CarrierAccess™

EAL3

Broadmore 1750, 1700, and 500

Release 4.1.1

Security Target

Release Date	June 15, 2006
Version	2.0

Prepared By: ***InfoGard Laboratories, Inc.***

Prepared For: ***Carrier Access Corporation***

5395 Pearl Parkway
Boulder, CO 80301-2490
Corporate Phone: (800) 495-5455
Fax: (303) 443-5908

Document History

Release Number	**Date**	**Author**	**Details**
Broadmore ST version 2.0	**6/15/06**	**Elizabeth Sullivan**	**Final Release**

Trademarks

pSOSystem® is a registered trademark of the WindRiver Systems Corporation.

SecurID® is a registered trademark of RSA Inc.

SSHield® is a registered trademark of TeamF1, Inc.

Broadmore® is a registered trademark of Carrier Access Corporation

Table of Contents

List of Tables

List of Figures

1 Introduction

This section identifies the Security Target, Target of Evaluation (TOE), conformance claims, ST organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 Identification

TOE Identification:	Carrier Access Broadmore 500 Release 4.1.1 P/N: 7665-500DC-CD, consisting of chassis 7665-05DC, CPU 7660-007, CPU i/o 7660-411 and Software Version 4.1.1 Carrier Access Broadmore 1700 Release 4.1.1 P/N: 7665-1700-CD, consisting of chassis 7665-17C, CPU 7660-007, CPU I/O 7660-411 and Software Version 4.1.1 Carrier Access Broadmore 1750 Release 4.1.1 P/N: 7665-1750-CD, consisting of chassis 7665-17B, CPU 7660-007, CPU I/O 7660-411 and Software Version 4.1.1 Note that refurbished units are distinguished from new units by adding the suffix "-REF" to the part number. All refurbished units provide the same functionality as new units with the same part number.
ST Identification:	EAL3 Broadmore 1750, 1700, and 500 Release 4.1.1 Security Target[1]
ST Publication Date:	June 15, 2006
ST version number:	Version 2.0
Author(s):	Elisabeth C. Sullivan

1.2 Conformance Claims

- The TOE is Common Criteria Version 2.1 (ISO/IEC 15408:1999) Part 2 conformant.
- The TOE is Common Criteria Version 2.1 (ISO/IEC 15408:1999) Part 3 conformant.
- The TOE is conformant with Assurance Package EAL3.
- The TOE is compliant with all International interpretations with effective dates on or before June 23, 2004. Specifically, this includes international interpretations 003, 004, 038, 051, 065, 111, 141, and 202.
- This TOE is not conformant to any Protection Profiles (PPs).

[1] Throughout this document, the Carrier Access Broadmore 1750, 1700, and 500 will be referred to collectively as “the Broadmore”, unless discussing differences between specific versions. In this case, the product being discussed will be called “the Broadmore 1750”, “the Broadmore 1700”, or ”the Broadmore 500”, whichever is appropriate. The TOE will be referred to as “the Broadmore TOE” or simply, “the TOE”. The ST may also be referred to as the “Broadmore ST”, or simply ”the ST.

1.3 Overview

The Broadmore is an Asynchronous Transfer Mode (ATM) service multiplexer enabling broadband and other non-ATM technologies to be transported across an ATM network. It is designed as an ATM network service access node that supports the transport of existing broadband services (voice, video, and data) over ATM networks. The Broadmore accepts signals from non-ATM-ready equipment, converts the signals to standard ATM cells, and multiplexes the cells onto a single ATM User Network Interface (UNI) port. Typically, the Broadmore is deployed at the edge of an ATM network as the ATM node element closest to the customer. Both Permanent Virtual Circuit (PVC) and Switched Virtual Circuit (SVC) service are available based upon user-defined module configuration. The Broadmore is designed as a modular system that can be configured to meet the service access and network interface requirements of the user. This is done by the use of different configuration of data-plane cards (that provide end-user traffic handling but do not involve any management or security services) and management cards that provide the management capabilities in a secure manner.

The security functionality claimed in this ST consists of the security management of the Broadmore device. No security claims are made for the data-plane cards that provide end-user traffic handling but do not involve any management or security services. The hardware/software cards implementing the multiplexer functionality are not considered a part of the TOE.

1.4 ST Organization

- Security Target Introduction (Section 1) – Provides identification of the TOE and ST, conformance claims, an overview of the TOE, this overview of the content of the ST, document conventions, and relevant terminology.

- TOE Description (Section 2) – Provides a description of the TOE security functions as well as the physical and logical scope and boundaries for the TOE.

- TOE Security Environment (Section 3) – Describes the threats, organizational security policies, and assumptions pertaining to the TOE and the TOE environment.

- TOE Security Objectives (Section 4) – Identifies the security objectives for the TOE and its supporting environment as well as a rationale that objectives are sufficient to counter the threats and assumptions identified for the TOE.

- TOE Functional and Assurance Requirements (Section 5) – Presents the Security Functional Requirements (SFRs) met by the TOE, the Strength of Function claims for the requirements, and the security functional requirements rationale. In addition this section presents Security Assurance Requirements (SARs) met by the TOE as well as the assurance requirements rationale.

- TOE Summary Specification (Section 6) – Describes the security functions provided by the TOE that satisfy the security functional requirements, provides the rationale for the security functions, and the rationale for the security function SOF claim. It also describes the security assurance measures for the TOE as well as the rationales for the assurance measures.

- Protection Profile Claims (Section 7) – Presents the rationale concerning Protection Profile (PP) conformance.

- Rationale (Section 8) – Provides pointers to all other rationale sections, to include the rationale for the selection of IT security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability.

1.5 Conventions

1.5.1 Convention for Operations

The CC defines four operations on security functional requirements. The conventions below are used in this ST to identify the operations performed.

Assignment	Made within the ST:	[**bold text in square brackets**]
Selection	Made within the ST:	[underlined text in square brackets]
Refinement	Made within the ST:	[***bold italicized text in square brackets***] for additions and [~~***strikethrough bold italicized text in square brackets***~~] for deletions
Iteration	Made within the ST:	indicated with a typical CC requirement naming followed by a lower case letter enclosed in square brackets e.g. FAU_SEL.1.1 [a].

1.5.2 Convention for Conditional Security Functional Requirements (SFR)

This ST contains conditional security functional requirements. The convention for these requirements is as follows:

CONDITION: the condition under which the following component is included in the ST.

SFR Component

END CONDITION

1.5.3 Convention for Interpretations

Security functional requirements and security assurance requirements are footnoted in cases where CCIMB interpretations are used in the statement of the requirements. The footnote identifies the number of the specific interpretation used.

1.6 Terminology

1.6.1 CC Terms

In the Common Criteria, many terms are defined in Section 2.3 of Part 1. A subset of those definitions is included in the list below. They are listed here to aid the reader of the Security Target.

Assurance Grounds for confidence that an entity meets its security objectives.

Attack potential The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.

Audit The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend indicated changes in controls, policy, or procedures

Audit Trail In an IT System, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized

Authentication To establish the validity of a claimed user or object

Authentication data Information used to verify the claimed identity of a user.

Authorized user A user who may, in accordance with the TSP, perform an operation.

Availability Assuring information and communications services will be ready for use when expected

Confidentiality Assuring information will be kept secret, with access limited to appropriate persons

Evaluation Assessment of a PP, a ST or a TOE, against defined criteria

Evaluation Assurance Level (EAL) A package consisting of assurance components from Part 3 that represents a point on the CC predefined assurance scale.

External IT entity Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

Information Technology (IT) System May range from a computer system to a computer network

Human user Any person who interacts with the TOE.

Identity A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

Object An entity within the TSC that contains or receives information and upon which subjects perform operations.

Organizational security policies Organizational security policies — One or more security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

Product A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.

Protection Profile (PP) An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Role A predefined set of rules establishing the allowed interactions between a user and the TOE.

Security attribute Information associated with subjects, users, and/or objects that is used for the enforcement of the TSP.

Security objective A statement of intent to counter identified threats and/or satisfy identified organization security policies and assumptions.

Security Target (ST) A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Strength of Function (SOF) A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behavior by directly attacking its underlying security mechanisms.

SOF-basic A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

Subject An entity within the TSC that causes operations to be performed.

System A specific IT installation, with a particular purpose and operational environment.

Target of Evaluation (TOE) An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE resource Anything useable or consumable in the TOE.

TOE Security Functions (TSF) A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP

TSF data Data created by and for the TOE, that might affect the operation of the TOE

TOE security policy model A structured representation of the security policy to be enforced by the TOE.

Threat The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. A potential violation of security

User Any entity (human user or external IT entity) outside the TOE that interacts with the TOE

User data Data created by and for the user that does not affect the operation of the TSF.

1.6.2 ST Specific Terms

These terms are specific to this ST, or are refinements of CC terminology to clarify specific meanings of the term in this ST.

Asynchronous Transfer Mode (ATM) A fast, cell-switched transmission technology based on a fixed-length 53-byte cell combining the best advantages of both circuit switching (for constant bit rate services) and packet switching (for variable bit rate services) that provides guaranteed service levels.

Craft access A user has craft access if the user has been given permission to access the Broadmore from the craft port. See also remote access

Craft port The serial port used to manage the device from a console.

Power Source The power source is provided by the Broadmore operational environment to supply power to the Broadmore via the Broadmore power supply.

Power Supply The Broadmore power supply is the hardware part(s) on the Broadmore chassis that supply power to the Broadmore from the power source.

pSOS, pSOSystem™ The real time operating system embedded on the CPU chip used in the Broadmore device. There is no known expansion of the acronym.

Remote access A user has remote access if the user has been given permission to access the Broadmore from a remote workstation. See also craft access

Time Division Multiplex (TDM) A technique for transmitting a number of separate data, voice, and/or video signals simultaneously over one communications medium by quickly interleaving a piece of each signal one after another.

1.6.3 Frequently Used Acronyms

The following list presents frequently used acronyms used in this ST. Some are defined in the previous lists.

APS	Automatic Protection Switching
ATM	Asynchronous Transfer Mode
CAMMI	Communication Access Multiplexer Management Interface
CLI	Command Line Interface
CPU	Central Processor Unit
GUI	Graphical User Interface
FTP	File Transfer Protocol
IOM	Input Output Module
IP	Internet Protocol
LAN	Local Area Network
LANE	LAN Emulation
NIM	Network Interface Module
RTOS	Real time operating system
SAM	Service Access Module
SSH	Secure Shell
SSH 2	Secure Shell, protocol version 2
SNMP	Simple Network Management Protocol
TDM	Time Division Multiplex

2 TOE Description

The Broadmore is an Asynchronous Transfer Mode (ATM) *service multiplexer* enabling broadband and other non-ATM technologies to be transported across an ATM network. This falls into the *miscellaneous* category of product types.

2.1 Overview

2.1.1 The Broadmore Product

The Broadmore is an Asynchronous Transfer Mode (ATM) service multiplexer enabling broadband and other non-ATM technologies to be transported across an ATM network. It is designed as an ATM network service access node that supports the transport of existing broadband services (voice, video, and data) over ATM networks. The Broadmore accepts signals from non-ATM-ready equipment, converts the signals to standard ATM cells, and multiplexes the cells onto a single ATM User Network Interface (UNI) port. Typically, the Broadmore is deployed at the edge of an ATM network as the ATM node element closest to the customer. Both Permanent Virtual Circuit (PVC) and Switched Virtual Circuit (SVC) service are available based upon user-defined module configuration. The Broadmore can be deployed in satellite (wireless) networks, using HSSI and CBI interfaces to transfer data over serial and cell-based links.

