HFMP Mobile Trusted Filter
Security Target

June 2006

Copy No:	
Issue No:	1.9
Doc Ref:	EC100453/P/T/1

REVIEW & APPROVAL
Originator:
C Lowe

Approval (PM):
C Lowe

Reviewer:
T. Bierzonski-Burczyk

BAE SYSTEMS AUSTRALIA LIMITED
78 Northbourne Avenue
Braddon ACT 2612
Phone: +61 (0)2 6229 1600
Fax: +61 (0)2 6230 4345

Distribution List

Copy No	Recipient
1	BAE SYSTEMS
2	Australasian Certification Authority
3	LogicaCMG AISEF
4	LogicaCMG PEC Consultant

Contents

1 Introduction

1.1 Purpose

This document defines the security target for the Australasian Information Security Evaluation Programme (AISEP) product evaluation of BAE Systems Australia's Mobile Trusted Filter.

1.2 Target of Evaluation

The Target of Evaluation (TOE) is BAE Systems Australia's Mobile Trusted Filter Issue 1. The TOE will be referred to as the "Trusted Filter" throughout this document.

Currently the following versions of the Trusted Filter have been certified, before this one:

BAE SYSTEMS Trusted Filter Version 1.0 – the originally certified version

(see reference 7 for a description of this version)

BAE SYSTEMS Trusted Filter Version 1.1

see SIA 1 (reference 4) for a description of changes in this version

BAE SYSTEMS Trusted Filter Version 1.2A.1

see SIA 2 (reference 5) for a description of changes in this version

BAE SYSTEMS Trusted Filter Version 1.2A.2

This version supersedes Version 1.2A.1

see SIA 3 (reference 6) for a description of changes in this version

1.3 Scope

1.3.1 The Security Target details the TOE's security objectives and the security enforcing functions proposed to address the assumed threats to the assets protected by the TOE.

1.3.2 This Security Target is structured as follows:

a) Chapter 1 outlines the purpose and scope of the document

b) Chapter 2 is a product rationale; the product's security objectives and a summary of its security features is presented, along with the intended method of use, the intended environment and the assumed threats within that environment

c) Chapter 3 is a specification of the security enforcing functions; these functions are countermeasures that are devised to address the assumed threats to the product in its intended environment

d) Chapter 4 identifies the security mechanisms used in the TOE and maps them to the security enforcing functions specified in Chapter 3

e) Chapter 5 states the claimed minimum strength of the security mechanisms identified in Chapter 4 and identifies the target evaluation level

f) Chapter 6 provides a formal model of the underlying security policy enforced by the TOE

g) Chapter 7 contains an informal interpretation of the formal model of underlying security policy in terms of the security target.

1.4 Glossary

This section comprises a glossary of terms related to the TOE and used in the security target.

BLACK A clearly definable area which is insecure and therefore must not contain classified data. The term BLACK can also be used to refer to data which is permitted in a BLACK area (i.e., data which is unclassified or which has been encrypted).

RED A clearly definable area which is secure and therefore may contain classified data. The term RED can also be used to refer to data which is in the RED area and which has not been encrypted.

1.5 References

1) Information Technology Security Evaluation Criteria, Commission of the European Communities, version 1.2, 28 June 1991

2) The Z Notation: A Reference Manual, Second Edition, J.M.Spivey, Prentice Hall International (UK) Ltd, 1992

3) Using Z - Specification, Refinement, and Proof, Jim Woodcock and Jim Davies, Prentice Hall Europe, 1996.

4) Generic Trusted Filter Security Impact Analysis 1- Generic Trusted Filter Changes, BAE SYSTEMS, 202A00072-001-AY, Issue 1, September 2001.

5) Generic Trusted Filter Security Impact Analysis 2 – One Channel Trusted Filter, BAE SYSTEMS, 202A00072-002-AY, Issue 1, September 2001.

6) Generic Trusted Filter Security Impact Analysis 3 – HFFN Channel Update, BAE SYSTEMS, 202A00072-003-AY, Issue 1, December 2001

7) Trusted Filter Security Target, Issue 1.4,November 2000.

