Indian CC Certification Scheme (IC3S)

Certification Report

Report Number : IC3S/KOL01/TEJAS/EAL2/1018/0012

Product / system : TJ5500 NMS (Network Management System) and TJ5100 EMS (Element Management System) version 8.1

Dated: 04-08-2022

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

This report contains a total of 21 pages. In case it needs to be reproduced, all the pages must be included.

Product developer:	**Tejas Networks Limited Plot no 25, J. P. Software Park, Electronic City, Phase I, Hosur Road, Bangalore 560100, India**
TOE evaluation sponsored by:	**Tejas Networks Limited Plot no 25, J. P. Software Park, Electronic City, Phase I, Hosur Road, Bangalore 560100, India**
Evaluation facility:	**CCTL, ERTL (East), Kolkata** **STQC Directorate, Govt. of India** **Ministry of Electronics & Information Technology,** **63 DN Block, Sector V Salt Lake City, Kolkata** **700091, India**
Evaluation Personnel:	1. Smt. Malabika Ghosh (Project Manager) 2 Sri Nischal 3. Sri Sumit Jaiswal

3

Evaluation Technical Report:	**IC3S/KOL01/Tejas/EAL2/1018/0012/ETR/0036**
Validation Personnel:	**Tapas Bandyopadhyay**

Table of Contents

Contents

PART A: CERTIFICATION STATEMENT AND BACKGROUND OF THE CERTIFICATION BODY

A1 Certification Statement

The product (TOE) 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	**Tejas Networks Limited Plot no 25, J. P. Software Park, Electronic City, Phase I, Hosur Road, Bangalore 560100, India**
Developer	**Tejas Networks Limited Plot no 25, J. P. Software Park, Electronic City, Phase I, Hosur Road, Bangalore 560100, India**
The Target of Evaluation (TOE)	**TJ5500 NMS (Network Management System) and TJ5100 EMS (Element Management System) version 8.1**
Security Target	**Security Target of TJ5500 NMS (Network Management System) and TJ5100 EMS (Element Management System) version 8.1., Version 1.9**
Brief description of product	The TOE is an integrated management application offering single window operation for end-to-end network management. It supports provisioning, operations & management of Packet Transport Networks, DWDM, SDH/SONET, GPON and OTN based services. This provide a unified management solution to manage multi-technology networks. The management functionality provides multiple roles in order to enable multiple levels of access for users. The managed appliances may be divided into different groups within the management platforms, with access to groups restricted on a per-user basis. The TOE is Network Management System (TJ5500) and Element Management System (TJ5100).TOE components providing control and monitoring functions for NE components that provide packet/optical transport services. These systems are intended for use in SP (Service Provider) environments. TJ5500 is referred as NMS and TJ5100 is referred as EMS. TJ5500 supports TJ5100 through the TMF 814 Interface. Each EMS instance has a unique EMS name.TJ5500 is a Network Management System which offers single window operation into the network for Fault, Configuration and Security management for carrier networks. The TJ5500 offers full FCAPS functionality support across the various Tejas product portfolios – SDH (TJ1000 Series), Carrier Ethernet (TJ2000 Series) etc.
CC Part 2 [CC-II]	**Conformant to CC Part 2 Version 3.1 Rev 5**
CC Part 3 [CC-III]	**Conformant CC Part 3 Version 3.1 Rev 5**
EAL	**EAL2**
Evaluation Lab	**Common Criteria Test Laboratory, ERTL(East) , Kolkata , India**
Date Authorized	**08-01-2019**

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 (CCTL, ERTL (East), Kolkata).

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 Rev 5
- Common Evaluation Methodology (CEM) Version 3.1.

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 body **Common Criteria Test Laboratory (CCTL, ERTL(East), Kolkata STQC Directorate, Govt. of India, Ministry of Electronics & Information Technology,63 DN Block, Sector V Salt Lake City, Kolkata ,700091, India has** conducted the evaluation of the product. Hereafter this has been referred as CCTL. The evaluation facility is recognized under the IC3S scheme of STQC IT Certification Body.