The Broadmore is designed as a modular system that can be configured to meet the service access and network interface requirements of the user. This is done by the use of different configuration of data-plane cards (that provide end-user traffic handling but do not involve any management or security services) and management cards that provide the management capabilities in a secure manner.

The Broadmore appliances provide user and system level auditing, local user account management, and role enforcement. The Broadmore appliances provide a redundant power supply to support continuous availability of the device. The redundant power supply can be attached to a second power source (if provided by the operating environment), providing continuous service if the primary power source fails. The Broadmore 1700 and 1750 provide optional redundancy of CPU and Network Interface Modules (NIMs). This allows the Broadmore 1700 to continue working in case of CPU or NIM failures. The Broadmore 1750 provides protection of Service Access Modules (SAMs) by offering a redundant SAM to take over if one of up to four identical SAMs fails. The Broadmore contains SSHield® version 2.0 from TeamF1 Inc., and for stronger authentication, a SecurID®[2] RSA Authentication Manager client from RSA Security Inc. SSHield uses Secure Shell version 2 (SSH2) protocol to provide data transfer security of network management traffic using encryption. It also provides key management.

The Broadmore appliances can operate in FIPS mode or non-FIPS mode of operation. The FIPS mode has been certified as compliant with FIPS 140-2. The FIPS mode of the Broadmore/SSHield Management Module has been validated as compliant with FIPS 140-2, Level 1 overall, certificate no. 478, posted at the NIST website, *Validation Lists for Cryptographic Standards* at http://csrc.nist.gov/cryptval. The TOE described for this ST uses the FIPS mode only.

An example of the use of the Broadmore is shown below in figure 2.1. This example shows communication between two legacy TDM-based devices using two Broadmore devices. This is just one sample of many different configurations in which the Broadmore can be used.

The differences among the Broadmore models are minimal and include the following:

- Capacity: the Broadmore 1700 and 1750 support up to twelve different slots with 1 to 8 ports per slot for non-ATM connections on one box, while the Broadmore 500 supports at most three different slots with 1 to 8 ports per slot for non-ATM connections.
- Optional CPU, NIM, and SAM Redundancy: The Broadmore 1700 and 1750 provide optional

[2] SecurID was developed and is maintained by RSA Security Incorporated.

redundancy for Network Interface Modules (NIMs) and Central Processing Units (CPU). The Broadmore 500 can only support a single CPU and a single NIM. The Broadmore 1750 additionally provides optional 1:4 protection for Service Access Modules (SAMs).

2.1.2 The TOE

The Broadmore TOE consists of the Broadmore Chassis and all components of the product except for the NIM and SAM cards. There are no security claims made for the ATM multiplexer functions, and a variety of NIM and SAM cards can be purchased for use in the Broadmore device. For these reasons the NIM and SAM cards are included as a part of the TOE environment, and not a part of the TOE. Furthermore, the SecurID®[3] RSA Authentication Manager client from RSA Security Inc. is not included in the TOE. The satellite networks and data transfer interfaces are not a part of the TOE.

There are two third party products that are included in the TOE, WindRiver's pSOS operating system and TeamF1's SSHield. SSHield source code was purchased by Carrier Access, making it possible to modify and/or integrate the code into the TOE. Only portions of the pSOS source code were purchased by Carrier Access: namely the *netutils* code. This portion of the code can be modified by Carrier Access. The remaining pSOS code is used in a "black box" style.

Note also that the command "Leftmost" is not permitted in the TOE.

2.2 Architecture Description

Figure 2.1 presents an example of the Broadmore device in its environment. In this example, two Broadmore devices are used to connect two non-ATM based devices. Non-ATM device 1 sends transmissions using the services it supports to the Broadmore, which converts the communications to an ATM format and sends them over the ATM service to another Broadmore. The second Broadmore converts the ATM format to the non-ATM format used by the second non-ATM device.

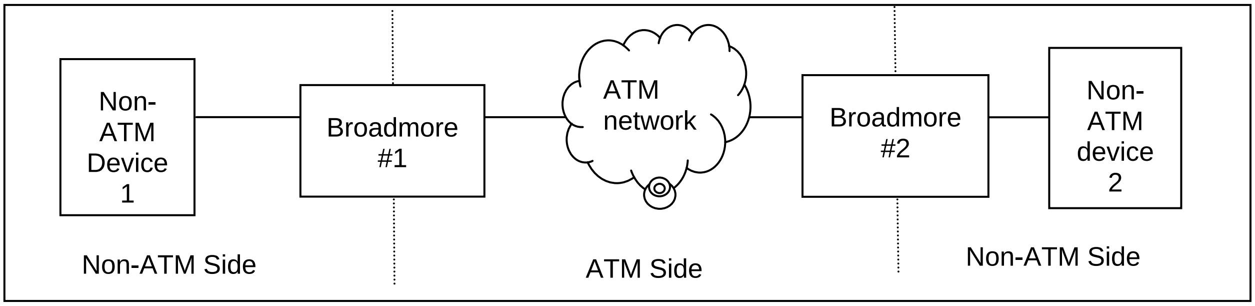

Figure 2-1: The Broadmore in a Sample Environment

Figure 2-2: The Broadmore architecture, presents a generic view of the components of the Broadmore appliance and its environment. Elements of the diagram are described in the following paragraphs. This sample architecture shows a Broadmore 1700 model configured with redundant NIM and CPU, and with a remote workstation connected via an Ethernet port to the CPU board. Note that this is one possible configuration for the model 1700.

[3] SecurID was developed and is maintained by RSA Security Incorporated.

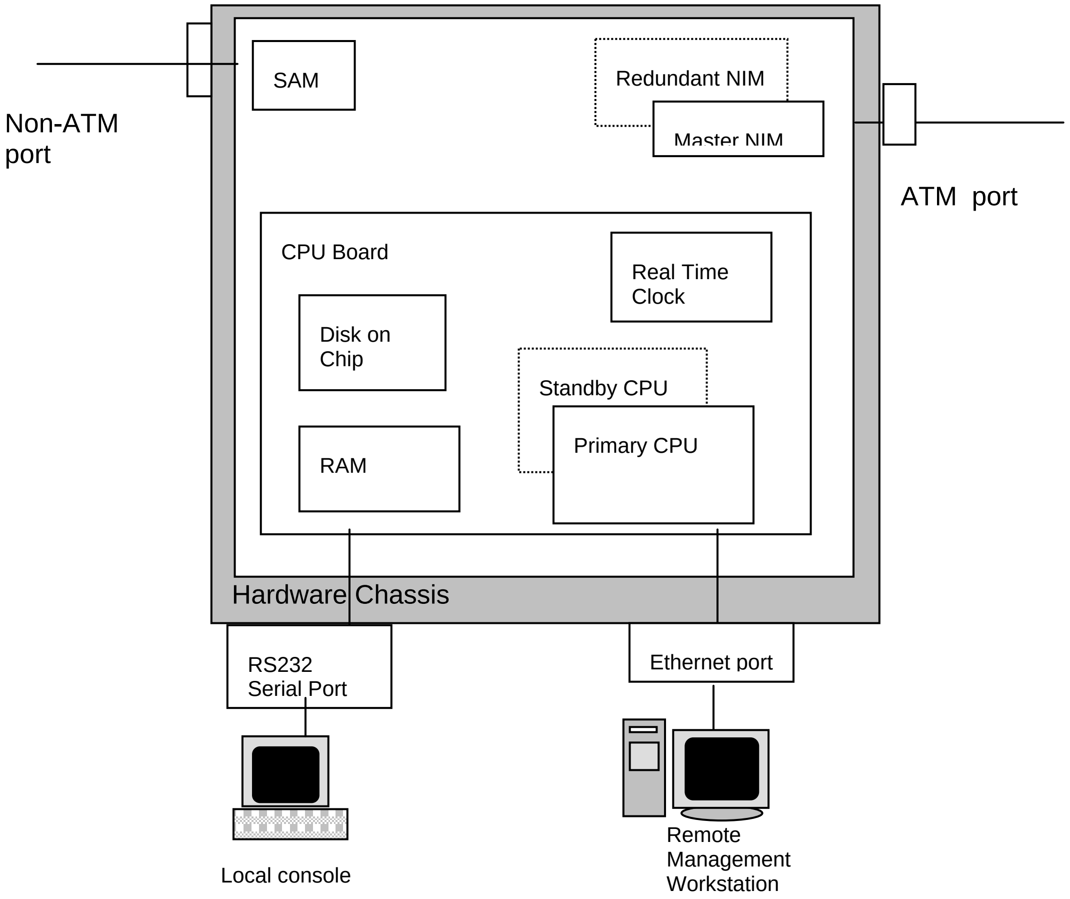

Figure 2-2: The Broadmore architecture

2.2.1 Hardware

The Broadmore appliance consists of a hardware chassis that contains a CPU board and SAM and NIM cards. The Broadmore requires a serially connected local console, and is capable of providing a remote management interface. Additionally, the Broadmore optionally uses SecurID to provide a second factor of authentication. An overview of each hardware component is described below. Differences among the Broadmore 1750, 1700 and 500 will be discussed in the appropriate sections. Note that items marked with * are not shown in figure 2.2.

Hardware Chassis: The Broadmore 500 has a five slot hardware chassis, and the Broadmore 1750 and 1700 have a 17 slot chassis. On the 1700 and 1750 models, one slot, labeled APM, is reserved for the Alarm Power Module, which is factory pre-installed. It provides EMI power conditioning and over-current protection for each of the two -48 VDC power sources. All other slots are front-loadable and hot-swappable, and can hold a variety of modules as described below. The Broadmore must be configured with at least one CPU, one SAM, and one NIM. Ports are connected to the appropriate SAM, NIM, or CPU by hardware IO modules which are accessible from the back of the chassis *. The hardware chassis provides two –48 V DC power supplies on the 500, 1700 and 1750 models.

SAM Cards: Service Access Modules (SAMs) reside in the hardware chassis. They receive and send information from non-ATM transmissions. Each different kind of non-ATM transmission requires a SAM designed to support that type of transmission. The Broadmore 500 can support 1, 2, or 3 SAMs; the Broadmore 1750 and 1700 can support 1 to 12 SAMs. Optionally, the 1750 can support a set of 1 to 4 similar SAMs with an additional similar SAM for redundancy if one of the 4 fails. The SAMs supported by the three models of the Broadmore are listed in the following table.

SAM	500	1700	1750
DS1 (T1) Circuit Emulation	Y	Y	
E1 Circuit Emulation	Y	Y	
DS3 (T3) Structured Circuit Emulation	Y	Y	Y
DS3 (T3) Unstructured Circuit Emulation	Y	Y	Y
E3 Unstructured Circuit Emulation	Y	Y	Y
Multiple Bit rate (MBR) Circuit Emulation	Y	Y	
MBR High Bit Rate Circuit Emulation	Y	Y	
Cell Bearing Interface (CBI) NIM/SAM;	Y	Y	
High Speed Synchronous Cell Bearing Interface (HSSI-CBI) NIM/SAM	Y	Y	
Serial Multiplexer SAM	Y	Y	
Serial De-Multiplexer SAM	Y	Y	
ATM DS3 (T3) NIM/SAM	Y	Y	

Table 2-1: SAMS suppoorted by Broadmore models

NIM Cards: Network Interface Modules (NIMs) reside in the hardware chassis. They receive and send ATM transmissions. The Broadmore 500 supports one NIM. The Broadmore 1700 and 1750 can support two identical NIMs to provide redundancy. The NIMs supported by the three Broadmore models are listed in the table below.

