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

VERSION 4.0.1

EWA-Canada Document No. 1443-002-D001
Version 0.6, 7 April 2003

Communications Security Establishment
Common Criteria Evaluation File Number: 383-4-16

Prepared for:

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

Prepared by:

Electronic Warfare Associates-Canada, Ltd.
55 Metcalfe St., Suite 1600
Ottawa, Ontario
K1P 6L5

SECURITY TARGET FOR THE SECURELOGIX CORPORATION® ENTERPRISE TELEPHONY MANAGEMENT (ETM®) SYSTEM VERSION 4.0.1

Document No. 1443-002-D001
Version 0.6, 7 April 2003

<Original> Approved by:

Deputy Project Manger:	Erin Connor	7 April 2003
Project Manager:	Mark Gauvreau	7 April 2003
Program Director:	Paul Zatychec	7 April 2003
	(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® System. 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® System is designed to protect telecommunications lines from abuse and provide extensive auditing capabilities on all telecommunications line traffic. The ETM® System acts as a voice traffic firewall to protect internal telecommunication resources (telephones, modems, faxes, etc.) from abuse, fraud, and attack. The system is capable of operating in conjunction with a Private Branch Exchange (PBX), but is not required to do so. The evaluated configuration for the ETM® System v4.0.1 consists of:

a. the ETM® Management Server, build 3;
b. the TeleView™ Infrastructure Manager, build 3; and
c. the ETM® appliances, with version 4.0.36 software.

The ETM® Management Server and TeleView™ Application 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 hardware components and use the Linux[2] 2.4.19 kernel as the underlying operating system.

The ETM® System mediates access between local telecommunication users and external telecommunication users based on rules defined by the administrator. Rule sets are created on the ETM® Management Server which are then pushed to the appliances. The appliances allow or deny calls based on their respective rule sets. The default behaviour is to allow calls that are not explicitly denied.

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

[1] The ST authors are Dave MacFarlane and Wayne M[ac]Dougall of EWA-Canada, Ltd.
[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 the ETM® Management Server;
b. between the TeleView™ Application and the ETM® Management Server; and
c. between the administrator and appliances.

The ETM® System includes an option to encrypt network communication using DES (by default) or Triple DES cryptography. Administrators may also communicate directly with an appliance through its serial port.

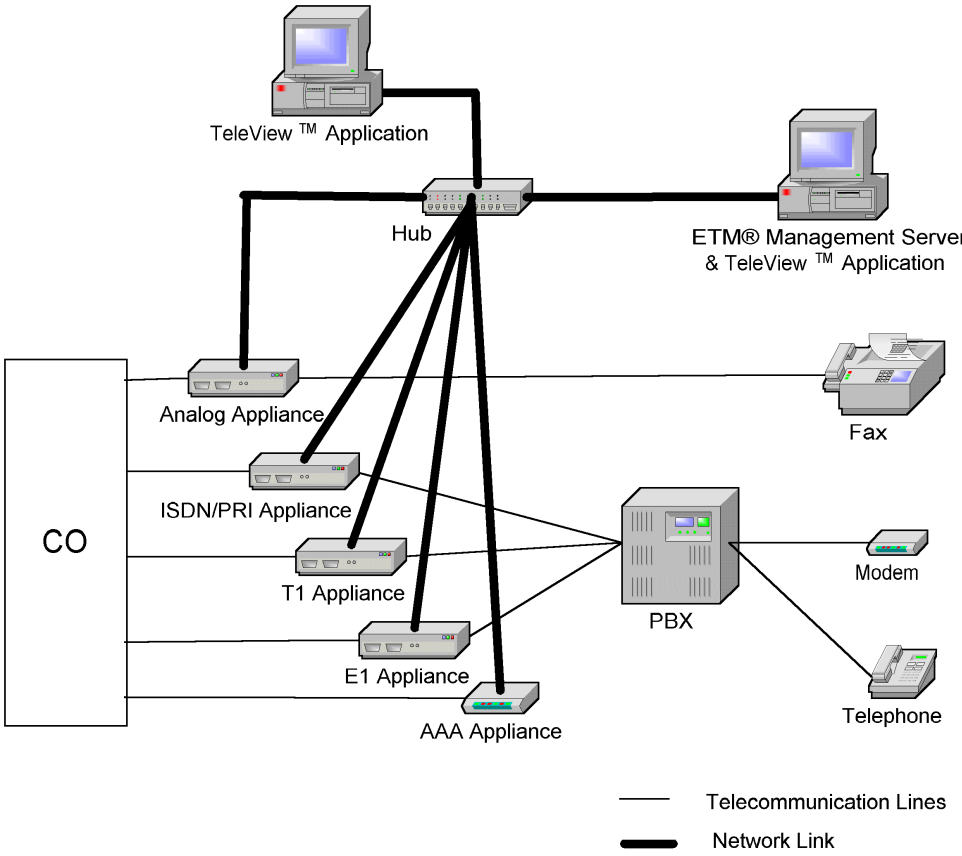

Figure 1: Example ETM® System Configuration

The ETM® System 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 reports and graphs may be generated from the historical data.

Appropriate security measures are expected to exist for the network on which the ETM® System is deployed to protect the communication between components. Appropriate mechanisms must be put in place on the commercial products being used that are external to any SecureLogix Corporation® components. The Target of Evaluation (TOE) consists of the ETM® Management Server, the TeleView™ Application, and the five types of appliances: analog, T1, ISDN/PRI, E1 ISDN/PRI, and AAA.