M/s Tejas Networks Limited Plot no 25, J. P. Software Park, Electronic City, Phase I, Hosur Road, Bangalore 560100, India is the developer and sponsor of the TOE under certification.

The certification process is concluded with the completion of this certification report. This evaluation was completed on 27thJune 2022 after submission of [ETR] to the certification body. The confirmation of the evaluation assurance level (EAL 2) 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 environment described.

This certification report applies only to the version and release/build 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 apply 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.

Common Criteria Test Laboratory (**CCTL, ERTL (East), Kolkata STQC** Directorate, Govt. of India, Ministry of Electronics & Information Technology,63 DN Block, Sector V Salt Lake City, Kolkata ,700091, India has performed the evaluation. The information in the Certification Report is derived from the [ST] written by the developer and the Evaluation Technical Report [ETR] written by Common Criteria Test Laboratory [CCTL, ERTL(East), Kolkata STQC Directorate, Govt. of India, Ministry of Electronics & Information Technology,63 DN Block, Sector V Salt Lake City, Kolkata ,700091, India The evaluation team has evaluated and confirmed that the security target [ST] that is used for evaluation of the product is CC Version 3.1, Rev 5 Part 2 and Part 3 conformant and concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL2) have been met.

B 1.2 Evaluated product and TOE

TJ5500 NMS (Network Management System) and TJ5100 EMS (Element Management System), the evaluated sub-set and configuration of the product is described in this report as the Target of Evaluation (TOE). The TOE version no. is 8.1. The Evaluated Configuration, its security functions, assumed operational environment, architectural information and evaluated configuration are given below (Refer B2 to B5). The TOE & Its Physical Environments & Boundaries are depicted in Figure 1 and Figure 2.

