SECURITY TARGET FOR THE SECURELOGIX CORPORATION® ENTERPRISE TELEPHONY MANAGEMENT (ETM™) PLATFORM

VERSION 3.0.1

EWA-Canada Document No. 1404-002-D001
Version 2.9, 14 February 2002

Communications Security Establishment
Common Criteria Evaluation File Number: 383-4-10

Prepared for:

Certification Body
Communications Security Establishment
P.O. Box 9703
Terminal
Ottawa, Ontario
K1G 3Z4

Prepared by:

Electronic Warfare Associates-Canada, Ltd.
275 Slater St., Suite 1600
Ottawa, Ontario
K1P 5H9

SECURITY TARGET FOR THE SECURELOGIX CORPORATION® ENTERPRISE TELEPHONY MANAGEMENT (ETM™) PLATFORM VERSION 3.0.1

Document No. 1404-002-D001
Version 2.9, 14 February 2002

<Original> Approved by:

Project Engineer: ______________________________ ____________

Project Manager: ______________________________ ____________

Program Director: ______________________________ ____________

(Signature) (Date)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

1.1 IDENTIFICATION

This document details the Security Target (ST) for the SecureLogix Corporation® ETM™ Platform. This ST has been prepared[1] in accordance with the Common Criteria for Information Technology Security Evaluation (CC), version 2.1, August 1999.

1.2 OVERVIEW

The ETM™ Platform is designed to protect telecommunications lines from abuse, and provide extensive auditing capabilities on all telecommunications line traffic. The system can operate in conjunction with a private branch exchange (PBX), but it is not required. The ETM™ Platform components are:

a. the ETM™ Management Server version 3.0.1 running on an Intel based PC with Windows NT 4 as the operating system (also available for Solaris and Windows 2000 platforms);

b. the administrator TeleView™ Console version 3.0.1 running on an Intel based PC with Windows NT, Windows 98, Windows 2000 or on a Solaris based platform;

c. hardware analog appliances;

d. hardware T1 appliances;

e. hardware ISDN/PRI appliances; and

f. hardware E1 ISDN/PRI appliances.

The ETM™ Management Server and TeleView™ Console are both written in the Java programming language and require a Java Virtual Machine to be installed on their host PC. All appliances are designed by SecureLogix Corporation® using commercially available components, and use the LINUX[2] 2.4 kernel as the underlying operating system.

The ETM™ Platform mediates access between local telecommunication users and external telecommunication users based on rules defined by the administrator. Rulesets are created on the ETM™ Management Server which are then pushed down to the appliances. The appliances allow or deny calls based on their respective rulesets. The default behaviour is to allow any calls not explicitly denied.

A hardware setting exists, for all 1000 series appliances, to determine the default behaviour should a ETM™ Platform appliance fail (due to a power outage for example). ETM™ Platform appliances can be configured to fail-safe (allow all calls), or fail-secure (deny all calls including emergency numbers).

[1] The ST author is Kim Frawley Braun of EWA-Canada.

[2] A stripped down version of Linux is used. There is no ftpd, inetd or login prompt.

Ethernet network links are used to facilitate the following communication channels:

a. between the appliances and ETM™ Management Server;
b. between the TeleView™ Console and ETM™ Management Server; and
c. between the administrator and appliances (Telnet).

ETM™ Platform includes an option to encrypt network communications using DES (by default) and Triple DES (upon request) cryptography. Administrators may also communicate directly with the appliances though a serial port located on the appliances.

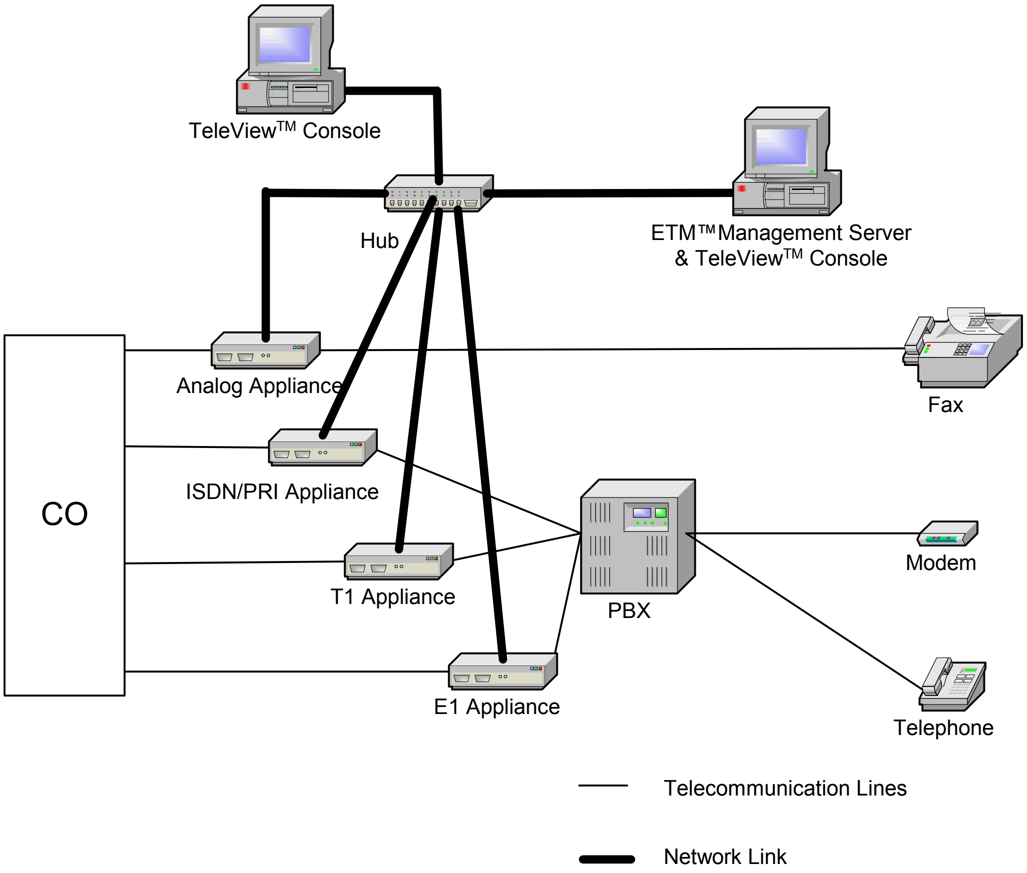

Figure 1: Example ETM™ Platform Configuration

The ETM™ Platform human machine interface (HMI) allows the administrator to perform the following functions:

a. specify rules governing how telecommunication access is mediated;
b. specify the level of network activity displayed; and
c. specify what telecommunication activity is logged.

The HMI also provides the user with current and historical views of individual calls, and their associated level of activity. Extensive report and graphs may be generated from the historical data.

Appropriate security measures are expected to exist for the network on which the ETM™ Platform is deployed to protect the communications between components.   Appropriate mechanisms must be put in place on the commercial products being used that are external to any SecureLogix components. The ETM™ Platform can be configured to encrypt communications between its components. The Target of Evaluation (TOE) consists of the ETM™ Management Server, the TeleView™ Console, and the four types of appliances (analog, T1, ISDN/PRI, E1 ISDN/PRI).

1.3 CC CONFORMANCE

The ETM™ Platform is conformant with the functional requirements specified in Part 2 of the CC. The ETM™ Platform is conformant to the assurance requirements for Evaluation Assurance Level (EAL) 2, as specified in Part 3, of the CC, with the following augmentations:

a. ACM_CAP.3 – Authorisation controls;
b. ACM_SCP.1 – TOE CM coverage; and
c. ALC_DVS.1 – Identification of security measures.

2 TARGET OF EVALUATION DESCRIPTION

The ETM™ Platform is designed to protect telecommunications lines from abuse, and provide extensive auditing capabilities on all telecommunications line traffic[3]. The system can operate in conjunction with a private branch exchange (PBX), but it is not required. The evaluated configuration consists of:

a. the ETM™ Management Server version 3.0.1 executing on an Intel based PC with Windows NT 4 SP6a, Windows 2000 and Solaris 7/8 as the operating systems;
b. the administrator TeleView™ Console version 3.0.1 executing on an Intel based PC with Windows NT 4 SP6a, and Windows 98 (unpatched), Windows 2000 and Solaris as the operating systems;
c. Java Virtual Machine software, version 1.3.1 on both the ETM™ Management Server and TeleView™ Console hosts;
d. hardware analog appliances software version 3.0.30, hardware Model ETM™ 1010;
e. hardware T1 appliances software version 3.0.30, hardware Model ETM™ 1020, Model ETM™ 2100 or Model ETM™ 3200;
f. hardware ISDN-PRI appliances software version 3.0.30, hardware Model ETM™ 1030, Model ETM™ 2100 or Model ETM™ 3200; and
g. hardware E1 ISDN-PRI appliances software version 3.0.30, hardware Model ETM™ 1040, Model ETM™ 2100 or Model ETM™ 3200.

The minimum hardware requirements for the ETM™ Management Server and TeleView™ Console are specified in the ETM™ Platform Installation and Configuration Guide provided as part of the ETM™ 3.0.1 Product Code CD.

The ETM™ Platform components (appliances, ETM™ Management Server, TeleView™ Console) can be distributed across an Ethernet network. The network access security policy requires administrators[4] to provide a valid username and password for authentication. Appliances maintain a file of “allowed” IP addresses and only allow communications from ETM™ Management Servers which have an IP address in the file. ETM™ Management Servers have a similar file for communications to remote TeleView™ Consoles.

The administrator uses the TeleView™ Console to communicate to ETM™ Management Server, and through it, communicate with the appliances. The administrator may also directly communicate to the appliances through a Telnet server or a serial port on the appliances. The Telnet access to a appliance can be disabled if desired, and will also be

[3] The TOE protects the telecommunications lines, but uses a TCP/IP network for internal communications. The use of the term “network” refers only to the TCP/IP network, not the telecommunications lines.

[4] The term “administrator” refers only to individuals who communicate over the network to configure and operate EMT™ Platform.

disabled automatically for a period of one hour, by the appliance, if there are six failed logins. The failed login count resets to zero after a successful login.