2 Product Rationale

2.1 Product Description

2.1.1 The Trusted Filter is a special purpose device designed to provide RED/BLACK separation in systems where control data which cannot be protected by encryption or other means must cross a RED/BLACK boundary.

2.1.2 The Trusted Filter is installed on the RED/BLACK boundary and provides its own RED/BLACK separation. On the RED side, the Trusted Filter connects to communications control equipment which itself is in the RED area. On the BLACK side, the Trusted Filter connects to transmission equipment.

2.1.3 The Trusted Filter allows the control equipment (on the RED side) to transmit only a specified set of control commands to the transmission equipment (on the BLACK side). The Trusted Filter does not allow the passage of invalid commands from the RED side to the BLACK side. If the Trusted Filter receives an invalid command, an alarm is raised to notify the user and the command is discarded.

2.1.4 The Trusted Filter allows transmission equipment to pass data (typically a command response) from the BLACK side to the RED side. The BLACK to RED communication path is constructed to prevent any possible leakage of information back from the RED to BLACK side.

2.1.5 The Trusted Filter has been designed and constructed to ensure that any single hardware failure will not result in an insecure state.

2.1.6 The Trusted Filter unit supports a single communications channel. Associated with this channel is a single green diagnostic Light Emitting Diode (LED) labelled “Operate”. An “Alarm” status is indicated as a signal to the Status connector which can be monitored by external equipment connected to the Trusted Filter Status connector.

2.1.7 The Operate LED indicates that the Trusted Filter control program is executing. The control program includes a “watchdog” feature which requires the control program to periodically reset a hardware timer. Failure to do so will result in the Operate LED being extinguished. This indicates that the Trusted Filter hardware or software is faulty.

2.1.8 The Alarm status signal indicates that data which has failed validation has been received. During normal operation it is possible for the Trusted Filter to receive corrupt data, noise or RED data. If any data is received that fails validation, the data will be discarded and the Alarm Signal will be activated. It will remain active until the channel is reset or the Trusted Filter is powered off. The channel will continue to process incoming data, restarting validation with the next character received. The Alarm Signal is for diagnostic purposes only. The Alarm Signal is also activated if the control program watchdog fails to reset its hardware timer.

2.1.9 A “Reset” signal may be supplied to the Trusted Filter via the Status connector. This externally applied signal invokes a hardware reset of the Trusted Filter causing it to go through a start-up sequence.

2.1.10 The Trusted Filter operates from an external 5V DC power source and includes safety protection against reverse polarity connection such that should it occur, the input voltage is isolated from the Trusted Filter Printed Circuit Assembly. It also has a single green LED labelled Operate that indicates the presence of DC power and that the unit is operating normally.

2.1.11 The Alarm Signal may be monitored by equipment such as a PC connected to the Status connector. The monitoring equipment may also apply a Reset signal to the Trusted Filter. The monitoring equipment connected to the Trusted Filter via the Status connector described above does not form part of the TOE.

2.2 Security Objectives

The security objective of the TOE is presented in Table 2-1.

O1	**Confidentiality** The TOE shall ensure only valid control data is allowed to pass unencrypted from a RED to a BLACK area.

Table 2-1: Security Objective

2.3 Intended Method of Use

2.3.1 The Trusted Filter is intended to be used in a situation where it is necessary to pass data (e.g., device commands) unencrypted across a RED/BLACK interface. An example installation is shown in Figure 2-1.

