Indian CC Certification Scheme (IC3S)

Certification Report

Report Number : IC3S/KOL01/ECITelecom/EAL2/0420/0019 /CR

Product / system : **Composite system comprised of ECI LightSOFT Software Version 15.5 (build 06301) along with required fixes as mentioned in Annex A; STMS Software Version 9.5R02.00 (build 354237) along with required fixes as mentioned in Annex A; Apollo Software Version 9.5R02.00 (build 355612).The Apollo Software executes on the following Apollo platforms: OPT9603, OPT9608, OPT9624, OPT9904X, OPT9914, and OPT9932.**

Dated: 07 March 2021
Version: 1.0

Government of India
Ministry of Electronics & Information Technology
Standardization, Testing and Quality Certification Directorate
6. CGO Complex, Lodi Road, New Delhi – 110003
India

Product developer:	**ECI Telecom Ltd.** 30 Hasivim Street, Petach Tikvah, 4959388 ,Israel
TOE evaluation sponsored by:	**ECI Telecom Ltd**. 30 Hasivim Street, Petach Tikvah, 4959388 ,Israel
Evaluation facility:	**Common Criteria Test Laboratory**, **ERTL (East**), 63 DN-Block, Sector V, Salt Lake, Kolkata-700091, India.
Evaluation Personnel:	**Evaluators:** Malabika Ghose & Sumit Jaiswal **Test engineers:** Abhisek Roy Chowdhury
Evaluation report:	C3S/KOL01/ECITelecom/EAL2/0420/0019/ETR/0031
Validation Personnel:	**T**apas Bandyopadhyay, Scientist F, STQC, Govt. of India

Table of Contents

Contents

PART A: CERTIFICATION STATEMENT AND BACKGROUND OF THE CERTIFICATION BODY

A1 Certification Statement

The product below has been evaluated under the terms of the Indian Common Criteria Certification Scheme (IC3S) and has met the stated Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.	
Sponsor	**ECI Telecom Ltd. ,**30 Hasivim Street, Petach Tikvah, 4959388 ,Israel
Developer	**ECI Telecom Ltd. ,**30 Hasivim Street, Petach Tikvah, 4959388 ,Israel
The Target of Evaluation (TOE)	**Composite system comprised of ECI LightSOFT Software Version 15.5 (build 06301) along with required fixes as mentioned in Annex A; STMS Software Version 9.5R02.00 (build 354237) along with required fixes as mentioned in Annex A; Apollo Software Version 9.5R02.00 (build 355612). The Apollo Software executes on the following Apollo platforms: OPT9603, OPT9608, OPT9624, OPT9904X, OPT9914, and OPT9932**.
Security Target	**ECI LightSOFT v15.5, STMS v9.5 and Apollo Software v9.5 on OPT9603, OPT9608, OPT9624, OPT9904X, OPT9914, and OPT9932 Security Target , Version 1.3**
Brief description of product	The TOE consists of the LightSOFT and STMS TOE components providing control and monitoring functions for the Apollo components (executing on supported appliances) that provide packet transport services. These systems are intended for use in Service Provider (SP) environments. 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. The STMS is an advanced EMS designed to manage the Apollo products. It has an advanced architecture that supports multiple operating systems for integrated management, either standalone or with the NMS. For this evaluation, the STMS is always integrated with the NMS and is only used to manage the Apollo family (and specifically the Apollo OPT9603, OPT9608, OPT9624, OPT9904X, OPT9914 and OPT9932. The Apollo OPT9603, OPT9608, OPT9624, OPT9904X and OPT9914 are NE appliances that provide Optical Transport (OPT) services within the SP network. The Apollo software is the software executing on the appliances. The appliances are a family of carrier-class Dense Wave Division Multiplexing (DWDM) and Optical Transport Networking (OTN) platforms providing multiservice layer 1 transport with integrated layer 2 services.
Common Criteria Standard	Common Criteria Standard Version 3.1 Revision 5
CC Part 2 [CC-II]	Conformant
CC Part 3 [CC-III]	Conformant
EAL	EAL2
Evaluation Lab	Common Criteria Test Laboratory, ERTL(E), Kolkata, India
Date Authorized	16-04-2020

A2. About the Certification Body

STQC IT Certification Services, the IT Certification Body of Standardization Testing and Quality Certification – was established in 1998 and offers a variety of services in the context of security evaluation and validation. It is the first Certification Body in India for BS 7799/ISO 27001 certification of Information Security Management Systems (ISMS). The Indian CC Certification Scheme (IC3S) is the IT security evaluation & certification Scheme based on Common Criteria standards, it is established by Govt. of India under Department of Information Technology, STQC Directorate to evaluate & certify the trustworthiness of security features in Information Technology (IT) products and systems. The IC3S is an Indian independent third party evaluation and certification scheme for evaluating the security functions or mechanisms of the IT products. It also provides framework for the International Mutual Recognition of such certificates with the member countries of CCRA (Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security). The principal participants in the scheme are:

a) Applicant (Sponsor/Developer) of IT security evaluations;
b) STQC Certification Body (STQC/MeitY/Govt. of India);
c) Common Criteria Testing Laboratories (CCTLs).