1.3 CC CONFORMANCE

The ETM® System is conformant with the identified functional requirements specified in Part 2 of the CC. The ETM® System 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.

1.4 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations are identified in this ST in the following manner:

- Selection: Indicated by surrounding brackets and italicised text, e.g., [*selected item*].
- Assignment: Indicated by surrounding brackets and regular text, e.g., [assigned item].
- Refinement: Indicated by underlined text, e.g., refined item.
- Iteration: Indicated by assigning a number at the functional component level, e.g., "FDP_ACC.1, Subset access control (1)" and "FDP_ACC.1, Subset access control (2)".

1.5 TERMINOLOGY

The following terminology is used throughout this ST:

Administrator	An individual that communicates over the network to configure and operate the TOE.

Network	The TOE protects telecommunications lines but uses a TCP/IP network for internal TOE communications. *Network* refers to the TCP/IP network.
Network attacker	An unauthorised individual or IT entity that communicates over the network.
Telecommunications user	An individual or IT entity that communicates over the telecommunications lines.
User	An administrator, as defined above, unless stated otherwise.

2 TARGET OF EVALUATION DESCRIPTION

The ETM® System is designed to protect telecommunications lines from abuse and provide extensive auditing capabilities on all telecommunications line traffic. The ETM® System acts as a voice traffic firewall to protect internal telecommunication resources (telephones, modems, faxes, etc.) from abuse, fraud, and attack. The system is capable of operating in conjunction with a PBX, but is not required to do so. The evaluated configuration for the ETM® System v4.0.1 consists of:

a. the ETM® Management Server Build 3 executing on an Intel®-based PC with Windows® NT 4 SP6a, Windows® 2000 SP3, and Solaris™ 7/8 as the operating systems;
b. the administrator TeleView™ Application Build 3 executing on an Intel®-based PC with Windows® NT 4 SP6a, Windows® 98 (not patched), Windows® 2000 SP3, and Solaris™ 7/8 as the operating systems;
c. Java® Virtual Machine software, version 1.3.1.04 on both the ETM® Management Server and the TeleView™ Application hosts;
d. hardware analog appliances software version 4.0.36, hardware model ETM® 1010;
e. hardware T1 appliances software version 4.0.36, hardware model ETM® 1020, model ETM® 2100 or model ETM® 3200;
f. hardware ISDN-PRI appliances software version 4.0.36, hardware model ETM® 1030, model ETM® 2100 or model ETM® 3200;
g. hardware E1 ISDN-PRI appliances software version 4.0.36, hardware model ETM® 1040, model ETM® 2100 or model ETM® 3200; and
h. hardware AAA appliances software version 4.0.36, hardware model ETM® 1000.

The minimum hardware requirements for the ETM® Management Server and TeleView™ Application are specified in the ETM® System Installation Guide and Technical Reference provided as part of the ETM® 4.0.1 Product Code CD-ROM.

The ETM® System components (appliances, ETM® Management Server, and TeleView™ Application) can be distributed across an Ethernet network. The network access security policy requires administrators to provide a valid user ID and password for authentication. Appliances maintain a file of approved IP addresses and only allow telnet communications from these addresses. ETM® Management Servers maintain a file of approved Appliance IP addresses and only allow connections from Appliances at these addresses. ETM® Management Servers also maintain a file of approved remote TeleView™ Console IP addresses and only allow communications from consoles at these addresses.

The administrator uses the TeleView™ Application to communicate with the ETM® Management Server, and through it, communicate with an appliance. The administrator may also directly communicate to an appliance through a Telnet server or a serial port on the appliance. The Telnet access to an appliance can be disabled, if desired, and can also be configured to automatically disable for a period of time if the specified number of failed

login attempts occur within the configured period of time. The failed login count resets to zero after a successful login.

The AAA appliance is used by a user to temporarily enable an ETM® appliance rule allowing a specific voice/data circuit to be enabled. The telecom user is required to enter a user ID and PIN and destination telephone number to be called. This call will then be allowed if the ETM administrator has previously created a rule allowing the call based on a successful AAA user request. An authorised telecommunications user is able to access telecommunications resources in accordance with the TELCO Security Function Policy but only for a set maximum time period, configurable from 0 to 30 minutes. Additionally, access to the telecommunication resources are restricted to a single call during the set maximum time period. If the AAA service user does not call the authorized telecommunication resource within the time specified in the AAA Service configuration, the authorization expires.

A hardware setting exists for all ETM™ 1000-series appliances, except the AAA appliance, to determine the default behaviour should an ETM® System appliance fail (e.g., due to a power outage). ETM® System appliances can be configured to fail-safe (allow all calls) or fail-secure (deny all calls, including emergency numbers). If the AAA appliance fails, the AAA session is terminated and all AAA services are unavailable.

The system can encrypt communications between components using DES or Triple DES cryptography. The ETM® System implementation of DES is based on the specifications in FIPS 46-3 and FIPS 81 and has been awarded certificate numbers 149 and 150 on the DES Validated Implementations list of the Cryptographic Module Validation Program. Similarly, the ETM® System implementation of Triple DES is based on the specifications in FIPS 46-3 and ANSI X9.52-1998 and has been awarded certificate numbers 89 and 90 on the Triple DES Validated Implementations list. Assessment of the cryptographic algorithm implementations does not form part of the CC evaluation but is separately validated under the Cryptographic Module Validation Program.