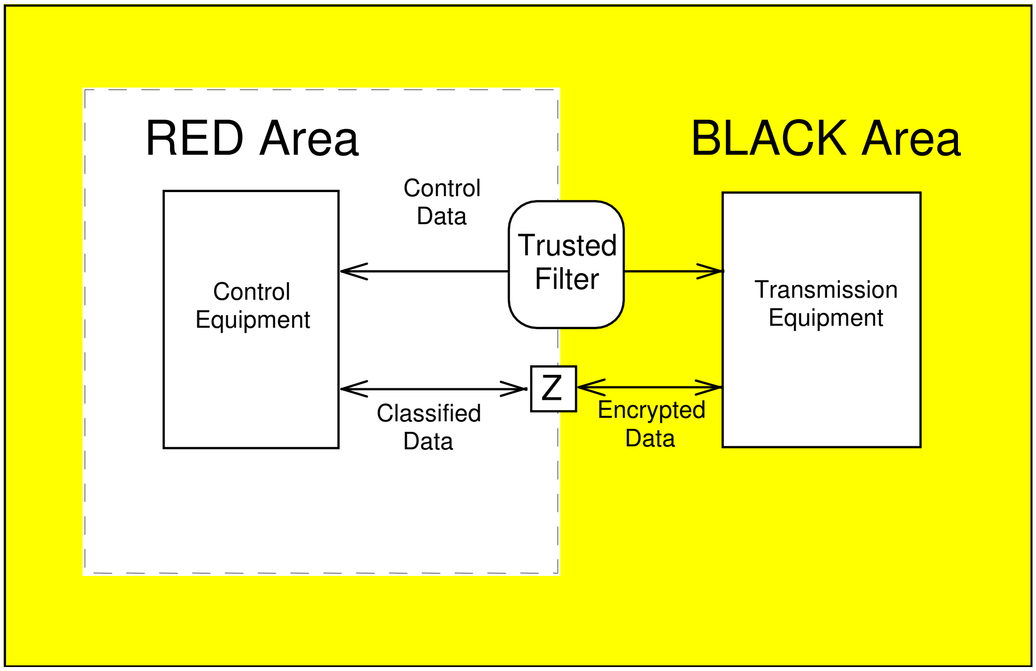

Figure 2-1: Example Trusted Filter Installation

2.3.2 A typical installation of the Trusted Filter is in a communications environment involving remotely controlled transmission equipment. In such an environment, it is assumed commands for controlling the transmission equipment are generated in the RED area but the transmission equipment itself is in a BLACK area. Control commands will be specific to a particular piece of transmission equipment, such as a modem or radio transmitter. Typical commands would be to start or stop data transmission or to change the equipment configuration, such as transmission speeds or frequencies.

2.3.3 Data for transmission is encrypted as it passes from the RED area to the BLACK area (the cryptographic device is depicted in Figure 2-1 by the box containing the 'Z' character). However, control commands must be received by the transmission equipment in plaintext.

2.3.4 Therefore, the situation arises where unencrypted information is communicated from the RED area to the BLACK area. The security objective of the TOE is to ensure only valid control data is allowed to pass unencrypted from the RED to the BLACK area. The Trusted Filter achieves this objective by ensuring only a strictly controlled set of device control commands can pass unencrypted into the BLACK area along the communications channel.

2.3.5 A state transition table defines the allowed set of control commands. This state transition table is programmed in a Programmable Read Only Memory (PROM). For a particular installation, an assessment of the allowable set of control commands needs to be made first. These are then programmed for the appropriate channel. There is one set of commands for the Trusted Filter, which forms part of the TOE.

2.3.6 The Trusted Filter validates commands one character at a time. As soon as a character is received which invalidates the current data sequence being processed, all data received is discarded and an alarm is raised. However, in order to minimise spurious alarms, at least three characters must have been received in order to trigger the alarm. Otherwise, the data is regarded as garbled rather than invalid. It is still discarded, but no alarm is raised.

2.3.7 Since information is passing from a classified to an unclassified area, a possibility exists for a covert channel. The assessment of allowable commands is primarily an issue for the user and any accreditation authority. However, it is recommended that any commands with parameters which can take large amounts of free form text should not be included in the allowable set of commands.

2.4 Intended Operational Environment

2.4.1 The following diagram explains how the Trusted Filter is connected within a target system. The Trusted Filter contains the following external connections:

a) 1 x DB9 female connector (J1) for 5 V DC power;

b) 1 x DB15 female connector (J3) for RED control data;

c) 1 x DB9 male connector (J4) for BLACK control data; and

d) 1 x DB15 male connector (J2) for the connection of monitoring equipment.