NIM	500	1700	1750
Optical carrier level 3 (OC-3)	Y	Y	
Optical Carrier level 12 (OC-12)		Y	Y
Cell Bearing Interface (CBI) NIM/SAM;	Y	Y	
High Speed Synchronous Cell Bearing Interface (HSSI-CBI) NIM/SAM	Y	Y	
ATM DS3 (T3) NIM/SAM	Y	Y	

Table 2-2: NIMs supported by Broadmore models

CPU Board: The CPU board resides in the hardware chassis. The model 500 supports a single CPU while the 1700 and 1750 can each support 2 redundant CPUs. The CPU board consists of the following main components:

- An x86 general purpose microprocessor (CPU) that is responsible for executing machine code. Broadmore 1700 and 1750 can support two identical CPUs to provide redundancy. If there is a redundant CPU, a Mid-plane inter-CPU Serial Bus* is used to coordinate data plane configurations with a “hot backup” CPU.

- RAM (Random Access Memory) that stores code for execution as well as data in a volatile fashion, so the CPU can access it and execute it or operate on it.*
- A “Disk-on-Chip” non-volatile memory containing the binary image of the SSHield cryptographic module and other files that are executed on power-up.
- An Ethernet port used to exchange management traffic secured with SSHield's SSH[4] implementation. Management traffic will be exchanged only over a CIP/LANE/ATM connection or the Ethernet port. They appear identical from the software module's perspective. Classical IP (CIP) over ATM can be used to exchange management traffic secured with SSHield's SSH implementation. Management traffic will be exchanged only over a CIP/LANE/ATM connection or the Ethernet port. They appear identical from the software module's perspective.
- A serial port (called ‘Craft port’) used to manage the device from a console.
- A real-time clock
- A Mid-plane Serial Bus* to SAM and NIM cards that carries bandwidth allocation and configuration messages from the CPU to the “data plane” cards in the chassis. This bus carries no security relevant information.

SecurID server* The Broadmore can optionally be configured to use a SecurID server to provide primary token-based user authentication, in addition to the authentication provided by the Broadmore itself. Note that the SecurID authentication is not claimed in the TOE of this evaluation.

Remote Management workstation

Management and administration are provided remotely via a networked workstation. Data transmissions are protected by the SSHield cryptographic module of the Broadmore. Remote management workstations are connected to the Broadmore via an Ethernet port. The remote management workstation must establish a session with the Broadmore using an SSH client using SSHv2, such as SecureCRT. The hardware for this workstation can be any that supports an OS that, in turn, supports the SSH client.

Local Console Local management and administration are provided by a serial-port connected PC that runs a VT100 emulator.

Non-ATM connection This is the connection between the Broadmore and systems that support legacy transmission such as TDM, serial, or cell data. The connection is made via a port that connects to the SAM for the specific type of transmission.

ATM Connection: This is the connection between the Broadmore and the ATM network. The connection is made via the ATM port connected to the NIM IO Module.

*not shown in diagram

2.2.2 Software /Firmware

The Broadmore is implemented as a standard embedded system software module where the run-time binary executable image is loaded at boot-time by the hardware, and executes continuously until power-

[4] SSH expands to Secure shell.

down. This image includes the operating system as well as the Broadmore software and the SSHield cryptographic module. Like most embedded systems, there is no concept of end-user-added software programs executing on this hardware or the possibility to modify runtime executables, except as allowed by the configuration parameters provided by the Broadmore itself.

The Broadmore software includes the management framework and the multiplexer application software. The Individual software/firmware components are described below.

WindRiver Systems pSOSystem® Version 2.2.7

The software operating system is WindRiver System's pSOSystem (pSOS), a real time operating system (RTOS) that resides on the embedded CPU module. It provides local and remote mechanisms to be used to monitor and configure the Broadmore.

TeamF1 SSHield® version 2.0

SSHield is TeamF1's implementation of the SSH protocol for embedded Operating Systems. The SSH protocol provides security at the application layer. It is used in the Broadmore/SSHield Management module for remote management of the device. It allows for strong authentication of users and hosts (e.g. using a password and, optionally, SecurID-based authentication mechanism), data confidentiality, and protects against IP spoofing, interception of passwords and data manipulation in transit.

Broadmore management framework software version 4.1.1

The Broadmore management framework software can be considered in two parts: one part that runs the multiplexer application and the other that provides the management framework.

The Multiplexer software includes application software resident on the CPU as well as firmware resident on the NIM and SAM cards. The Broadmore application provides the multiplexer functions that allow the Broadmore device to accept, reformat, and transmit information between ATM and non-ATM networks. Note that there are no claims made in the ST that are relevant to the SAM and/or NIM functionality.

Management Framework software also resides on the embedded CPU module. It interfaces with all other components on the Broadmore device to provide management of configuration parameters, security functions, security auditing.

The embedded operating system includes the Communication Access Multiplexer Management Interface (CAMMI) for local management of the Broadmore through a series of easy-to-use windows and pull-down menus. A Command Line Interface (CLI) feature is also provided.

RSA SecurID® software

When the SSHield is operating with SecurID enabled, SecurID provides additional protection by providing token-based authentication by an external authentication server before SSHield authenticates the user name and password. SecurID®authentication is not provided on the local Console port. Note that the RSA SecurID authentication is not claimed as a part of this TOE.

Secure terminal software

Remote management workstations must run a software security package that has an SSH client supporting SSHv2 (such as SecureCRT). The operating system of the remote management workstations can be any that support the SSH client software. The console PC must run VT100 terminal emulator software.

2.3 Scope of the TOE

2.3.1 TOE Physical Scope and Boundary

The following table identifies the physical boundary and scope of the TOE.

Component	**TOE or Environment**
Broadmore hardware chassis and CPU cards installed in it.	TOE
pSOSystem Operating System version 2.2.7	TOE
SSHield® version 2.0	TOE
Broadmore management framework software version 4.1.1	TOE
SAM and NIM cards to be installed in the Broadmore device.	TOE Environment
Power source and Redundant power source, if provided	TOE Environment
Local console hardware and software	TOE Environment
Remote management workstation hardware and software (including the operating system, applications, and SSH client). The SSH client must be compatible with OpenSSH. OS software can be any OS that supports the SSH client. The hardware can be any that supports the OS.	TOE Environment
HSSI and CBI	TOE Environment

Table 2-3: Physical Scope and Boundary of TOE and TOE Environment

2.3.2 TOE Logical Scope and Boundary

The TOE is composed of the logical components described in the following sections.

2.3.2.1 Audit

The Broadmore provides an audit function to record information about successful and unsuccessful events such as modifications to configuration parameters and logins. Audit trail data is stamped with dependable date and time information. Modification or deletion of audit data is restricted to the highest level of authorized administrator (Super_User). Audit logs are managed with rotating buffers of a fixed size, and when a buffer is full, the administrator is notified and appropriate action can be taken to preserve audit records.

2.3.2.2 Identification and Authentication

The TOE restricts access to a single user at a time. The login can take place from a remote workstation if the user has “remote access” permission, or a local console attached to the craft port if the user has “craft access” permission. The user logs into the combined OS/Broadmore management module. Note that the Broadmore application and the embedded operating system are a single image, and users log into this image with no distinction of logging into the OS or the application. Users must be authenticated by the TOE using the user ID and password based login process. There is an authentication failure management process on the Broadmore that curtails excessive login attempts.

2.3.2.3 Security Management

All users of the Broadmore are authorized administrators. There are two basic roles, Admin User and Crypto Officer. Access is controlled by role enforcement based on the privileges of the user. The privileges further subdivide the roles into Browser, Operations, and SysAdmin. The Crypto Officer role is available only to the Super_User. Because these two names are synonymous, the term Super_User will be used in the remainder of this document. Access is controlled by role enforcement based on the role of the user. In the remainder of this document, the term “role” will refer to the Browser, Operations, SysAdmin, or Super_User.

The TOE restricts access to security relevant functions by role enforcement. TSF data is also protected from unauthorized access by role enforcement.

2.3.2.4 TOE Protection

The TOE protects itself by providing a domain for its own execution that cannot be accessed by untrusted subjects, and by ensuring that the TSF cannot be bypassed. A TOE execution domain is provided by a combination of physical protection of the TOE and TSF that prevent access by unauthorized users. Nonbypassability of the TSF is provided by forbidding unauthorized users to access the TOE and by role enforcement.

The TOE also protects communication between the remote users and the TOE using an SSH session, which provides both integrity and confidentiality to the transmissions. When an authorized administrator accesses the TOE remotely, he must first log into the system. A secure data transmission path is set up using the SSHield cryptographic capabilities and the SSH 2 compatible client on the workstation.

2.3.2.5 Redundancy

The Broadmore models have two –48V DC power supplies on the chassis of each model.[5]When the backup power supply is active and the active power supply fails, the Broadmore switches to the backup power supply. This is especially useful when the operating environment has two power sources that can be attached to the two power supplies.

Broadmore CPU, SAM, and/or NIM redundancy is provided by the midplane and CPU software of the corresponding model and is independent of the functionality of the CPU, NIM, or SAM.

The Broadmore 1750 and 1700 configurations have two optional, configurable redundancy features that serve to minimize system downtime. Redundancy options include the following:

The Central Processing Unit: The Broadmore 1750 and 1700 can have an online and a standby CPU. The CPUs are maintained in a consistent state so the standby can take over processing from a failing on-line CPU.

The Network Interface Modules: There can be two identical NIMs in the Broadmore 1750 or 1700. As with the redundant CPUs, the standby NIM can take over processing from a failing, online NIM. The automatic protection switching (APS) mechanism is configured to define the activities of the two NIMs after the failing part is repaired.

On the Broadmore 1750 configuration, an optional SAM may be configured to provide protection to up to four similar SAMs with a single “spare part” called a protection SAM. If one of the identified SAMs fails,

[5] . A stand-alone A/C converter chassis can be optionally connected to the 1700 and 1750 that can include either one or two independent A/C converters. On the 500, either or both of the DC supplies can be removed and exchanged for A/C converters that are housed inside the 500 chassis (but the -48 VDC inputs still exist). The A/C converters and use of the A/C power supply are not a part of the TOE.

the protection SAM can take over for the failing SAM.

2.3.3 Items not claimed in the TOE

- Local Console and VT100 emulator code
- Remote management workstation and secure client emulator/replacement software
- SecurID server hardware and software
- SecurID enabled mode of operation
- NIMs and the SAMs
- FTP
- SNMP
- Static Routes

2.3.4 Configurations not claimed in the TOE

- Running in non-FIPS mode
- Running the model 1750 with SAM redundancy disabled.

3 TOE Security Environment

This section contains assumptions regarding the security environment and the intended usage of the TOE.

3.1 Assumptions

The following conditions are assumed to exist in the operational environment. The assumptions are categorized into two groups: Personnel Assumptions and Physical Environment Assumptions.

3.1.1 Personnel Assumptions

A.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

3.1.2 Physical Environment Assumptions

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

A.PHYSEC The TOE hardware and software critical to the TOE will be protected from unauthorized physical modification.

3.2 Threats

The following are threats identified for the TOE. The assumed level of expertise of the attacker for all the threats is *unsophisticated*. The threat agents are users authorized to use the TOE as well as unauthorized persons or external IT entities not authorized to use the TOE.

3.2.1 Threats Addressed by the TOE

The TOE addresses the threats discussed below. The assumed level of expertise of the attacker for all threats is unsophisticated.

T.NOACCT Users may not be accountable for actions they perform that violate the security policies of the TOE because there is no record of their security relevant actions.

T.AUDPROT A user or process may cause audit records to be lost or modified, thus masking a user’s action.

T.NOAUTH An unauthorized person may attempt to bypass the security of the TOE in order to access and use security functions provided by the TOE.