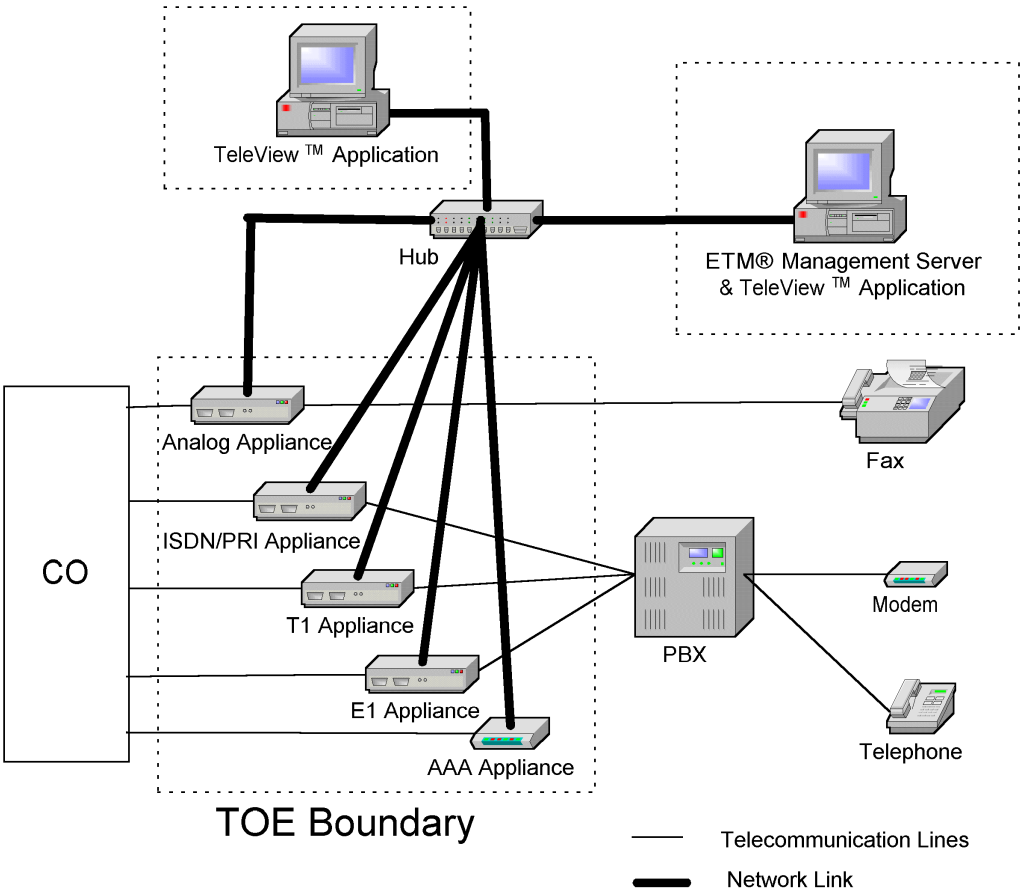

Figure 2: TOE Boundary Diagram

There is an authentication AAA appliance type and four appliance types corresponding to different types of telecommunications lines: analog, T1, ISDN/PRI, and E1 ISDN/PRI. All five appliances are created by SecureLogix Corporation® using commercially available hardware components and execute on the Linux 2.4.19 operating system. The analog, T1, ISDN/PRI, and E1 ISDN/PRI appliances control and enforce the information flow security policy on the telecommunication lines based on the rule set and configuration settings downloaded from the ETM® Management Server. The appliances can be configured individually or as a group.

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, an ASCII command line window opened in the TeleView™ Application, or an RS-232 serial (console) link. However, a small subset of the ETM® commands can only be performed locally at the appliance through the serial link. All appliance types are included in the ETM® System evaluation.

The TeleView™ Application allows the administrator to manage one or multiple ETM® Systems using graphical windows. The administrator can configure appliances by creating a configuration file on the ETM® Management Server that, in turn, gets pushed to the appliances. Checks are performed on a regular basis to ensure the appliances are executing the latest configuration file as defined (i.e., stored) on the ETM® Management Server. It is important to note that, where possible, any configuration changes to the appliances should be made through the TeleView™ Application; 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 it would be changed to match the ETM® Management Server.)

The default telecommunications information flow security policy for ETM® System telecommunications users is "telecommunications that are not explicitly denied, are allowed". The rule set is traversed from top to bottom, triggering on the first applicable rule. A default rule, which cannot be removed, exists at the top of the rule set to always allow emergency calls (e.g., 911). Administrators can create rules by specifying:

a. call source (calling number, or telecommunications user ID for AAA service);
b. call destination (called number);
c. call type (voice, fax, modem, modem energy[3], STU III, busy, unanswered, data, or undetermined);
d. call direction (inbound, outbound);
e. days and time of day;
f. call duration;
g. whether to allow or terminate a call;
h. tracks (Log, Real-Time Alert, E-mail, Page, and SNMP Alert); and
i. span[4] groups[5] that are assigned to the Security Policy to enforce rules.

The ETM® System includes the ability to examine the rule set for ambiguous rules (e.g., rules that will never be triggered due to a previous rule).