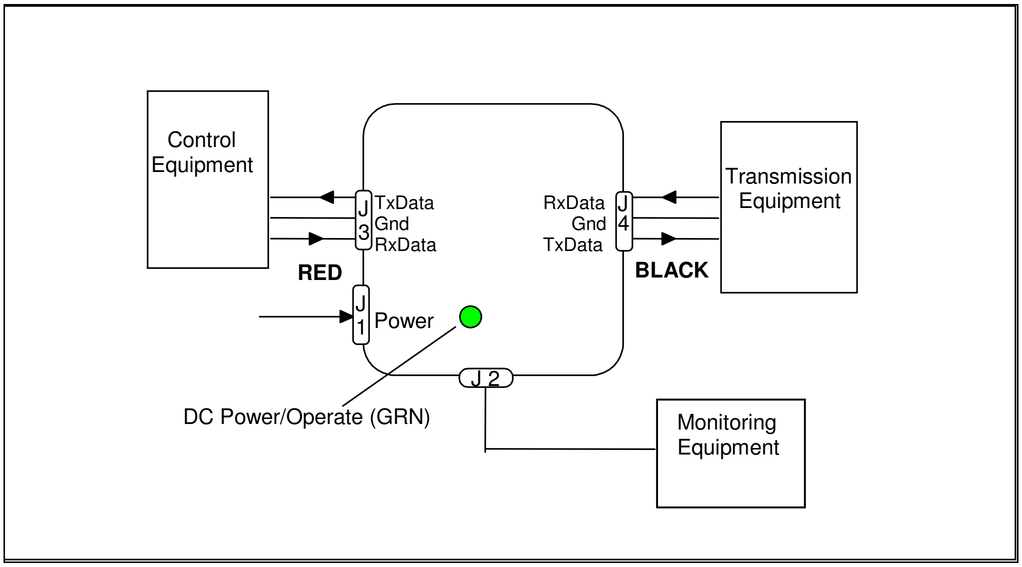

Figure 2-2: Connection of Trusted Filter into System

2.4.2 The RED and BLACK control data connectors (J3 - J4) support the following signals:

a) Transmit Data

b) Receive Data

c) Signal Ground.

2.4.3 The RED and BLACK control data connectors (J3 - J4) support RS-232 electrical levels.

2.4.4 The Trusted Filter case conforms to the VME standard for card assemblies. All external interfaces, J1 - J4 inclusive and Operate LED, are on the front panel of the Trusted Filter

2.4.5 The Trusted Filter will operate in an essentially benign environment where there is little opportunity, or motive, for a direct physical attack. Such an environment would have the following characteristics:

a) all personnel with access to the Trusted Filter will either be security cleared, or escorted by security cleared personnel;

b) the Trusted Filter enclosure shall be securely mounted at all times, and only removed or replaced by end-user approved personnel;

c) the Trusted Filter enclosure shall only ever be opened by manufacturer approved personnel. Wafer seals will be placed over the case assembly screws to make any tampering evident.

2.5 Evaluated Configuration

2.5.1 The version of the product to be evaluated is “Issue 1”. The product contains two separate firmware components stored in a PROM and a microcontroller. The versions of these components are identified in Table 2-2.

Item	**Version**	**Location**	**Checksum**	**Label**
Front End PROM	V1.02	U16	73A6	19k2 TF C/S 73A6 U6/16 (HFFN) V1.02
Back End Microcontroller	V1.02	U20	9916	19k2 TF C/S 9916 U20 (BE) V1.02

Table 2-2: Software Version Numbers

2.5.2 Part of the communication channel is implemented by a "Front End" PROM , which incorporates a stored program and a validation table for the channel. The stored program performs the following functions:

a) implements the finite state machine used to traverse the finite state transition table which defines the command validation table for the channel

b) converts serial data, received from the control equipment in the RED area, into parallel data for communication to the BLACK side of the Trusted Filter

c) negotiates communication of parallel data between the Front End and Back End of the Trusted Filter.

2.5.3 The communication channel also contains a "Back End" microcontroller containing a program which performs the following functions:

a) negotiates communication of parallel data between the Front End and Back End of the Trusted Filter

b) regenerates parallel data as serial data for transmission from the BLACK side of the Trusted Filter to the communications equipment in the BLACK area.