The system can encrypt communications between components using DES or Triple DES cryptography. The DES and Triple DES algorithms (cryptographic module identifier – NIST validated implementation version 3) have been evaluated and approved to the FIPS 46-3 DES and FIPS 81 DES Modes of Operation standards.

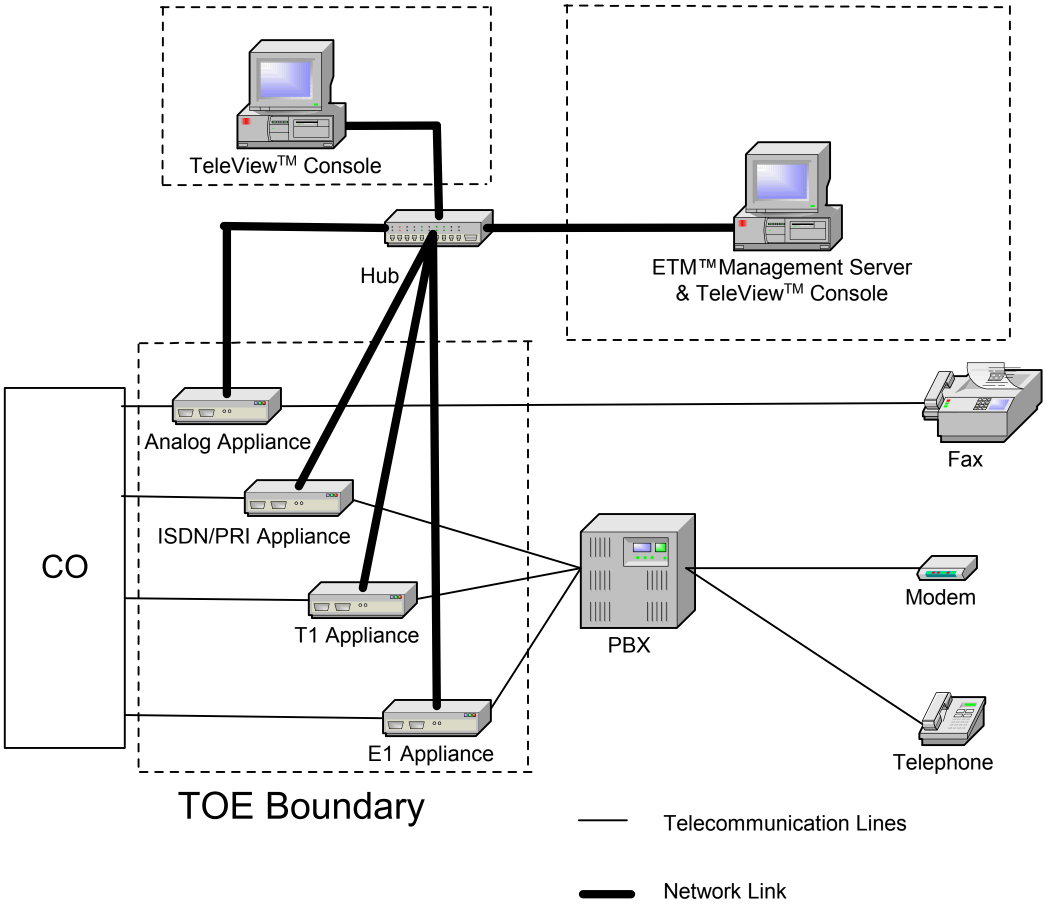

Figure 2: TOE Boundary Diagram

The appliances control and enforce the information flow security policy on the telecommunication lines based on the ruleset and configurations downloaded from the ETM™ Management Server. The appliances can be configured individually, or as a group. There are four appliance types corresponding to different types of telecommunications lines: analog, T1, ISDN/PRI and E1 ISDN/PRI. All four appliances were created by SecureLogix Corporation® using commercially available hardware components and execute on the LINUX operating system. SecureLogix Corporation® has added an extensive set of appliance command line instructions called ETM commands. The ETM command set can be accessed through a Telnet connection, command line window opened in the TeleView™ Console, or serial link, however a small subset of the ETM commands can only be performed locally at the appliance through the serial link. Each appliance type is included in the ETM™ Platform evaluation.

The TeleView™ Console allows the administrator to manage one or multiple ETM™ Platforms using graphical windows. The administrator can configure appliances by creating a configuration file on the ETM™ Management Server, which gets pushed down to the appliances. Checks are performed on a regular basis to ensure the appliances are executing the latest configuration file as defined (stored) on the ETM™ Management Server. It is important to note that any changes to the appliance configurations should be made through the TeleView™ Console (where possible), otherwise, changes made by communicating directly to the appliances can be overwritten when the next check occurs (the configuration file on the appliance would be different than that on the ETM™ Management Server so would be changed to match the ETM™ Management Server).

The default telecommunications information flow security policy for ETM™ Platform telecommunications users is “telecommunications that are not explicitly denied, are allowed”. The ruleset is traversed from top to bottom, triggering on the first applicable rule. A default rule exists at the top of the ruleset to always allow emergency calls (e.g. 911). The default rule cannot be removed. Administrators can create rules based on: calling number; called number; call type (voice, fax, modem, STU III, busy, unanswered, wide-band and undetermined), call direction (inbound, outbound), time of day, and call duration. ETM™ Platform includes the ability to examine the ruleset for ambiguous rules (e.g. rules that will never get triggered due to a previous rule).

ETM™ Platform has extensive auditing and reporting capabilities. The levels of events to be audited can be set by the administrator. Each audit record contains a unique identification number, date and time stamps, and the appliance or appliance array which originated the record. All call details (numbers, times, telecommunication line specifics, etc.) are recorded and can be viewed in a generated report (from canned or created templates) or plotted in a graph through the TeleView™ Console.

Most of the data produced during the operation of the ETM™ Platform is stored in the ETM™ Database, which is part of the ETM™ Management Server. The ETM™ RDBMS supports Oracle DBMS. The DBMS used for the ETM™ Database can be installed on the same computer as an ETM™ Management Server, or on a remote computer.

Audit records concerning telecommunication information flow and appliance status are generated at the appliances. The audit data is then uploaded to the ETM™ Management Server. Each appliance contains a memory card, which can store the audit records temporarily if the ETM™ Management Server is unavailable. The memory cards can hold the audit data in a circular buffer where they will eventually get overwritten with newer records, however there is sufficient memory to hold multiple days of audit logs even under heavy telecommunications traffic.

3 TOE SECURITY ENVIRONMENT

3.1 ASSUMPTIONS

The following conditions are assumed to exist in the operational environment:

Application Note: The TOE protects the telecommunications lines, but uses a TCP/IP network for internal communications. The use of the term "network" refers only to the TCP/IP network, not the telecommunications lines. The term "telecommunications user" refers only to individuals or IT entities that communicate over the telecommunications lines. The term "network attacker" refers only to individuals or IT entities that communicate over the network. As security functional refinement and unless stated otherwise in this ST, the term "user" is meant to be administrator(s) who communicate over the network to configure and operate the ETM™ Platform.

A.PHYSEC The TOE is physically secure.

A.PRONET Network protection mechanisms are in place for the server and TeleView™ Console client.

A.NOEVIL Administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

A.ADMKNW The administrator is knowledgeable of TCP/IP networking and Telecommunication systems.

3.2 THREATS

The following threats are addressed either by the TOE or the environment.

3.2.1 Threats Addressed By The TOE

The threats discussed below are addressed by a compliant TOE. The threat agents are either human users or external IT entities not authorised to use the TOE. The assets that are subject to attack are telecommunications resources.

T.SNIFF A network attacker may observe authentication data or system configuration info as it is transmitted between portions of the TOE.

T.REPLAY A network attacker may use previously captured or falsified data to authenticate to the TOE or alter its configuration.

T.ATKNET A network attacker may attack the TOE appliances.

T.INTRES An unauthorised external telecommunications user may gain access to internal telecommunication resources (telephones, modems, faxes, etc.).

T.EXTRES An internal telecommunications user may gain unauthorised access to external telecommunications resources (telephones, modems, faxes, etc.).

T.MISUSE A telecommunications user may use internal telecommunications resources in an unauthorised manner (make a voice call on a fax line, etc.).

T.TOEPRO A telecommunications user may bypass, deactivate, corrupt or tamper with TOE security functions.

T.ATKVIS A telecommunications user may conduct undetected attack attempts against the TOE.

T.TOEDAT A telecommunications user may read, modify or destroy TOE internal data.

T.TOEFCN A telecommunications user may access and use security and/or non-security functions of the TOE.

T.NONAPP An administrator may be unaware that an unauthorised application, executing on the TOE, is accessing the telecommunications lines or network via TOE interfaces.

T.NOCOM An administrator may be unaware that TOE internal communications have failed.

T.AUDEXH An administrator may be unaware that the audit storage of the TOE has been exhausted.

3.2.2 Threats To Be Addressed By Operating Environment

The threat possibilities discussed below must be countered by procedural measures and/or administrative methods. The threat agents are either human users or external IT entities not authorised to use the TOE. The assets that are subject to attack are telecommunications resources.

T.USAGE The TOE may be configured, used and administered in an insecure manner unwittingly by the user.

T.BADADM Compromise of the integrity and/or availability of the TOE may occur as a result of an administrator not following proper security procedures.

T.TROJAN Compromise of the integrity and/or availability of the TOE may occur as a result of an administrator unwittingly introducing a virus or trojan into the system.

4 SECURITY OBJECTIVES

4.1 TOE SECURITY OBJECTIVES

The following are the IT security objectives for the TOE:

O.CRYPTO The TOE must protect the confidentiality of authentication and system configuration data using cryptography as it passes between distributed components of the TOE.

O.ATKNET The TOE appliances must protect themselves against attack from the network. Replay attacks, in appliance to server communications, are countered by the communications being authenticated with a variable handshake and encrypted with valid cryptokey/algorithm.

O.MEDTEL The TOE must mediate telecommunications access both inbound and outbound on the telecommunications lines. The TOE shall be capable of allowing or denying the communication based on predefined attributes.

O.TELTOE The TOE should not allow access to the TOE from the telecommunications interfaces.

O.COMM The TOE must provide a mechanism to handle internal communication failures.

O.AUDCHK The TOE must provide a mechanism that advises the administrator when local audit storage has been exhausted.