The ETM® System has extensive auditing and reporting capabilities. The level of detail of each audited event is configurable by the administrator; however, each audit record contains a unique identification number, date and time stamp, and the appliance or span/span group which originated the record. Also, all call details (call destination/source; call type, duration, and direction; date and time; telecommunication line specifics; etc.) are recorded. Audit records may be viewed in a report generated using pre-defined or custom templates, or plotted in a graph in the TeleView™ Application. Reports may be generated on an automated schedule or as requested basis.

[3] Applicable only for the appliance models ETM® 2100 and ETM® 3200.
[4] A *span* refers to the interface between an appliance and the telecommunications network.
[5] A *span group* combines related spans into units so they can be managed as a single unit.

Most of the data produced during the operation of the ETM® System is stored in the ETM® Database, which is part of the ETM® Management Server. The ETM® Database supports the Oracle® 8*i* and 9*i* DBMSs on both Windows® and Solaris™. The DBMS used for the ETM® Database can be installed on the same PC as an ETM® Management Server or on a remote PC.

Audit records concerning telecommunication information flow and appliance status are generated at the appliances and are uploaded to the ETM® Management Server. Each appliance, except the AAA 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 be 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:

A.PHYSEC The TOE is physically secure.

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 telecommunications systems.

3.2 THREATS

The following threats are addressed by either 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 the telecommunications resources and the ETM® System itself.

T.SNIFF A network attacker may observe authentication data or system configuration information during transmission between 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.

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, telecommunications or internet service providers, 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 internal TOE 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 internal TOE communications have failed.

T.AUDEXH An administrator may be unaware that the audit storage on the ETM® Management Server of the TOE has been exhausted.

3.2.2 Threats To Be Addressed By Operating Environment

The potential threats discussed below must be countered by procedural measures and/or administrative methods. The threat agents are either human users or external IT entities that are unauthorised to use the TOE. The assets that are subject to attack are telecommunications resources.

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

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 cryptographic algorithm and key.

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 must not allow unauthorised 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 on the ETM® Management Server 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 administrator 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 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.

O.AAA The TOE must provide functionality that restricts access to AAA appliances to authorised telecommunications users.

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.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 components from Part 2 of the CC listed in Table 1.

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, respectively.

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 (1)	Cryptographic operation
FCS_COP.1 (2)	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_ACC.1 (3)	Subset access control
FDP_ACF.1 (3)	Security attribute based access control
FDP_IFC.1 (1)	Subset information flow control
FDP_IFF.1 (1)	Simple security attributes
FDP_IFC.1 (2)	Subset information flow control
FDP_IFF.1 (2)	Simple security attributes

Functional Components	
Identifier	**Name**
FIA_AFL.1 (1)	Authentication failure handling
FIA_AFL.1 (2)	Authentication failure handling
FIA_ATD.1 (1)	User attribute definition
FIA_ATD.1 (2)	User attribute definition
FIA_SOS.1 (1)	Verification of secrets
FIA_SOS.1 (2)	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 (1)	Management of security attributes
FMT_MSA.1 (2)	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, log, email with or without attachments, pager, 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; and
c. [exhaustion of log storage;
d. changes in TOE security function configuration;
e. failed and successful logins by administrators to an appliance;
f. logins and logouts by administrators to ETM® Management Server;
g. failed and successful logins by telecommunications user to an AAA 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;
m. rule violations;
n. AAA user account locked
o. AAA service disconnected; and
p. second dial tone detected after call answer].

Application Note: Auditable events for the basic level of audit include all minimum requirements and are identified in Table 2.

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:
    - [log time;
    - date;
    - call start time;
    - call end time;
    - call duration;
    - call direction (inbound or outbound);
    - phone number;
    - call source;
    - call destination;
    - call type (fax, modem, modem energy, voice, STU III, busy, unanswered, data or undetermined);
    - "in-call" digits;
    - call trailing digits;
    - tracks;
    - appliance;
    - span/span group;
    - text;
    - call trunk channel;
    - trunk group;
    - channel;
    - name of rule set;
    - rule number;
    - rule comment;
    - unique record ID;
    - unsuccessful login attempts;

- call information (LOC-local call, INTL-international call, VSC-vertical service code, etc.); and
- telecommunications users that have authenticated to an AAA appliance].

Table 2. Additional Auditable Events from CC Functional Components

Functional Component	Level	Auditable Event
FAU_ARP.1	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.
	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 flow.
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.

Functional Component	Level	Auditable Event
	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, dialling plan and call monitoring definition and based on call source, call destination, call type, call direction, call duration, time of day, and caller ID restricted].

Application Note: "Caller ID restricted" specifies that the rule applies to any call for which the caller has blocked caller ID information.

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 (1) – The TSF shall provide the ability to perform [*searches*, *ordering*] of audit data based on:

a. [log time;
b. date;
c. call start time;
d. call end time;
e. call duration;
f. call direction (inbound or outbound);
g. phone number;
h. call source;
i. call destination;
j. call type (fax, modem, modem energy, voice, STU III, busy, unanswered, data or undetermined);
k. "in-call" digits;
l. call trailing digits;
m. tracks;
n. appliance;
o. span/span group;
p. text;
q. call trunk channel;
r. trunk group;
s. channel;
t. name of rule set;
u. rule number;
v. rule comment;
w. unique record ID;
x. unsuccessful login attempts;
y. call information (LOC-local call, INTL-international call, VSC-vertical service code, etc.); and
z. telecommunications users that have authenticated to an AAA appliance].