A3 Specifications of the Certification Procedure

The certification body operates under the official administrative procedures according to the criteria and procedures laid down in the following:

- ISO/IEC Guide 65, and the requirements laid down in Annex C of CCRA
- Indian Common Certification Scheme (IC3S)
- STQC/CC/DO2: Standard Operating Procedure (SOP) for Certification Body - Quality Manual – describes the quality management system for the Scheme.
- Common Criteria for Information Technology Security Evaluation (CC) part 1-3, Version 3.1, Revision 5
- Common Evaluation Methodology (CEM) Version 3.1., Revision 5

A4 Process of Evaluation and Certification

The certification body monitors each individual evaluation to ensure uniform procedures, interpretations of the criteria, and ratings. The TOE has undergone the certification procedure at **STQC IT Certification Body**. The evaluation of the product was conducted by the evaluation body Common Criteria Test Laboratory (CCTL), ERTL (East), DN Block, Sector V, Salt Lake, Kolkata-700091, India. Hereafter this has been referred as CCTL. The evaluation facility is recognized under the IC3S scheme of STQC IT Certification Body. **ECI Telecom Ltd**., 30 Hasivim Street, Petach Tikvah, 4959388, Israel is the developer and sponsor of the TOE evaluation.

The certification process is concluded with the completion of this certification report.

This evaluation was completed on **19 January 2022** after submission of [ETR] to the certification body. The confirmation of the evaluation assurance level (EAL) only applies on the condition that

- all stated condition regarding configuration and operation, as given in part B of this report, are observed,
- The product is operated – where indicated – in the operating environment described.

This certification report applies only to the version and release of the product indicated here. The validity of the certificate can be extended to cover new versions and releases of the product, provided the applicant applies for re-certification of the modified product, in accordance with the procedural requirements, and provided the evaluation does not reveal any security deficiencies.

A5 Publication

The following Certification Results consist of Sections B1 to B11 of this report. The TOE will be included in the list of the products certified under IC3S Scheme of STQC IT Certification Body. The list of certified products is published at regular intervals in the Internet at http://www.commoncriteria-india.gov.in. Further copies of this certification report may be ordered from the sponsor of the product. The certification report may also be obtained in electronic form on request to the Certification Body.

PART B: CERTIFICATION RESULTS

B.1 Executive Summary

B.1.1 Introduction

The Certification Report documents the outcome of Common Criteria security evaluation of the TOE. It presents the evaluation results and the conformance results. This certificate is intended to assist the prospective buyers and users when judging the suitability of the IT security of the product for specified requirements.

Prospective buyers and users are advised to read this report in conjunction with the referred [ST] of the product, which specifies the functional, environmental and assurance requirements.

The evaluation was performed by Common Criteria Test Laboratory (CCTL), ERTL (East), DN Block, Sector V, Salt Lake, Kolkata-700091, India. The information in the test report is derived from the [ST] written by the developer and the Evaluation Technical Report [ETR] written by Common Criteria Test Laboratory [CCTL, ERTL (E)], ERTL (EAST), Block-DN Sector-V, Kolkata, India. The evaluation team determined the product to be CC Version 3.1, Part 2 and Part 3 conformant and concluded that the Common Criteria requirements for Evaluation Assurance Level (**EAL 2**) have been met.

B 1.2 Evaluated product and TOE

The TOE consists of the LightSOFT and STMS TOE components providing control and monitoring functions for the Apollo components (executing on supported appliances) that provide packet transport services. These systems are intended for use in Service Provider (SP) environments. Composite system comprised of ECI LightSOFT Software Version 15.5 (build 06301) along with required fixes; STMS Software Version 9.5R02.00 (build 354237) along with required fixes; Apollo Software Version 9.5R02.00 (build 355612).The Apollo Software executes on the following Apollo platforms: OPT9603, OPT9608, OPT9624, OPT9904X, OPT9914, and OPT9932.

The TOE consists of the LightSOFT and STMS TOE components providing control and monitoring functions for the Apollo components (executing on supported appliances) that provide packet transport services. These systems are intended for use in Service Provider (SP) environments.

The evaluated sub-set and configuration of the product is described in this report as the Target of Evaluation (TOE). The Evaluated Configuration, its security functions, assumed environment, architectural information and evaluated configuration are given below (Refer B2 to B5).

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.

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. STMS) is tailored to a specific type of NE. For this evaluation, only the STMS (for the Apollo platforms) is used with LightSOFT, and the only NEL types managed are the Apollo OPT9603, OPT9608, OPT9624, OPT9904X, OPT9914 and OPT9932.

The **STMS is** an advanced EMS designed to manage the Apollo products. It has an advanced architecture, which supports multiple operating systems for integrated management, either standalone or with the NMS. For this evaluation, the STMS is always integrated with the NMS and is only used to manage the Apollo family (and specifically the Apollo OPT9603, OPT9608, OPT9624, OPT9904X, OPT9914 and OPT9932).