2.6 Assumed Threats

T1	**Passage of RED data** The operating system, application software or operator that is operating control equipment in the RED area could inadvertently or maliciously direct RED data to circuits not covered by cryptographic equipment.
T2	**RED to BLACK leakage on return data path** The Trusted Filter provides for connection of data signals from the RED to the BLACK area (transmitted data) and from the BLACK to the RED area (received data). The transmitted data is filtered by mechanisms described elsewhere, but there is potential for transmitted data to be sent on the received data lines. This could occur due to a wiring error. This would allow RED data to be present in the BLACK area.
T3	**Internal hardware failure** The failure of a hardware component within the Trusted Filter could produce a condition that allows data to pass unfiltered from the RED area to the BLACK area, thus negating the security objective of the Trusted Filter.

Table 2-3: Assumed Threats

3 Specification of Security Enforcing Functions

3.1 Introduction

3.1.1 In this chapter, each Security Enforcing Function (SEF) of the TOE is specified. For each SEF, a statement of its security functionality is made in the "Specification" subsection. In the "Description and Explanation" subsection, the characteristics of the SEF are enumerated and a rationale for the characteristics is provided. Finally, a semi-formal specification of the SEF, in an appropriate notation, is presented.

3.1.2 Following the specification of the SEFs, tables are presented which explain:

a) how the functionality embodied in the SEFs fulfils the TOE's Security Objective (see section 2.2) and is appropriate to the TOE's method of use (see section 2.3)

b) how the functionality embodied in the SEFs is adequate to counter the assumed threats to the assets protected by the TOE (see section 2.6).

3.2 Filtering SEF

3.2.1 Specification

The TOE shall ensure, that only data strings which are validated against a pre-defined set of allowable control data can be transmitted from a RED to a BLACK area.

3.2.2 Description and Explanation

3.2.2.1 The TOE shall maintain a data buffer for the communication channel it controls. Whenever the TOE is powered on, or the channel is reset, the data buffer shall be initialised to empty. This ensures the buffer does not contain any invalid or unvalidated characters when validation of a new string commences.

3.2.2.2 The TOE shall define a set of allowed control data for the communication channel. The TOE shall validate received data strings character by character. The TOE shall declare a data string valid only when all characters have been received. Only control data declared valid shall be transferred to the BLACK side of the filter. These characteristics ensure:

a) all characters in the data string are subject to validation before they are transmitted to the BLACK side

b) only complete valid data strings are transmitted to the BLACK side.

3.2.2.3 The TOE shall reject as invalid any data string received which is three or more characters long and which is not validated against any control data defined for the input channel. The data string shall be invalidated as soon as it is apparent that the string being received is not a member of the pre-defined set of control data (i.e., on the first character received which fails to match any valid control data string for the channel). Invalid data shall be overwritten and data validation shall restart with the next character received. This ensures no invalid data will be transferred to the BLACK side.

3.2.2.4 Whenever an invalid data string is received on the communication channel, the alarm signal shall be activated. The alarm shall remain active until the reset signal is activated to clear the alarm.

3.2.2.5 Raising the alarm shall not affect the normal operation of the communication channel of the TOE. Since the TOE handles invalid data securely, and the alarm is only for information and diagnostic purposes, it is not necessary to suspend operation on the channel.

3.2.2.6 Any string of two characters or less which is not validated by the TOE shall be identified as garbled data rather than invalid data. The data buffer shall be overwritten but no alarm shall be raised. This provides a degree of tolerance for receiving corrupted data or noise and reduces the incidences where the operator is required to respond to an alarm.

3.2.2.7 <commercially sensitive material removed>

3.3 Data Diode SEF

3.3.1 Specification

The TOE shall ensure any BLACK to RED data path it controls is strictly one way.

3.3.2 Description and Explanation

3.3.2.1 The TOE shall include a “data diode” on the BLACK to RED data path. . The BLACK to RED data path allows equipment controlled in the BLACK area to respond to control data with status information.

3.3.2.2 The data diode is implemented in hardware and ensures that data can pass only in one direction, from BLACK to RED. This prevents any possible passage of data from RED to BLACK on the BLACK to RED path.

3.3.3 Semi-formal Specification

3.3.3.1 The Data Diode SEF is specified semi-formally in the following diagram (Figure 3-2). It depicts the operation of the data diode, which is placed in the BLACK to RED data path in the TOE.