FAU_SAR.3.1 (2) – 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 (fax, modem, modem energy, voice, STU III, busy, unanswered, data or undetermined);
f. "in-call" digits;
g. call trailing digits;

h. track;
i. appliance;
j. span/span group;
k. text; and
l. call information (LOC-local call, INTL-international call, VSC-vertical service code, etc.)].

Application Note: For several of the searchable audit fields, there are sub-types. The reporting tool included with ETM® System allows filters to be used to provide a finer layer of granularity.

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:
a. [*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 underlying database server provides the audit protection mechanisms.

FAU_STG.3 Action in case of possible audit data loss

FAU_STG.3.1 – The TSF shall take [the following action: generate a security message] if the audit trail exceeds [the local storage capacity on the ETM® Management Server].

FCS_COP.1 Cryptographic operation (1)

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 for the export version of the ETM® System] and cryptographic key sizes [64 bits] that meet the following: [FIPS 46-3 and FIPS 81].

FCS_COP.1 Cryptographic operation (2)

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 for the domestic version of the ETM® System] and cryptographic key sizes [192 bits] that meet the following: [FIPS 46-3 and ANSI X9.52-1998].

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 [user ID, password, and source 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. [a user account for 'user ID' exists;
b. 'password' matches the password for the identified user account and has not expired; and
c. 'source IP address' is included in the list of allowable IP addresses].

FDP_ACF.1.3 – The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [allow access if user is exempted from NETWORK_SFP, specially password expiry].

Note: This is an exemption from the password expiry control only.

FDP_ACF.1.4 – The TSF shall explicitly deny access of subjects to objects based on the [user account is disabled].

Note: The 'Account disabled' security attribute prevents login to the system from this account. Note that this setting prevents future logins from this account, but does not terminate an active login.

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 [the number of administrators editing an 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: [only one administrator shall be granted access to edit an 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 [none].

FDP_ACC.1 Subset access control (3)

FDP_ACC.1.1 – The TSF shall enforce the [TELCO_SFP] on [telecommunications users authenticating to an AAA appliance].

FDP_ACF.1 Security attribute based access control (3)

FDP_ACF.1.1 – The TSF shall enforce the [TELCO_SFP] to objects based on [user ID and PIN].

FDP_ACF.1.2 – The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [the user ID and PIN are valid authorisation credentials for the AAA appliance].

FDP_ACF.1.3 – The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [allow access within a set maximum time period, configurable from 0 to 30 minutes].

Note: This allows an authorised telecommunications user to access to telecommunications resources in accordance with the TELCO_SFP but only for the set maximum time period, configurable from 0 to 30 minutes. Additionally, access to the telecommunication resources are restricted to a single call during the set maximum time period.

FDP_ACF.1.4 – The TSF shall explicitly deny access of subjects to objects based on the [none].

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: call direction, call type, call source, call destination, call duration, caller ID restricted option, and time of day].

FDP_IFF.1.2 – The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [an administrator-created rule (based on the information security attributes identified in FDP_IFF.1.1) does not explicitly deny the information flow].

Application Note: Rules that deny an information flow based on call duration do not deny the call from starting, but terminate the call once it has reached the specified duration.

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 only applies to all ETM™ 1000 Series appliances except the AAA appliance.

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: [the call destination is an emergency number (i.e., 911)].

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

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: user ID, password, and source IP address; and
b. information security attributes: cryptographic algorithm and cryptographic key].

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

a. client to server communications – source IP address is on the allowable IP address list, user ID and password are valid, and communications are encrypted with a valid cryptographic algorithm and key (i.e., DES or Triple DES);
b. appliance to server communications – source IP address is on the allowable IP address list and communications are authenticated with a variable handshake and encrypted with a valid cryptographic algorithm and key (i.e., DES or Triple DES); or
c. appliance to appliance communications – source IP address is on the allowable IP address list and communications are encrypted with a valid cryptographic algorithm and key (i.e., DES or Triple DES)].

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 (1)

FIA_AFL.1.1 – The TSF shall detect when [six] unsuccessful authentication attempts occur related to [administrator login to an appliance via Telnet during a period of ten minutes].

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

FIA_AFL.1 Authentication failure handling (2)

FIA_AFL.1.1 – The TSF shall detect when [a number, configurable from one to ten, of] unsuccessful authentication attempts occur related to [telecommunications user login to an AAA appliance during a period of time configurable from zero to four weeks].

FIA_AFL.1.2 – When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [generate an audit event and deny the telecommunications user all access to the AAA appliance for a period of time configurable from zero minutes to ten weeks, or until explicitly granted by an administrator].

FIA_ATD.1 User attribute definition (1)

FIA_ATD.1.1 – The TSF shall maintain the following list of security attributes belonging to individual users: [user ID, password, and privileges (a combination of Allow Server Management; Allow User Modifications; Manage Policies; Manage Telecommunications Configuration; Support Appliance Login via Telnet/Serial; and Call Terminate Capability)].

FIA_ATD.1 User attribute definition (2)

FIA_ATD.1.1 – The TSF shall maintain the following list of security attributes belonging to individual telecommunications users: [user ID and PIN].

FIA_SOS.1 Verification of secrets (1)

FIA_SOS.1.1 – The TSF shall provide a mechanism to verify that secrets meet [a minimum length of eight characters, including at least one change of case and one digit, for administrator passwords].