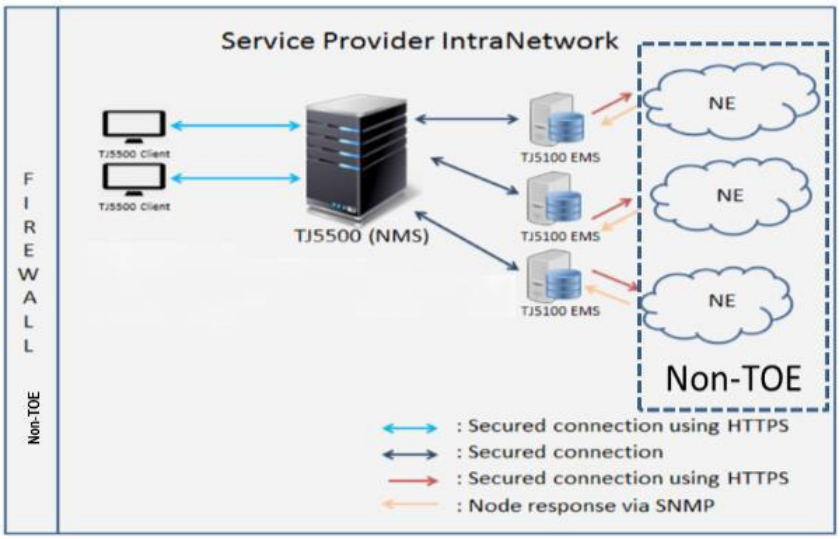

Figure 1: TOE Boundary

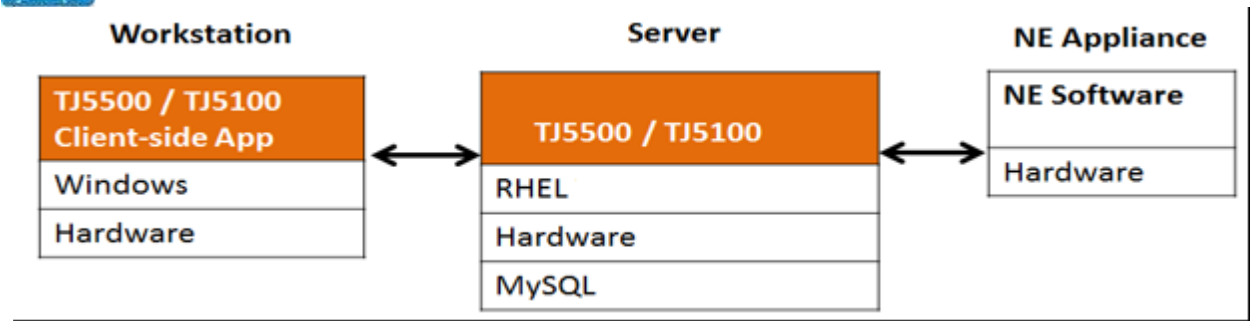

Figure2: Physical boundary of the TOE

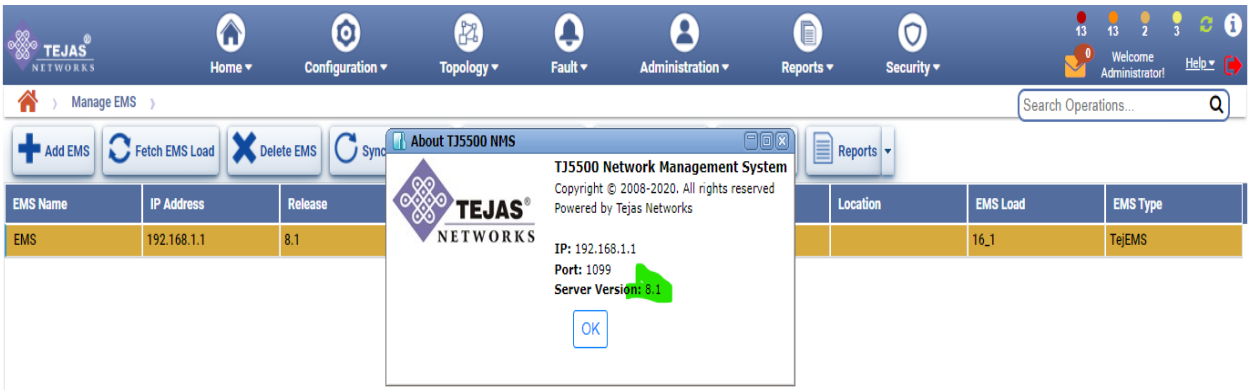

Figure 3: TOE Identification: TJ5500 Software Version 8.1

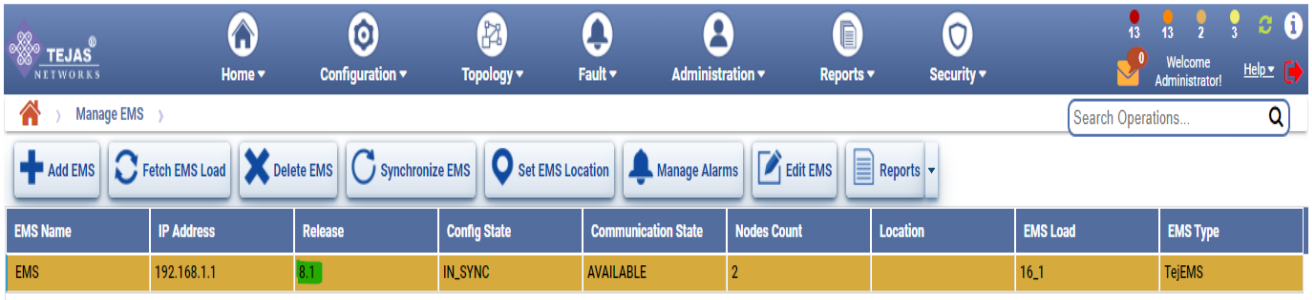

Figure 4: TOE Identification: TJ5100 (EMS) Software Version 8.1

B 1.3 Security Claims

The [ST] specifies the security objectives of the TOE and the threats that they counter. The Security Functional Requirements (SFRs) are taken from CC Part 2.

B 1.4 Conduct of Evaluation

The common criteria evaluation of the TOE was initiated by the **IC3S Certification** Scheme of STQC Certification Body vide communication no. IC3S/KOL01/TEJAS/EAL2/1018/0012 dated 08/01/2019 later.