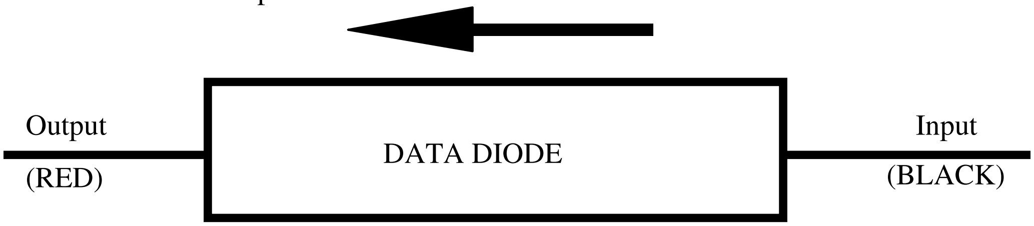

Figure 3-2: Data Diode Specification

3.3.3.2 The data diode is constructed of electronic components so that it obeys the single rule:

Output ⇐ Input;

where the symbol “⇐” can be read as “takes the value of”.

3.3.3.3 The Input node is connected to the BLACK side and the Output node is connected to the RED side.

3.4 Secure Failure SEF

3.4.1 Specification

The design of the TOE shall ensure that any conceivable failure of any single discrete hardware component shall not compromise the security objective of the TOE.

3.4.2 Description and Explanation

3.4.2.1 The TOE comprises software and hardware. The correct operation of the TOE is assured by testing and by examination of design and implementation deliverables during formal evaluation. However, the failure of a hardware component could alter the operation of the TOE to the extent that its security objective is compromised.

3.4.2.2 The design and implementation of the hardware for the TOE will ensure any failure of a single discrete hardware component will not allow the TOE to operate insecurely. The following techniques are used to ensure secure failure:

a) minimum complexity, which allows complete analysis of failure modes and effects of hardware components, to ensure such failures do not induce an insecure state

b) serial design, which ensures no alternative paths exist for data in the event of a component failure

c) component separation (physical and electrical), which ensures no unintentional alternative paths for data exist (i.e., data signals cannot be carried on paths not intended to carry them).

3.4.2.3 <commercially sensitive material removed>

3.5 Relationship between Security Objective, Method of Use and SEFs

3.5.1 The TOE's security objective is stated in section 2.2. The TOE's intended method of use is identified in section 2.3. The intended method of use relates the security objective of the TOE to the way in which it is designed to be used in order to fulfil the security objective. Therefore, relating the TOE's SEFs to its intended method of use also relates the SEFs to the TOE's security objective.

3.5.2 The following table maps the TOE's SEFs to its intended method of use. An explanation is provided of how the functionality of the SEFs fulfils the TOE's security objective and is appropriate for its intended method of use.

Use	SEFs	Notes
Allow only a restricted set of defined control commands to pass from RED area to BLACK area.	Filtering	The Filtering SEF ensures any data read by the TOE must match one of a restricted set of data strings pre-defined for the channel on which the command was received. If received data does not match a pre-defined string, it is not communicated to the BLACK area. In this way, the Filtering SEF fulfils the security objective by ensuring only valid control data (i.e., the restricted set of pre-defined data strings) can pass unencrypted from a RED area to a BLACK area.
	Data Diode	The Data Diode SEF ensures no data can bypass the Filtering SEF by leaking the wrong way down any BLACK to RED data path. The Data Diode SEF ensures any unfiltered path between the RED and BLACK sides of the TOE is strictly one-way from BLACK to RED. It uses a hardware device to ensure no data can pass from RED to BLACK down such a path, thereby ensuring the security objective is fulfilled for possible data paths through the TOE not covered by the Filtering SEF.

Use	SEFs	Notes
	Secure Failure	The Secure Failure SEF ensures any single failure of a discrete hardware component will not compromise the security of the TOE. The hardware design of the TOE ensures any such failure will either: a) be covered by other, operational components, which will continue to operate correctly and therefore continue to maintain the security objective; this will occur because of the serial design of the hardware - no failure can introduce an alternative, insecure path for information b) or will result in the TOE ceasing to operate altogether, which represents a secure state. Therefore, any single failure of a discrete hardware component will not allow unfiltered data to pass from the RED to the BLACK side of the TOE. This ensures the security objective continues to be fulfilled in the event of a hardware error which could affect either the Filtering or Data Diode SEFs.