The Apollo family members included in the evaluation are:

1. OPT9603 – 2 RU converged solution platform supporting 1.6T of Ethernet, SDH, and Fiber Channel interfaces for Access networks and WDM with ROADM functionality.
2. OPT9608 – 5 RU converged solution platform supporting 4.8T of Ethernet, SDH, and Fiber Channel interfaces for Metro/Access networks, and WDM with ROADM functionality.
3. OPT9624 – 15 RU converged solution platform supporting 14.4T of Ethernet, SDH, and Fiber Channel interfaces for Core/Metro networks and WDM with ROADM functionality.
4. OPT9904X – 5 RU multiservice platform integrates 2.8T ODU cross connect of Ethernet/MPLS, SDH, and Fiber Channel interfaces for metro access networks.
5. OPT9914 – 22 RU multiservice platform integrate 5.6T ODU cross connect of Ethernet/MPLS, SDH, and Fiber Channel interfaces.
6. OPT9932 – Full rack multiservice platform integrate 16T ODU cross connect of Ethernet/MPLS, SDH, and Fiber Channel interfaces.

The evaluated version of the product, with its guidance documents, have been described as the Target of Evaluation (TOE) in this report. The Evaluated Configuration of the product, its security functions, assumed environment are given below (Refer B2 to B5).

B 1.3 Security Claims

The [ST] specifies the security objectives of the TOE and the threats that they counter (Refer 3.3 and 4.1 of ST). All the Security Functional Requirements (SFRs) (listed in 6.1 of ST) are taken from CC Part 2. The threats considered by the developer are as below:

1. An unauthorized person may attempt to compromise the integrity of TOE data by bypassing a security mechanism.
2. An unauthorized person may attempt to remove or destroy data from the TOE.
3. An unauthorized person may attempt to compromise the continuity of the TOE's functionality by halting execution of the TOE.
4. An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

B 1.4 Conduct of Evaluation

The evaluation was initiated by the IC3S Certification Scheme of STQC IT Certification Body vide communication no. IC3S/CB/2019/0006 Dated 16-04-2020, registered with reference No.

IC3S/KOL01/ECITelecom/EAL2/0420/0019. The TOE as described in the [ST] is the **Composite system comprised of ECI LightSOFT Software Version 15.5 (build 06301) along with required fixes as mentioned in Annex A; STMS Software Version 9.5R02.00 (build 354237) along with required fixes as mentioned in Annex A; Apollo Software Version 9.5R02.00 (build 355612).The Apollo Software executes on the following Apollo platforms: OPT9603, OPT9608, OPT9624, OPT9904X, OPT9914, and OPT9932**.

The TOE was evaluated through assessment of its Architecture, design and Development documentation, testing of Security functions, and Vulnerability Assessment, using methodology stated in Common Evaluation Methodology [CEM] of CC Standards and Operating Procedure, OP-07 of Common Criteria Test Laboratory, ERTL (E), Kolkata.

The evaluation has been carried out under written agreement [29th January 2019] between Common Criteria Test Laboratory, ERTL (E), Kolkata and the sponsor.

The evaluation has been carried out under written agreement [22 June 2020] between Common Criteria Test Laboratory, ERTL (E), Kolkata and the sponsor.

B 1.5 Independence of Certifier

The certifier did not render any consulting or other services for the company ordering the certification and there was no relationship between them, which might have an influence on this assessment.

B 1.6 Disclaimers

The certification results only apply to the version and release of the product as indicated in the certificate. The certificate is valid for stated conditions as detailed in this report. This certificate is not an endorsement of the IT product by the Certification Body or any other organization that recognizes or gives effect to this certificate. It is also not an endorsement of the target of evaluation (TOE) by any agency of the Government of India and no warranty of the TOE is either expressed or implied.

B 1.7 Recommendations and conclusions

- The conclusions of the Certification Body are summarized in the Certification Statement at Section A1.
- The specific scope of certification should be clearly understood by reading this report along with the [ST].
- The TOE should be used in accordance with the environmental assumptions mentioned in the [ST].
- The TOE should be used in accordance with the supporting guidance documentation.
- This Certification report is only valid for the evaluated configurations of the TOE.

B2 Identification of TOE

Composite system comprised of ECI LightSOFT Software Version 15.5 (build 06301) along with required fixes as mentioned in Annex A; STMS Software Version 9.5R02.00 (build 354237) along with required fixes as mentioned in Annex A; Apollo Software Version 9.5R02.00 (build 355612).The Apollo Software executes on the following Apollo platforms: OPT9603, OPT9608, OPT9624, OPT9904X, OPT9914, and OPT9932.

The TOE consists of the LightSOFT and STMS TOE components providing control and monitoring functions for the Apollo components (executing on supported appliances) that provide packet transport services. These systems are intended for use in Service Provider (SP) environments.

TOE environment: Operating System Solaris Hardened Solaris x86 11.4 Rev 03, DBMS Oracle 12.1

Required Non-TOE Hardware/Software/Firmware:

Table 1 - LightSOFT/STMS 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
DBMS	Oracle 12.1

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

Table 3: The TOE and its guidance document

TOE Component	Description
The product	**Composite system comprised of ECI LightSOFT Software Version 15.5 (build 06301) along with required fixes as mentioned in Annex A; STMS Software Version 9.5R02.00 (build 354237) along with required fixes as mentioned in Annex A; Apollo Software Version 9.5R02.00 (build 355612).The Apollo Software executes on the following Apollo platforms: OPT9603, OPT9608, OPT9624, OPT9904X, OPT9914, and OPT9932**
Users' Manual	1. *LightSOFT Getting Started & Administration Guide Version 15.5* 2. *LightSOFT Fault Management and Performance Monitoring Guide Version 15.5* 3. *LightSOFT Version 15.5 Installation Guide* 4. *STMS Getting Started and Administration Guide Version 9.5* 5. *STMS User Guide Version 9.5* 6. *STMS Performance Management Guide Version 9.5* 7. *STMS Installation/Upgrade/Migration V9.1 to V9.5* 8. *Apollo Version 9.5 Reference Manual* 9. *LCT-STMS Getting Started & Administration Guide Version 9.5* 10. *ECI LightSOFT, STMS and Apollo Software Common Criteria Supplement* 11. *Common Phase 11.4 Activities for Preparation, Installation and Upgrade of Management Systems Infrastructure* 12. *Common Management HW Preparation and Configuration Activities* 13. *Oracle DB v19 - Installation and Upgrade Procedure*

B3 Security policy

There are following organizational security policy that the TOE must meet.

