Password Expiration Date</li> <li>• Inactivity Timeout Value</li> <li>• Account Idle Value</li> <li>• Consecutive Unsuccessful Login Count</li> <li>• EMS-NPT associated Role (or none)</li> </ul>

TOE Data	Description
LightSOFT User Groups	Define user groups within LightSOFT. Attributes include: <ul style="list-style-type: none"> <li>• Group name</li> <li>• Associated Users</li> <li>• Associated Profile</li> <li>• Associated Resource Domains</li> </ul>

## 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-NPT, and the permissions for those Roles are not modified.
3. User Accounts are defined in LightSOFT and synced between LightSOFT and EMS-NPT.
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-NPT 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-NPT 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)
6. Management of the NEs via any mechanisms other than LightSOFT and EMS-NPT.
7. HTTP for remote Xterminal access.



## **2. Conformance Claims**

### **2.1 Common Criteria Conformance**

Common Criteria version: Version 3.1 Revision 5, dated April 2017

Common Criteria conformance: Part 2 conformant 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**

<b>A.Type</b>	<b>Description</b>
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 private, 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.
A.ORBIX	Orbix provides reliable communication for TSF data transmitted between LightSOFT and EMS-NPT.
A.SOLARIS	Solaris provides separation between LightSOFT, EMS-NPT and Oracle zones on a single physical server.

#### 3.3 Threats

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

**Table 5 - Threats**

<b>T.Type</b>	<b>Description</b>
T.COMINT	An unauthorized person may attempt to compromise the integrity of TOE data by bypassing a security mechanism.

<b>T.Type</b>	<b>Description</b>
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.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**

<b>P.Type</b>	<b>Description</b>
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.MGMTNET WORK	The operational environment will provide a private, 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.
OE.ORBIX	Orbix provides reliable communication for TSF data transmitted between LightSOFT and EMS-NPT.
OE.SOLARIS	Solaris provides separation between LightSOFT, EMS-NPT and Oracle zones on a single physical server.



## **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-NPT 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 ‘ <i>username</i> ’	User Account
User Account deleted	A: Delete User ‘ <i>username</i> ’	User Account
User Account modified	A: Edit User ‘ <i>username</i> ’	User Account
Security Preferences modified	A: Edit Security Rules	
Data item created	A: Create <i>item type</i> “ <i>item name</i> ”	Item name
Data item deleted	A: Create <i>item type</i> “ <i>item name</i> ”	Item name
Data item created	A: Create <i>item type</i> “ <i>item name</i> ”	Item name

**Table 10 - EMS-NPT Auditable Events**

Event	Audit Record Event + Result	Details
NE (or NE component) created, deleted, or modified	A: <i>action</i> - Successful	NE or component identifier, type of item, all configuration parameter values for the item
Service created, deleted, or modified	A: <i>action</i> - 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, maintaining the configured number of records*, stored audit records will be maintained when the following conditions occur: audit storage exhaustion.

*Application Note: The audit logs are automatically archived according to a configured time interval (in days). When the archival is performed, the content of the log is reduced to the configured number of records.*

#### **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 *rule that all traffic received on a port for which no ACL is configured is permitted to flow*.

FDP\_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: *none*.

FDP\_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules:  
*none.*

### **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-NPT 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-NPT 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.
Alarms (M:Acknowledge Alarms)	Q,M	Q	Q,M	Q,M	Q	Q
Alarm Counters	Q,M,D,C	Q,M,D,C	Q	Q	Q	Q
Alarm Indicators	Q,M,D,C	Q,M,D,C	Q	Q	Q	Q
Fault Mgmt Administration – Event Log Configuration	Q,M,C	Q,M,C				
Fault Mgmt Administration – Alarm Forwarder Configuration	Q,M,D,C	Q,M,D,C				
Activity Log	Q	Q				

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

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

*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-NPT

FMT\_MTD.1.1(2) The TSF shall restrict the ability to query, modify, delete, create the TSF data in EMS-NPT identified in the following table to the authorised roles identified in the following table.

**Table 12 - EMS-NPT TSF Data Access Details**

TSF Data	Admin	Config.	Provis.	Maint.	Obs.
EMS-NPT Activity Log	Query	n/a	n/a	n/a	n/a
EMS-NPT Alarms	Query Modify* Delete	Query Modify* Delete	Query Modify* Delete	Query Modify* Delete	Query
EMS-NPT Network Elements	Query, Modify, Delete, Create	Query Modify**	Query Modify**	Query	Query
EMS-NPT Security Log	Query	n/a	n/a	n/a	n/a
EMS-NPT Services	Query, Modify, Delete, Create	Query, Modify, Delete, Create	Query, Modify, Delete, Create	Query	Query
EMS-NPT 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-NPT Security role is only relevant when the EMS-NPT is accessed independently from LightSOFT. Since the EMS-NPT is only accessed via LightSOFT GCT functionality in the evaluated configuration, the EMS-NPT Security role is not relevant.*

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

*Application Note \*\*: The only modification allowed for NEs by these roles is changing an NE name.*

### 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.*

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-NPT 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
	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_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-NPT 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-NPT.

The user access functionality of the TOE does not provide any mechanism to modify audit records. On a configured periodic basis, audit records are automatically archived. This prunes the audit log to the configured number of records, with the most recent records being retained.

Users with the Security Administration capability in LightSOFT, or the Admin or Security Admin role in EMS-NPT, 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-NPT 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-NPT 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-NPT 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-NPT Role is also configured via the capabilities. For EMS-NPT, 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.INFLW	O.PROTCT	OE.ECI	OE.CREDEN	OE.INSTAL	OE.MGMTNETWORK	OE.PERSON	OE.PHYCAL	OE.TIME	OE.ORBIX	OE.SOLARIS
A.ECI							X								
A.LOCATE												X			
A.MANAGE											X				
A.MGMTNETWORK										X					
A.NOEVIL								X	X			X			
A.NOTRST								X				X			
A.PROTCT												X			
A.ORBIX														X	
A.SOLARIS															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.

*.TYPE	Security Objectives Rationale
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.
A.MGMTNETWORK	The OE.MGMTNETWORK objective ensures that a private, 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.
A.ORBIX	The OE.ORBIX objective ensures that Orbix provides reliable communication for TSF data transmitted between LightSOFT and EMS-NPT.
A.SOLARIS	The OE.SOLARIS objective ensures that Solaris provides separation between LightSOFT, EMS-NPT and Oracle zones on a single physical server.
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.

## **Annex A Available Updates**

At the time of the evaluation, the following updates are available for LightSOFT and EMS-NPT:

### **LightSoft updates**

- NA1491\_1307-100 27
- NG1491\_1307-100 27
- NG1491\_1307-200 8
- NG1491\_1307-300 12
- NSx1491\_1307-100 27
- NSx1491\_1307-200 8
- NSx1491\_1307-300 12
- NT1491\_1307-100 27
- OR0600-01 4
- PMx1491\_1307-100 27
- WL0213-001 1

### **EMS-NPT updates**

- BC0760-01 1
- BS0760-01 1
- BS0760-02 1
- BS0760-03 1