T.PROCOM An unauthorized user may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.

T.PRODAT An unauthorized user may read, modify, or destroy security critical TOE configuration data.

T.POWFAIL Failure of the active power supply may cause denial or delay of service

The following threat applies only to Broadmore models 1750 and 1700 with redundant CPU and/or NIM cards.

T.CRDFAIL For Broadmore models 1750 and 1700 with redundant CPU and/or NIM cards, hardware component failure related to the CPU or NIM cards may cause denial or delay of service.

The following threat applies only to Broadmore models 1750 with a redundant SAM card.

T.SAMFAIL For Broadmore model 1750 with a protection SAM card, hardware component failure related to a protected SAM card may cause denial or delay of service.

3.2.2 Threats Addressed by Operating Environment

TE.TUSAGE The TOE may be inadvertently configured, used, and administered in an insecure manner by either authorized or unauthorized persons.

TE.CONSOLE The console fails to display and/or transmit information correctly causing unpredictable results.

TE.RMTRM The remote workstation fails to work securely allowing an unauthorized user to view, modify, and/or delete security related information that is intended for transmission to the TOE.

3.3 Organizational Security Policies

This ST has no Organizational Security Policies.

4 Security Objectives

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

4.1 Security Objectives For The TOE

The following are the IT security objectives for the TOE:

O.AUDACC The TOE must provide a means to record an audit trail of security related events, with accurate dates and times.

O.AUDPROT The TOE must provide the capability to protect the audit records from unauthorized access, modification, or deletion.

O.PRODAT The TOE must protect the confidentiality and integrity of TOE data in storage or in transit.

O.ENCRYP The TOE must protect the confidentiality and integrity of its dialogue with an authorized administrator using a remote connection.

O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.

O.SECFUN The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.

O.SLFPRO The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

O. RDDPOW The TOE must be able to support a redundant power supply with automatic failover.

The following objectives apply to the Broadmore 1750 and 1700 model only:

O.RDDCPU Broadmore models 1750 and 1700 must be able to provide an option for CPU redundancy with automatic failover.

O.RDDNIM The Broadmore models 1750 and 1700 must be able to provide an option for NIM redundancy with automatic failover.

The following objective applies to the 1750 model only

O.RDDSAM The Broadmore models 1750 must be able to provide a configurable option for SAM redundancy with failover.

4.2 Security Objectives For The Environment

The following objectives address non-IT issues that are satisfied by procedural or administrative means, as well as IT objectives addressed by the TOE Environment.

OE.CONSOLE The console must display and/or transmit information correctly

OE.RMTRM The remote workstation must work securely providing transmission of reliable data

OE.ADMTRA Authorized administrators are trained regarding establishment and maintenance of security policies and practices.

OE.GUIDAN The TOE must be delivered, installed, administered, and operated in a manner that maintains security.

OE.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

OE.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

OE.PHYSEC The TOE hardware and software critical to the TOE will be protected from unauthorized physical modification.

4.3 Security Objectives Rationale

4.3.1 Tracing for Objectives

The following table demonstrates that all security objectives for the TOE trace to aspects of the identified threats to be countered by the TOE, and that all objectives for the TOE environment map to threats or assumptions about the environment.

	T.NOACCT	T.AUDPROT	T.NOAUTH	T.PROCOM	T.PRODAT	T.POWFAIL	T.CRDFAIL	T.SAMFAIL	TE.CONSOLE	TE.RMTRM	TE.TUSAGE	A.NOEVIL	A.LOCATE	A.PHYSEC
O.AUDACC	x													
O.AUDPROT		x												
O.PRODAT				x	x									
O.ENCRYP				x										
O.IDAUTH			x											
O.SECFUN			x											
O.SLFPRO			x											
O.RDDPOW			x			x								
O.RDDCPU			x				x							
O.RDDNIM			x				x							
O.RDDSAM			x					x						
OE.CONSOLE									x					
OE.RMTRM										x				
OE.ADMTRA											x			
OE.GUIDAN											x			

	T.NOACCT	T.AUDPROT	T.NOAUTH	T.PROCOM	T.PRODAT	T.POWFAIL	T.CRDFAIL	T.SAMFAIL	TE.CONSOLE	TE.RMTRM	TE.TUSAGE	A.NOEVIL	A.LOCATE	A.PHYSEC
OE.NOEVIL												x		
OE.LOCATE													x	
OE.PHYSEC														x

Table 4-1: Objectives Mappings

4.3.2 Security Objectives Rationale: Threats to the TOE

T.NOACCT

Users may not be accountable for actions they perform that violate the security policies of the TOE because there is no record of their security relevant actions.

This threat is met by objective O.AUDACC, which requires an audit trail of events identifying the user, the event, and the date and time of the event.

T.AUDPROT

A user or process may cause audit records to be lost or modified, thus masking a user's action.

This threat is met by the objective O.AUDPROT, which requires that the TOE protect audit records from unauthorized access, modification, or deletion.

T.NOAUTH

An unauthorized person may attempt to bypass the security of the TOE in order to access and use security functions provided by the TOE.

This threat is mitigated by O.IDAUTH, O.SECFUN, and O.SLFPRO. O.IDAUTH requires each user to be identified and authenticated prior to using the TOE. O.SECFUN stipulates appropriate security functions and appropriate controls on their use, providing protection from bypass O.SLFPRO requires the TOE to protect itself from bypass, deactivation, and tampering of the security functions.

If the TOE is connected to two power supplies, the threat mitigation is contributed to by O.RDDPOW, which provides automatic failover should one supply source fail. This provides a change of power source without interrupting operation, protecting from inadvertent or intentional bypass of security functions.

For models 1700 and 1750, if the redundant CPU or redundant NIM options are selected, the threat is further contributed to by O.RDDCPU and O.RDDNIM, respectively. These objectives provide for automatic failover of the CPU and/or NIM. This provides a change of a CPU (a NIM) without interrupting operation, protecting from inadvertent or intentional bypass of security functions.

Finally, for model 1750, if the redundant SAM option is selected, O.RDDSAM further contributes to mitigation of this threat by providing failover for the SAM. This provides a change of a SAM without interrupting operation, protecting from inadvertent or intentional bypass of security functions.

T.PROCOM An unauthorized user may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.

This threat is met by O.ENCRYP, which requires that data transmission between an authorized administrator using a remote connection must be encrypted and by O.PRODAT, which requires that the TOE protect confidential TOE data in transit.

T.PRODAT An unauthorized user may read, modify, or destroy security critical TOE configuration data.

This treat is mitigated by the objective O.PRODAT, which requires the TOE to protect the confidentiality and integrity of TOE data in storage or in transit.

T.POWFAIL Failure of the active power supply when the backup power supply is still active may cause denial or delay of service.

This threat is met by the objective O.RDDPOW, which requires the TOE to provide a redundant power supply and automatic failover.

T.CRDFAIL For Broadmore models 1750 and 1700 with redundant CPU and/or NIM cards, hardware component failure related to the CPU or NIM cards may cause denial or delay of service.

This threat is met by the objective O.RDDCPU and O.RDDNIM, which require the TOE to provide an option for a redundant CPU or NIM and automatic failover.

T.SAMFAIL For Broadmore model 1750 with a protection SAM card, hardware component failure related to a protected SAM card may cause denial or delay of service.

This threat is met by the objective O.RDDSAM, which requires the TOE to provide an option for a redundant SAM and failover.

4.3.3 Security Objectives Rationale: Threats to the TOE Environment

TE.TUSAGE The TOE may be inadvertently configured, used, and administered in an insecure manner by either authorized or unauthorized persons.

This threat is met by objectives OE.GUIDAN and OE. ADMTRA, which require that administrators be appropriately trained and the administrator guidance be provided that describes the secure and correct operation of the TOE.

TE.CONSOLE The console fails to display and/or transmit information correctly causing unpredictable results.

This threat is met by the objective OE.CONSOLE, which requires that the console support reliable and correct transmission and data display.

TE.RMTRM The remote workstation fails to work securely allowing an unauthorized person or unauthorized user to view, modify, and/or delete security related information that is intended for transmission to the TOE.

This threat is met by the objective OE.RMTRM, which requires that the remote terminal support reliable and correct transmission and data display.

4.3.4 Security Objectives Rationale: Assumptions

The three assumptions, A.NOEVIL, A.LOCATE, and A.PHYSEC, map to objectives for the environment that have matching names, OE.NOEVIL, OE.LOCATE, and OE.PHYSEC. Each assumption and its matching objective for the environment have identical text, and therefore no further rationale is necessary.

4.3.5 Security Objectives Rationale: Organizational Security Policies

There are no organizational security policies in this ST.

5 IT Security Requirements

This section provides functional and assurance requirements for this Security Target (ST). These requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL3) containing assurance components from Part 3 of the CC. Note that there are no security functional requirements defined for the IT environment.

5.1 TOE Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC.

Security Functional Requirement	**Name of requirement**
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_STG.1	Protected audit trail storage
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_UAU.1 [a], [b]	Timing of authentication
FIA_UID.1 [a], [b]	Timing of identification
FMT_MOF.1	Management of security functions behavior
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_FLS.1 [a], [b], [c]	Failure with preservation of secure state
FPT_ITC.1	Inter-TSF confidentiality during transmission
FPT_ITI.1	Inter-TSF detection of modification
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation
FPT_STM.1	Reliable time stamps
FRU_FLT.1 [a], [b], [c]	Degraded fault tolerance

Table 5-1: Security Functional Requirements for the TOE

5.1.1 Security Audit (FAU)

5.1.1.1 FAU_GEN.1 Audit data generation[6]

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [not specified] level of audit; and

c) [

- **Modification of the groups of users that are part of the role definition for authorized administrators**
- **Modifications to the system clock**
- **Successful logon attempts**
- **Every third consecutive unsuccessful login attempt on each physical login interface to the Broadmore device.**
- **Changes made in a user's security attributes].**

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, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**network ports or local console connection associated with the event for all auditable event types.**]

5.1.1.2 FAU_SAR.1 Audit review

.FAU_SAR.1.1 The TSF shall provide [**Super_User**] with the capability to read [**any audit information**] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.1.3 FAU_SAR.2 Restricted audit review

.FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.1.1.4 FAU_STG.1 Protected audit trail storage

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

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

[6] This function is used consistently with international interpretation 202, which requires one to select one of three options. The selection, when applied, does not show the change to the SFR.

5.1.2 Identification and Authentication (FIA)

5.1.2.1 FIA_AFL.1 Authentication failure handling[7]

FIA_AFL.1.1 The TSF shall detect when [**each third consecutive**] unsuccessful authentication attempt[~~***s]***~~occur[***s***] related to [**user authentication on each physical login interface to the Broadmore device**]**.**

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met ~~***or surpassed***~~, the TSF shall [**delay ten seconds then offer the login prompt again if the login is from the local console, or disconnect the session if the login is from a remote workstation**].

5.1.2.2 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**user ID, password, role, craft access, and remote access**].

5.1.2.3 FIA_UAU.1 [a] Timing of authentication: Local authentication

FIA_UAU1.1 [a] The TSF shall allow [**no TSF mediated actions**] on behalf of the user to be performed before the user is authenticated [***from the local console***].

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

5.1.2.4 FIA_UAU.1 [b] Timing of authentication: Remote authentication

FIA_UAU1.1 [b] The TSF shall allow [**negotiation of an SSHield session**] on behalf of the user to be performed before the user is authenticated [***from a remote location***].

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

5.1.2.5 FIA_UID.1 [a] Timing of identification: Local authentication

FIA_UID.1.1 [a] The TSF shall allow [**no TSF mediated actions**] on behalf of the user to be performed before the user is identified [***from the local console***].