O.ADMACC An administer role will exist on the TOE with access control mechanisms such that only authenticated administrators are able to perform security relevant functions.

O.HMI The TOE must provide functionality that enables an administrator to effectively manage the TOE and its security functions from its local HMI.

O.DSPACT The TOE must display to the user the current and recent history of telecommunications activity associated with the telecommunication lines.

O.AUDIT The TOE must record and store a readable audit trail of TOE telecommunications activity and security relevant events, and permit their review only by authorised administrators. The TOE will be capable of performing audit reduction, and of triggering alarms as required by the administrator.

O.SELFPRO The TOE must protect itself against attempts by a telecommunications user from the telecommunications side to bypass, deactivate, corrupt or tamper with TOE security functions.

4.2 ENVIRONMENT SECURITY OBJECTIVES

The following are non-IT security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

O.NETPRO The organisation responsible for the server and TeleView™ Console client portions of the TOE must ensure to their satisfaction that these components are protected against network attacks.

O.GUIDAN The administrator responsible for the TOE must ensure that the TOE is delivered, installed, configured, administered, and operated in a manner that maintains its security.

O.AUTHUSR Only authorised administrators are permitted physical access to the TOE.

5 IT SECURITY REQUIREMENTS

5.1 TOE SECURITY REQUIREMENTS

This section provides functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL) containing assurance components from Part 3 of the CC.

5.1.1 TOE Security Functional Requirements

The functional security requirements for this ST consist of the following components from Part 2 of the CC, summarised in Table 1. All users of the TOE can be divided into three distinct groups: administrators, telecommunication users and network attackers. The three types are quite different in their interactions with the TOE. As such, access control for administrators is addressed by FDP_ACC.1 (1), FDP_ACF.1 (1), FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, and FIA_UID.1, while telecommunications users are addressed by FDP_IFC.1 (1) and FDP_IFF.1 (1) and network attackers are addressed by FDP_IFC.1 (2) and FDP_IFF.1 (2).

The TOE Security Policy (TSP) is comprised of the TELCO, FILE, and NETWORK Security Function Policies (SFPs) that define the rules by which the TOE governs access to its telecommunication, file, and network resources.

Table 1 Summary of Security Functional Requirements

Functional Components	
Identifier	**Name**
FAU_ARP.1	Security Alarms
FAU_GEN.1	Audit data generation
FAU_SAA.1	Potential violation analysis
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_SEL.1	Selective audit
FAU_STG.1	Protected audit trail storage
FAU_STG.3	Action in case of possible audit data loss
FCS_COP.1	Cryptographic operation
FDP_ACC.1 (1)	Subset access control
FDP_ACF.1 (1)	Security attribute based access control
FDP_ACC.1 (2)	Subset access control
FDP_ACF.1 (2)	Security attribute based access control
FDP_IFC.1 (1)	Subset information flow control

Functional Components	
Identifier	**Name**
FDP_IFF.1 (1)	Simple security attributes
FDP_IFC.1 (2)	Subset information flow control
FDP_IFF.1 (2)	Simple security attributes
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of identification
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_SMR.1	Security Roles
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_STM.1	Reliable time stamps
FTP_TRP.1	Trusted Path

FAU_ARP.1 Security Alarms

FAU_ARP.1.1 – The TSF shall take [one or more of the following actions: audible alarm, SNMP trap, email with or without attachments, pager, TeleSweep Secure® scan, visual alert] upon detection of a potential security violation.

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 [basic] level of audit identified in Table 2 (Application Note: Basic level includes all minimum requirements as well);
c. exhaustion of log storage;
d. changes in TOE security function configuration;
e. failed and successful logins by administrators to an appliance;
f. logins/logouts by administrators to ETM™ Management Server;
g. failed and successful logins by user to an appliance;
h. changes to rulesets that are applied to an appliance;

i. the additions/deletions/clones/modifications an administrator performs in the ETM™ Management Server;
j. appliance and telephone circuit errors;
k. requests from unknown appliances;
l. detection of an ambiguous rule; and
m. rule violations.

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 (when available), 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 ST:
   - [call destination (called number);
   - call source (calling number), if available;
   - call trunk channel; call trunk group;
   - call begin time;
   - call end time;
   - call type as fax, modem, voice, STU voice, STU data, STU generic, unknown, busy, unanswered, wideband or undetermined;
   - call direction as inbound or outbound;
   - call duration;
   - call "in-call" digits;
   - call trailing digits;
   - a unique identifying number for each entry;
   - the appliance which originated the event; and
   - the appliance array the appliance belongs to].

Table 2 Additional Auditable Events from CC Functional Components

Functional Component	Level	Auditable Event
FAU_ARP	Minimum	Actions taken due to imminent security violations.
FAU_SAA.1	Minimum	Enabling and disabling of any of the analysis mechanisms.
	Minimum	Automated responses performed by the tool.
FAU_SAR.1	Basic	Reading of information from the audit records.
FAU_SEL.1	Minimum	All modifications to the audit configuration that occur while the audit collection functions are operating.
FAU_STG.3	Basic	Actions taken due to exceeding of a threshold.
FCS_COP.1	Minimum	Success and failure and the type of cryptographic operation.

Functional Component	Level	Auditable Event
	Basic	Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.
FDP_ACF.1	Minimum	Successful requests to perform an operation on an object covered by the SFP.
	Basic	All requests to perform an operation on an object covered by the SFP.
FDP_IFF.1	Minimum	Decisions to permit requested information flows.
	Basic	All decisions on requests for information flows.
FIA_AFL.1	Minimum	The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).
FIA_SOS.1	Minimum	Rejection by the TSF of any tested secret.
	Basic	Rejection or acceptance by the TSF of any tested secret.
FIA_UAU.1	Minimum	Unsuccessful use of the authentication mechanism.
	Basic	All use of the authentication mechanism.
FIA_UID.1	Minimum	Unsuccessful use of the user identification mechanism, including the user identity provided.
	Basic	All use of the user identification mechanism, including the user identity provided.
FMT_MOF.1	Basic	All modifications in the behaviour of the functions in the TSF.
FMT_MSA.1	Basic	All modification of the values of security attributes.
FMT_MSA.3	Basic	Modifications of the default setting of permissive or restrictive rules.
	Basic	All modifications of the initial values of security attributes.
FMT_MTD.1	Basic	All modifications to the values of TSF data.
FMT_SMR.1	Minimum	Modifications to the group of users that are part of a role
FPT_STM.1	Minimum	Changes to the time.
FTP_TRP.1	Minimum	Failures of the trusted path functions.
	Minimum	Identification of the user associated with all trusted path failures if available.
	Basic	All attempted uses of the trusted path functions.
	Basic	Identification of the user associated with all trusted path invocations if available.

FAU_SAA.1 Potential violation analysis

FAU_SAA.1.1 – The TSF shall be able to apply a set of rules in monitoring the audited events, and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2 – The TSF shall enforce the following rules for monitoring audited events:

a. Accumulation or combination of [communication failure] known to indicate a potential security violation;

b. [Administrator created rules set by configurable security policy, dialing plan and call monitoring definition and based on calling number, called number, call type (voice, fax, modem, STU voice, STU data, STU generic, busy, unanswered, wideband, undetermined), call direction (inbound, outbound), call duration, and time of day.]

FAU_SAR.1 Audit review

FAU_SAR.1.1 – The TSF shall provide [an administrator] with the capability to read [all audit data] 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.

FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 – The TSF shall provide the ability to perform [searching and ordering] of audit data based on:

a. [log time;
b. start time;
c. end time;
d. duration;
e. in/out call direction;
f. source;
g. destination;
h. type;
i. “in-call” digits;
j. trailing digits;
k. tracks;
l. appliance array;
m. appliance;
n. trunk group;
o. channel;

p. name of ruleset;
q. rule number;
r. rule comment;
s. unique record ID;
t. unsuccessful login attempts; and
u. call information (LOC-local call, INTL-international call, VSC-vertical service code, etc.)].

The TSF shall provide the ability to perform [filtering] of audit data based on:

a. [date;
b. call direction;
c. call duration;
d. phone number;
e. call type;
f. "in-call" digits;
g. trailing digits;
h. track;
i. appliance array;
j. appliance;
k. text ; and
l. call information (LOC-local call, INTL-international call, VSC-vertical service code, etc.)

Application Note: For the several of the searchable audit fields, there are sub-types. The reporting tool included with ETM™ Platform allows filters to be used to provide a finer layer of granularity. For example, if a user wished to see audit records only for modems, the user would have to search based on call type, leaving only modem records.

FAU_SEL.1 Selective audit

FAU_SEL.1.1 – The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes: [event type].

FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 – The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2 – The TSF shall be able to [prevent] modifications to the audit records.

Application Note: The audit protection mechanisms are provided by the underlying database server.

FAU_STG.3 Action in case of possible audit data loss

FAU_STG.3 – The TSF shall take [the following action: generate a security message] if the audit trail exceeds [the local storage capacity].

Application Note: Upon trying to transfer audit files to the ETM™ Management Server, a window pops up saying audit log will be deleted.

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 - The TSF shall perform [encryption and decryption of all data communications between TOE components] in accordance with a specified cryptographic algorithm [DES in CFB mode] and cryptographic keys sizes [64 bits] that meet the following: [FIPS 46-3 and FIPS 81] when using the export version of the ETM™ Platform.

FCS_COP.1.1 - The TSF shall perform [encryption and decryption of all data communications between TOE components] in accordance with a specified cryptographic algorithm [Triple DES in CFB mode] and cryptographic keys sizes [64 bits] that meet the following: [FIPS 46-3 and ANSI X9.52-1998] when using the domestic version of the ETM™ Platform.

FDP_ACC.1 Subset access control (1)

FDP_ACC.1.1 – The TSF shall enforce the [NETWORK SFP] on [administrators authenticating to the TOE].

FDP_ACF.1 Security attribute based access control (1)

FDP_ACF.1.1 – The TSF shall enforce the [NETWORK SFP] to objects based on [username, password, and IP address].

FDP_ACF.1.2 – The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a. [the password entered for a given username matches that kept by the TOE; and
b. the source IP address matches one listed as acceptable within the TOE].