FIA_SOS.1 Verification of secrets (2)

FIA_SOS.1.1 – The TSF shall provide a mechanism to verify that secrets meet [a minimum length of three digits to a maximum length of ten digits for telecommunications users PINs].

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 – The TSF shall allow [any human with physical access to an appliance to gain access to the appliance security functions within a period of time, configurable from zero seconds to two minutes, of appliance start-up] before the user is authenticated.

FIA_UAU.1.2 – The TSF shall require each user and telecommunications user accessing an AAA appliance to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user or telecommunications user.

FIA_UID.1 Timing of identification

FIA_UID.1.1 – The TSF shall allow [any human with physical access to an appliance to gain access to the appliance security functions within a configurable period of time, from zero seconds to two minutes, of appliance start-up] before the user is identified.

FIA_UID.1.2 – The TSF shall require each user and telecommunications user accessing an AAA appliance to be successfully identified before allowing any other TSF-mediated actions on behalf of that user or telecommunications user.

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 – The TSF restrict the ability to [*enable*, *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 (1)

FMT_MSA.1.1 – The TSF shall enforce the [NETWORK_SFP] to restrict the ability to

a. [*delete*, [create]] the security attributes [user ID]; and
b. [*modify*, [none]] the security attributes [password, privileges, allowable IP addresses, PIN]

to [an administrator].

Application Note: Deleting and creating the security attribute 'user ID' is analogous to deleting and creating a user account.

FMT_MSA.1 Management of security attributes (2)

FMT_MSA.1.1 – The TSF shall enforce the [TELCO_SFP] to restrict the ability to [*modify*, *delete*, [create]] the security attributes [groups of phone numbers and 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® System 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*, *delete*, [none]] the [audit logs];
b. [generate] the [audit reports];
c. [*modify*, [none]] the [audit level, appliance configuration, and date and time of the host machine and appliance];
d. [display] the [appliance status and current telecommunications activity]

to [an administrator].

FMT_SMR.1 Security Roles

FMT_SMR.1.1 – The TSF shall maintain the roles [administrator].

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: In this context, "reliable" means that the chronological order of auditable events is preserved.

FTP_TRP.1 Trusted Path

FTP_TRP.1.1 – The TSF shall provide a communication path between itself and [*remote*, *local*] users 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 users*, *remote users*] 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 security assurance requirements for EAL 2, as specified in Part 3 of the CC, with the augmentations of ACM_CAP.3, ACM_SCP.1, and ALC_DVS.1 are given in Table 3.

Table 3. Assurance Requirements for ETM® System

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
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

Assurance Class	Assurance Components	
	Identifier	**Name**
Vulnerability Assessment	AVA_SOF.1	Strength of TOE security function evaluation against the claim of SOF-BASIC
	AVA_VLA.1	Developer vulnerability analysis

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

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 typical attacker in the intended telecommunications environment for the ETM® System is deemed to possess only limited knowledge of the telecommunications systems and lack the skills and resources required to manipulate telecommunications interfaces. The purpose of the attacks would be to abuse services, use services fraudulently or simply to attack the services to cause service interruptions. The appliances include firewall protection on the network interfaces and the network environment provides additional network protection mechanisms for the TeleView™ Application client and ETM® Management Server. Therefore, for an EAL 2 evaluation of the ETM® System, the attack potential to meet or exceed for AVA_SOF.1 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 and applies to F.ADMIN and F.AAA.

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 user ID and password and by authenticating communications with a variable handshake.

F.TELBLK The TOE does block telecommunications access based on: call destination, call source, call type (voice, fax, modem, modem energy, STU III, busy, unanswered, data, 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 ETM™ 1000 Series appliances, except AAA appliances.

F.FAILNOT Upon detection of a potential security violation, the TOE does provide an audible alarm, SNMP trap, log, email with or without attachments, page to a pager or visual alert.

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. change user password expiry;
l. modify and delete user ID;
m. add and delete privileges and IP addresses;
n. create, modify and delete phone numbers and time of day;
o. modify audit level;
p. generate audit reports;
q. modify appliance configuration;
r. modify date and time of host machine and appliances;
s. display appliance status;
t. manage server;
u. modify users;
v. edit policies;
w. edit appliance parameters;
x. login directly to an appliance; and
y. change telecommunications user PIN.

F.LOCK The TOE does provide locking of objects to prevent multiple administrators from editing the same object. Locking is provided at the object level. Multiple administrators are able to view 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;
q. failed and successful logins by telecommunications user to an AAA appliance;
f. changes to rule sets 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;
r. AAA user account locked;
l. second dial tone detected after call answer;
m. AAA service disconnected; and
n. 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. user ID;
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 start time;
i. call end time;
j. call source (calling number or telecommunications user ID for AAA service) if available;
k. call destination (called number);
l. call type (fax, modem, modem energy, voice, STU III, busy, unanswered, data or undetermined);
m. call direction (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 span/span group 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 types of signals include: audible alarm, SNMP trap, log, email with or without attachments, page to a pager or visual alert .

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. date;
c. unsuccessful login attempts;
d. call start time;
e. call end time;
f. call duration;
g. call direction (inbound or outbound);
h. phone number;
i. call source;
j. call destination;
k. call type (fax, modem, modem energy, voice, STU III, busy, unanswered, data or undetermined);
l. “in-call” digits;
m. call trailing digits;
n. tracks;
o. appliance;
p. span/span group;
q. text;
r. call trunk channel;
s. trunk group;
t. channel;
u. name of rule set;
v. rule number;
w. rule comment;
x. unique record ID;
y. call information (LOC-local call, INTL-international call, VSC-vertical service code, etc.); and
z. telecommunications users that have authenticated to an AAA appliance].