FIA_UID.1.2 [a] The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.2.6 FIA_UID.1 [b] Timing of identification: Remote authentication

FIA_UID.1.1 [b] The TSF shall allow [**negotiation of an SSHield session**] on behalf of the user to be performed before the user is identified [***from a remote location***].

FIA_UID.1.2 [b] The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

[7] Changed to meet interpretation 111.

5.1.3 Security Management (FMT)

5.1.3.1 FMT_MOF.1 Management of security functions behavior[8]

FMT_MOF.1.1 The TSF shall restrict the ability to [determine the behavior of, disable, enable, modify the behavior of] the functions [**listed in column 1 of the table below**] to [**the authorized identified roles in column 2 of the table below**].

Function	**Authorized Roles**
Add, delete, or modify the security attributes described in FIA_ATD.1 for any user: role, craft access, and remote access; Add or delete User ID	**Super_User**
CPU Redundancy switchover request	**Super_User, SysAdmin**
Configure NIM redundancy	**Super_User, SysAdmin**
Enable or disable SAM redundancy	**Super_User, SysAdmin**
Configure SAM redundancy parameters if SAM redundancy is enabled	**All Roles**
Enable/disable FIPS mode	**Super_User**
Display or delete data using shell commands	**Super_User**
modify and set the time and date	**Super_User; SysAdmin**
Delete and review the audit trail; audit.txt **Delete and review the audit trail: syslogs**	**Super_User**
Review audit trail: syslog records to which the role has access	**All roles**
Modify personal password	**All Roles**
Connect to the TOE from a remote terminal running an OpenSSH compatible client	**All Roles**

5.1.3.2 FMT_MTD.1 Management of TSF data[9]

FMT_MTD.1.1 The TSF shall restrict the ability to [modify, delete, **view**] the [**TSF data listed in the first column of the table below**] to **[the authorized identified roles listed in**

[8] The list of dependencies has changed for this function as a result of international interpretation 065.

[9] The list of dependencies has changed for this function as a result of international interpretation 065.

column 2 of the table below.]

Data	Authorized Actions	Authorized Roles
Security attributes for any user as described in FIA_ATD.1	**Modify, delete, view**	**Super_User**
NIM redundancy parameters	**Modify**	**Super_User, SysAdmin**
SAM redundancy enable or disable	**Modify**	**Super_User, SysAdmin**
SAM redundancy parameters if SAM redundancy is enabled	**Modify**	**All Roles**
FIPS on/off parameter	**Modify, view**	**Super_User**
CPU Redundancy switchover request parameter	**Modify**	**Super_User, SysAdmin**
System time and date	**Modify**	**Super_User, SysAdmin**
Audit trail: audit.txt	**delete, view**	**Super_User**
Audit trail: syslogs	**view data to which the role has access**	**All roles**
Audit trail: syslogs	**Delete**	**Super_User**
Syslogs by role authorization	**view**	**All roles**
Personal Password	**Modify**	**All roles**

5.1.3.3 FMT_SMF.1 Specification of Management Functions[10]

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [**The security management functions described in column one of the table in section 5.1.3.1**].

5.1.3.4 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [**Super_User, SysAdmin, Operations, and Browser**].

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

[10] *Th*is function is in accordance with international interpretation 065.

5.1.4 Protection of the TSF (FPT)

5.1.4.1 FPT_FLS.1 [a] Failure with preservation of secure state: All TOE models

FPT_FLS 1.1 [a] The TSF shall preserve a secure state when the following types of failures occur: [**the active power supply fails and the backup power supply is live**].

5.1.4.2 FPT_FLS.1 [b] Failure with preservation of secure state: Models 1750 &1700

CONDITION: The following SFR applies to the Broadmore 1750 and 1700 versions only.

FPT_FLS 1.1 [b] The TSF shall preserve a secure state when the following types of failures occur: [**The TOE has a standby CPU card and the online CPU fails; The TOE has a standby NIM card and the online NIM fails**].

END CONDITION

5.1.4.3 FPT_FLS.1 [c] Failure with preservation of secure state: Model 1750 Only

CONDITION: The following SFR applies to the Broadmore 1750 version only.

FPT_FLS 1.1 [c] The TSF shall preserve a secure state when the following types of failures occur: [**The TOE has a protection SAM card that protects a set of up to 4 identical SAMs, and one of the protected SAMs fails**].

END CONDITION

5.1.4.4 FPT_ITC.1 Inter-TSF confidentiality during transmission

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorised disclosure during transmission.

5.1.4.5 FPT_ITI.1 Inter-TSF detection of modification

FPT_ITI 1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: [**at least one MAC error in SSH transmissions**].

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform [**a re-send of network packet(s) that caused the error**] if modifications are detected.

5.1.4.6 FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.4.7 FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.4.8 FPT_STM.1 Reliable time stamps

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

5.1.5 Resource Utilization (FRU)

5.1.5.1 FRU_FLT.1 [a] Degraded fault tolerance: all models

FRU_FLT.1.1 [a] The TSF shall ensure the operation of [**all operations**] when the following failures occur: [**the active power supply fails and the backup power supply is live**]**.**

5.1.5.2 FRU_FLT.1 [b] Degraded fault tolerance: Models 1750 and 1700 only

CONDITION: The following SFR applies to the Broadmore 1750 and 1700 models only

FRU_FLT.1.1 [b] The TSF shall ensure the operation of [**all operations]** when the following failures occur: [**The TOE has a standby CPU card and the online CPU fails; The TOE has a standby NIM card and the online NIM fails**]**.**

END CONDITION

5.1.5.3 FRU_FLT.1 [c] Degraded fault tolerance: Model 1750 only

CONDITION: The following SFR applies to the Broadmore 1750 models only

FRU_FLT.1.1 [c] The TSF shall ensure the operation of [**all operations**] when the following failures occur: [**The TOE has a protection SAM card that protects a set of up to 4 identical SAMs, and one of the protected SAMs fails**]**.**

END CONDITION

5.2 Security Requirements Rationale

5.2.1 TOE Requirements to Objectives Tracing

Security Functional Requirement	O.AUDACC	O.AUDPROT	O.PRODAT	O.ENCRYP	O.IDAUTH	O.SECFUN	O.SLFPRO	O.RDDPOW	O.RDDCPU	O.RDDNIM	O.RDDSAM
FAU_GEN.1	X										
FAU_SAR.1	X	X									
FAU_SAR.2		X									
FAU_STG.1		X									
FIA_AFL.1					X						
FIA_ATD.1					X						

Security Functional Requirement	O.AUDACC	O.AUDPROT	O.PRODAT	O.ENCRYP	O.IDAUTH	O.SECFUN	O.SLFPRO	O.RDDPOW	O.RDDCPU	O.RDDNIM	O.RDDSAM
FIA_UAU.1 [a] & [b]					X						
FIA_UID.1 [a] & [b]					X						
FMT_MOF.1			x			X					
FMT_MTD.1			X			X					
FMT_SMF.1			x			X					
FMT_SMR.1			x			X					
FPT_FLS.1 [a]								X			
FPT_FLS.1 [b]									X	X	
FPT_FLS.1 [c]											X
FPT_ITC.1		x	X	X							
FPT_ITI.1		x	X	X							
FPT_RVM.1							X				
FPT_SEP.1							X				
FPT_STM.1	X										
FRU_FLT.1 [a]								X			
FRU_FLT.1 [b]									X	X	
FRU_FLT.1 [c]											X

Table 5-2: TOE security functional requirements to objectives mapping

5.2.2 Rationale for Security Requirements on the TOE.

O.AUDACC The TOE must provide a means to record an audit trail of security related events, with accurate dates and times.

This objective is met by the following SFR: FAU_GEN.1, FAU_SAR.1. FAU_GEN.1 requires the existence of an auditing function and identifies the events to be audited. FAU_GEN.1 describes the specific information, such as date, time, that must be recorded in the audit records. FAU_SAR.1 requires a readable audit trail of events. FPT_STM.1 requires reliable time stamps.

O.AUDPROT The TOE must provide the capability to protect the audit records from unauthorized access, modification, or deletion.

This objective is met by the following SFR: FPT_ITC.1, FPT_ITI.1, FAU_SAR.1, FAU_SAR.2, and FAU_STG.1. FPT_ITC.1 and FPT_ITI.1 protect the confidentiality and integrity of audit data in transit between the TOE and the remote management workstation.FAU_SAR.1 provides authorized users the capability to review the audit logs and FAU_SAR.2 restricts access to those who have been granted read access. FAU_STG.1 requires that audit logs be protected from unauthorized deletion and modification.

O.ENCRYP The TOE must protect the confidentiality and integrity of its dialogue with an authorized administrator using a remote connection.

This objective is met by the following SFR: FPT_ITC.1 and FPT_ITI.1. FPT_ITC.1 requires that data in transit be protected for confidentiality and FPT_ITI.1 requires that data in transit be protected for integrity. .

O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.

This objective is met by the following SFR: FIA_ATD.1, FIA_UAU.1 [a], FIA_UAU.1 [b], FIA_UID.1 [a], and FAU_UID.1 [b], FIA_AFL.1. FIA_ATD.1 identifies the security attributes that are stored in the TOE and used for identification and authentication. FIA_UID.1 [a] and FIA_UAU.1 [a] contribute to meeting this objective by providing the rules for identification and authentication from the local console. FIA_UID.1 [b] and FIA_UAU.1 [b] contribute to meeting this objective by providing the rules for identification and authentication from a remote location. FIA_AFL.1 supports this objective by deterring multiple login attempts (password guessing).

O.PRODAT The TOE must protect the confidentiality and integrity of TOE data in storage or in transit.

This objective is met by the following SFR: FPT-ITC.1, FPT_ITI.1, FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1. FPT_ITC.1 and FPT_ITI.1 protect the confidentiality and integrity of data in transit. Data in storage is protected by role enforcement. FMT_SMR.1 defines the roles that are the basis for role enforcement of the functions identified by FMT_SMF.1. FMT_MOF.1 describes the restrictions on the use of these functions, by role and by type of use. FMT_MTD.1 contributes to this objective by describing the restrictions on access to TSF data by role and by type of access.

O.SECFUN The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.

This objective is met by the following SFR: FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, and FMT_SMR.1. FMT_SMR.1 defines the roles that are the basis for role enforcement of the functions identified by FMT_SMF.1. FMT_MOF.1 describes the restrictions on the use of these functions, by role and by type of use. FMT_MTD.1 contributes to this objective by describing the restrictions on access to TSF data by role and by type of access.

O.SLFPRO The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

This objective is met by the following SFR: FPT_RVM.1, FPT_SEP.1. FPT_RVM.1 require that the TOE protect itself from bypass of enforcement functions. FPT_SEP.1 requires that the TOE provide a protection domain.

O. RDDPOW The TOE must be able to support a redundant power supply with automatic failover.

This objective is met by the following SFR: FPT_FLS.1 [a] and FRU_FLT.1 [a]. FPT_FLS.1 [a] ensures that when two power supplies are used and the active supply fails, the secondary or backup supply takes over with preservation of a secure state. FRU_FLT.1 [a] ensures operation of all functions when the power source failure occurs for the active power supply.

O.RDDCPU The TOE must be able to provide a configurable option for CPU redundancy with automatic failover.

This objective is met by the following SFR: FPT_FLS.1 [b] and FRU_FLT.1 [b]. When the TOE is configured with a redundant CPU, and the online CPU fails, FPT_FLS.1 [b] ensures that the standby CPU takes over with preservation of a secure state. FRU_FLT.1 [b] ensures continued operation of all functions when the CPU failure occurs.