FDP_ACF.1.3 – The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none].

FDP_ACF.1.4 – The TSF shall explicitly deny access of subjects to objects based on the [any request not matching the previous condition (see FDP_ACF.1.3)].

FDP_ACC.1 Subset access control (2)

FDP_ACC.1.1 – The TSF shall enforce the [FILE SFP] on [administrators editing TOE objects].

FDP_ACF.1 Security attribute based access control (2)

FDP_ACF.1.1 – The TSF shall enforce the [FILE SFP] to objects based on [number of administrators editing object].

FDP_ACF.1.2 – The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a. [only one administrator shall be granted access to edit a TOE object at a time].

FDP_ACF.1.3 – The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none].

FDP_ACF.1.4 – The TSF shall explicitly deny access of subjects to objects based on the [any request not matching the previous condition (see FDP_ACF.1.3)].

FDP_IFC.1 Subset information flow control (1)

FDP_IFC.1.1 – The TSF shall enforce the [TELCO SFP] on:

a. [subjects: telecommunications channels; and
b. operations: circuit request or change].

FDP_IFF.1 Simple security attributes (1)

FDP_IFF.1.1 – The TSF shall enforce the [TELCO SFP] based on the following types of subject and information security attributes:

a. [subject security attributes: none; and

b. information security attributes:

- [calling number;
- called number;
- call type (voice, fax, modem, STU generic, busy, unanswered, wideband and undetermined);
- call direction (inbound, outbound);
- call duration; and
- time of day].

FDP_IFF.1.2 – The TSF shall permit an information flow through a controlled subject and controlled information via a controlled operation if the following rule holds: [called number is an emergency number (e.g. 911) OR an administrator created rule does not explicitly deny the connection based on the following attributes:

a. the called phone number;
b. the calling phone number;
c. the call direction;
d. the type of call;
e. the call duration; and
f. the time of day]).

FDP_IFF.1.3 – The TSF shall enforce the [default TOE behaviour in the event of a TOE failure to be either fail-safe (all calls allowed) or fail-secure (no calls allowed) based on a hardware setting.].

Application Note: This applies only to 1000 Series appliances.

FDP_IFF.1.4 – The TSF shall provide the following [none].

FDP_IFF.1.5 – The TSF shall explicitly authorise an information flow based on the following rules:

a. [Emergency 911 calls – called number is 911; and
b. Default – information flow is allowed unless explicitly denied.]

FDP_IFF.1.6 – The TSF shall explicitly deny an information flow based on the following rules:

a. Blocked by number – an administrator created rule explicitly denies the calling or called number;
b. Blocked by type – an administrator created rule explicitly denies the call type (i.e. voice, fax, modem, STU generic, busy, unanswered, wideband or undetermined);

c. Blocked by direction – an administrator created rule explicitly denies the direction of the call (inbound, outbound);
d. Blocked by length – an administrator created rule explicitly denies calls that extend beyond a defined duration; and
e. Blocked by time – an administrator created rule explicitly denies calls based on the time of day].

Application Note: Calls blocked by length are not blocked from starting, but terminated once they have reached a defined duration.

FDP_IFC.1 Subset information flow control (2)

FDP_IFC.1.1 – The TSF shall enforce the [NETWORK SFP] on:

a. [subjects: network channels; and
b. operations: data communications].

FDP_IFF.1 Simple security attributes (2)

FDP_IFF.1.1 – The TSF shall enforce the [NETWORK SFP] based on the following types of subject and information security attributes:

a. [subject security attributes: username, password and IP addresses; and

b. information security attributes:
- [client to server communications – IP address is on allowed list and username and password are valid and communications are encrypted with valid cryptokey/algorithm;
- appliance to server communications – IP address is on allowed list and communications authenticated with a variable handshake and encrypted with valid cryptokey/algorithm; and
- appliance to appliance communications – IP address is on allowed list and communications are encrypted with valid cryptokey/algorithm].

FDP_IFF.1.2 – The TSF shall permit an information flow through a controlled subject and controlled information via a controlled operation if the following rule holds: [DES or Triple DES algorithm implemented]).

FDP_IFF.1.3 – The TSF shall enforce the [none].

FDP_IFF.1.4 – The TSF shall provide the following [none].

FDP_IFF.1.5 – The TSF shall explicitly authorise an information flow based on the following rules: [none]

FDP_IFF.1.6 – The TSF shall explicitly deny an information flow based on the following rules: [none].

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 – The TSF shall detect when [six] unsuccessful authentication attempts occur related to [attempted administrator logins using Telnet, to an appliance].

FIA_AFL.1.2 – When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [deny all Telnet access to the appliance for a period of one hour and generate an audit event].

FIA_ATD.1 User attribute definition

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

a. password; and
b. privileges (manage server, modify users, edit policies, edit appliance parameters, login directly to appliance)].

FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 – The TSF shall provide a mechanism to verify that secrets meet [a minimum of eight characters including one change of case character and one digit for the administrator password].

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 – The TSF shall allow, [within the first two minutes of appliance start-up, any human with physical access to the appliance to gain access to appliance security functions] before the user is authenticated.

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

FIA_UID.1 Timing of identification

FIA_UID.1.1 – The TSF shall allow, [within the first two minutes of appliance start-up, any human with physical access to the appliance to gain access to appliance security functions] 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.

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 – The TSF restrict the ability to [enable and disable] the functions:

a. [bypass of the TOE security functions;
b. the setting of the various configurations of the TOE security functions;
c. the setting of the level of telecommunications activity detail that is displayed;
d. the logging of selected telecommunications traffic;
e. the capturing of "in-call" digits;
f. the display of errors;
g. the display of current telecommunications activity; and
h. the display of the audit log reports

to an administrator].

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 – The TSF shall enforce the [NETWORK SFP] to restrict the ability to:

a. [change] the security attribute [user password];
b. [modify and delete] the security attribute [username];
c. [add or delete] the security attribute [privileges]; and
d. [add or delete] the security attribute [IP addresses]

to [an administrator].

FMT_MSA.1.1 – The TSF shall enforce the [TELCO SFP] to restrict the ability to:

a. [create, modify, and delete] the security attribute [groups of phone numbers]; and
b. [create, modify, and delete] the security attribute [groups of specified times of day]

to [an administrator].

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 – The TSF shall enforce the [information flow control TELCO SFP] to provide [permissive] default values for information flow security attributes that are used to enforce the TELCO SFP.

Application Note: The default rule configuration for the ETM™ Platform is to allow all information flows. An authorised user must create an explicit deny rule in order to restrict any information flows.

FMT_MSA.3.2 – The TSF shall allow the [administrator] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 – The TSF shall restrict the ability to:
a. [query, modify, and delete] the [audit logs];
b. [modify] the [audit level];
c. [generate] the [audit reports];
d. [modify] the [appliance configurations];
e. [modify] the [date and time of the host machine];
f. [modify] the [date and time of the appliance];
g. [display] the [appliance status]; and
h. [display] the [current telecommunications activity]
to [administrators].

FMT_SMR.1 Security Roles

FMT_SMR.1.1 – The TSF shall maintain the roles: [administrators with some combination of the following privileges:

a. manage server;
b. modify users;
c. edit policies;
d. edit appliance parameters; and
e. login directly to appliance].

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

FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 – The TSF shall protect TSF data from [disclosure] when it is transmitted between separate parts of the TOE.

FPT_STM.1 Reliable time stamps

FPT_STM.1.1 – The TSF shall be able to provide reliable time stamps for its own use.

Application Note: The word "reliable" in the above requirement means that the order of occurrence of auditable events is preserved.

FTP_TRP.1 Trusted Path

FTP_TRP.1.1 – The TSF shall provide a communication path between itself and [local and remote] administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2 – The TSF shall permit [local administrators and remote administrators] to initiate communication via the trusted path.

FTP_TRP.1.3 – The TSF shall require the use of the trusted path for [internal TSF data communications].

5.1.2 TOE Security Assurance Requirements

The assurance security requirements for EAL2, as specified in Part 3, of the CC with the following augmentations are noted in Table 3. The assurance components are summarised in the following table:

Table 3 Assurance Requirements for ETM™ Platform

Assurance Class	Assurance Components	
	Identifier	Name
Configuration Management	ACM_CAP.3	Authorisation controls (AUGMENTED)
	ACM_SCP.1	TOE CM coverage (AUGMENTED)
Delivery and Operation	ADO_DEL.1	Delivery Procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance

Assurance Class	Assurance Components	
	Identifier	Name
Life Cycle Support	ALC_DVS.1	Identification of security measures (AUGMENTED)
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent testing – sample
Vulnerability Assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

Evaluation Note: All of the above assurance requirements apply only to the ETM™ Platform itself, and not to the underlying operating system. The portions of the OS, which interface with the ETM™ Platform, were indirectly verified however, as a part of ATE_IND.2 testing.

ACM_CAP.3 Authorisation controls

Developer action elements:

ACM_CAP.3.1D – The developer shall provide a reference for the TOE.

ACM_CAP.3.2D – The developer shall use a configuration management (CM) system.

ACM_CAP.3.3D – The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.3.1C – The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.3.2C – The TOE shall be labelled with its reference.

ACM_CAP.3.3C – The CM documentation shall include a configuration list and a CM plan.

ACM_CAP.3.4C – The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.3.5C – The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.3.6C – The CM system shall uniquely identify all configuration items.

ACM_CAP.3.7 – The CM plan shall describe how the CM system is used.

ACM_CAP.3.8 – The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.3.9 – The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.3.10 – The CM system shall provide measures such that only authorised changes are made to the configuration items.

Evaluator action elements:

ACM_CAP.3.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ACM_SCP.1 TOE CM coverage

Developer action elements:

ACM_SCP.1.1D – The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_SCP.1.1C – The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, and CM documentation.

ACM_SCP.1.2C – The CM documentation shall describe how configuration items are tracked by the CM system.

Evaluator action elements:

ACM_SCP.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_DEL.1 Delivery Procedures

Developer Action elements:

ADO_DEL.1.1D – The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D – The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL1.1C – The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

ADO_DEL1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1 Installation, generation, and start-up procedures

Developer action elements:

ADO_IGS.1.1D – The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C – The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E – The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

ADV_FSP.1 Informal functional specification

Developer action elements:

ADV_FSP.1.1D – The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C – The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C – The functional specification shall be internally consistent.