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 (fax, modem, modem energy, voice, STU III, busy, unanswered, data or undetermined);
f. call “in-call” digits;
g. call trailing digits;
h. span/span group;
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 user ID, password and password expiration, 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.

F.AAA Access to AAA appliances is restricted to authorised telecommunications users through the use of user ID and PIN. A mechanism is provided to verify that telecommunications user PINs meet a minimum length of three digits up to a maximum of ten digits.

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 set-up 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 are 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. A mapping between developer test cases and TOE functionality is provided by the developer. 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 claim conformance to a Protection Profile.

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			
O.AAA				X	X								

T.SNIFF *A network attacker may observe authentication data or system configuration information during transmission between components 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 cryptographic algorithm and key. O.CRYPTO protects the

confidentiality of authentication and system configuration data using cryptography as it passes between distributed components of the TOE. Falsified data can not be properly encrypted for use by the TOE 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. O.AAA ensures that only authorised telecommunications users may access AAA appliances.

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

O.MEDTEL mediates telecommunications access across the telecommunication lines, preventing unauthorised use of telecommunication resources. O.AAA ensures that only authorised telecommunications users may access AAA appliances.

T.MISUSE *A telecommunications 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 unauthorised 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 unauthorised 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 unauthorised 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 unauthorised 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 *An administrator may be unaware that the audit storage on the ETM® Management Server of the TOE has been exhausted.*

O.AUDCHK ensures that the TOE notifies the administrator when the audit storage on the ETM® Management Server 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.NOEVIL	A.ADMKNW	T.USAGE	T.BADADM	T.TROJAN
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.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 unwittingly be configured, used and administered in an insecure manner by the administrator.*

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 TOE 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 TOE Security Objectives

	O.CRYPTO	O.ATKNET	O.MEDTEL	O.TELTOE	O.COMM	O.AUDCHK	O.ADMACC	O.HMI	O.DSPACT	O.AUDIT	O.SELFPRO	O.AAA
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 (1)	X											
FCS_COP.1 (2)	X											
FDP_ACC.1 (1)											X	
FDP_ACF.1 (1)											X	
FDP_ACC.1 (2)							X					
FDP_ACF.1 (2)							X					
FDP_ACC.1 (3)				X							X	X
FDP_ACF.1 (3)				X							X	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 (1)							X					

	O.CRYPTO	O.ATKNET	O.MEDTEL	O.TELTOE	O.COMM	O.AUDCHK	O.ADMACC	O.HMI	O.DSPACT	O.AUDIT	O.SELFPRO	O.AAA
FIA_AFL.1 (2)												X
FIA_ATD.1 (1)							X					
FIA_ATD.1 (2)												X
FIA_SOS.1 (1)							X				X	X
FIA_SOS.1 (2)							X				X	X
FIA_UAU.1							X				X	X
FIA_UID.1							X				X	X
FMT_MOF.1								X	X	X		
FMT_MSA.1 (1)											X	
FMT_MSA.1 (2)											X	
FMT_MSA.3											X	
FMT_MTD.1										X	X	
FMT_SMR.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 cryptographic algorithm and key.*

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

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.*

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 administrator-defined conditions.

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

FDP_ACC.1 (3), FDP_ACF.1 (3), FDP_IFC.1 (1), and FDP_IFF.1 (1) define the only allowed access control security policies which ensure there are no 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 audit storage on the ETM® Management Server has been exhausted.*

FAU_STG.3 provide the administrator with notification that the audit storage on the ETM® Management Server 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 (1), FIA_SOS.1 (2), 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 (1) are the security attributes which identify administrators and their privileges. FIA_AFL**.**1 (1) adds extra assurance that attempts to guess the administrator's password using brute force will be blocked (for Telnet access 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 administrator 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 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 administrator with the capability to review both a complete and reduced audit trail. FAU_SEL.1 and FMT_MOF.1 combine to provide the administrator 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), FDP_ACC.1 (3), FDP_ACF.1 (3), FIA_SOS.1 (1), FIA_SOS.1 (2), 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 (1), FMT_MSA.1 (2), FMT_MSA.3, FMT_SMR.1 and FMT_MTD.1 ensure that all security functions are managed only by administrators who have the correct privileges.

O.AAA *The TOE must provide functionality that restricts access to AAA appliances to authorised telecommunications users.*

FDP_ACC.1 (3), FDP_ACF.1 (3), FIA_SOS.1 (1), FIA_SOS.1 (2), FIA_UAU.1 and FIA_UID.1 ensure that all telecommunications users are properly identified and authenticated before gaining access to an AAA appliance. FIA_ATD.1 (2) lists the security attributes which identify telecommunications users. FIA_AFL.1 (2) adds extra assurance that attempts to guess a telecommunications user's PIN using brute force will be blocked.

8.2.2 Assurance Requirements Rationale

The ETM® System is designed to mediate telecommunications traffic over telecommunication lines and be simple enough for an average PC user to manage. An assurance level 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® System 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® System. 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 Security Functional Requirements and their immediate dependencies, and also indicates whether the ST explicitly addresses each dependency. 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_STG.1	Y
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	Y
FDP_ IFF.1	FDP_IFC.1	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_ ITT.1	–	Y
FPT_ STM.1	–	Y
FPT_ TRP.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 (i.e., 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 Security Assurance Requirements and their immediate dependencies, and also indicates whether the ST explicitly addresses each dependency. All dependencies for assurance components have been met.

Table 8. Security 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_GEN.1 Audit data generation

In FAU_GEN.1.2, changed "… at least the following information: … subject identity…" to "… at least the following information: … subject identity (when available)…" as the subject identity is not always available for audit generation.

FAU_SAR.3 Selectable audit review

Added an additional category to FAU_SAR.3.1 (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.

FIA_ATD.1 User attribute definition (2)

In FIA_ATD.1.1, changed "…belonging to individual users" to "…belonging to individual telecommunications users" since the requirement only applies to individuals who communicate over the telecommunications network to operate an AAA appliance.

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.

In FIA_UAU.1.2, changed "user" to "user and telecommunications user accessing an AAA appliance" since only these TOE users authenticate to the TOE.

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.

In FIA_UID.1.2, changed "user" to "user and telecommunications user accessing an AAA appliance" since only these TOE users are required to authenticate to the TOE.

FMT_MSA.3 Static Attribute initialisation

In FMT_MSA.3.1, changed "…default values for security attributes…" to "…default values for information flow security attributes…" since the requirement only applies to the information flow SFP.

In FMT_MSA.3.1, 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.

8.2.6 Rationale for Audit Exclusions

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

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 TOE 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 TOE 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 (1)	FCS_COP.1 (2)	FDP_ACC.1 (1)	FDP_ACF.1 (1)	FDP_ACC.1 (2)	FDP_ACF.1 (2)	FDP_ACC.1 (3)	FDP_ACF.1 (3)	FDP_IFC.1 (1)	FDP_IFF.1 (1)	FDP_IFC.1 (2)	FDP_IFF.1 (2)	FIA_AFL.1 (1)	FIA_AFL.1 (2)	FIA_ATD.1 (1)	FIA_ATD.1 (2)	FIA_SOS.1 (1)	FIA_SOS.1 (2)	FIA_UAU.1	FIA_UID.1	FMT_MOF.1	FMT_MSA.1 (1)	FMT_MSA.1 (2)	FMT_MSA.3	FMT_MTD.1	FMT_SMR.1	FPT_ITT.1	FPT_STM.1	FTP_TRP.1
F.CRYPTO									X	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	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						X			
F.INIT																																X					
F.AAA															X	X						X		X	X	X	X	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, password expiry, 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_ACC.1 *Subset access control* (3)

F.AAA satisfies the requirement for access control of an AAA appliance through authentication of telecommunications users.

FDP_ACF.1 *Security attribute based access control* (3)

F.AAA satisfies the requirement for access control to an AAA appliance based on security attributes of user ID and PIN.

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 a cryptographic key and algorithm.

FIA_AFL.1 *Authentication failure handling (1)*

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_AFL.1 *Authentication failure handling (2)*

F.AAA satisfies the requirement to restrict access to AAA appliances to authorised telecommunications users by turning off access after a set number of failed login attempts

FIA_ATD.1 *User attribute definition (1)*

F.ADMIN satisfies the requirement for user attributes.

FIA_ATD.1 *User attribute definition (2)*

F.AAA satisfies the requirement for telecommunications user attributes.

FIA_SOS.1 *Verification of secrets*

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

FIA_UAU.1 *Timing of authentication*

F.ADMIN and F.AAA satisfy the requirement for user authentication.

FIA_UID.1 *Timing of identification*

F.ADMIN and F.AAA satisfy 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 (1)*

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.1 *Management of security attributes (2)*

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 between separate components of the TOE.

FPT_STM.1 *Reliable time stamps*

F.AUDINF and F.TIME combine to satisfy the requirement for 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 Security Assurance Requirements and is followed by a short discussion of how the Security Assurance Requirements are addressed by the corresponding Assurance Measures.

Table 11. Mapping of Assurance Measures to Security 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 configuration items and associated 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
AAA	Authorisation, Authentication, and Accounting
ANSI	American National Standards Institute
ASCII	American Standard Code for Information Interchange
CC	Common Criteria for Information Technology Security Evaluation
CD-ROM	Compact Disc, read-only-memory
CFB	Cipher-feedback mode
CM	Configuration Management
CO	Central Office (Telecommunication provider)
DBMS	DataBase Management System
DES	Data Encryption Standard
E1	E-carrier First level
EAL	Evaluation Assurance Level
ETM	Enterprise Telephony Management
FIPS	Federal Information Processing Standards
HMI	Human Machine Interface
ID	Identification
INTL	international call
IP	Internet Protocol
ISDN	Integrated Services Digital Network
IT	Information Technology
LOC	local call
NETWORK_SFP	NETWORK Security Functional Policy
Windows® NT	Windows® New Technology
PBX	Private Branch Exchange
PC	Personal Computer
PIN	Personal Identification Number
PRI	Primary Rate Interface
RS-232	Recommended Standard-232
SFP	Security Functional Policy
SNMP	Simple Network Management Protocol
SOF	Strength of Function
SP6A	Service Pack Six A – for Windows NT 4.0
ST	Security Target
STU	Secure Telephone Unit
TELCO_SFP	TELCO Security Functional Policy
T1	T-carrier First level
TCP	Transmission Control Protocol

Acronym	Definition
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
VSC	vertical service code