O.RDDNIM The TOE must be able to provide a configurable option for NIM redundancy with automatic failover.

This objective is met by the following SFR: FPT_FLS.1 [b] and FRU_FLT.1 [b]. When the TOE is configured with a redundant NIM, and the online NIM fails, FPT_FLS.1 [b] ensures that the standby NIM takes over with preservation of a secure state. FRU_FLT.1 [b] ensures continued operation of all functions when the NIM failure occurs.

O.RDDSAM The TOE must be able to provide a configurable option for SAM redundancy with failover.

This objective is met by the following SFR: FPT_FLS.1 [c] and FRU_FLT.1 [c]. When the TOE is configured with a protection SAM, and one of the protected SAMs fails, FPT_FLS.1 [c] ensures that the protection SAM takes over with preservation of a secure state. FRU_FLT.1 [c] ensures continued operation of all functions when the SAM failure occurs.

5.2.3 Rationale For Security Requirements on the IT Environment

There are no security functional requirements defined for the IT environment.

5.2.4 Rationale For Security Requirement Dependencies

The following table lists all the SFR dependencies with a note as to whether or not the dependency is satisfied.

Security Functional	**Dependencies**	**Dependency Met?**
FAU_GEN.1	FPT_STM.1	Yes
FAU_SAR.1	FAU_GEN.1	Yes
FAU_SAR.2	FAU_SAR.1	Yes
FAU_STG.1	FAU_GEN.1	Yes
FIA_AFL.1	FIA_UAU.1	Yes
FIA_ATD.1	none	Yes

Security Functional	Dependencies	Dependency Met?
FIA_UAU.1	FIA_UID.1	Yes
FIA_UID.1	none	Yes
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	Yes
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	Yes
FMT_SMF.1	None	Yes
FMT_SMR.1	FIA_UID.1	Yes
FPT_FLS.1 [a], [b], & [c]	ADV_SPM.1	No*
FPT_ITC.1	None	Yes
FPT_ITI.1	None	Yes
FPT_RVM.1	None	Yes
FPT_SEP.1	none	Yes
FPT_STM.1	None	Yes
FRU_FLT.1 [a], [b], & [c]	FPT_FLS.1	Yes

Table 5-3: Dependencies mapping

The following dependencies that are not met: the dependencies of FPT_FLS.1 [a], [b], and [c] on ADV_SPM.1.

- FPT_FLS.1 requires the preservation of a secure state, and as such, depends on ADV_SPM.1 to provide a definition of the secure state. In the Broadmore, state elements are on the CPU board, the SAM cards, and the NIM cards. FPT_FLS.1 [a]: The change of power supply does not impact the state of the system as all the state elements are on the CPU, SAM, and NIM cards. FPT_FLS.1 [b]: The two CPUs are kept synchronized so if the standby CPU takes over the online CPU role, the state defined in this functionality is preserved (regardless of its definition). The same argument applies for the NIM module replacements. The replacements are identical, and they are also hot swappable, thus the state contained in the NIM remains constant over failure and replacement. FPT_FLS.1 [c]: a similar argument holds for the protection SAM as for the duplicate NIM or CPU described above. The replacement part is identical to that which is being replaced, so the state elements it contains are not altered.

5.2.5 Security Requirements Rationale

The requirements selected for this TOE are internally consistent and mutually supportive. The ST includes security functional requirements that address the security functionality provided by the TOE, with no contradictory requirements. All operations performed on the security requirements comply with the rules and intent required by the operation in the CC.

The selected requirements together form a mutually supportive whole by:

- satisfying all dependencies as demonstrated in Table 5-3.
- tracing security functional requirements to security objectives and justifying that tracing as demonstrated in Section 5.2.2
- including the SFRs FPT_RVM.1 and FPT_SEP.1 as appropriate on the TOE to protect the TSF

- including audit requirements to detect security-related actions and potential attacks
- including security management requirements to ensure that the TOE is managed and configured securely.

5.2.6 SOF Claim and Rationale for Security Functional Requirements

The minimum strength level for the TOE security functions realized by a probabilistic or permutational mechanism is SOF-basic. Specific strength of function claims apply to the following requirements:

FIA_UAU.1 (a) Strength of Function shall be demonstrated such that the probability that authentication data can be guessed is no greater than one in one million.

FIA_UAU.1 (b) Strength of Function shall be demonstrated such that the probability that authentication data can be guessed is no greater than one in one million.

The rationale for the chosen level of SOF-basic is based on the low attack potential of the threat agents identified. The evaluated TOE is intended to operate in commercial and DoD low robustness environments processing unclassified information. The strength of function is in turn consistent with the security objectives described in section 4 of this document.

The authentication mechanisms and the cryptographic algorithms are the only security function realized by a probabilistic or permutational security mechanism. Cryptographic mechanisms do not require an SOF claim. Therefore, the password authentication mechanism used for FIA_UAU.1 [a] and [b] is the only relevant security function realized by a probabilistic or permutational security mechanism.

The minimum password length for users and administrators is 6 characters and the maximum length is 9 characters (with a character set of at least 94 characters). The rationale for choosing SOF-basic is based on a low-to-moderate attack potential for the threats defined in this ST. The security objectives provide probabilistic security mechanisms and the strength of function claim is satisfied by the password management features provided by the TOE.

5.3 TOE Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 3 (EAL3) as defined by the CC with no augmentation. The assurance components are summarized in the following table.

Assurance Class	**Assurance Components**	
ACM: Configuration management	ACM_CAP.3	Authorisation controls
	ACM_SCP.1	TOE CM coverage
ADO: Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1	Informal functional specification
	ADV.HLD.2	Security enforcing high level design

Assurance Class	Assurance Components	
	ADV_RCR.1	Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
ALC: Life cycle support	ALC_DVS.1	Identification of security measures
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_MSU.1	Examination of guidance
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

Table 5-4: Security Assurance Requirements

5.3.1 Configuration Management (ACM)

5.3.1.1 ACM_CAP.3 Authorization controls

Developer action elements:

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

ACM_CAP.3.2D The developer shall use a CM system.

ACM_CAP.3.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

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

ACM_CAP.3.2C The TOE shall be labeled with its reference.

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

ACM_CAP.3.XC The configuration list shall uniquely identify all configuration items that comprise the TOE.[11]

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

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

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

[11] This component was added to comply with international interpretation 003.

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

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

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

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

Evaluator action elements:

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

5.3.1.2 ACM_SCP.1 TOE CM coverage

Developer action elements:[12]

ACM_SCP.1.1D The developer shall provide a list of configuration items for the TOE.

Content and presentation of evidence elements[13].

ACM_SCP.1.1C The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST.

Evaluator action elements

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

5.3.2 Delivery and Operation (ADO)

5.3.2.1 ADO_DEL.1 Delivery procedures

Developer action elements:

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

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

Content and presentation of evidence elements:

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

[12] The element is changed as a result of Interpretation 004.

[13] The content and presentation of evidence elements are replaced as a result of Interpretations 004 and 038.

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

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

Developer action elements:

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

Content and presentation of evidence elements:

ADO_IGS.1.1C The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation, and start-up of the TOE. [14]

Evaluator action elements:

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

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

5.3.3 Development (ADV)

5.3.3.1 ADV_FSP.1 Informal Functional Specification

Developer action elements:

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

Content and presentation of evidence elements:

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

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

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

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

Evaluator action elements:

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

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

[14] This component was modified to comply with international interpretation 051.

5.3.3.2 ADV_HLD.2 Security enforcing High-Level Design

Developer action elements:

ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.2.1C The presentation of the high-level design shall be informal.

ADV_HLD.2.2C The high-level design shall be internally consistent.

ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

Evaluator action elements:

ADV_HLD.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.2.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security requirements.

5.3.3.3 ADV_RCR.1 Informal Correspondence Demonstration

Developer action elements:

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

Content and presentation of evidence elements:

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

Evaluator action elements:

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

5.3.4 Guidance Documents (AGD)

5.3.4.1 AGD_ADM.1 Administrator Guidance

Developer action elements:

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

Content and presentation of evidence elements:

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

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

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

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

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

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

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

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

Evaluator action elements:

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

5.3.4.2 AGD_USR.1 User Guidance

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

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

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

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

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

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

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

Evaluator action elements:

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

5.3.5 Life cycle support (ALC)

5.3.5.1 ALC_DVS.1 Identification of security measures

Developer action elements

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

Content and presentation of evidence elements

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

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

Evaluator action elements

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

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

5.3.6 Tests (ATE)

5.3.6.1 ATE_COV.2 Analysis of coverage

Developer action elements:

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation of evidence elements:

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

Evaluator action elements:

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.2 ATE_DPT.1 Testing: high-level design

Developer action elements

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

Content and presentation of evidence elements

ATE_DPT.1.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

Evaluator action elements

ATE_DPT.1.2E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.3 ATE_FUN.1 Functional Testing

Developer action elements:

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

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

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

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

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

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

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

Evaluator action elements:

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

5.3.6.4 ATE_IND.2 Independent testing - sample

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.7 Vulnerability Assessment (AVA)

5.3.7.1 AVA_MSU.1 Examination of guidance

Developer action elements

AVA_MSU.1.1D The developer shall provide guidance documentation.

Content and presentation of evidence elements

AVA_MSU.1.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.1.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.1.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.1.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

Evaluator action elements

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

AVA_MSU.1.2E The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.1.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

5.3.7.2 AVA_SOF.1 Strength Of TOE Security Function Evaluation

Developer action elements:

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

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level ***SOF-Basic.***

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric ***SOF-Basic.***

Evaluator action elements:

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

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

5.3.7.3 AVA_VLA.1 Developer Vulnerability Analysis

Developer action elements:[15]

AVA_VLA.1.1D The developer shall perform a vulnerability analysis.

AVA_VLA.1.2D The developer shall provide vulnerability analysis documentation.

Content and presentation of evidence elements:[16]

AVA_VLA.1.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2C The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

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

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

[15] These elements have been modified to comply with interpretation 051.

[16] These elements have been modified to comply with interpretation 051.

5.4 Assurance Requirements Rationale

EAL3 was chosen to provide a moderate level of assurance that is consistent with good commercial practices. The chosen assurance level is appropriate with the threats defined for the environment. At EAL3, the TOE will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

6 TOE Summary Specification

6.1 TOE Security Functions

6.1.1 Audit

The TOE auditing function is distributed throughout the TOE and provides the following functionality:

Audit Data Generation	Audit data is collected by the Broadmore auditing function.
Audit data Review	Audit data review is provided by special commands that allow a Super_User to view the beginning of a file, the end of a file, or entire file.
Audit data storage and protection	Audit data is stored in the TOE and protected by role enforcement. Measures are taken to address auditing in the event of audit data storage exhaustion.

6.1.1.1 Audit Data Generation

FAU_GEN.1.1: The audit trail consists of the audit records found in a special audit file, audit.txt, and in the system logs.

Note that each syslog record is marked with the roles that are authorized to view that record. Audit data collected by the system logs includes the following list of events;

- Start-up and shutdown of the OS syslogs. Note that the syslogs are started up when the system is started up and shut down when the system is shut down. Thus the audit records associated with starting up and shutting down the syslogs are the same records as those that describe starting up and shutting down the Broadmore system.
- Successful logon attempts
- Every third consecutive unsuccessful login attempt on each physical login interface to the Broadmore device.Modifications to the system clock.

The following audit data is collected by the TOE in the file audit.txt.