Table 3-1: Mapping of SEFs to Method of Use

3.6 Relationship between Threats and SEFs

The following table maps the TOE's SEFs to the threats identified in Chapter 2. An explanation is provided of how the functionality of the SEFs is adequate to counter the assumed threats.

Threat	SEFs	Adequacy
T1	Filtering	The Filtering SEF addresses this threat by ensuring only data strings which exactly match members of a pre-defined set of control commands for the communication channel are allowed to be transmitted from a RED area to a BLACK area through the channel. Any data string not recognised as a valid control command for the channel is rejected. This ensures any operating system, application software or operator data that is inadvertently or maliciously directed to a channel guarded by the TOE will not be passed to the BLACK area.
T2	Data Diode	The Data Diode SEF addresses this threat by ensuring any data path from BLACK to RED controlled by the TOE is strictly one-way, so that no possibility exists for RED data to be leaked into the BLACK area down this path.
T3	Secure Failure	The Secure Failure SEF addresses this threat by ensuring that any single discrete hardware component failure will not result in the TOE operating in an insecure manner. Such a failure will be covered either by additional correctly operating components or by making the TOE non-operational (which ensures no data can pass from the RED to the BLACK area, thus maintaining the security objective of the TOE).

Table 3-2: Mapping of SEFs to Threats

4 Security Mechanisms

4.1 Specified Mechanisms

4.1.1 Introduction

The TOE shall employ the following security mechanisms:

a) Finite State Machine (FSM)

b) hardware data diode.

4.1.2 Finite State Machine

4.1.2.1 The TOE shall implement a FSM, for the communication channel it controls, to validate data strings received as input on the RED side of the channel.

4.1.2.2 Valid data is stored as a representation of a Finite State Transition Table (FSTT). The FSM validates data by traversing the FSTT, in accordance with the data it contains. Only when the validated state is achieved will the data be declared valid and passed on to the BLACK side. The FSTT explicitly includes all allowable control data for that channel. Any data not defined in the table is not valid and the valid state will not be reached.

4.1.2.3 While the FSM is traversing the FSTT in response to received control data, the control data is buffered and not sent to the BLACK side. This buffer is initialised (cleared) when the FSM arrives at the “Start” node. Any control data received which causes the FSM to follow valid transitions will be appended to the buffer. When the FSM arrives at the “Valid” state, the buffer contains the control data that caused the FSM to arrive at that state. The buffer contents can then be declared valid and passed to the BLACK side.

4.1.2.4 <commercially sensitive material removed>

4.1.3 Hardware Data Diode

4.1.3.1 The TOE shall implement a hardware data diode for the BLACK to RED data path it controls.

4.1.3.2 The hardware data diode shall be built from electronic circuitry that will only pass data in one direction.

4.1.3.3 Functionally, the hardware data diode shall be the equivalent of a diode. However, to provide the correct operating voltage and adequate fail-safe protection, it shall be constructed of several components.

<commercially sensitive material removed>

4.2 Relationship between Mechanisms and SEFs

The mapping of SEFs to Security Mechanisms is shown in Table 4-1.

Security Mechanisms	SEFs
Finite State Machine	Filtering SEF
Hardware Data Diode	Data Diode SEF

Table 4-1: Mapping of SEFs to Security Mechanisms

5 Claimed Strength of Mechanisms and Evaluation Level

5.1 Target Evaluation Level

The target evaluation level is E5.

5.2 Strength of Mechanisms

5.2.1 The following table identifies for each security mechanism its type (Type A or Type B) and its claimed strength (Basic, Medium or High).

Security Mechanisms	Type	Claimed Strength
Finite State Machine	B	n/a
Hardware Data Diode	B	n/a

Table 5-1: Mechanism Types and Strengths

5.2.2 As no Type A mechanisms are identified for implementation in the TOE, no claim regarding the minimum strength of mechanisms is required. An explanation of why the security mechanisms are Type B is provided in the Strength of Mechanisms Analysis, which will be supplied during the evaluation.