Table 4 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.

B.4 Assumptions

There are following assumptions exist in the TOE environment.

Table 5: 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 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.ORACLE	The Oracle DBMS protects the confidentiality and integrity of the TSF data for LightSOFT and STMS.
A.ORBIX	Orbix provides reliable communication for TSF data transmitted between LightSOFT and STMS.
A.SOLARIS	Solaris provides separation between LightSOFT, STMS and Oracle zones on a single physical server.

Table 6: Assumptions

Assumption	Description
A.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide computing platform for general purpose applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the ST.
A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the ST will not include any requirements on physical tamper protection or other physical attack mitigations. The ST will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.

B.5 Evaluated configuration

Description	Software Version and Release	The image files	File size in bytes	Hash values of the image files
Lightsoft NMS Server	Version 15.5 (build 06301)	NMSsrv_v1550.06301.Sol_vol1-X93540.iso	3364072 KB	MD5: 1748a82f8bc1d376db75053b3982d3e4 SHA2: 3f93fe02c78a900f0298dd8ef1995a747ebf5c7f97cf8ffdc43f27b2d929d909
		NMSsrv_v1550.06301.Sol_vol2-X93540.iso	1674822 KB	MD5: 866574346537675828b14758e0f810bf SHA2: d61c8bbe9cf6869cca8661b0aebf52ad90be269c2b9dfa75c794ba9269f9ee3f
Lightsoft NMS Client	Version 15.5 (build 06301)	NMScli_v1550.06301.Sol-X93542.iso	1004052 KB	MD5: 2a9c038d236f6df58de17435d6499d83 SHA2: 2f9199013d69f502d7d223b1551394b8b5458d30ffb0de399b61f07807ce48f6
EMS STMS	Version 9.5R02.00 (build 354237)	STMS_V9.5R02.00_354237-X93648.Sol.iso	3657906 KB	MD5: 4d86278e13d45b22318592d4c4f2803a SHA2: 202b74af94beabe9d30d1fcf82bccd9224b44f92ae7906436f292c6624bd962a
OPT 9603	Version 9.5R02.00 (build 355612)	SR9603-9.5R02.00-355612-image.tar.gz	3048621 KB	MD5: cda692e7e2543eb02d16c4ff0914464c SHA2: d5ca88603054002f7767506adae3549a871a91ec5c7adfc78eb02ceeaadd0e28
OPT 9608	Version 9.5R02.00 (build 355612)	SR9608L-9.5R02.00-355612-image.tar.gz	3053204 KB	MD5: e985298d769c02a9c7391106d8165e69 SHA2: 4f35843032b18254ddb0f375c2f49161cc4e0e2a98065ce3c9315930af88dd4c
OPT 9624	Version 9.5R02.00 (build 355612)	SR9624L-9.5R02.00-355612-image.tar.gz	3097488 KB	MD5: 0d347544748ce9516557c2d06c73eccd SHA2: bd8e18ae3855ad99e00feca2ecbc59d7816f4dd6d02bf6c5e38b4664325d6223
OPT 9904X	Version 9.5R02.00 (build 355612)	SR9904-9.5R02.00-355612-image.tar.gz	2093806 KB	MD5: bd03d500db195bd7d9538108210746d8 SHA2: f1d31d1be7c7700368fb3975feda6450c637d8eb022078c145c5e8ee65d118e1
OPT 9914	Version 9.5R02.00 (build 355612)	SR99XX-9.5R02.00-355612-image.tar.gz	2238872 KB	MD5: a66f65bd37b9a30488cad48ec0d20e36 SHA2: 94d91e46978a71aad114773df7d2f2fc29186fddea44fa4246197cfcbcea0ae4
OPT 9932	Version 9.5R02.00 (build 355612)	SR99XX-9.5R02.00-355612-image.tar.gz	2238872 KB	MD5: a66f65bd37b9a30488cad48ec0d20e36 SHA2: 94d91e46978a71aad114773df7d2f2fc29186fddea44fa4246197cfcbcea0ae4
Oracle Server	Version 19.032	OraSrv_19.032_Sol-X18818.iso	11540384 KB	MD5: 92ce65a66b2be6a9d8a112bdfc4b093a SHA2: aba384ba6d12c16250ead7a2126eb6a38cf2586d73fb517c7648bca0568637a6