The Target of Evaluation (TOE) is **TJ5500 NMS (Network Management System), TJ5100 EMS (Element Management System) Version 8.1;** The TOE is an integrated management Software application offering single window operation for end-to-end network management. It supports provisioning, operations & management of Packet Transport Networks, DWDM, SDH/SONET, GPON and OTN based services. This provide a unified management solution to manage multi-technology networks. The management functionality provides multiple roles in order to enable multiple levels of access for users. The managed appliances may be divided into different groups within the management platforms, with access to groups restricted on a per-user basis. The TOE is Network Management System (TJ5500) and Element Management System (TJ5100).TOE components providing control and monitoring functions for NE components that provide packet/optical transport services. These systems are intended for use in SP (Service Provider) environments. TJ5500 is referred as NMS and TJ5100 is referred as EMS. TJ5500 supports TJ5100 through the TMF 814 Interface. Each EMS instance has a unique EMS name.TJ5500 is a Network Management System which offers single window operation into the network for Fault, Configuration and Security management for carrier networks. The TJ5500 offers full FCAPS functionality support across the various Tejas product portfolios – SDH (TJ1000 Series), Carrier Ethernet (TJ2000 Series) etc.

TOE was evaluated through evaluation of its documentation; independent testing and vulnerability assessment using methodology stated in Common Evaluation Methodology [CEM]. The Evaluation Assurance Level is **EAL 2 as per Common Criteria Version 3.1 Rev 5.**

The evaluation has been carried out under written agreement [05-12-2018] between **CCTL, ERTL (East), Kolkata** and the developer/ sponsor **M/s Tejas Networks Limited, Bengaluru**.

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 document].
- 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.

B 2 Identification of TOE

The TOE is the **TJ5500 NMS (Network Management System), TJ5100 EMS (Element Management System) Version 8.1;**

The TOE has the following identification details:

Product (TOE): **TJ5500 NMS (Network Management System), TJ5100 EMS (Element Management System)**

TOE Version: 8.1

The md5 hash of the TOE as given below

- **TJ5500 (NMS_Release_8_1_0_a16_1.tgz): 2dd9fdf4adbf8d6ad6627ddbadf330c7**
- **TJ5100 (EMS_Release_8_1_0_a16_1.tgz): 1adaf98d91d3cb50eb005b048583d7f2**

B 3 Security policy

Following is the list of security features available in the TOE:

- Audit Data Generation
- Audit Review
- Protected Audit Trail Storage
- Cryptographic Key Generation
- Cryptographic Key Distribution
- Cryptographic Key Destruction
- Cryptographic Operation
- Subset Information Flow Control
- Simple Security Attributes
- Subset Residual Information Protection
- User attribute definition
- Verification of secrets
- User authentication before any action
- User identification before any action
- Management of Security Functions Behavior
- Management of Security Attributes
- Secure Security Attributes
- Static Attribute Initialization
- Management of TSF Data
- Specification of Management Functions
- Security Roles
- Reliable Time Stamps
- TSF-initiated termination
- Trusted Path

B.4 Assumptions

There are following assumptions exist in the TOE environment.

Table 1: Assumptions

Item	Assumption Code	Assumption Description
1	A.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
2	A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance.
3	A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access
4	A.PUBLIC	The TOE does not host public data.
5	A.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.
6	A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
7	A.TEJAS	Administrators perform installation of the TOE in conjunction with TEJAS personnel.
8	A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

B.5 Evaluated configuration

The **Target of Evaluation (TOE**) is **TJ5500 NMS (Network Management System), TJ5100 EMS (Element Management System) version 8.1**

TOE description

The TOE is identified as **TJ5500 NMS (Network Management System), TJ5100 EMS (Element Management System)** Version 8.1

Product (TOE): **TJ5500 NMS (Network Management System), TJ5100 EMS (Element Management System)**

TOE Version: 8.1

The md5 hash of the TOE as given below

- TJ5500 (NMS_Release_8_1_0_a16_1.tgz): 2dd9fdf4adbf8d6ad6627ddbadf330c7
- TJ5100 (EMS_Release_8_1_0_a16_1.tgz): 1adaf98d91d3cb50eb005b048583d7f2

The TOE is an integrated management application offering single window operation for end-to-end network management. It supports provisioning, operations & management of Packet Transport Networks, DWDM, SDH/SONET, GPON and OTN based services. This provide a unified management solution to manage multi-technology networks. The management functionality provides multiple roles in order to enable multiple levels of access for users. The managed appliances may be divided into different groups within the management platforms, with access to groups restricted on a per-user basis.