ADV_FSP.1.3C – The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4C – The functional specification shall completely represent the TSF.

Evaluator action elements:

ADV_FSP.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E – The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

ADV_HLD.1 Descriptive high-level design

Developer action elements:

ADV_HLD1.1D – The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.1.1C – The presentation of the high-level design shall be informal.

ADV_HLD.1.2C – The high-level design shall be internally consistent.

ADV_HLD.1.3C – The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C – The high-level design shall describe the security functionality provided by each subsystem of the TSF

ADV_HLD.1.5C – The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6C – The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C – The high-level design shall identify which of the interfaces the subsystems of the TSF are externally visible.

Evaluator action elements:

ADV_HLD.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2E – The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_RCR.1.1D – The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representation that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C – For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_ADM.1 Administrator guidance

Developer action elements:

AGD_ADM.1.1D – The developer shall provide administrator guidance addressed to system administration personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C – The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C – The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C – The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C – The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5C – The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C – The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C – The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C – The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_USR.1 User guidance

Developer action elements:

AGD_USR.1.1D – The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C – The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C – The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C – The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C – The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5C – The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C – The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1 Identification of security measures

Developer action elements:

ALC_DVS.1.1D – The developer shall produce development security documentation.

Content and presentation of evidence elements:

ALC_DVS.1.1C – The development security documentation shall describe all the physical, procedural, personnel, and other security, measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C – The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

Evaluator action elements:

ALC_DVS.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E – The evaluator shall confirm that the security measures are being applied.

ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_COV.1.1D – The developer shall provide evidence of the test coverage.

Content and presentation of evidence elements:

ATE_COV.1.1C – The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Evaluator action elements:

ATE_COV.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Functional testing

Developer action elements:

ATE_FUN.1.1D – The developer shall test the TSF and document the results.

ATE_FUN.1.2D – The developer shall provide test documentation

Content and presentation of evidence elements:

ATE_FUN.1.1C – The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C – The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C – The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C – The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C – The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

ATE_FUN.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 Independent testing – sample

Developer action elements:

ATE_IND.1.1D – The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.1.1C – The TOE shall be suitable for testing.

ATE_IND.1.1C – The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF

Evaluator action elements:

ATE_IND.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2E – The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.1.3E – The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

AVA_SOF.1 Strength of TOE security function evaluation

A typical attacker in the intended telecommunications environment for the ETM™ Platform is deemed to possess only limited knowledge of the telecommunications systems and lack the skills and resources required to manipulate telecommunications interfaces. The network environment provides addition protection mechanisms for ETM™ Platform. Therefore, for an EAL2 level evaluation of ETM™ Platform, the attack potential to meet or exceed for AVA_SOF calculations is LOW. Any remaining vulnerabilities can be only be exploited by an attacker of moderate or high attack potential. The strength of function claim is therefore SOF-BASIC.

Developer action elements:

AVA_SOF.1.1D – The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C – For each mechanism with a strength of TOE security function claim, the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C – For each mechanism with a specific strength of TOE security function claim, the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

AVA_SOF.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.1E – The evaluator shall confirm that the strength claims are correct.

AVA_VLA.1 Developer vulnerability analysis

Developer action elements:

AVA_VLA.1.1D – The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2D – The developer shall document the disposition of obvious vulnerabilities.

Content and presentation of evidence elements:

AVA_VLA.1.1C – The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

AVA_VLA.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2E – The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements. A separate appendix to this ST is available from SecureLogix Corporation which shows the correspondence between the TOE security functions, as defined in this section of the ST, and the ETM™ Platform security functions as defined in the ETM™ Platform functional specification.

A typical attacker in the intended telecommunications environment for the ETM™ Platform is deemed to possess only limited knowledge of the telecommunications systems and lack the skills and resources required to manipulate telecommunications interfaces. The appliances include firewall protection on the network interfaces and the network environment provides addition protection mechanisms for TeleView™ Console client and server. Therefore, for an EAL2 level evaluation of the ETM™ Platform, the attack potential to meet or exceed for AVA_SOF calculations is LOW. Any remaining vulnerability can be only be exploited by an attacker of moderate or high attack potential. The strength of function claim is therefore SOF-BASIC.

6.1 TOE SECURITY FUNCTIONS

A description of each of the TOE security functions follows.

F.CRYPTO The TOE does provide secure internal data communications through the use of cryptography. The TOE can encrypt communications between components using DES or Triple DES cryptography.

F.NETBLK The TOE does provide security to its appliances from attack through the network. Data is protected from modification or disclosure when it is transmitted between separate parts of the TOE, by validating IP address and username and password and by authenticating communications with a variable handshake.

F.TELBLK The TOE does block telecommunications access based on: called number, calling number, call type (voice, fax, modem, STU generic, busy, unanswered, wideband or undetermined), call direction (inbound, outbound), call duration and time of day, excluding 911 calls.

F.TELALW All other telecommunications traffic not specifically denied in accordance with F.TELBLK, are allowed.

F.FAIL In the event of TOE failure (such as during a power outage), the TOE does provide an option to either fail-safe (all calls allowed), or fail secure (all calls denied including emergency calls).

Application Note: This applies only to 1000 Series appliances.

F.FAILNOT Upon detection of a potential security violation, the TOE does provide audible alarm, SNMP trap, email with or without attachments, pager, or TeleSweep Secure® scan.

F.HMI The TOE does provide the administrator with the capability to perform HMI functions including:

a. start-up, shutdown, and configure the TOE security functions;
b. select the level of telecommunications activity detail that is displayed to the user;
c. view and modify the settings that enable or disable the logging of selected telecommunications traffic;
d. enable or disable the capturing of "in-call" digits;
e. view on-line administrator guidance;
f. modify and set the system time and date;
g. archive, modify, create, delete, and display the audit logs;
h. display errors;
i. display current telecommunications activity;
j. change user password;
k. modify and delete username;
l. add and delete privileges and IP addresses;
m. create, modify and delete phone numbers and time of day;
n. modify audit level;
o. generate audit reports;
p. modify appliance configuration;
q. modify date and time of host machine and appliances;
r. display appliance status;
s. manage server;
t. modify users;
u. edit policies;
v. edit appliance parameters; and
w. login directly to appliance.

F.LOCK The TOE does provide locking of objects to prevent multiple users from editing the same object. Locking is provided at the object level. Multiple users are able to view the same object, but not edit the same object.

F.AUDEVT The TOE does generate an audit log of the following events:

a. Start-up and shutdown;
b. exhaustion of log storage;
c. changes in TOE security function configuration;

d. failed and successful logins by administrators to an appliance;
e. logins/logouts by administrators to ETM™ Management Server;
f. changes to rulesets that are applied to an appliance;
g. the additions/deletions/clones/modifications an administrator performs in the ETM™ Management Server;
h. appliance and telephone circuit errors;
i. requests from unknown appliances;
j. detection of an ambiguous rule;
k. rule violations; and
l. all other remaining auditable events for the basic level of audit identified in Table 2.

F.AUDINF For each audit event entry, the TOE does record, where applicable, the
a. date and time;
b. administrator's name;
c. type of event;
d. event details;
e. a unique identifying number for each entry;
f. call trunk channel;
g. call trunk group;
h. call begin time;
i. call end time;
j. call source (calling number) if available;
k. call destination (called number);
l. call type as fax, modem, voice, STU voice, STU data, STU generic, unknown, busy, unanswered, wideband or undetermined;
m. call direction as inbound or outbound;
n. call duration;
o. call "in-call" digits;
p. call trailing digits;
q. the appliance that originated the event; and
r. the appliance array the appliance belongs to.

F.AUDLVL The types of audit events recorded by the TOE is configurable.

F.TIME The TOE does provide a reliable time and date for the time stamping audit log entries.

F.ALARM The TOE monitors telecommunication traffic and detects events defined by security policies. The TOE does signal the administrator based on a specified event. The type of signals will include: audible alarm, SNMP trap, emails with or without attachments, pager, and TeleSweep Secure® scan.

F.AUDRPT The TOE does provide the ability to generate reports of audit data by searching and ordering the following categories:

a. log time;
b. unsuccessful login attempts;
c. start time;
d. end time;
e. duration;
f. in/out call direction;
g. source;
h. destination;
i. type;
j. “in-call” digits;
k. call trailing digits;
l. tracks;
m. appliance array;
n. appliance;
o. trunk group;
p. channel;
q. name of ruleset;
r. rule number;
s. rule comment;
t. unique record ID; and
u. call information (LOC-local call, INTL-international call, VSC-vertical service code, etc.).

F.AUDFLTR The TOE does provide improved granularity of reporting for F.AUDRPT by filtering the sub-types/ranges of audit data based on:

a. date;
b. call direction;
c. call duration;
d. phone number;
e. call type;
f. call “in-call” digits;
g. call trailing digits;
h. appliance array;
i. appliance;
j. track;
k. text ; and
l. call information (LOC-local call, INTL-international call, VSC-vertical service code, etc.).

F.AUDSTO The TOE does protect audit data from unauthorised modification or deletion by managing log file size and location.

F.ADMIN Access to the TOE is restricted to authorised administrators through the use of username and password, and enforced upon an acceptable IP address. Each administrator does have a set of privileges, which only allow the administrators to perform those tasks associated with their duties. A mechanism is provided to verify that administrator passwords meet a minimum of eight characters including one change of case character and one digit.

F.INIT When TOE security functions are started, the TOE does initialise with the security settings in effect when it was last shutdown. If this saved configuration cannot be loaded or does not exist, the TOE does warn the user via a pop-up dialog that the default configuration is being loaded.

6.2 ASSURANCE MEASURES

A description of each of the TOE assurance measures follows.

M.ID The TOE incorporates a unique version identifier that can be displayed to the user.

M.SYSTEM The TOE is developed and maintained using a system to ensure only authorised changes are implemented in the evaluated version of the TOE. A list of all TOE documentation and all configuration items required to create the TOE is maintained.

M.GETTOE The developer has a controlled process and procedures whereby the developer ships a shrink-wrapped copy of the TOE to a customer on CD-ROM. Both the process and procedures are documented.