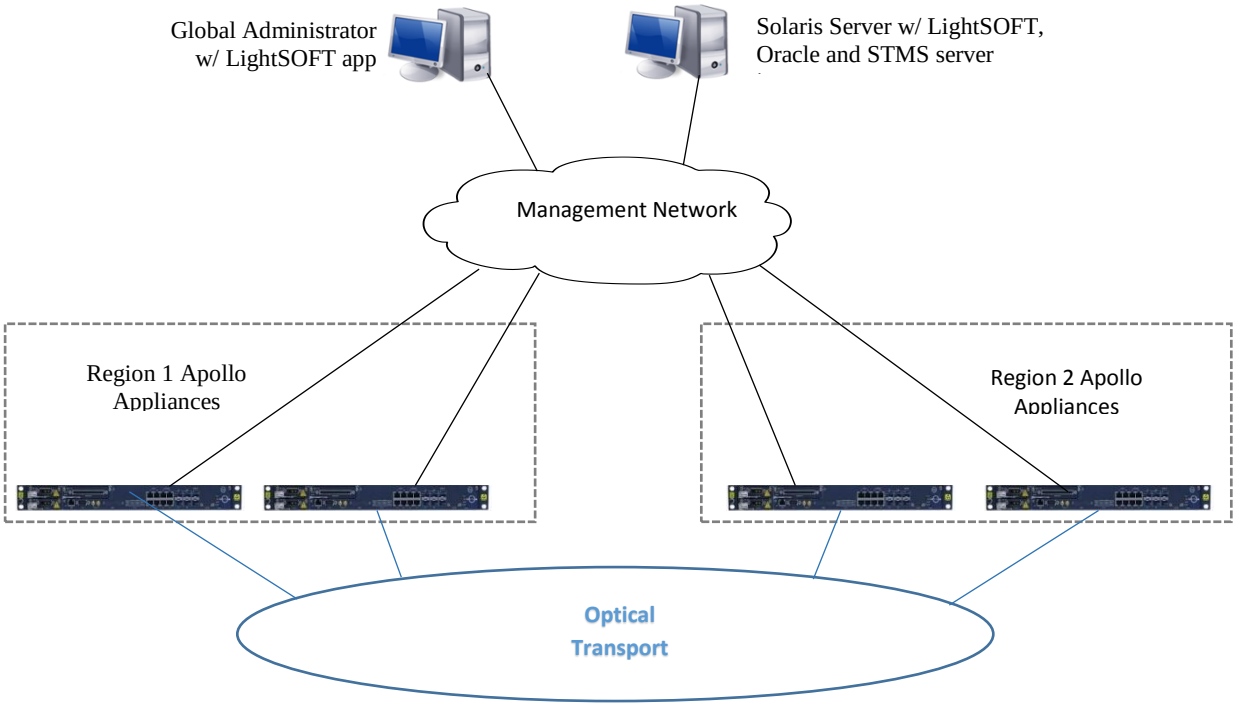

Figure 1: Representative TOE Deployment

B6 Document Evaluation

B.6.1 Documentation

The list of documents, those were presented, as evaluation evidences to the evaluators at the evaluation facility, are given below:

1. **Security Target**: ECI LightSOFT v15.5, STMS v9.5 and Apollo Software v9.5 on OPT9603, OPT9608, OPT9624, OPT9904X, OPT9914, and OPT9932 Security Target Version 1.3 , 10 January 2021
2. **TOE Architecture**: ECI LightSOFT, STMS and Apollo Software Development Document version 1111111.2 , 10 January 2021
3. **TOE Functional Specification**: : ECI LightSOFT, STMS and Apollo Software Development Document version 1111111.2 , 10 January 2021
4. **TOE Design description**: : ECI LightSOFT, STMS and Apollo Software Development Document version 1111111.2 , 10 January 2021
5. **Preparative Guidance**: ECI LightSOFT v15.5, STMS v9.5 and Apollo Software v9.5 Common Criteria Supplement Version 1.1 12 August 2021
6. **Operational Guidance**:

   I. *LightSOFT Getting Started & Administration Guide Version 15.5, Revision 01*

   II. *LightSOFT Fault Management and Performance Monitoring Guide Version 15.5, Revision 01*

   III. *LightSOFT Version 15.5 Installation Guide, Revision 01*

   IV. *STMS Getting Started and Administration Guide Version 9.5, Revision 01*

V. *STMS User Guide Version 9.5, Revision 01*

VI. *STMS Performance Management Guide Version 9.5, Revision 01*

VII. *STMS Installation/Upgrade/Migration V9.1 to V9.5, Revision 03*

VIII. *Apollo Version 9.5 Reference Manual, Revision 02*

IX. *LCT-STMS Getting Started & Administration Guide Version 9.5, Revision 01*

X. *ECI LightSOFT, STMS and Apollo Software Common Criteria Supplement v 1.1*

XI. *Common Phase 11.4 Activities for Preparation, Installation and Upgrade of Management Systems Infrastructure, Revision D05*