6 Formal Model of Underlying Security Policy

6.1.1 <commercially sensitive material removed>

7 Informal Interpretation of Formal Model

7.1 Introduction

7.1.1 In addition to the formally specified model of underlying security policy (Chapter 6), ITSEC requires an informal interpretation of the model in terms of the security target.

7.1.2 The interpretation must correlate the model to the SEFs and show that:

a) the model does not contain any aspects of policy which are not completely reflected by one or more SEFs (i.e., the security target is complete with respect to the security policy)

b) no SEFs within the security target conflict with the policy within the model (i.e., the security target is consistent with the model).

7.1.3 This chapter provides an interpretation of the formal security policy in terms of the security target which explains how the security target satisfies the underlying security policy.

7.2 Completeness

7.2.1 The following aspects of security policy are contained in the formal security policy model:

a) only valid control commands can cross from a RED area to a BLACK area

b) at any time, the contents of the input buffer must form a prefix of a valid control command defined for the channel

c) at any time, the output buffer must be empty or must contain a valid control command for the channel

d) a character is only added to the input buffer if, by adding the character, the contents of the buffer remain a prefix of a valid control command defined for the channel

e) the contents of the input buffer are transferred to the output buffer only if they constitute a valid control command defined for the channel

f) only the contents of the output buffer are ever transmitted by the Trusted Filter to the BLACK area.

7.2.2 Each of these aspects is satisfied by the Filtering SEF, as explained in the following paragraphs.

7.2.3 The functionality of the Filtering SEF is to ensure that only data strings validated against a pre-defined set of allowable control data can be transmitted from a RED to a BLACK area. Section 3.2 provides an informal explanation of how the Filtering SEF achieves this.

7.2.4 The Filtering SEF specifies that the channel maintains an input buffer. The channel is initialised to empty on power on or reset. Control data is validated character by character and only complete, validated commands are transferred to the BLACK side of the channel. Therefore, the input buffer only ever contains a prefix of a control command which is valid for the channel. A prefix can be no data, one or more characters which comprise the start of a valid command, or the entire command.

7.2.5 The Filtering SEF initialises the output buffer to empty at power on. The only data written to the output buffer after power on are validated control commands. Therefore, at any time the output buffer is either empty or contains a valid control command for the channel.

7.2.6 The Filtering SEF validates data strings a character at a time. Anytime it receives a character which does not form a prefix of a valid command when added to the current contents of the input buffer, it deletes the contents of the input buffer and restarts validation with the next character received. Therefore, a received character is added to the input buffer only if the contents can still result in a valid control command for the channel.

7.2.7 The Filtering SEF transfers the contents of the input buffer to the output buffer on the BLACK side only after the contents have been confirmed as a valid control command for the channel. No transfer to the output buffer occurs until validation of the command has completed.

7.2.8 Only the contents of the output buffer are ever written to the BLACK area by the Filtering SEF. The Filtering SEF does not write any other data to the output port on the BLACK side of the channel.

7.3 Consistency

7.3.1 As stated above, and in Chapter 6, the security policy enforced by the TOE is that only validated control commands are passed from the RED side to the BLACK side of the TOE. Each of the SEFs defined for the TOE (see Chapter 3) is consistent with this policy.

7.3.2 The Filtering SEF provides the primary security functionality to ensure the security policy is enforced. Therefore, it is obviously consistent with the underlying security policy.

7.3.3 The Data Diode SEF specifies a function to prevent any leakage of unvalidated data from the RED to the BLACK side via the BLACK to RED data path. This SEF supports the security policy of the TOE by ensuring a possible method of bypassing the Filtering SEF is addressed. Therefore, the Data Diode SEF is consistent with the underlying security policy.

7.3.4 The Secure Failure SEF specifies a hardware design for the TOE which ensures any single failure of a discrete hardware component of the TOE will not allow the security objective of the TOE to be compromised i.e., no single hardware failure will allow unvalidated data to pass from the RED to the BLACK side of the TOE. The Secure Failure SEF also provides a means for ensuring possible bypass paths for unvalidated data cannot be created in the TOE due to hardware failure. Therefore, the Secure Failure SEF is consistent with the underlying security policy.