The TOE consists of:

- One instance of the TJ5500 server component executing on RHEL server 8.2 or higher version (64-bit).
- One instance of the TJ5100 server component executing on the same server as the TJ5500 server.
- One or more instances of the TJ5500 client-side application. The instances may be installed on Windows 7/ Windows 10/ Red Hat Enterprise Linux 8.2 or higher version workstations

Table 2: TOE components along with users' manuals

S/N	Part Number	Description (Version/ Model No.)
1	400-SW0000106-S	TJ5500 Version 8.1
2	400-SW0000106-S	TJ5100 Version 8.1
3	400-DOC000118-E	TJ5500 operation manual (User interface guide)
4	400-DOC000117-E	TJ5500 Installation and Commissioning Guide
5	400-DOC000116-E	TJ5100 operation manual (User interface guide)
6	400-DOC000115-E	TJ5100 Installation and Commissioning Guide

TOE Environment:

Non-TOE Description

One or more instances of NE software executing on supported appliances, which is Non-TOE. The software is pre-installed on appliances by Tejas. The modular appliances may be populated via any supported combination of modules/cards.

Server Requirements:

The table below lists the hardware and the software requirements of the server where TJ5500 software is to be installed.

Table 3: Configuration for the Non-TOE

Non-TOE Components of TJ5500 & TJ5100	Version / Model No.	
Hardware	Processor	64-bit Dual processor Quad Core Intel 3.0 GHz or higher (8 cores in total with HT Enabled)
	Memory	• 32 GB Physical Memory (RAM) • 2*600 GB Hard Disk Drive in RAID1
Software	Operating System	RHEL server release 8.2 / later version (ootpa) (64-bit)

	Messaging/JMS	Apache Active MQ - 5.13.0 / later version
	Platform	Java Development Kit 8, Update 171 (JDK 8u171)
	Database	MySQL Version 5.7.22 / later version(64-bit)

Client System Requirements:
The table below lists the hardware and the software requirements of the client system for accessing the TJ5500 application.

Table 4: Non-TOE Components

Non-TOE Components of TJ5500 Client	Version / Model No.	
Hardware	Processor	Intel/AMD Quad core (3GHz)
	Memory	• 8 GB Physical Memory (RAM) • 40 GB Hard Disk Drive
Software	Client Configuration	19 inch TFT monitor supporting 1280x1024 or 1366 x 768 or 1920 × 1080 resolution with "true color" graphics card of same resolution.
	Operating System	Windows 10 /Red Hat Enterprise Linux 8.3
	Platform	Java JRE 8 Update 171

Non-TOE Components	Version / Model No.
Client	Firefox browser running on Windows 10 OS
RADIUS or TACACS+ AAA Server	This includes any authentication server that can be leveraged for remote user authentication.
Hardware (NE- Network element)	• TJ1400 POTP / PTN • TJ1600 POTP / PTN • TJ1270

TOE features under evaluation are:

- Manages users and their profiles
- User Identification and Authentication
- Audit log generation and verification
- User Session Management
- Tejas Networks Ltd. Company Confidential Page 11 of 49
- Client IP Configuration
- Password complexity and usage settings configuration
- Cryptographic Support
- Trusted Path/Channels
- Topology: Dashboard, Topological View, Manage TL, Manage EMS, and Manage Nodes
- Circuit Management.

TOE features not under evaluation are:

- Alarms/Fault: Filtering and managing alarms
- Configuration: Ethernet, GPON, Ports and Manage Customers.
- Planning: All Planning features are not under evaluation

Users of the TOE

The TSF maintains the roles Administrator, User Manager, Operator and Viewer for TJ5500 and Admin, Operators and Users for TJ5100

B.6 Document evaluation

B.6.1 Documentation

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

1. **Security Target: Security Target Of TJ5500 NMS (Network Management System), TJ5100 EMS (Element Management System) Version 8.1, Version 1.9**
2. **TOE Functional Specification document**: **Functional Specifications (ADV_FSP.2) TJ5500 NMS (Network Management System) & TJ5100 EMS (Element Management System) Version 8.1**, Version 1.4
3. **Design and Architecture Of TJ5500 NMS (Network Management System) & TJ5100 EMS (Element Management System) ,Version 8.1,** Version 1.8
4. **Preparative procedures**: **TJ5500/TJ5100 Preparatory Procedure**, Version1.2
5. **Operational User guidance**: **TJ5500 R8.1 User Interface Guide** , Version 1.1
6. **Configuration Management, Capability and scope and Delivery procedure : Life-cycle Support process TJ5500 NMS (Network Management System) & TJ5100 EMS (Element Management System**, Version 1.6
7. **Test and Coverage: Family Functional tests and Coverage (ATE_FUN & ATE_COV) TJ5500 NMS (Network Management System) & TJ5100 EMS (Element Management System) Version 8.1**, Version 1.1

B.6.2 Analysis of document

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

Development process: The evaluators have analyzed the functional specification of the TOE and found that the TOE security function interfaces [TSFI} are described clearly and unambiguously. The evaluators have analyzed the Security Architecture and Design Documents. The security architecture description explains how the properties described below are exhibited by the TSF. It describes how domains are defined and how the TSF keeps them separate. It describes what prevents untrusted processes from getting to the TSF and modifying it. It describes what ensures that all resources under the TSF's control are adequately protected and all actions related to the SFRs are mediated by the TSF. It explains what role the environment plays in any of these. The security architecture description presents the TSF's properties of self-protection, domain separation, and non-bypassability to protect the TOE itself and the TSF.

Guidance Documents: The evaluators have 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 was also clear and unambiguous.

Configuration management: The evaluators have analyzed configuration management documentation and determined that the TOE and its associated components and documents are clearly identified as configurable items (CI).

Delivery Procedure: The TOE is supplied in the CD, for burning of software in CD's as per the Product or customer requirement for shipment to the customer premises. Customer should verify the hash value of the

delivered Software file against hash value of the product list in the CC portal at the time of installation and commission. The Customer Support team will install Tejas products at the Customer site and configure it as per the customer requirements

B 7 Product Testing

Testing at EAL2 consists of the following three steps: Testing by developer, Independent Testing by Evaluation Team, and Vulnerability analysis 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 have analyzed 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 test 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 TOE has been installed properly as per the preparative procedure document. 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. Independent testing is designed to verify the correct implementation of security functionalities available to different categories of users and to check whether audit record is being generated for auditable events, also checked for the privilege escalation is prevented.

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

a. Security Audit

The TOE's auditing capabilities generates audit records for security events. TOE generates a set of AUDIT records, which are stored in database tables. The logs are only accessible through the Web-Based administrative interface, which only authenticated Administrators are authorized access. Administrator can view, filter, purge and save the logs. When logs are saved from the TOE, they are transferred to the PC connected to the Web-Based administrative. TOE has backup and purge facilities to maintain circular buffer for audit records. After the audit log records reached to maximum configured limit for logs in database, The oldest audit log records are overwritten by new records (If Auto-purge configured with backup option then backup will be taken before overwriting the records).

Cryptographic Operations

TOE provides and encrypted path between users and TOE. Users connect to TOE using a secure connection using AES encryption algorithms supported by TJ5500. The secure connection ensures that user passwords and data are protected from modification and disclosure

.

b. User Data Protection and Protection of the TSF

TOE enforces flow control policy between source and destination IP address and ports of two different network elements as per standard architecture. Before any access is granted, users must log into TJ5500. Each user account is associated with one user profile. Only the Administrator profile has privilege to set the flow control SFP.

c. Identification and authentication

TOE performs identification and authentication of all users and administrators. TOE has the ability to authenticate users locally using a password or can integrate with a remote authentication server. In the evaluated configuration, TOE will perform the authentication locally. Users enter a username and password, which is validated by TOE against the user information stored by the TOE. If the authentication succeeds, the user receives a session token that is used for identification of subsequent requests during that session.

d. Security management

TJ5500

The security feature in NMS is designed on **a RBAC (Role Based Access Control) model. Each profile** has a set of allowed actions associated with the profile. Each user is associated with a profile. The system by default provides four non-modifiable profiles.