XII. *Common Management HW Preparation and Configuration Activities, Revision B00*

XIII. *Oracle DB v19 - Installation and Upgrade Procedure, Revision B05*

7. **Configuration Management Capability:** ECI LightSOFT, STMS and Apollo Software Configuration Management Plan version 1.0 16 March 2021
8. **Configuration Management Scope:** ECI LightSOFT v15.5, STMS v9.5 and Apollo Software v9.5 on OPT9603, OPT9608, OPT9624, OPT9904X, OPT9914, and OPT9932 Configuration Item List version 1.2 29 October2021
9. **TOE delivery:** ECI LightSOFT v15.5, STMS v9.5 and Apollo Software v9.5 Delivery Document version 1.0 16 March 2021
10. **Test cases, logs and coverage**:
    I. ECI LightSOFT v15.5, STMS v9.5 and Apollo Software v9.5 on OPT9603, OPT9608, OPT9624, OPT9904X, OPT9914, and OPT9932 Test Results , Version 1.0 14 September 2021
    II. ECI LightSOFT v15.5, STMS v9.5 and Apollo Software v9.5 on OPT9603, OPT9608, OPT9624, OPT9904X, OPT9914, and OPT9932 Test Plan and Procedures version1.0, 8 April 2021

B.6.2 Analysis of document

The documents related to the following areas were analyzed using [CEM]. The summary of analysis is as below:

The ST:

The evaluation team checked, analysed the ST document, presented for the TOE and confirmed that ST complies all requirements of the Common Criteria Standards, ver. 3.1 and internally consistent

Development process:

TOE Development (Functional Specification, Architecture, and Design**):**

Functional Specification:

The evaluation team analyzed the functional specification of the TOE in consultation with TOE Design, Guidance Document, and found that the TOE security function interfaces are described clearly and unambiguously.

Security Architecture description:

The Apollo Software includes a hardened Linux operating system and the appliance is dedicated to TOE functions. When the appliances begin execution, the operating system performs its initialization, followed by initialization of the services and applications. Configuration information is stored within the TOE. Initialization is not complete until all configuration information has been processed. No incoming network connections are accepted while operating system initialization is in process. Once the internal initialization process is complete, the Apollo Software listens for incoming messages from the STMS. No processing of Apollo Management Interface traffic is performed while initialization of the subsystem is in process.

Design description:

The description of the TOE has been made in terms of sub-systems: The evaluators have analysed the subsystems.

Guidance Documents: *The evaluators analysed guidance documents like preparative procedure and operational user guidance and determined that preparative procedure describes clear and unambiguous steps to bring the TOE to its secure state. The operational user guidance information were also clear and unambiguous.*

Life-cycle support documents: *The Life cycle support process document, containing information on Configuration Management and Delivery Procedure were evaluated.*

Configuration management: *The evaluators analyzed configuration management documentation and determined that the TOE and its associated documents are clearly identified as configurable items. The evaluators also analyzed access control measures defined in the documentation and found satisfactory***.**

Delivery procedure: *The delivery procedure document was audited with the objective to ascertain whether it covers secure delivery of the TOE to the end-users. The secure delivery procedure has been described in the document and the same has been audited by the evaluators during their virtual site visit. The end-users can check integrity of the evaluated TOE using hash value of that, if felt necessary.*

The final version of the respective evaluation evidences was found to comply with the requirements of CCv3.1 for EAL2.

B7 Product Testing

Testing at EAL2 consists of the following three steps: Testing by developer, Independent Testing by Evaluation Team, and Penetration testing.

B 7.1 IT Product Testing by Developer

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the [ETR].

The evaluators analysed the developer's test coverage and found them to be complete and satisfactory. The correspondence between the tests identified in the developer's test documentation and the functional specification and TOE design was complete.

B 7.2 IT Product Independent Testing by Evaluation Team

The evaluators' independent functional testing effort is summarized as below.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and reproducibility of results. The evaluators have examined the TOE and it is found to be configurable as per the description given in the developer's preparative guidance document. It is also observed that the test configuration is consistent with the description as given in the security target document. Highlights of Independent testing are given below:

The evaluators have examined the TOE and it is found to be configurable as per the description given in the developer's preparative guidance document. It is also observed that the test configuration is consistent with the description as given in the security target document. Highlights of Independent testing are given below:

The TOE has been installed properly as per the preparative procedure document. The evaluators have repeated the developer's test at CCTL, Kolkata to confirm the reproducibility of the test results in the with the devices with Apollo Software v9.5 on OPT9603, OPT9608, OPT9624, OPT9904X, OPT9914. The Apollo device OPT9932 was tested remotely keeping system at developer's site. While making the test strategy for independent testing, consideration is given to cover the security requirements, as well as the security specification as defined in the security target, interfaces available to the users to cover each of security functional requirements, TOE design and security architecture information. Independent testing is designed to verify the correct implementation of security functionalities available to different levels of users and to check whether audit is being generated for auditable events.

The tests were designed to cover following TSFs and associated TSFIs of the TOE:

1. **Security Audit**
   The LightSOFT and STMS 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.
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 STMS 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. LightSOFT and STMS provide functionality for authorized users to manage the following items:
   - *Security configuration (including User Accounts)*
   - *Log management*
   - *NEs*
   - *Services*
   - *Alarms*
3. **Identification and Authentication (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. 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.

B 7.3 Vulnerability Analysis and Penetration testing

A scanning has been conducted on the TOE with Nessus (Plugin Set: 202110010228)of the tool 'nessus' to find out presence of hypothesized potential vulnerabilities, identified in the public domain, pertaining to this type of product. All High-level vulnerabilities, found from Scanning Tool ('nessus' with plugin set Nessus (Plugin Set: 202110010228 for different zones of Solaris (containing TOE components), are addressed with proper fixes and patches, issued by the developer. After fixing, no High and Critical Level vulnerabilities are found during scanning of the different components of the TOE. The results of vulnerability scanning did not reveal any vulnerabilities, which are known in the public domain. Port map scanning has been carried out with 'NMap' tool. Based on the results of Port Scanning. NVD (National Vulnerability Data base in the US was searched, but no results/ matches found.