- Start-up and shutdown of the audit functions that collect data into the file audit.txt;
- Modification of the groups of users that are part of the role definition for authorized administrators
- Changes made in a user’s security attributes

FAU_GEN.1.2: The audit.txt and syslog records include the date and time of the event recorded, the event type, the relevant subject for the audit event., and the outcome of the event is recorded in terms of success or failure. Note that for audit records stored in the syslogs, the relevant subject identifier is the CPU slot letter, and for records in audit.txt, it is the user name. For identification and authentication attempts to the TOE both the user identity and the location of the attempted access (remote or via local console) are recorded in the log record.

6.1.1.2 Security Audit review

FAU_SAR.1, FAU_SAR.2: the TOE provides for audit review by allowing appropriately authorized users read access to the audit files and prohibits unauthorized personnel from having this access. This is accomplished by the *head, cat,* and *tail* [17] commands which provide the ability to view the log files. Only Super_User can view the audit.txt files. Access to syslog files is controlled by role enforcement, on a per-record basis. The embedded operating system creates each syslog entry with a field that indicates what roles have access to viewing it. All users can view the syslog (Super_User, SysAdmin, Operations and Browser), however only lines for which they have privilege to will be displayed. Note also that display commands are disabled for all files except for the audit data files.

6.1.1.3 Audit Data Storage and Protection

Audit logs are managed with rotating buffers of a fixed size, and when a buffer is full, the administrator is notified and appropriate action can be taken to preserve audit records.

The TOE can prevent unauthorized viewing, deletion, or modification of the audit trail and takes specific measures in event of audit trail storage exhaustion. Prevention of unauthorized viewing is described above.

FAU_STG.1.1: Only Super_User is able to delete audit.txt or the syslogs.

FAU_STG.1.2: The TOE prevents unauthorized modification to the audit logs by role enforcement. Only Super_User can access audit.txt in any way, only Super_User can modify the audit data in the syslogs, and the only type of modification that is allowed is deletion. While Super_Users have the privilege to use pSH commands that can overwrite audit.txt and system logs, this use is strictly prohibited by administrative guidance.

6.1.1.4 Reliable Time Stamps

FPT_STM.1: The TOE provides a real-time clock installed on the motherboard. The Operating system supports a clock driver to access the clock and provide consistent time stamps for all audit data.

6.1.2 Identification and Authentication

The Broadmore offers several identification and authentication features. They are identified briefly below.

Identification and authentication	The TOE requires identification and authentication before allowing any actions to be taken on behalf of the user (with the exception of negotiation of a remote session for remote logins).
Authentication failure handling	The TOE has authentication failure handling

6.1.2.1 Identification and Authentication

A user can log into the Broadmore from the local console or via a remote connection. Only one user is allowed to log into the TOE at a time. Recall that the Broadmore uses and embedded OS, so there is a single image and a single login capability provided by the combined OS and application.

FIA_ATD.1: Users are identified and authenticated based on login names and passwords. Login names and hashed versions of passwords are stored locally on the TOE. Other user attributes stored in the TOE include the craft access and remote access parameters, which determine if a user is allowed to access the TOE via the local console (Craft access enabled) or via a remote networked connection (remote

[17] The “head” command allows a user to view a specified number of lines from the beginning of a file. The “tail” command allows the user to view a specified number of lines from the end of a file. The “cat” command allows a user to view a whole file.

access enabled).

Once a user has been identified and authenticated, a role is associated with the user's session. The role is set when the user account is created. Only Super_Users can add, delete, or modify user accounts. Only Super_Users can modify the roles and privilege levels assigned to an individual account. See section 6.1.3.1 for details on roles and role management.

For the Broadmore TOE, a password is a string of characters based on the 94 printable and readable characters on a standard keyboard. This includes all upper an lower case alphabetic characters, the digits 0 through 9, and the special characters ` ~ ! @ # $ % ^ & * ( ) _ +- = [ ] \ { } |; ‘ , . / : “ < > ?. The minimum length of the password is settable by a Super_User, but cannot be any less than six characters. The maximum password length is 9 characters.

FIA_UAU.1 [a] and [b], FIA_UID.1 [a] and [b]:

All users must be identified and authenticated by the TOE. If the user is attempting to log in remotely, the SSHield module must negotiate an SSH session with the remote user before identification and authentication can take place. If the user is logging in locally there is no need for SSH and there are no actions taken prior to identification and authentication. Users attempting to log in via the craft port to the local console must have craft access enabled, or the login will fail. Users attempting to log in remotely must have remote access enabled, or the login will fail. In either case, identification is performed using login names and authentication is performed using password verification.

Note that the password authentication mechanism used for FIA_UAU.1 [a] and [b], is realized by a probabilistic or permutational security mechanism. The minimum password length for users and administrators is 6 characters (with a character set of at least 94 characters), which meets the SOF claim of SOF-basic.

6.1.2.2 Authentication Failure Handling

FIA_AFL.1: The Broadmore login functionality contains a login attempt threshold of three consecutive failed login attempts per physical login interface. For a user connected to the local console via one of the two craft ports, after every third consecutive failed login attempt from that port, the TOE pauses for ten seconds before offering the login prompt again. For a user connected via a remote workstation, when a third consecutive unsuccessful login is detected, there is a ten second delay then the remote connection is broken. This limits the number of brute force login attempts that can be made within a small amount of time.

6.1.3 Security Management

The security management features of the TOE are as follows:

Definition and management of security roles	These roles are used to enforce restrictions of access to functions and data.
Definition and management of security functions	These features identify the management functions required for the TOE and how their use is controlled.
Management of TSF data	These functions manage data that is necessary for the TOE to perform its security functions.

6.1.3.1 Roles

FMT_SMR.1: The TOE supports the following roles; Browser, Operations, SysAdmin, Super_User. All users of the Broadmore are authorized administrators. There are two basic roles, Admin User and Crypto Officer. The Admin User role is further subdivided into Browser, Operations, and SysAdmin, which are called "privilege levels" in the Broadmore documentation. The Crypto Officer role is available only to the Super_User. Because these two names are synonymous, the term Crypto_officer is not used in this Security Target. Access is controlled by role enforcement based on the role of the user. Only users with the Super_User privilege (also called Crypto Role) can change user accounts, including changes to the role assigned to a user. The following table provides samples of the tasks the roles can perform[18].

Admin User[19]	Browser	User is able to look at most all data plane information (current configurations, statistics, and system logs) but is not able to affect anything. To protect security data, no file access is permitted. This role cannot access the security settings.
	Operations	Operations can do everything a Browser can do, as well as connection management and module configuration. This user is able to perform data plane configurations, such as defining PVCs, SVCs, configuring service card parameters. To protect security data, no file access is permitted under this privilege level. This role cannot access the security settings.
	SysAdmin	SysAdmins can do everything Operations can do. This user is able to perform global configuration operations such as redundancy. To protect security data, no file access is permitted. This role cannot access the security settings.
Crypto Officer	Super_User	Super_Users can do everything a SysAdmin can do, as well as the following: This role is required to manage system accounts (add, delete, modify user accounts, including setting/modifying roles and privilege levels), and alter security settings, card diagnostics, system test, and security relevant actions. Security relevant actions include viewing audit logs and audit data in the syslogs, displaying data using shell commands, changing files using shell commands, management of user accounts, and zeroizing. Only users at this privilege level may turn FIPS mode on or off (disallowed by the TOE administrator guidance).

The TOE restricts access to security relevant functions by role enforcement. TSF data is also protected from unauthorized access by role enforcement.

[18] Note that no attempt is made here to provide an exhaustive list of tasks that can be performed by various roles.

[19] Note that in other Carrier Access documentation, the role "Admin User" is simply called "user". It is presented as "Admin User" in the ST to distinguish it from the use of the term "user" in a generic sense.

All users can change their own passwords, connect to the system remotely via the SSH 2 compatible client, view syslog information that is accessible to their role, and view environmental indicators.

6.1.3.2 Definition and Management of TSF Functions

The embedded operating system includes the Communication Access Multiplexer Management Interface (CAMMI) for local management of the Broadmore through a series of easy-to-use windows and pull-down menus. A Command Line Interface (CLI) feature is also provided. Access to all CAMMI windows and all commands is restricted by role enforcement.

FMT_SMF.1 and FMT_MOF.1: As described in section 5, the TOE defines the management functions and the users as indicated below are authorized to access them. The table of functions and their respective authorizations are found in section 5.1.3.1. Note that the TOE requires that the system be run in FIPS mode. While it is physically possible to switch to a non-FIPS mode, this is forbidden by administrator guidance when running in the evaluated configuration.

6.1.3.3 Management of TSF Data

FMT_MTD.1: As described in section 5, the TOE defines the TSF data and the users authorized to query, modify, delete and create them. The table of data items and their respective authorizations are found in section 5.1.3.2, FMT_MTD.1 Management of TSF data.

6.1.4 TOE Protection

The TOE protects itself from untrusted subjects and from bypass of the TSF. The protections are described below.

6.1.4.1 Non-Bypassability of the TSP

FPT_RVM.1: The TSP enforcement functions that must be invoked and succeed before the functions within the TSC are allowed to proceed include the following:

- Identification and authentication: these functions ensure that no unauthorized users can gain access to the TOE.
- Role enforcement prior to access to any Broadmore operation: these functions ensure that authorized users only gain access to the functions to which they are authorized.

6.1.4.2 TSF Domain Separation

FPT_SEP.1: Only a single user can log into the Broadmore at a time, ensuring one user's session cannot interfere with that of another user. Single user activity is enforced on each CPU by ensuring that no two SSH connections are active at any time and ensuring that both the serial port and SSH connections are not active simultaneously. There are no physical ports to the TOE other than those previously described for service and network connections, local administration, and remote administration. Furthermore, the traffic passing through the device between the ATM and non-ATM networks cannot be used to access any of the TOE functions or data because the traffic does not pass through the TOE.

6.1.4.3 Protection of Data in Transit

FPT_ITC.1 and FPT_ITI.1: SSHield uses Secure Shell version 2 (SSH2) protocol to provide data transfer security of network management traffic using encryption. This provides both integrity and confidentiality to the transmissions. When an authorized administrator accesses the TOE remotely, he must first log into the system. A secure data transmission path is set up using the SSHield cryptographic capabilities and the SSH 2 compatible client on the workstation. From that point, all session traffic is encrypted.

Furthermore, traffic is resent if at least one message authentication code error is found in an SSH transmission.

6.1.5 Redundancy

The Broadmore provides the following redundancy features

Power Supply Redundancy The Broadmore models provide have two redundant –48V DC power supplies.

Redundant CPU The Broadmore 1750 and 1700 provide the optional capability to have a redundant CPU.

Redundant NIM The Broadmore 1750 and 1700 provide the optional capability to have a redundant NIM.

Redundant SAM The Broadmore 1750 provides the optional capability to have 1:4 protection for Service Access Modules (SAMs).

Broadmore redundancy is provided by the midplane and CPU software of the corresponding model. Thus Power redundancy is solely provided by the midplane and is independent of CPU or software. CPU and NIM redundancy are both provided by the midplane and installed CPU code on the 1700 and 1750. Also, SAM redundancy is provided by the midplane and installed CPU software on the 1750. That's why a particular CPU or NIM can work in any of the three models (500, 1700, or 1750) but only provide NIM redundancy in the 1700 or 1750 when the proper midplane is available.

6.1.5.1 Redundant Power Supply

All models of the Broadmore TOE provide two power source capabilities in the form of two power supplies for receiving –48 VDC. These two independent DC inputs are available on all three models all the time. A stand-alone A/C converter chassis can be optionally connected to the 1700 and 1750 that can include either one or two independent A/C converters. On the 500, either or both of the DC supplies can be removed and exchanged for A/C converters that are housed inside the 500 chassis, but the -48 VDC inputs still exist. Note that the A/C converters and how A/C is converted to DC are not a part of the TOE. The user may provide power to these supplies from different sources as one form of redundancy.