M.SETUP The TOE includes an automated installation and setup program compatible with the TOE operating system. The installation process is self-explanatory, or provides additional instructions to clearly document the installation process. The default installation results in the secure installation and start-up of the TOE.

M.SPEC A high level TOE design and functional specification have been provided by the developer for the evaluation which describes the TOE security functionality, subsystems, and interfaces.

M.TRACE Correspondence mappings are provided by the developer such that the security functionality detailed in the TOE functional specification is upwards traceable to this ST, and downwards traceable to the high level design.

M.DOCS Sufficient user and administrator guidance documentation is provided.

M.TEST A suitably configured TOE is tested in a controlled environment to confirm that TOE functionality operates as specified, and that the TOE is protected from a representative set of well-known attacks. The developer provides a mapping between developer test cases and TOE functionality. The assurance requirements also ensure the TOE functionality is tested in a real-world environment.

M.SECASS The developer examines the TOE design to ensure the security functions adequately address perceived threats in the security environment. The results of the examination are documented. Threats include deliberate attempts to disable, bypass, and brute-force attack the TSF.

7 PROTECTION PROFILE CLAIMS

This ST does not make compliance claims with respect to any Protection Profiles.

8 RATIONALE

This section contains the Rationale arguments and proof.

8.1 SECURITY OBJECTIVES RATIONALE

8.1.1 TOE Security Objectives Rationale

Table 4 provides a mapping of TOE Security Objectives to Threats, and is followed by a discussion of how each Threat is addressed by the corresponding TOE Security Objectives.

Table 4 Mapping of TOE Security Objective to Threats

	T.SNIFF	T.REPLAY	T.ATKNET	T.INTRES	T.EXTRES	T.MISUSE	T.TOEPRO	T.ATKVIS	T.TOEDAT	T.TOEFCN	T.NONAPP	T.NOCOM	T.AUDEXH
O.CRYPTO	X	X											
O.ATKNET		X	X										
O.MEDTEL				X	X	X							
O.TELTOE							X	X	X	X			
O.COMM												X	
O.AUDCHK													X
O.ADMACC									X	X	X		
O.HMI								X		X	X		
O.DSPACT								X			X		
O.AUDIT								X					
O.SELFPRO							X			X			

T.SNIFF *A network attacker may observe authentication data or system configuration info as it is transmitted between portions of the TOE.*

O.CRYPTO protects the confidentiality of authentication and system configuration data using cryptography as it passes between distributed components of the TOE.

T.REPLAY *A network attacker may use previously captured or falsified data to authenticate to the TOE or alter its configuration.*

O.ATKNET protects the TOE appliances against attack from the network. Replay attacks, in appliance to server communications, are countered by the communications being authenticated with a variable handshake and encrypted with valid cryptokey/algorithm. O.CRYPTO protects the confidentiality of authentication and system configuration data using cryptography as it passes between distributed components of the TOE. The TOE can not properly encrypt falsified data for use since the network attacker does not have access to the cryptographic key.

T.ATKNET *A network attacker may attack the TOE appliances.*

O.ATKNET ensures the TOE appliances protect themselves against attack from the network.

T.INTRES *An unauthorised external user may gain access to internal telecommunication resources (telephones, modems, faxes, etc.).*

O.MEDTEL mediates telecommunications access across the telecommunication lines, preventing unauthorised use of telecommunication resources.

T.EXTRES *An internal user may gain unauthorised access to external telecommunications resources (telephones, modems, faxes, etc.).*

O.MEDTEL mediates telecommunications access across the telecommunication lines, preventing unauthorised use of telecommunication resources.

T.MISUSE *A user may use internal telecommunications resources in an unauthorised manner (make a voice call on a fax line, etc.).*

O.MEDTEL mediates telecommunications access across the telecommunication lines, preventing unauthorised use of telecommunication resources.

T.TOEPRO *A telecommunications user may bypass, deactivate, corrupt or tamper with TOE security functions.*

O.TELTOE does not allow connections to the TOE itself. O.SELFPRO protects the TOE from attempts by a telecommunications user from the telecommunications side to bypass, deactivate, corrupt or tamper with TOE security functions.

T.ATKVIS *A telecommunications user may conduct undetected attack attempts against the TOE.*

O.TELTOE does not allow connections to the TOE itself. O.DSPACT and O.HMI display, to the administrator, the current activity associated with telecommunications entities accessing, or attempting to access, the TOE.

O.AUDIT records a readable audit trail of allowed and denied telecommunications access attempts, administrator login attempts, and permits the administrator to review the audit log entries.

T.TOEDAT *A telecommunications user may read, modify or destroy TOE internal data.*

O.TELTOE does not allow connections to the TOE itself. O.ADMACC restricts access to security functions only to authorised administrators.

T.TOEFCN *A telecommunications user may access and use security and/or non-security functions of the TOE.*

O.TELTOE does not allow connections to the TOE itself. O.ADMACC restricts access to security functions only to authorised administrators. O.HMI permits the administrator to manage the TOE security functions to detect/prevent this threat. O.SELFPRO protects the TOE from tampering by a telecommunications user.

T.NONAPP *An administrator may be unaware that an unauthorised application, executing on the TOE, is accessing the telecommunications lines or network via TOE interfaces.*

O.ADMACC restricts access to security functions only to authorised administrators. O.HMI permits the user to manage the toe security functions to detect/prevent this threat. O.DSPACT displays to the user the current activity associated with telecommunications entities accessing, or attempting to access, the TOE.

T.NOCOM An administrator may be unaware that TOE internal communications have failed.

O.COMM ensures the TOE notifies the administrator of an internal communications failure.

T.AUDEXH The administrator may be unaware that the audit storage of the TOE has been exhausted.

O.AUDCHK ensures that the TOE notifies the administrator when the local audit storage is exhausted.

8.1.2 Environment Security Objectives Rationale

Table 5 provides a mapping of Environment Security Objectives to Assumptions and Threats, and is followed by a discussion of how each Assumption or Threat is addressed by the corresponding Environment Security Objectives.

Table 5 Mapping of Environment Security Objectives to Threats and Assumptions

	A.PHYSEC	A.PRONET	A.NOEVIL	A.ADMKNW	T.USAGE	T.BADADM	T.TROJAN
O.NETPRO		X					
O.GUIDAN			X	X	X	X	X
O.AUTHUSR	X						

A.PHYSEC *The TOE is physically secure.*

O.AUTHUSR ensures that only authorised users be permitted physical access to the TOE.

A.PRONET *Protection mechanisms are in place for the server and* TeleView™ Console *client.*

O.NETPRO ensures that the organisation responsible for the server and TeleView™ Console client portions of the TOE has taken any security measures they feel are appropriate to meet this assumption.

A.NOEVIL *Administrators are non-hostile and follow all administrator guidance; however, they are capable of error.*

O.GUIDAN ensures that administrators administer and operate the TOE in a manner that maintains its security.

A.ADMKNW *The administrator is knowledgeable of TCP/IP networking and Telecommunication systems.*

O.GUIDAN ensures that administrators are knowledgeable in the areas required to operate the TOE in a manner that maintains its security.

T.USAGE *The TOE may be configured, used and administered in an insecure manner unwittingly by the user.*

O.GUIDAN provides administrators with instructions on how to securely maintain the TOE.

T.BADADM *Compromise of the integrity and/or availability of the TOE may occur as a result of an administrator not following proper security procedures.*

O.GUIDAN provides administrators with instructions on how to securely maintain the TOE.

T.TROJAN *Compromise of the integrity and/or availability of the TOE may occur as a result of an administrator* unwittingly introducing a virus or trojan into the system.

O.GUIDAN provides administrators with instructions on how to securely maintain the TOE.

8.2 SECURITY REQUIREMENTS RATIONALE

8.2.1 Security Functional Requirements Rationale

Table 6 provides a mapping of Security Functional Requirements to IT Security Objectives, and is followed by a discussion of how each IT Security Objective is addressed by the corresponding Security Functional Requirements.

Table 6 Mapping of Security Functional Requirements to IT Security Objectives

	O.CRYPTO	O.ATKNET	O.MEDTEL	O.TELTOE	O.COMM	O.AUDCHK	O.ADMACC	O.HMI	O.DSPACT	O.AUDIT	O.SELFPRO
FAU_ARP.1					X					X	
FAU_GEN.1										X	
FAU_SAA.1					X					X	
FAU_SAR.1										X	
FAU_SAR.3										X	
FAU_SEL.1										X	
FAU_STG.1										X	
FAU_STG.3						X					
FCS_COP.1	X										
FDP_ACC.1 (1)				X							X
FDP_ACF.1 (1)				X							X
FDP_ACC.1 (2)							X				
FDP_ACF.1 (2)							X				
FDP_IFC.1 (1)			X	X							

FDP_IFF.1 (1)			X	X							
FDP_IFC.1 (2)		X									
FDP_IFF.1 (2)		X									
FIA_AFL.1							X				
FIA_ATD.1							X				
FIA_SOS.1							X				X
FIA_UAU.1							X				X
FIA_UID.1							X				X
FMT_MOF.1								X	X	X	
FMT_MSA.1											X
FMT_MSA.3											X
FMT_SMR.1							X				X
FMT_MTD.1										X	X
FPT_ITT.1		X									
FPT_STM.1										X	
FTP_TRP.1		X									

O.CRYPTO *The TOE must protect the confidentiality of authentication and system configuration data using cryptography as it passes between distributed components of the TOE.*

FCS_COP.1 requires a cryptographic operation to be performed in accordance with a specified algorithm and with a cryptographic key of a specified size.

O.ATKNET *The TOE appliances must protect themselves against attack from the network. Replay attacks, in appliance to server communications, are countered by the communications being authenticated with a variable handshake and encrypted with valid cryptokey/algorithm.*

FDP_IFC (2), FDP_IFF (2), FPT_ITT.1 and FTP_TRP together require that the TOE protect its appliances against attack from the network.

O.MEDTEL *The TOE must mediate telecommunications access inbound and outbound on the telecommunications lines. The TOE shall be capable of revoking access privileges based on predefined attributes.*

FDP_IFC.1 (1) together with FDP_IFF.1 (1) require that the TOE mediate communications across the telecommunications lines based on a combination of default and user defined conditions.