The evaluator has analyzed the evaluation evidences like, the ST, the Functional Specification, the TOE Design, the Security Architecture Description and the Guidance Documentation and as well as the operational environment, stated in the ST and then hypothesized the security vulnerabilities considering five categories of attack to the Security functions, viz. 'Bypassing', 'Tampering', 'Direct Attacks', 'Monitoring' and 'Misuse'.

Considering the type of the TOE and its intended use, the possibility of "Direct Attack" is negligible; evaluator's judgement is justified and supported by analysis. The evaluator has identified the following Attack scenarios.

The evaluator has analysed the evaluation evidences like, the ST, the Functional Specification, the TOE Design, the Security Architecture Description and the Guidance Documentation and as well as the operational environment, stated in the ST and then hypothesized the security vulnerabilities considering five categories of attack to the Security functions, viz. 'Bypassing', 'Tampering', 'Direct Attacks', 'Monitoring' and 'Misuse'.

Considering the type of the TOE and its intended use, the possibility of "Direct Attack" is negligible; evaluator's judgement is justified and supported by analysis. The evaluator has identified the following Attack scenarios.

AT1. ***Administrator Role*** *of LS Server for GUI based login can access and manage the ECI Apollo system through GCT. However, he is not authorized to login as super user in LS Server via SSH and access sensitive files. Application user with highest privilege tries to access sensitive TOE files using SSH to the TOE environment bypassing security mechanism of the application.* Attack Potential: 6 (Within Basic) *[*Penetration Testing is required]

AT2. ***Accessing OPTs*** *directly and all its data bypassing STMS interface to access OPTs.* Attack Potential: 7 (Within Basic) [Penetration Testing is required]

AT3: ***Accessing Sensitive*** *Data of Oracle Database bypassing access control mechanism of database using blank credential or default credential.* Attack Potential: 8 (Within Basic) [Penetration Testing is required]

AT4: ***Accessing Sensitive*** *data of TOE during booting process by tampering security mechanism when security functions are not fully invoked.* Attack Potential: 8 (Within Basic) [Penetration Testing is required]

AT5: ***Attacker takes*** *the role of Admin and changes any other user's password after creation of account and before first login without knowledge of the user.* Attack Potential: 11 (Beyond Basic) [*Penetration Testing is not required]*

The attack potential for each of the vulnerabilities was calculated using guidance given in CEMv3.1 and considering various factors like the time to identify & exploit the vulnerability, expertise required, knowledge of the TOE, windows of opportunity and equipment requirement.

The relevant attack potentials, corresponding to the identified vulnerabilities have been estimated considering various factors like the 'time to identify & exploit', 'expertise required', 'knowledge of the TOE', 'windows of opportunity' and 'equipment required'. The potential vulnerabilities with 'Basic' attack potential were considered for penetration testing. The calculated attack potentials are as follows:

The relevant attack potentials, corresponding to the identified vulnerabilities have been estimated considering various factors like the 'time to identify & exploit', 'expertise required', 'knowledge of the TOE', 'windows of opportunity' and 'equipment required'. The calculated attack potentials are as follows:

The evaluator conducted Penetration Testing:

1. ***PT1 for attack scenario AT1****: Administrator Role of LS Server for GUI based login can access and manage the ECI OPT system through GCT. However, he is not authorized to login as super user in LS Server via SSH and access sensitive files. Application user with highest privilege tries to access sensitive TOE files using SSH to the TOE environment bypassing security mechanism of the application.*
2. ***PT2: Accessing TOE OPTs*** *directly and all its data bypassing STMS interface to access OPTs.*
   As per ST document and Design Document, OPT related management data can be read, modified or deleted from STMS by appropriate privileged users. In this test, a user with admin credentials of accessing OPTs via SSH tries to login and access management related data bypassing STMS interface.
3. ***PT3: Accessing Sensitive data of TOE*** *during booting process by tampering security mechanism when security functions are not fully invoked.*
   : An attacker tries to intrude into the system from any vulnerability during the booting process of TOE and access sensitive data.
4. ***PT4 Access Control mechanism of Oracle Database*** *needs to be analysed*
   If no or default access control for Oracle Database is enabled, an attacker can easily gain access to sensitive data in the database by misusing improper configuration

The Evaluator could not able to exploit the hypothesized Security vulnerabilities/ concern of the TOE evolved through analysis of evaluation objects. Hence, it is concluded that the TOE does not contain any exploitable vulnerability for ***'Basic' Attack Potential****.*

As the target assurance level is EAL 2, the evaluation team has restricted their Penetration Testing activities to the attack scenarios for which the estimated attack potential is less than 10. Considering the attack potential as 'Basic', the evaluators could exploit no identified vulnerabilities.

Hence, the TOE does not contain any exploitable vulnerability for 'Basic Attack Potential'. However, these Vulnerabilities may be exploited with higher attack potential.

The identified vulnerability, having attack potential more than 'Basic' was not considered for penetration Testing. Hence, this vulnerability may be considered as residual vulnerabilities. The residual vulnerabilities given below.