FPT_FLS.1 [a], FRU_FLT.1 [a]: The Broadmore hardware detects the health of the power supply and automatically switches to the backup supply if the active supply fails for any reason.

6.1.5.2 Network Interface Module Redundancy on the 1700 and 1750

FPT_FLS.1 [b], FRU_FLT.1 [b]: NIM redundancy is provided when two identical NIMs are installed in the appropriate slots of the Broadmore 1700 hardware chassis. NIM redundancy is automatically activated when a second NIM is detected in the system. If two NIMs are detected at initial boot, the first to boot becomes “on-line” and the other goes into the standby mode. NIM redundancy allows the standby NIM to take control if the on-line NIM experiences a failure. The product provides automatic protection switching (APS), a mechanism that determines actions to be taken when the nonfunctioning unit is repaired. For example, after redundancy switching, the system can be programmed to switch back to the original online NIM when repairs are completed, or the standby NIM will remain the system primary NIM after repairs are completed, with the repaired NIM becoming the standby NIM. Because the NIM has no security functionality, it dos not impact the secure state of the TOE.

6.1.5.3 CPU Redundancy in the 1700 and 1750

FPT_FLS.1 [b], FRU_FLT.1 [b]: CPU redundancy is automatically activated when a second CPU is detected in the system. If two CPUs are detected at initial boot, the first to boot becomes “on-line” and the other goes into the standby mode. CPU redundancy allows the standby CPU to take control if the on-line CPU experiences a failure. Data files on the two CPUs are synchronized automatically when the standby CPU is powered up. This synchronization process occurs automatically when the standby CPU is powered up. Once both CPUs are functioning (one on-line and the other in standby), any subsequent changes to the system are mirrored (i.e., recorded in the on-line CPU and sent to the standby CPU). This process keeps the standby CPU up to date.

6.1.5.4 SAM redundancy in the 1750

FPT_FLS.1 [c], FRU_FLT.1 [c]: A model 1750 is specifically designed for SAM redundancy. A cluster of up to four similar SAMs has a single replacement SAM, called the protection SAM, if any one of the cluster member SAMs fails. The chassis slots for the cluster SAMs are numbered alphabetically, which orders the “priority” of the SAMs, lowest to highest. The protection SAM is installed in slot P of the model 1750 chassis. When a cluster SAM becomes non-operational, the protection SAM takes over the activities of the failed cluster SAM and assumes its operational capabilities. When the SAM being protected is repaired and ready for operation**,** it will sit idle in its slot with the protection SAM in slot P still carrying its traffic. If or when a card in a higher priority slot becomes disabled or is pulled, the protection SAM will begin protecting the SAM in the higher priority slot. For example, suppose the protection SAM is protecting a lower priority slot (like C) and someone pulls a higher priority slot (like M). In that case, if the SAM in the previously protected slot C is ok to go back in service it will reassume its operational capabilities and the protection SAM in slot P will start protecting M now. If the card in slot C is still disabled, its operational capabilities will no longer be taken over by the protection SAM, and it will remain unusable, and the protection SAM will continue protecting the card in slot M.

Because the SAM has no security functionality, it does not impact the secure state of the TOE.

Note also that the command “Leftmost” is excluded from the TOE and its use is forbidden by administrator guidance.

6.2 Rationale for TOE Security Functions

This section provides a table demonstrating the tracing of the TOE security functions back to aspects of the security functional requirements (SFRs).

A justification that the security functions are suitable to cover the SFRs can be found in Section 6.1.

Security Functional Requirement	Audit	Identification & authentication	Security management	TOE Protection	Redundancy
FAU_GEN.1	X				
FAU_SAR.1	X				
FAU_SAR.2	X				

Security Functional Requirement	Audit	Identification & authentication	Security management	TOE Protection	Redundancy
FAU_STG.1	X				
FIA_AFL.1		X			
FIA_ATD.1		X			
FIA_UAU.1 [a] & [b]		X			
FIA_UID.1 [a] & [b]		X			
FMT_MOF.1			X		
FMT_MTD.1			X		
FMT_SMF.1			X		
FMT_SMR.1			X		
FPT_FLS.1 [a], [b], & [c]					X
FPT_ITC.1				X	
FPT_ITI,1				X	
FPT_RVM.1				X	
FPT_SEP.1				X	
FPT_STM.1	X				
FRU_FLT.1 [a], [b], & [c]					X

Table 6-1: TOE Security Functions Rationale

6.3 Security Assurance Measures

The assurance measures provided for this Security Target are described in detail in evidence documentation to be provided to the evaluation team during the course of the evaluation of this TOE.

Assurance Measures for ACM_CAP.3

- EAL3 Configuration Management Broadmore 500, 1700, & 1750, CCCM-0001 Rev. 0.9

Assurance Measures for ACM_SCP.1

- EAL3 Configuration Management Broadmore 500, 1700, & 1750, CCCM-0001 Rev. 0.9

Assurance Measures for ADO_DEL.1

- EAL3 Secure Delivery Document Broadmore 500, 1700, & 1750, CCDD-0001 Rev. 0.9, June 13, 2006

Assurance Measures for ADO_IGS.1

- EAL3 Installation and Administration Guide, CCIG-0001 Rev. 12, June 2006

Assurance Measures for ADV_FSP.1

- EAL3 Design Document, CCF-0001 Rev. 1.6, March 13, 2006, Sections 4, 5, & 7

Assurance Measures for ADV_HLD.2

- EAL3 Design Document, CCF-0001 Rev. 1.6, March 13, 2006, Sections 1-7

Assurance Measures for ADV_RCR

- EAL3 Design Document, CCF-0001 Rev. 1.6, March 13, 2006, Section 7

Assurance Measures for AGD_ADM.1

- EAL3 Installation and Administration Guide, CCIG-0001 Rev. 12, June 2006
- Broadmore 500 User Manual
- Broadmore 1700 User Manual
- Broadmore 1750 User manual

Assurance Measures for AGD_USR.1

There are no non-administrative users of this TOE, and therefore there are no User guidance documents other than those described above.

Assurance Measures for ALC_DVS.1

- EAL3 Life Cycle Document Broadmore 500, 1700 & 1750, CCL-0001 Rev. 0.5, November 14, 2005
- EAL3 Configuration Management Broadmore 500, 1700, & 1750, CCCM-0001 Rev. 0.9
- Standard Operating Procedure, Engineering Design Control, SOP 02, July 31, 2003, Rev. H.
- Standard Operating Procedure, Customer Assurance Design Control, SOP 25, Aug. 30, 2004, Rev. G.
- Standard Operating Procedure, Operations Design Control, SOP 26, May 4, 2004, Rev. F.
- Standard Operating Procedure, Product Creation and Delivery Process, SOP 100, May 17, 2004, Rev. G.
- Engineering Reference Specification for Product X (Artifact A11).

Assurance Measures for ATE_COV.2

- EAL3 Test Plan Document Broadmore 500, 1700, 1750, CCTP-0001 Rev. 2.5, May 12, 2006
- EAL3 Design Document Broadmore 500, 1700 & 1750, CCF-0001 Rev. 1.6, March 13, 2006, Sections 4, 6, 7

Assurance Measures for ATE_DPT.1

- EAL3 Test Plan Document Broadmore 500, 1700, 1750, CCTP-0001 Rev. 2.5, May 12, 2006
- EAL3 Design Document Broadmore 500, 1700 & 1750, CCF-0001 Rev. 1.6, March 13, 2006, Sections 4, 6, and 7.
- EAL3 Design Document Broadmore 500, 1700 & 1750, CCF-0001 Rev. 1.6, March 13, 2006

Assurance Measures for ATE_FUN.1

- EAL3 Test Plan Document Broadmore 500, 1700, 1750, CCTP-0001 Rev. 2.5, May 12, 2006
- EAL3 Test Results Document Broadmore 500, 1700 & 1750, CCTP-0001 Rev. 2.5, May 12, 2006

Assurance Measures for ATE_IND.2

The TOE and testing documentation were made available to the CC testing laboratory for independent testing.

Assurance Measures for AVA_SOF

- EAL3 Strength of Function Analysis Broadmore 500, 1700, & 1750, CCSF-0001 Rev. 3.0, January 4, 2006

Assurance Measures for AVA_VLA

- EAL3 Vulnerability Analysis Broadmore 500, 1700, & 1750, CCV-0001 Rev. 5.0, May 16, 2006

6.4 Rationale for Security Assurance Measures

The following presents the rationale for each assurance measure.

ACM_CAP.3, ACM_SCP.1

The configuration management documents provide a CM Plan, define a unique reference to the TOE, identify the configuration items, contain the necessary information to demonstrate that a CM system is used in accordance with the CM Plan, and provide for maintenance controls for the configuration items. The items under configuration control are indicated and include the implementation representation and evaluation evidence required for EAL3.

ADO_DEL.1

The delivery document describes the steps performed to deliver the TOE. It describes the process used to create distribution copies of the TOE software and the steps taken to ensure consistent, dependable delivery of the TOE to the customer.

ADO_IGS.1

The installation, documents describe the steps necessary for secure installation, generation, and start-up of the TOE.

ADV_FSP.1

The informal functional specification document identifies the external interfaces that completely represent the TSF and describes the purpose and method of use of all external TSF interfaces. It also describes the effects, exceptions, and error messages for each of the external TSF interfaces.

ADV_HLD.2

The descriptive high-level design describes the complete TSF in terms of subsystems. The security functions for each subsystem are described. The subsystem interfaces are defined and the externally visible interfaces are identified. The HLD evidence also addresses the purpose and method of use of all interfaces providing details of effects, exceptions, and error messages. Furthermore, the subsystems that are TSP-enforcing are separated from other TOE subsystems.

ADV_RCR.1

The informal correspondence document maps the security functionality as described in the FSP and ST and as described in the FSP and HLD.

AGD_ADM.1

The administrator guidance documents provide complete administrative guidance for the TOE, including all security features and configuration items.

AGD_USR.1

There are no non-administrative users of the Broadmore products.

ALS_DVS.1

The life cycle documentation describes the security measures used to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ATE_COV.2

The test coverage document provides an analysis of the test coverage and includes a mapping that demonstrates the correspondence of the test cases performed against the TSF to the FSP.

ATE_DPT.1

The test depth document provides an analysis of the depth of testing that demonstrates the TSF operates in accordance with its high level design.

ATE_FUN.1

The functional testing document includes the test plans, test procedures, and associated test cases of the TOE functional testing effort.

ATE_IND.2

The TOE hardware, software, guidance, and testing documentation are made available to the CC testing laboratory for independent testing.

AVA_SOF.1

The strength of function analysis document provides the SOF argument for the password authentication mechanism.

AVA_VLA.1

The vulnerability analysis document identifies and describes the process used to discover obvious vulnerabilities, the results of the vulnerability analysis, and the mitigation of each identified obvious vulnerability.

Table 6-2: Security Assurance Measures Rationale

7 Protection Profile Claims

This ST does not conform to a PP.

8 Rationale

8.1 Rationale for Security Objectives

The rationale for the security objectives is found in section 4.3.

8.2 Security Requirements Rationale

The rationale for the security functional requirements is found in section 5.2 and all its subsections. The rationale for the security assurance requirements is found in section 5.4.

8.3 TOE Summary Specification Rationale

The TOE security functions rationale is found in section 6.1and 6.2, and the assurance measures rationale is found in 6.4.

8.4 Protection Profile Rationale

There is no protection profile claim in this ST.