O.TELTOE *The TOE should not allow access to the TOE from the telecommunications interfaces.*

FDP_ACC.1 (1), FDP_ACF.1 (1), FDP_ICF.1 (1), and FDP_IFF.1 (1) define the only allowed accesses control security policies which ensure there are not other ways to access the TOE.

O.COMM *The TOE must provide a mechanism to handle internal communication failures.*

FAU_ARP.1 and FAU_SAA.1 combine to provide the administrator with real-time notification of a communication failure.

O.AUDCHK *The TOE must provide a mechanism that advises the administrator when local audit storage has been exhausted.*

FAU_STG.3 provide the administrator with notification that the local audit storage has been exhausted.

O.ADMACC *An administer role will exist on the TOE with access control mechanisms such that only authenticated administrators are able to perform security relevant functions.*

FDP_ACC.1 (2), FDP_ACF.1 (2), FIA_SOS.1, FIA_UAU.1 and FIA_UID.1 ensure that all users are properly identified and authenticated before gaining access to the TOE. FMT_SMR.1 defines the security roles such that the only users are administrators. FIA_ATD.1 are the security attributes, which identify administrators and their privileges. FIA_AFL.1 adds extra assurance that attempts to guess the administrator's password using brute force will be blocked (for Telnet attempts to sensor only).

O.HMI *The TOE must provide functionality that enables an administrator to effectively manage the TOE and its security functions from its local HMI.*

FMT_MOF.1 provides the administrator with the capability to manage the TOE and its security functions from its local HMI.

O.DSPACT *The TOE must display to the user the current and recent history of telecommunications activity associated with the telecommunications lines.*

FMT_MOF.1 provides the user with the capability to select the level of telecommunications activity that is displayed on the HMI.

O.AUDIT *The TOE must record and store a readable audit trail of TOE telecommunications activity and security relevant events, and permit their review only by authorised administrators. The TOE will be capable of* *performing audit reduction, and of triggering alarms as required by the administrator.*

FAU_GEN.1 and FPT_STM.1 combine to require that a readable audit trail of network activity and security related events is recorded with reliable time stamps. FAU_STG.1 provides secure storage for the audit data. FAU_SAA.1 and FAU_ARP.1 provide the administrator with additional, real-time notification of some audit events. FAU_SAR.1 and FAU_SAR.3 provide the user with the capability to review both a complete and reduced audit trail. FAU_SEL.1 and FMT_MOF.1 combine to provide the user with the capability to select what level of network activity is recorded in the audit trail. FMT_MTD.1 restricts access to the audit logs to administrators.

O.SELFPRO *The TOE must protect itself against attempts by a telecommunications user from the telecommunications side to bypass, deactivate, corrupt or tamper with TOE security functions.*

FDP_ACC.1 (1), FDP_ACF.1 (1), FIA_SOS.1, FIA_UAU.1 and FIA_UID.1 ensure that all users are properly identified and authenticated before gaining access to the TOE. FMT_MSA.1, FMT_MSA.3, FMT_SMR.1 and FMT_MTD.1 ensure that only administrators who have the correct privileges manage all security functions.

8.2.2 Assurance Requirements Rationale

The ETM™ Platform is designed to mediate telecommunications traffic over telecommunication lines, and be simple enough for an average PC user to manage. An assurance of EAL 2, structurally tested, was selected as the threat to security is considered to be unsophisticated telecommunications attackers, and the data to be protected consists mainly of system resources (although the ETM™ Platform can prevent data leakage by blocking telecommunications access). Additional augmented assurance requirements (ACM_CAP.3, ACM_SCP.1, and ALC_DVS.1) were added to gain increased security throughout the development of the ETM™ Platform. It is felt that an evaluation at this level provides evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.

8.2.3 Rationale for Satisfying Functional Requirement Dependencies

Table 7 identifies the ST Security Functional Requirements and their associated dependencies. The tables also indicate whether the ST explicitly addresses each dependency. For the ETM™ Platform, all but four of the dependencies for functional components have been met.

Table 7 Security Functional Requirement Dependencies

ST Requirement	Dependencies	Dependency Satisfied?
FAU_ARP.1	FAU_SAA.1	Y
FAU_ GEN.1	FPT_STM.1	Y
FAU_SAA.1	FAU_GEN.1	Y
FAU_ SAR.1	FAU_GEN.1	Y
FAU_SAR.3	FAU_ SAR.1	Y
FAU_ SEL.1	FAU_GEN.1	Y
	FMT_MTD.1	Y
FAU_STG.1	FAU_GEN.1	Y
FAU_STG.3	FAU_GEN.1	Y
	FMT_MTD.2	N
FCS_COP.1	FCS_CKM.1	N
	FCS_CKM.4	N
	FMT_MSA.2	N
FDP_ACC.1	FDP_ACF.1	Y
FDP_ACF.1	FDP_ACC.1	Y
	FMT_ MSA.3	Y
FDP_ IFC.1	FDP_IFF.1 (1)	Y
FDP_ IFF.1	FDP_IFC.1 (1)	Y
	FMT_MSA.3	Y
	FMT_MSA.3	Y
FIA_AFL.1	FIA_UAU.1	Y
FIA_ATD.1	–	Y
FIA_SOS.1	–	Y
FIA_UAU.1	FIA_UID.1	Y
FIA_UID.1	–	Y
FMT_ MOF.1	FMT_SMR.1	Y
FMT_MSA.1	FDP_IFC.1	Y
	FMT_SMR.1	Y
FMT_ MSA.3	FMT_MSA.1	Y
	FMT_SMR.1	Y
FMT_MTD.1	FMT_SMR.1	Y
FMT_SMR.1	FIA_UID.1	Y
FPT_ STM.1	–	Y

FMT_MTD.2 This security functional requirement has been excluded because the size of the threshold cannot be set. The size of the local storage is limited by hardware and cannot be changed by any software settings.

FCS_CKM.1 This security functional requirement has been excluded because the cryptographic keys are pre-generated outside the scope of the TOE.

FCS_CKM.4 This security functional requirement has been excluded because the cryptographic keys are simply overwritten and follow no standard cryptographic key destruction method.

FMT_MSA.2 This security functional requirement has been excluded because the TSF does not generate the security attributes (cryptographic keys) itself. Instead the security attributes are generated in the TOE environment and then loaded into the TOE.

8.2.4 Rationale for Satisfying Assurance Requirement Dependencies

Table 8 identifies the ST Assurance Requirements and their associated dependencies. The tables also indicate whether the ST explicitly addresses each dependency. For the ETM™ Platform, all dependencies for assurance components have been met.

Table 8 Assurance Requirement Dependancies

ST Requirement	Dependencies	Dependency Satisfied?
ACM_CAP.3	ACM_SCP.1	Y
	ALC_DVS.1	Y
ACM_SCP.1	ACM_CAP.3	Y
ADO_DEL.1	–	Y
ADO_IGS.1	AGD_ADM.1	Y
ADV_FSP.1	ADV_RCR.1	Y
ADV_HLD.1	ADV_FSP.1	Y
	ADV_RCR.1	Y
ADV_RCR.1	–	Y
AGD_ADM.1	ADV_FSP.1	Y
AGD_USR.1	ADV_FSP.1	Y
ALC_DVS.1	–	Y
ATE_COV.1	ADV_FSP	Y
	ATE_FUN.1	Y
ATE_FUN.1	–	Y
ATE_IND.2	ADV_FSP.1	Y
	AGD_ADM.1	Y
	AGD_USR.1	Y
	ATE_FUN.1	Y
AVA_SOF.1	ADV_FSP.1	Y
	ADV_HLD.1	Y
AVA_VLA.1	ADV_FSP.1	Y
	ADV_HLD.1	Y
	AGD_ADM.1	Y
	AGD_USR.1	Y

8.2.5 Rationale for Security Functional Refinements

FAU_SAR.3 Selectable audit review

Added an additional category to FAU_SAR.3.1 to include filtering of audit data. The original wording of FAU_SAR.3.1 remains unchanged. See application note for FAU_SAR.3 for further details.

FCS_COP.1 Cryptographic operation

Added words to specify which version of the ETM™ Platform (export or domestic) uses each key type.

FIA_ATD.1 User attribute definition

Changed "…belonging to individual users" to "…belonging to individual administrators" since the requirement only applies to individuals who communicate over the network to configure and operate ETM™ Platform.

FIA_UAU.1 Timing of authentication

Reworded FIA_UAU.1.1 for clarity and proper English by removing "…on behalf of the user to be performed…". The original intent of FIA_UAU.1.1 (specifying actions, which can be performed before authentication) remains unchanged.

FIA_UID.1 Timing of identification

Reworded FIA_UID.1.1 for clarity and proper English by removing "…on behalf of the user to be performed…". The original intent of FIA_UID.1.1 (specifying actions, which can be performed before identification) remains unchanged.

FMT_MSA.3 Static Attribute initialisation

Changed "…default values for security attributes…" to "…default values for information flow security attributes…" since the requirement only applies to the information flow SFP.

Changed "…to enforce the SFP" to "…to enforce the TELCO SFP" since there is more than one SFP, and this requirement only applies to the TELCO SFP.

FTP_TRP.1 Trusted Path

Changed "users" to "administrators", since only the administrators will be performing these functions.

8.2.6 Rationale for Audit Exclusions

Table 9 lists events that would normally be subject to audit at the Basic audit level which are not audited for the reasons indicated:

Table 9 Rationale for Audit Exclusions

Functional Component	Auditable Event	Rationale for Exclusion
FPT_STM.1	Changes to the time.	This audit requirement has not been included because: • The only security functionality that relies on TOE system time is the time stamping of audit log entries. Since the TOE maintains the sequence of audit entries in the log, regardless of changes in system time, any relevant changes in system time would be apparent. • Authorised users, or applications executing on the TOE must initiate system time changes. Users are assumed to be knowledgeable of the applications they are running, and hence are aware of changes in system time they initiate. If the operating system itself changes system time (e.g., daylight saving time changes), the user is notified. • System time is maintained by the operating system. In this case, the TOE operating system, Windows NT, does not support a capability to audit system time changes.