AT5: Attacker takes the role of Admin and changes any other user's password after creation of account and before first login without knowledge of the user.

B 8 Evaluation Results

The evaluation results have been documented in the [ETR].

Report No: ***IC3S/KOL01/ECITelecom/EAL2/0420/0019/ETR/0031***

The TOE was evaluated through evaluation of its documentation, testing and vulnerability assessment using methodology stated in [CEM] and laboratory operative procedure [OP-07 CC EAL 4].

Documentation evaluation results:

The documents for TOE and its development life cycle were analyzed by the evaluator in view of the requirements of the respective work units of the [CEM]. The final versions of the documents were found to comply with the requirements of CCv3.1 Revision 5 for EAL2.

Testing:

The developer's tests and the independent functional tests yielded the expected results, giving assurance that 'Composite system comprised of ***ECI LightSOFT Software Version 15.5 (build 06301) along with required fixes as mentioned in Annex A; STMS Software Version 9.5R02.00 (build 354237) along with required fixes as mentioned in Annex A; Apollo Software Version 9.5R02.00 (build 355612).The Apollo Software executes on the following Apollo platforms: OPT9603, OPT9608, OPT9624, OPT9904X, OPT9914, and OPT9932****" behaves as specified in its [ST], functional specification and TOE design.*

Vulnerability assessment and penetration testing:

The penetration testing with 'Basic' attack potential could not exploit the potential vulnerabilities identified through vulnerability assessment.

B 9 Validator Comments

The Validators have reviewed the Evaluation Technical Report [ETR] along with all relevant evaluation evidences, documents, records, etc. and are in agreement with the conclusion made in it i.e.

- **The [ST]** ***ECI LightSOFT v15.5, STMS v9.5 and Apollo Software v9.5 on OPT9603, OPT9608, OPT9624, OPT9904X, OPT9914, and OPT9932 Security Target Version 1.3*** *has satisfied all the requirements of the assurance class ASE.*
- *The results of evaluation of product and process documentation, testing and vulnerability assessment confirm that the TOE* ***" Composite system comprised of ECI LightSOFT Software Version 15.5 (build 06301) along with required fixes as mentioned in Annex A; STMS Software Version 9.5R02.00 (build 354237) along with required fixes as mentioned in Annex A; Apollo Software Version 9.5R02.00 (build 355612).The Apollo Software executes on the following Apollo platforms: OPT9603, OPT9608, OPT9624, OPT9904X, OPT9914, and OPT9932*** *", satisfies all the security functional requirements and assurance requirements as defined in the [ST]. Hence, the TOE is recommended for EAL2 Certification as per Common Criteria version: Version 3.1 Revision 5, dated April 2017.*

However, it should be noted that there are no Protection Profile (PP) compliance claims.

B 10 List of Acronyms

ACL: Access Control List
CC: Common Criteria
CCTL: Common Criteria Test Laboratory
CEM: Common Evaluation Methodology
DVS: Development security
EAL: Evaluation Assurance Level
ETR: Evaluation Technical Report
FSP: Functional Specification
IC3S: Indian Common Criteria Certification Scheme
IT: Information Technology
PP: Protection Profile
ST: Security Target
TOE: Target of Evaluation
TDS: TOE Design Specification
TSF: TOE Security Function
TSFI: TOE Security Function Interface

B 11 References

1. [CC-I]: Common Criteria for Information Technology Security Evaluation: Part 1: Version 3.1
2. [CC-II]: Common Criteria for Information Technology Security Evaluation: Part 2: Version 3.1, Revision 5
3. [CC-III]: Common Criteria for Information Technology Security Evaluation: Part 3: Version 3.1 Revision 5
4. [CEM]: Common Methodology for Information Methodology: Version 3.1 Revision 5
5. [ST] : ECI LightSOFT v15.5, STMS v9.5 and Apollo Software v9.5 on OPT9603, OPT9608, OPT9624, OPT9904X, OPT9914, and OPT9932 Security Target, Version 1.3
6. [ETR]: Evaluation Technical Report No. Report No**: IC3S/KOL01/ECITelecom/EAL2/0420/0019/ETR/0031**
7. [OP-07 CC EAL 4]: CCTL, ERTL(E) Operating procedure

Annexure – A: Configuration of the TOE

Composite system comprised of ECI LightSOFT Software Version 15.5 (build 06301) along with required fixes as mentioned in Annex A; STMS Software Version 9.5R02.00 (build 354237) along with required fixes as mentioned in Annex A; Apollo Software Version 9.5R02.00 (build 355612).The Apollo Software executes on the following Apollo platforms: OPT9603, OPT9608, OPT9624, OPT9904X, OPT9914, and OPT9932

At the time of the evaluation, the following updates are available for LightSOFT and STMS.

Fix	Build #	Release date
NG1550_6301-050	15	Feb 28, 2021
NG1550_6301-100	36	May 30, 2021
NG1550_6301-200	21	June 30, 2021
NSx1550_6301-050	15	Feb 28, 2021
NSx1550_6301-100	36	May 30, 2021
NSx1550_6301-200	21	June 30, 2021
NC1550_6301-050	15	Feb 28, 2021
NC1550_6301-100	36	May 30, 2021
NC1550_6301-200	21	June 30, 2021