 Administrator: The user assigned with this profile setting will have permissions like, to view and purge audit logs, managing of EMS, topology, TL, nodes, alarms, circuits, service and tunnels function.

I. **Operator:** The user assigned with this profile has the permission to view audit logs and make changes in configuration, manage circuits and acknowledge alarms.
II. **Viewer:** The user assigned with this profile has only the permission to view audit logs, alarms and configuration data.
III. **User Manager:** The user assigned with this profile has permission to create, delete and modify the user account and security attributes. Also has privilege to create custom profile as per requirement.

TJ5100

Security management controls access to the network resources to ensure the reliability of the network. The security feature in EMS is designed on a user based security module. Different users are assigned different permissions (read, write, delete) on the tasks that they are authorized to perform. EMS defines certain terms such as actions, action table permissions, profiles, and groups that are associated with security.

The actions include viewing, configuring and modifying the network attributes. Each action has a certain set of tables associated with it. The user will have access to these tables with the permissions (read, write, and/or delete) based on the action table permissions defined.

The profiles consist of a set of pre-defined actions. User is authorized to assign a profile with the permissions associated. The group consists of authorized users. The users in a group have access to all the objects that the group is assigned to and their access levels are defined by their profiles.

I. **EMS_Admin**: The user assigned with this profile setting will have permissions like, to view audit logs and create, delete and modify the user account and security attributes.
II. **EMS_Operator**: The user assigned with this profile has the permission to make changes in configuration and acknowledge alarms and doesn't have privilege to access to TSF data.
III. **EMS_User**: The user assigned with this profile has only the permission to view alarms and configuration data and doesn't have privilege to access to TSF data.

e. Protection of the TSF

TOE provides a timestamp for its own use. The timestamp is used from the clock provided in the TOE environment hardware. The Protection of the TSF function is designed to satisfy the following security functional requirements

f. TOE Access

TOE provides a limitation on multiple concurrent graphical user interface session. Maximum of sessions depends on the license. TOE protects all current sessions from compromise by enforcing a timeout. When a session becomes idle for more than 30 minutes or reaches a maximum lifetime of 120 minutes, the session times out and is deleted from the session table. Session timeouts are enforceable on sessions initiated on both the administrator and user interfaces of the TOE.

g. Trusted Path/Channels

The TOE client is a web based graphical user interface, which enables the operator or the user to visualize the network and perform management operations. The user-interface facilitates the various FCAPS functionality as well as allows a graphical user interface cut through to the underlying TOE. Also communications among all service are secure via SSL over CORBA or JMS.

The tests were carried out under isolated and controlled environment which complied with the operational environment, as specified in ST. Test cases were developed using information available in the ST and FSP containing information on TOE interfaces. The manual tests were carried out using the interfaces of the TOE.

B 7.2 Vulnerability Analysis and Penetration testing

The evaluators have considered the threats identified in ST and conducted vulnerability search from the information available in the public domain in search of potential vulnerabilities from public domain, scanning tools are used. Nmap tools was used for scanning to find out open ports. Nessus Vulnerability scanning tool is used with the latest plug in to find out hypothesized potential vulnerabilities present in the TOE.

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 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.

AT1: Encrypted channel may be intercepted if attacker becomes successful to decrypt algorithms used to encrypt the channel. Attack Potential: 10 (Beyond Basic)) Penetration Testing is not required]

AT2: Password may be accessed from the storage if password is used in clear text and stored in clear

text and remains accessible to the attacker through the open port. Attack Potential: 8 (Within Basic) Penetration Testing is required]

AT3: the attacker through the open port and form fields to exploit its vulnerabilities and to make the TSF fail may access Database containing TSF data. Attack Potential: 8 (Within Basic) Penetration Testing is required]

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**:

PT1 for attack scenario AT1: Password may be accessed from the storage if password is used in clear text and stored in clear text and remains accessible to the attacker

PT2: the attacker through the open port to misuse the TSF data and the TSFs may access the database containing TSF data

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.

Subsequent to the independent review of public domain vulnerability databases and all evaluation evidences, potential vulnerabilities were identified with their attack potentials. The potential vulnerabilities with '**Basic**' attack potential were considered for penetration testing.

The penetration testing could not exploit any vulnerability in the intended operational environment of the TOE. However, these vulnerabilities may be exploited with higher attack potential.

Residual Vulnerabilities

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 vulnerabilities, having attack potential more than 'Basic' were not considered for penetration testing. Hence, these vulnerabilities may be considered as residual vulnerabilities. The residual vulnerabilities are given below.

AT1: Encrypted channel may be intercepted if attacker becomes successful to decrypt algorithms used to encrypt the channel. Attack Potential: 10 **(Beyond Basic**).

B 8 Evaluation Results

The evaluation team has documented the evaluation results in the Evaluation Technical Report [ETR]. The TOE was evaluated through evaluation of its evaluation evidences, documentation, testing and vulnerability assessment using methodology stated in [CEM] and laboratory operative procedures.

Documentation evaluation results:

The documents for TOE and its development life cycle have been 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 CC Version 3.1 Revision 5 for Evaluation level EAL2.

Testing:

The independent functional tests yielded the expected results, giving assurance that '**TJ5500 NMS (Network Management System) and TJ5100 EMS (Element Management System) Version 8.1**' behaves as specified in its [ST].

Vulnerability assessment and penetration testing:

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

Table 3: Assurance classes and components wise verdict

Assurance classes and components			Verdict
Security target document evaluation		ASE	PASS
1.	ST introduction	ASE_INT.1	PASS
2.	Conformance claims	ASE_CCL.1	PASS
3.	Security problem definition	ASE_SPD.1	PASS
4.	Security objectives	ASE_OBJ.2	PASS
5.	Extended component definition	ASE_ECD.1	PASS
6.	Derived Security requirements	ASE_REQ.2	PASS
7.	TOE Summary Specification	ASE_TSS.1	PASS
TOE Development evaluation		ADV	PASS
1	Security architecture description	ADV_ARC.1	PASS
2	Security-enforcing functional specification	ADV_FSP.2	PASS
3	Basic design	ADV_TDS.1	PASS
TOE Guidance document evaluation		AGD	PASS
1	Operational user guidance	AGD_OPE.1	PASS
2	Preparative procedure	AGD_PRE.1	PASS
TOE Life cycle support evaluation		ALC	PASS

Assurance classes and components			Verdict
1	Use of a CM system	ALC_CMC.2	PASS
2	Parts of the TOE CM coverage	ALC_CMS.2	PASS
3	Delivery procedures	ALC_DEL.1	PASS
Testing of the TOE		ATE	PASS
1	Evidence of coverage	ATE_COV.1	PASS
2	Functional Testing	ATE_FUN.1	PASS
3	Independent Testing - Sample	ATE_IND.2	PASS
Vulnerability assessment of the TOE		AVA	PASS
1	Vulnerability Analysis	AVA_VAN.2	PASS

B 9 Validator Comments

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

- **The [ST] 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 'TJ5500 NMS (Network Management System) and TJ5100 EMS (Element Management System) Version 8.1"satisfies all the security functional requirements (SFR) and Security assurance requirements(SAR) as defined in the [ST]. Hence, the TOE is recommended for EAL2 Certification as per CC version 3.1 Revision 5.**

However, it should be noted that there are no **Protection Profile** compliance claims.

B 10 List of Acronyms

ACL: Access Control List
CC: Common Criteria
CCTL: Common Criteria Test Laboratory
CEM: Common Evaluation Methodology
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
3. [CC-III]: Common Criteria for Information Technology Security Evaluation: Part 3: Version 3.1
4. [CEM]: Common Methodology for Information Methodology: Version 3.1
5. [ST] : Security Target Of TJ5500 NMS (Network Management System), TJ5100 EMS (Element Management System) Version 8.1, Version 1.9
6. [ETR]: Evaluation Technical Report No. IC3S/KOL01/Tejas/EAL2/1018/0012/ETR/0036