8.3 TOE SUMMARY SPECIFICATION RATIONALE

8.3.1 TOE Security Functions Rationale

Table 10 provides a mapping of Security Functions to Security Functional Requirements, and is followed by a discussion of how each Security Functional Requirement is addressed by the corresponding Security Function.

Table 10 Mapping of Security Functions to Security Functional Requirements

	FAU_ARP.1	FAU_ GEN.1	FAU_SAA.1	FAU_ SAR.1	FAU_SAR.3	FAU_ SEL.1	FAU_STG.1	FAU_STG.3	FCS_COP.1	FDP_ACC.1 (1)	FDP_ACF.1 (1)	FDP_ACC.1 (2)	FDP_ACF.1 (2)	FDP_ IFC.1 (1)	FDP_ IFF.1 (1)	FDP_ IFC.1 (2)	FDP_ IFF.1 (2)	FIA_AFL.1	FIA_ATD.1	FIA_SOS.1	FIA_UAU.1	FIA_UID.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.3	FMT_SMR.1	FMT_MTD.1	FPT_ITT.1	FPT_ STM.1	FTP_TRP.1
F.CRYPTO									X								X													
F.NETBLK																X	X											X		X
F.TELBLK														X	X															
F.TELALW														X	X															
F.FAIL														X	X															
F.FAILNOT	X		X																											
F.HMI																							X	X		X	X			
F.LOCK												X	X																	
F.AUDEVT		X						X																						
F.AUDINF		X																											X	
F.AUDLVL						X																								
F.TIME		X																											X	
F.ALARM	X		X					X																						
F.AUDRPT				X	X																									
F.AUDFLTR				X	X																									
F.AUDSTO							X																							
F.ADMIN										X	X							X	X	X	X	X				X				
F.INIT																									X					

FAU_ARP.1 *Security Alarms*

F.ALARM and F.FAILNOT combine to satisfy the requirements for detecting security violations based on administrator created rules and TOE communication failure respectively.

FAU_GEN.1 *Audit data generation*

F.AUDEVT, F.AUDINF, and F.TIME combine to satisfy the requirement for the generation of audit data for the specified set of TOE events.

FAU_SAA *Potential violation analysis*

F.ALARM and F.FAILNOT combine to satisfy the requirements for detecting security violations based on administrator created rules and TOE communication failure respectively.

FAU_SAR.1 *Audit review*

F.AUDRPT and F.AUDFLTR combine to satisfy the requirements for the reviewing of audit data by providing a capability for report generation and filtering.

FAU_SAR.3 *Selectable audit review*

F.AUDRPT and F.AUDFLTR combine to satisfy the requirements for the selectable reviewing of audit data.

FAU_SEL.1 *Selective audit*

F.AUDLVL satisfies the requirement for the selectable recording of audit data.

FAU_STG.1 Protected audit trail storage

F.AUDSTO satisfies the requirement for protected storage of audit data by managing log file size and location.

FAU_STG.3 Action in case of possible audit data loss

F.AUDEVT and F.ALARM combine to satisfy the requirement for protected storage of audit data by generating a security message and alarm in the event of possible audit data loss.

FCS_COP.1 Cryptographic operation

F.CRYPTO satisfies this requirement for cryptographic operations which are used to protect the confidentiality of internal data communications. The TOE can encrypt communications between components using DES or Triple DES cryptography.

FDP_ACC.1 *Subset access control* (1)

F.ADMIN satisfies the requirement for access control to the TOE through authentication of administrators.

FDP_ACF.1 *Security attribute based access control* (1)

F.ADMIN satisfies the requirement for access control to the TOE based on security attributes of user name, password, and IP address.

FDP_ACC.1 *Subset access control* (2)

F.LOCK satisfies the requirement for access control for the editing of TOE objects.

FDP_ACF.1 *Security attribute based access control* (2)

F.LOCK satisfies the requirement for access control to the TOE and it's objects based on number of concurrent users by preventing users from editing the same object.

FDP_IFC.1 *Subset information flow control (1)*

F.TELBLK, F.TELALW, and F.FAIL combine to satisfy the requirement to enforce information flow control on external IT entities that send and receive information across the telecommunications lines, based on security attributes. Telecommunication calls are allowed/blocked based on call attributes. In the event of TOE failure, fail-safe or fail-secure operation is allowed (for 1000 series appliances).

FDP_IFF.1 *Simple security attributes (1)*

F.TELBLK, F.TELALW, and F.FAIL combine to satisfy the requirement to enforce information flow control on external IT entities that send and receive information across the telecommunication lines, based on security attributes.

FDP_IFC.1 *Subset information flow control (2)*

F.NETBLK satisfies the requirement to enforce information flow control on external IT entities that send and receive information across the network, based on security attributes.

FDP_IFF.1 *Simple security attributes (2)*

F.NETBLK and F.CRYPTO satisfy the requirement to enforce information flow control on external IT entities that send and receive information across the network based on security attributes. Data is protected from modification or disclosure when it is transmitted between separate parts of the TOE by validating IP address and username and password, by authenticating communications with a variable handshake and by encrypting the data with valid cryptokey/algorithm.

FIA_AFL.1 *Authentication failure handling*

F.ADMIN satisfies the requirement to restrict access to authorised administrators by turning off access to the TOE (Telnet to sensor only) after a set number of failed login attempts

FIA_ATD.1 *User attribute definition*

F.ADMIN satisfies the requirement for user attributes.

FIA_SOS.1 *Verification of secrets*

F.ADMIN satisfies the requirement for quality metrics of secrets (user attributes).

FIA_UAU.1 *Timing of authentication*

F.ADMIN satisfies the requirement for user authentication.

FIA_UID.1 *Timing of identification*

F.ADMIN satisfies the requirement for user identification.

FMT_MOF.1 *Management of security functions behaviour*

F.HMI satisfies the requirement for the TOE to provide the user with the capability to manage the security functions of the TOE through external interfaces.

FMT_MSA.1 *Management of security attributes*

F.HMI satisfies the requirement for the TOE to provide the user with the capability to manage the security attributes of the TOE.

FMT_MSA.3 *Static attribute initialisation*

F.INIT satisfies the requirement for the default TOE configuration.

FMT_SMR.1 *Security Roles*

F.ADMIN satisfies the requirement for various (administrator) security roles and F.HMI satisfies the requirement for the TOE to provide the administrator with the capability to manage the security attributes of the TOE.

FMT_MTD.1 *Management of TSF data*

F.HMI satisfies the requirement for the TOE to provide the user with the capability to manage the TSF data.

FPT_ITT.1 *Basic internal TSF data transfer protection*

F.NETBLK satisfies the requirement to protect TSF data when transmitted from within the TOE to the appliance.

FPT_STM.1 *Reliable time stamps*

F.AUDINF and F.TIME combine to satisfy the TOE to provide a reliable time and date for the time stamping audit log entries.

FTP_TRP.1 Trusted Path

F.NETBLK satisfies the requirement to provide a trusted path to the TOE appliances.

8.3.2 TOE Assurance Measures Rationale

Table 11 provides a mapping of Assurance Measures to Assurance Requirements, and is followed by a short discussion of how the Assurance Requirements are addressed by the corresponding Assurance Measures.

Table 11 Mapping of Assurance Measures to Assurance Requirements

	ACM_CAP.3	ACM_SCP.1	ADO_DEL.1	ADO_IGS.1	ADV_FSP.1	ADV_HLD.1	ADV_RCR.1	AGD_ADM.1	AGD_USR.1	ALC_DVS.1	ATE_COV.1	ATE_FUN.1	ATE_IND.2	AVA_SOF.1	AVA_VLA.1
M.ID	X														
M.SYSTEM	X	X								X					
M.GETTOE			X												
M.SETUP				X											
M.SPEC					X	X									
M.TRACE							X								
M.DOCS								X	X						
M.TEST											X	X	X		X
M.SECASS														X	X

ACM_CAP.3 *Authorisation controls*

M.ID and M.SYSTEM combine to satisfy the requirement for configuration management.

ACM_SCP.1 *TOE CM coverage*

M.SYSTEM satisfies the requirement for CM tracking of all TOE documentation.

ADO_DEL.1 *Delivery procedures*

M.GETTOE satisfies the requirement for delivery procedures.

ADO_IGS.1 *Installation, generation, and start-up procedures*

M.SETUP satisfies the requirement for installation, generation, and start-up procedures.

ADV_FSP.1 *Informal functional specification*

M.SPEC satisfies the requirement for a functional specification.

ADV_HLD.1 *Descriptive high-level design*

M.SPEC satisfies the requirement for a high-level design specification.

ADV_RCR.1 *Informal correspondence demonstration*

M.TRACE satisfies the requirement for design specifications that are consistent throughout the documentation.

AGD_ADM.1 *Administrator guidance*

M.DOCS satisfies the requirement for administrator guidance documentation.

AGD_USR.1 *User guidance*

M.DOCS satisfies the requirement for user guidance documentation

ALC_DVS.1 *Identification of security measures*

M.SYSTEM satisfies the requirement for TOE developmental security.

ATE_COV.1 *Evidence of coverage*

M.TEST satisfies the requirement for evidence that all TOE security functions have been tested.

ATE_FUN.1 *Functional testing*

M.TEST satisfies the requirement for evidence that TOE security functions have been tested.

ATE_IND.2 *Independent testing – sample*

M.TEST satisfies the requirement for evidence that TOE security functions have been tested.

AVA_SOF.1 *Strength of TOE security function evaluation*

M.SECASS satisfies the requirement for evidence that all TOE security functions have been examined to ensure their strength against threats.

AVA_VLA.1 *Developer vulnerability analysis*

M.TEST and M.SECASS combine to satisfy the requirement for evidence that the TOE has been examined and tested in an effort to discover vulnerabilities.

9 ACRONYMS AND ABBREVIATIONS

Acronym	Definition
CC	Common Criteria for Information Technology Security Evaluation
CO	Central Office (Telecommunication provider)
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
GUI	Graphical user interface
HMI	Human Machine Interface
IP	Internet Protocol
IT	Information Technology
NIC	Network Interface Card
PC	Personal Computer
PP	Protection Profile
SOF	Strength of Function
SP6A	Service Pack Six A – for windows NT 4.0
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy