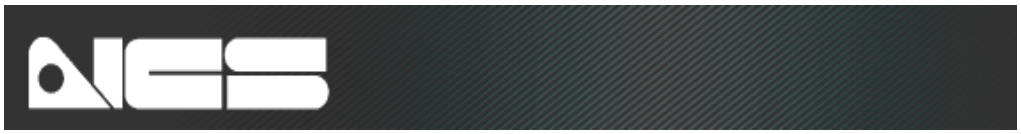


NCS Technologies Model Stratus CM 4110

and

Stratus CM 4120

Security Target

Document Version
Part Number: V001851
Version: 1.778
2013-04-26

Prepared For:

InfoGard Laboratories, Inc.
709 Fiero Lane, Suite 25
San Luis Obispo, CA 93401

Prepared By:
Gordon McIntosh

Notices:

Table of Contents

TABLE OF CONTENTS 3

TABLES 6

1 SECURITY TARGET (ST) INTRODUCTION 7

1.1 SECURITY TARGET REFERENCE 7
1.2 TARGET OF EVALUATION REFERENCE 7
1.3 TARGET OF EVALUATION OVERVIEW 8
1.3.1 TOE PRODUCT TYPE 8
1.3.2 TOE USAGE 8
1.3.3 TOE MAJOR SECURITY FEATURES SUMMARY 8
1.3.4 TOE IT ENVIRONMENT HARDWARE/SOFTWARE/FIRMWARE REQUIREMENT SUMMARY 8
1.4 TARGET OF EVALUATION DESCRIPTION 8
1.4.1.1 Target of Evaluation Physical Boundaries 9
1.4.1.1.1 Control Module Description 10
1.4.1.1.2 Secure KVM Description 10
1.4.1.1.3 Remote Control Description 11
1.4.1.2 TOE Guidance Documentation 12
1.4.2 TARGET OF EVALUATION LOGICAL BOUNDARIES 12
1.4.2.1 User data protection 12
1.4.2.2 Security Management 13
1.4.2.3 Protection of the TSF 13
1.4.2.4 Extended requirements 13
1.5 ROLES, USER DATA, AND TSF DATA 13
1.6 NOTATION, FORMATTING, AND CONVENTIONS 13

2 CONFORMANCE CLAIMS 15

2.1 COMMON CRITERIA CONFORMANCE CLAIMS 15
2.2 CONFORMANCE TO PROTECTION PROFILES 15
2.3 CONFORMANCE TO SECURITY PACKAGES 15
2.4 CONFORMANCE CLAIMS RATIONALE 15

3 SECURITY PROBLEM DEFINITION 17

3.1 THREATS 17
3.1.1 THREATS COUNTERED BY THE TOE AND TOE IT ENVIRONMENT 17
3.2 ORGANIZATIONAL SECURITY POLICIES 17
3.2.1 ORGANIZATIONAL SECURITY POLICIES FOR THE TOE 17
3.3 ASSUMPTIONS ON THE TOE OPERATIONAL ENVIRONMENT 17

3.3.1 ASSUMPTIONS ON PHYSICAL ASPECTS OF THE OPERATIONAL ENVIRONMENT: 17
3.3.2 ASSUMPTIONS ON PERSONNEL ASPECTS OF THE OPERATIONAL ENVIRONMENT 18
3.3.3 ASSUMPTIONS ON CONNECTIVITY ASPECTS OF THE OPERATIONAL ENVIRONMENT: 18

4 SECURITY OBJECTIVES 19

4.1 SECURITY OBJECTIVES FOR THE TOE 19
4.1.1 RATIONALE FOR THE SECURITY OBJECTIVES FOR THE TOE 19
4.1.1.1 Mappings of TOE Security Objectives to Threats and OSP 19
4.1.1.2 Security Objectives Rationale for Threats 20
4.2 SECURITY OBJECTIVES FOR THE TOE OPERATIONAL ENVIRONMENTAL 22
4.2.1 RATIONALE FOR THE SECURITY OBJECTIVES FOR THE TOE OPERATIONAL ENVIRONMENT 22
4.2.1.1 Mappings of Security Objectives to Threats, OSP, and Assumptions 22
4.2.1.2 IT Security Objectives Rationale for Assumptions 22

5 EXTENDED COMPONENTS DEFINITION 24

5.1 EXTENDED SECURITY FUNCTION REQUIREMENTS DEFINITIONS 24
5.1.1 CLASS FPT: PROTECTION OF THE TSF 24
5.1.1.1 Device pairing (FPT_PAR_EXP) 24
5.2 EXTENDED SECURITY ASSURANCE REQUIREMENT DEFINITIONS 25
5.3 RATIONALE FOR EXTENDED SECURITY REQUIREMENTS 25
5.3.1 RATIONALE FOR EXTENDED SECURITY FUNCTION REQUIREMENTS 25
5.3.2 RATIONALE FOR EXTENDED SECURITY ASSURANCE REQUIREMENTS 25

6 SECURITY REQUIREMENTS 26

6.1 SECURITY FUNCTION REQUIREMENTS 26
6.1.1 CLASS FDP: USER DATA PROTECTION 26
6.1.1.1 Information flow control policy (FDP_IFC) 26
6.1.1.1.1 FDP_IFC.1 (Subset Information Flow Control) 26
6.1.1.2 Information flow control functions (FDP_IFF) 26
6.1.1.2.1 FDP_IFF.1 (Simple Security Attributes) 26
6.1.2 CLASS FMT: SECURITY MANAGEMENT 27
6.1.2.1 FMT_MSA.1 Management of Security Attributes 27
6.1.2.2 FMT_MSA.3 (Static Attribute Initialization) 27
6.1.3 CLASS FPT: PROTECTION OF THE TSF 27
6.1.3.1 FPT_PAR_EXT.1 Device pairing 27
6.1.4 CLASS EXT: EXTENDED REQUIREMENTS 27
6.1.4.1 EXT_VIR.1 (Visual Indication Rule) 27
6.1.4.2 EXT_IUC.1 (invalid USB Connection) 28
6.1.4.3 EXT_ROM.1 Read-Only ROMs 28
6.2 SECURITY ASSURANCE REQUIREMENTS FOR THE TOE 29
6.3 SECURITY REQUIREMENTS RATIONALE 30
6.3.1 SECURITY FUNCTION REQUIREMENTS RATIONALE 30
6.3.1.1 Security Function Requirements Rationale 30

6.3.1.2 Security requirement dependency analysis 31
6.3.1.2.1 Rationale for unsatisfied dependencies: 32
6.3.2 SECURITY ASSURANCE REQUIREMENTS RATIONALE 32
6.3.2.1.1 Security requirement dependency analysis 33

7 TOE SUMMARY SPECIFICATION 34

7.1 IMPLEMENTATION DESCRIPTION OF TOE SFRS 34
7.2 TOE SECURITY FUNCTIONS 34
7.2.1 USER DATA PROTECTION 34
7.2.2 SECURITY MANAGEMENT 34
7.2.3 PROTECTION OF THE TSF 35
7.2.4 EXTENDED REQUIREMENTS 36

8 REFERENCES 39

Tables

Table 1 - Threats countered by the TOE and TOE IT Environment 17
Table 2 - Organizational Security Policies for the TOE 17
Table 3 - Assumptions on Physical Aspects of the Operational Environment 18
Table 4 - Assumptions on Personnel Aspects of the Operational Environment 18
Table 5 - Security Objectives for the TOE 19
Table 6 - Mapping of TOE Security Objectives to Threats and OSP 20
Table 7 - Security Objectives for the TOE Operational Environmental 22
Table 8 - Mapping of TOE Operational Environment Security Objectives to Assumptions 22
Table 9 - TOE Security Functional Requirements CC Part 2 Extended 24
Table 10 - TOE Security Functional Requirements 26
Table 11 – Assurance Requirements 29
Table 12 - TOE SFR/SAR to Objective Mapping 30
Table 13 - SFR Component Dependency Mapping 31
Table 14 - Evaluation assurance level summary 32
Table 15 - SAR Component Dependency Mapping 33
Table 16 – LCD Display Messages 36
Table 17 - TOE Related Abbreviations and Acronyms 38
Table 18 - CC Related Abbreviations and Acronyms 38
Table 19 - TOE Guidance Documentation 39
Table 20 - Common Criteria v3.1 References 39
Table 21 – Supporting Documents 39

1 Security Target (ST) Introduction

The structure of this document is defined by CC v3.1r3 Part 1 Annex A.2, "Mandatory contents of an ST":

- Section 1 contains the ST Introduction, including the ST reference, Target of Evaluation (TOE) reference, TOE overview, and TOE description.
- Section 2 contains conformance claims to the Common Criteria (CC) version, Protection Profile (PP) and package claims, as well as rationale for these conformance claims.
- Section 3 contains the security problem definition, which includes threats, Organizational Security Policies (OSP), and assumptions that must be countered, enforced, and upheld by the TOE and its operational environment.
- Section 4 contains statements of security objectives for the TOE, and the TOE operational environment as well as rationale for these security objectives.
- Section 5 contains definitions of any extended security requirements claimed in the ST.
- Section 6 contains the security function requirements (SFR), the security assurance requirements (SAR), as well as the rationale for the claimed SFR and SAR.
- Section 7 contains the TOE summary specification, which includes the detailed specification of the IT security functions

1.1 Security Target Reference

The Security Target reference shall uniquely identify the Security Target.

ST Title:	NCS Technologies Model Stratus CM 4110 and Stratus CM 4120 Security Target
ST Part Number:	V001851
ST Version Number:	Version 1.778
ST Author(s):	Gordon D McIntosh
ST Publication Date:	2013-04-26

Keywords: Multi-way SWITCH, PERIPHERAL switching, Keyboard-Video-Mouse (KVM) SWITCH

1.2 Target of Evaluation Reference

The Target of Evaluation reference shall identify the Target of Evaluation.

TOE Developer NCS Technologies, Inc.
7669 Limestone Drive
Gainesville, VA, 20155-4038

This Security Target describes two TOEs; however, the differences between the TOEs are power supply options that are not security relevant. These differences will be identified in Section 1.4.1.1, Target of Evaluation Physical Boundaries; because all security relevant features are identical, the majority of the Security Target will refer to the TOE as singular.

TOE 1 Name:	Stratus CM 4110
TOE 1 Version:	F103540-1

TOE 2 Name:	Stratus CM 4120
TOE 2 Version:	F103786-1

1.3 Target of Evaluation Overview

1.3.1 TOE Product Type

The TOE is classified as Peripheral Sharing Switch; a device that allows the sharing of a single set of peripheral components such as Keyboard, Video Monitor and Mouse (KVM) devices among multiple computers using a standard USB interface.

1.3.2 TOE Usage

The intended usage of the TOE is to share the connections from a single set of peripherals (Keyboard, Mouse, and Display) with multiple computers so a user can easily interface to these computers while maintaining complete isolation between computers.

1.3.3 TOE Major Security Features Summary

- User data protection
  - Provides secure user data transmission, and residual data protection mechanisms
- Security Management
  - Provides authorized administrators to manage the security features provided by the TOE
- Protection of the TSF
  - Pairing of the remote control and rest of the TSF
- Extended requirements
  - Visual indication of connected devices
  - Detection of invalid USB devices
  - Read-only ROM code

1.3.4 TOE IT environment hardware/software/firmware requirement summary

The TOE may be packaged with two (2) or three (3) independent NCST computers and may be used to control an additional customer-supplied computer that is not in the same physical package. The computers packaged with the TOE are termed “internal” computers; the computer not in the same package is termed “external.” The only requirement on the external computer is it must use USB v2.0 compatible keyboard and mouse and be compatible with version 1.1a of the DisplayPort specification; however, NCST recommends the Stratus ST 9196 or Stratus LT 9196, so the TOE can control the power state of the external computer.

1.4 Target of Evaluation Description

The TOE is a Peripheral Sharing Switch (PSS) that shares a Peripheral Port Group among up to four (4) computers, allowing a user with limited workspace to access these computers while maintaining isolation between the computers.

A Peripheral Port Group is a collection of device ports treated as a single entity by the TOE; it consists of a single keyboard port, dual monitor ports, and a single mouse port. There is one group for the set of shared peripherals and one group for each connected switched computer. Each switched computer group has some unique associated logical id. The shared peripheral group id is considered the same as that of the switched computer group currently selected by the TOE.

The peripheral port group allows the TOE to support a single keyboard, dual monitors, and a single mouse, restricting the connections so no other peripheral device shall be connected to the switch. These are also referred to as the shared peripherals. In operation, the TOE will be connected to only one computer at a time. To select different computers, the user presses the KVM button on the Remote Control.

The TOE precludes any features that permit user information to be shared or transferred between computers via the TOE.

1.4.1.1 Target of Evaluation Physical Boundaries

As stated above, this Security Target describes two TOEs, the Stratus CM 4110 vF103540-1 and the Stratus CM 4120 vF103786-1; which are comprised of a Control Module and a Remote Control; the Control Module provides the basic components to integrate multiple (up to three) independent (internal) computer modules in a stacked configuration referred to as a Stack. The Control Module is described in Section 1.4.1.1.1, Control Module Description where the power supply options for each TOE are fully described.

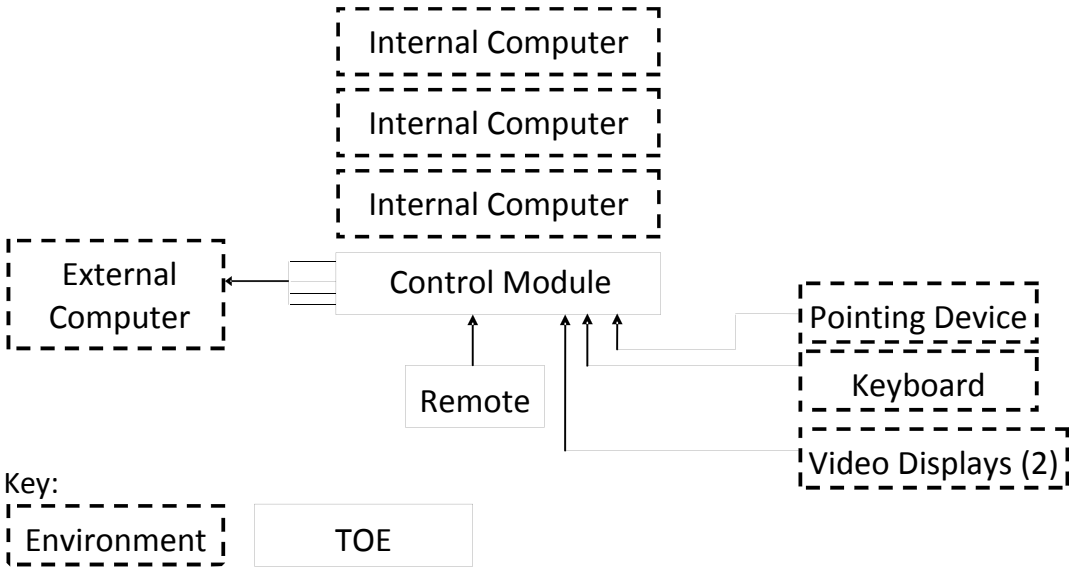


Figure 1: TOE Boundaries

For the Stratus CM 4110 vF103540-1, the TOE consists of:

- Control Module:
  - Model: STRATUS CM 4110
  - Revision: F103540-1
  - Including one (1) 50W auxiliary power supply (as each computer module has its own PSU).
- Remote Control:
  - Model: STRATUS SRC
  - Revision: 1023716-1
- Other components such as cables, metal chassis, power adapter board

The following NCST computers are compatible with the Stratus CM 4110 for use as internal computers:

- ST 9195 and LT 9195: small and large modules that will go on the top of the stack.
- SM 9195 and LM 9195: small and large modules that will be in the middle or bottom of the stack.

The following NCST cables are required to connect the internal computers to the Stratus CM 4110:

- 3 internal computers – Communication Backplane Part Number: 1022062-1
- 2 internal computers – Communication Backplane Part Number: 1024702-1

For the Stratus CM 4120 vF103786-1, the TOE consists of:

- Control Module:
  - Model: STRATUS CM 4120
  - Revision: F103786-1
  - Including one (1) Common ATX Power Supply Unit

- Remote Control:
  - Model: STRATUS SRC
  - Revision: 1023716-1
- Other components such as cables, metal chassis, power adapter board

The following NCST computers are compatible with the Stratus CM 4120 for use as internal computers:
- ST 9190 and LT 9190: small and large modules that will go on top of the stack.
- SM 9190 and LM 9190: small and large modules that will be in the middle or bottom of the stack.

The following NCST cables are required to connect the internal computers to the Stratus CM 4120:
- 3 internal computers
  - Communication Backplane Part Number: 1022062-1
  - Power Backplane Part Number: 1022063-1
- 2 internal computers
  - Communication Backplane Part Number: 1024702-1
  - Power Backplane Part Number: 1024703-1

The single external computer refers to a customer-supplied computer that may be connected to the TOE using the connectors on the secure KVM as described below.

1.4.1.1.1 Control Module Description

The Control Module is a secure KVM switch allowing the sharing of video display, USB keyboard, and USB mouse among Computer Modules on the Stack. The Master Controller in the secure KVM switch allows user to interact with the Stack through the Remote Control instead of having to reach for the buttons on the individual computer modules.

The Stratus CM 4110 includes one (1) 50W auxiliary power supply (as each computer module has its own PSU).

The Stratus CM 4120 includes one (1) Common ATX Power Supply Unit (PSU) providing power to all components, including all computer modules on the Stack and one (1) Power Adapter board to connect the ATX PSU to the flexible Power backplane.

1.4.1.1.2 Secure KVM Description

The secure KVM component of the TOE includes a general-purpose processor that executes internal TOE software, as well as volatile and non-volatile storage components. The TOE includes the following connectors, indicators and switches:
- The following connectors for shared peripheral devices (Peripheral Port Group):
  - Two (2) USB type A connectors for the keyboard and mouse
  - One 4 position DIP switch to enable or disable the USB type A connector for a Common Access Card (CAC) reader on the Remote Control. This switch will be set to disable (off) position by default.
    - Position 1 is used to enable/disable the USB connector for CAC card reader on the Remote Control when it is connected to internal computer 1
    - Position 2 is used to enable/disable the USB connector for CAC card reader on the Remote Control when it is connected to internal computer 2
    - Position 3 is used to enable/disable the USB connector for CAC card reader on the Remote Control when it is connected to internal computer 3
    - Position 4 is used to enable/disable the USB connector for CAC card reader on the Remote Control when it is connected to external computer
  - Two (2) DisplayPort[1] connectors for up to two monitors.
    - DisplayPort video using DisplayPort cables

[1] DisplayPort is a digital display interface standard put forth by the Video Electronics Standards Association (VESA) intended to be used primarily between a computer and its display.

    - DVI video using a DisplayPort to DVI cables to connect to DVI monitor.
    - HDMI video using a DisplayPort to HDMI cable to connect to HDMI monitor
    - VGA video using a DisplayPort to VGA cable to connect to VGA monitor.

- The following connectors for one external computer:
  - One (1) USB type B connector
  - Two (2) DisplayPort connectors to connect to the video ports of the external computer[2]
  - One (1) TRS (tip, ring, sleeve) jack to connect to the external computer
    - The tip bit is used to turn on and off the external computer
    - The ring bit is used to monitor the state of the external computer (on, off, sleep)
- The following connectors for up to three Internal Computers:
  - One (1) gold finger connector with the PCIeX16 form factor
- The following connector for connection to the Remote Control
  - One (1) HDMI connector (USB bus signals are used on this connector)
- The following connectors (headers):
  - One (1) power connector to connect to the power supply
  - One (1) ten (10) pin (2X5) connector (header) for the following:
    - Two pins are used to connected to the power button of the system
    - Two pins are used to connected to the LED to display power status (on/off)
    - The remaining 6 pins are not used
  - One four pin UART header for manufacturing tests; this header is disabled prior to shipment

1.4.1.1.3 Remote Control Description

The Remote Control, which provides the user interface, is used to control the switching of the KVM signals from the peripheral devices, the keyboard, video monitor(s), and mouse; switching those signals to one of the internal computers, or optionally, to a single external computer. Internal computers include those computers delivered as part of the NCST product offering, into which the TOE is integrated.

- The Remote Control has the following LCD and LED[3] indicators:
  - A small LCD screen provides operating state and error state information for the user.
  - Four (4) LEDs for the KVM switch used to indicate which computer is connected to the set of peripheral devices connected to the KVM.
  - Four (4) LEDs to indicate the power status of each computer and are provided for user convenience; they provide the same function as the LEDs in front of the computers. An ON LED indicates the computer has power, an OFF LED indicates the computer is off, and a blinking LED indicates that the computer is in sleep mode.
  - One (1) LED to indicate the state of the enable button; when the user presses the enable button, this LED turns on. It indicates that the computers can be turned on/off from the Remote Control. Use of the enable button avoids accidentally turning the computer on/off.
- Upon intrusion, all LEDs will blink to get user's attention, and the LCD will display "INTRUSION DETECTED" as described in Table 16 – LCD Display Messages.
- The Remote Control has the following switches for management:
  - Four (4) switches to control which computer is connected to the Shared Peripheral Group
    - These buttons are labeled 1 to 4 (Computer Module 1 to Computer Module 4)
  - Four (4) power on/off switches, one for each computer module
  - One (1) dual function switch for Master Power and power enable/disable mode
    - Pressing this button once will toggle it between enable and disable modes
      - In disable mode, the enable LED will be off and the four power on/off switches, don't work. This is to avoid accidently powering on and off the modules.

[2] The external computer must support DisplayPort video compatible with version 1.1a of the specification. DVI, HDMI and VGA will not work.

[3] The color of all KVM and power LEDs on the Remote Control can be programmed to cyan, red, green, yellow, or blue; prior to programming the default color of all KVM LEDs is cyan, all power LEDs is blue and enable LED is always blue. Programming details are found in User guidance [1].

        - Note that the KVM buttons always work regardless whether the power buttons are in enable or disable mode.
      - In enable mode, the enable LED will be on; pressing this button again will
        - Turn on the entire stack if all computers are off
        - Turn off the entire stack if all computers are on
        - Wake up the sleeping computer and turn on computers in the stack if they are in different power modes (mix of sleep, off and on).
      - In enable mode, the enable LED will be on. Press and hold this button for more than 4 seconds will force all computers to turn off.
      - In enable mode, the enable LED will be on. Pressing power on/off switch above will turn on/off the corresponding computer or wake the corresponding sleeping computer up.
      - In enable mode, the enable LED will be on. Press and hold the power button above for more than 4 seconds will force the corresponding compute off.
    - If the Master Power button is idle (not use) for more than 10 seconds, firmware will disable it. This is done to avoid accidentally powering on and off the entire stack. The user will need to press it once to enable it again.
  - One (1) LED color programming switch
    - The LED color programming switch allows user to program the color of the LEDs on the Remote Control.
- The Remote Control has the following connectors:
  - One (1) USB type A connector for a CAC card reader (only a CAC reader can work on this port). This USB connector is not included in the evaluated configuration. By default, this USB connector is disabled by the 4-position DIP switch on the KVM.
  - One HDMI type C connector to connect to the Control Module
  - One security tab for pairing the Remote Control with the KVM in the Control Module[4]

1.4.1.2 TOE Guidance Documentation

The TOE guidance documentation is listed in Section 8, “References,” within Table 19 - TOE Guidance Documentation.

1.4.2 Target of Evaluation Logical Boundaries

The logical boundaries of the TOE include those security functions implemented exclusively by the TOE. These security functions were summarized in Section 1.3.3 above and further described in the following subsections. A more detailed description of the implementation of these security functions are provided in Section 7, “TOE Summary Specification.”

1.4.2.1 User data protection

The TOE protects user data by enforcing the information flow control policy, which assures that the TOE connects the Peripheral Port Group to only a single computer at one time. Switches on the Remote Control allow the operator to select which computer is connected to the shared Peripheral Port Group at any given time. Each connected computer has a discrete switch and hub on the TOE assigned to its USB port and each switched computer has its own logical ID within the TOE through this switch arrangement. Through this dedicated switching mechanism, the connection between the shared Peripheral port group and the selected computer is activated. The design of these switches and associated circuitry assure that only a single computer can be engaged by the keyboard, mouse and video monitor resources. Through this information flow security function, the TOE precludes the sharing or transfer of data between computers by the TOE.

[4] The security tab is a thin plastic tape that user has to pull out to activate pairing of the Remote Control with the KVM in the Control Module.

1.4.2.2 Security Management

The TOE supports management of the data flows using a user actuated manual switching mechanism; data can flow to or from the Shared Peripheral Group only if it was received from the same switched computer. This switching mechanism precludes activating two switched computers at once or partial activation of more than a single computer to the Shared Peripheral Group.
When power is applied to the TOE, the Shared Peripheral Group is always connected to computer 1.

1.4.2.3 Protection of the TSF

The TOE requires that the remote control portion of the TOE be paired with the KVM portion of the TOE to prevent other users from using a different remote control to access a KVM to which they are not authorized. The pairing of the remote control and the KVM is performed during initial setup.

1.4.2.4 Extended requirements

The TOE provides a LED indicator light above the push button switch that indicates to the user which computer is connected to the Shared Peripheral Group; the LED remains on as long as the indicated computer is connected to the Shared Peripheral Group. The selected computer is also displayed on the small LCD screen, for example, “COMPUTER 1 SELECTED”.

The TOE ensures the USB devices connected to the Shared Peripheral Group are a valid pointing device, and/or keyboard. If an invalid device is detected, the TOE will cease communication with the device.

The TOE protects the firmware through the usage of a one-time programmable device so that the device becomes read only; after which, no modifications can be made. Additionally, all programmable devices in the TOE are permanently attached (soldered) to the PCB board.

1.5 Roles, User Data, and TSF Data

The TOE is not required to associate users with roles; hence, there is only one “role”, that of user.

a. Users can pass data through the TOE but do not have direct access

User data is any data that passes through the TOE; it does not affect the operation of the TSF.

TSF data includes the following:

- None

1.6 Notation, formatting, and conventions

The notation, formatting, and conventions used in this security target are defined below; these styles and clarifying information conventions were developed to aid the reader.

Where necessary, the ST author has added application notes to provide the reader with additional details to aid understanding; they are italicized and usually appear following the element needing clarification. Those notes specific to the TOE are marked “TOE Application Note;” those taken from the PSS Protection Profile are marked “PP Application Note.”

The notation, formatting, and conventions used in this security target are defined below; these styles and clarifying information conventions were developed to aid the reader.

The notation conventions that refer to iterations, assignments, selections, and refinements made in this security target are in reference to SARs and SFRs taken directly from CC Part 2 and Part 3 as well as any SFRs and SARs taken from a protection profile.

The notation used in those PP to indicate iterations, assignments, selections, and refinements of SARs and SFRs taken from CC Part 2 and Part 3 is not carried forward into this document. Additionally, obvious errors in the PP will be corrected and noted as such.

The CC permits four component operations: assignment, iteration, refinement, and selection to be performed on requirement components. These operations are defined in Common Criteria, Part 1; paragraph 6.4.1.3.2, “Permitted operations on components” as:

- Iteration: allows a component to be used more than once with varying operations;
- Assignment: allows the specification of parameters;
- Selection: allows the specification of one or more items from a list; and
- Refinement: allows the addition of details.

Iterations made by the ST author are indicated by a letter following the requirement number, e.g., FIA_UAU.1.1a; the iterated requirement titles are similarly indicated, e.g., FIA_UAU.1a.

Assignments made by the ST author are identified with ***bold italics;*** selections are identified with **bold text.**

Refinements made by the ST author are identified with "**Refinement:**" right after the short name; the refined text indicated by underlined text; any refinement that performs a deletion in text is noted in the endnotes sections indicated.

2 Conformance Claims

2.1 Common Criteria Conformance Claims

This Security Target is conformant to the Common Criteria Version 3.1r3, CC Part 2 extended [8], and CC Part 3 [9].

2.2 Conformance to Protection Profiles

This Security Target claims strict conformance to the Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, Version 2.1, dated September 7, 2010.[11]; therefore, it meets EAL 2 augmented with ALC_FLR.2.

2.3 Conformance to Security Packages

This Security Target does not claim conformance to any security function requirements package, neither as package-conformant or package-augmented.

This Security Target is Evaluation Assurance Level 2 (EAL2).

2.4 Conformance Claims Rationale

The TOE conforms to the Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile, Version 2.1, dated September 7, 2010.[11]. This Protection Profile will be called PSS PP for convenience through this Security Target.

This ST claims strict conformance to the PSS PP as specified in Section D2 of CC Part 1 [7]. To meet this requirement, the ST must show that the requirements in the PP are met, that the ST is an instantiation of the PP, though the ST could be broader than the PP. In essence, the ST specifies that the TOE does at least the same as in the PP, while the operational environment does at most the same as in the PP.

To demonstrate that strict conformance is met, this rationale must show all threats are addressed, all OSP are satisfied, no additional assumptions are made, all objectives have been addressed, and all SFRs and SARs have been instantiated.

The following address the completeness of the threats, OSP, objectives, and limitations on the assumptions:

- Threats
  - All threats defined in the PSS PP are carried forward to this ST
  - No additional threats have been defined in this ST
- Organizational Security Policies
  - All OSP defined in the PSS PP are carried forward to this ST;
  - One additional OSP has been defined in this Security Target as follows:
    - P.RC_PROTECTION
- Assumptions
  - All assumptions defined in the PSS PP are carried forward to this ST;
  - No additional assumptions for the operational environment have been defined in this ST
- Objectives
  - All objectives defined in the PSS PP are carried forward to this ST

All SFRs and SARs defined in the PSS PP are carried forward to this Security Target; all were fully defined with no selections or assignments allowed, additionally, no iterations were made. The SFR EXT_IUC.1.1 was refined to reflect the lack of USB display devices available; the word display was removed from the list of allowed devices.

Rationale presented in the body of this ST shows all assumptions on the operational environment have been upheld, all the OSP are enforced, all defined objectives have been met and these objectives counter the defined threats.

Additionally, all SFRs and SFRs defined in the PSS PP have been properly instantiated in this Security Target; therefore, this ST shows strict conformance to the PSS PP.

3 Security Problem Definition

3.1 Threats

The following subsections define the security threats for the TOE, characterized by a threat agent, an asset, and an adverse action of that threat agent on that asset. These threats are taken directly from the PP unchanged.

3.1.1 Threats countered by the TOE and TOE IT Environment

Table 1 - Threats countered by the TOE and TOE IT Environment		
#	Threat	Description
1	T.INVALIDUSB	The AUTHORIZED USER will connect unauthorized USB devices to the peripheral switch.
2	T.RESIDUAL	RESIDUAL DATA may be transferred between PERIPHERAL PORT GROUPS with different IDs.
3	T.ROM_PROG	The TSF may be modified by an attacker such that code embedded in reprogrammable ROMs is overwritten, thus leading to a compromise of the separation-enforcing components of the code and subsequent compromise of the data flowing through the TOE.
4	T.SPOOF	Via intentional or unintentional actions, a USER may think the set of SHARED PERIPHERALS are CONNECTED to one COMPUTER when in fact they are connected to a different one.
5	T.TRANSFER	A CONNECTION, via the TOE, between COMPUTERS may allow information transfer.

3.2 Organizational Security Policies

3.2.1 Organizational Security Policies for the TOE

Table 2 - Organizational Security Policies for the TOE	
OSP	Description
P.RC_PAIRING_PROTECTION	The KVM portion of the TOE shall establish a unique logical pairing with a given remote control; if a different pairing is attempted, the KVM portion of the TOE will ignore commands from the remote control, and instruct the remote control to display an error message.

3.3 Assumptions on the TOE Operational Environment

This section describes the assumptions that are made on the operational environment in which the TOE is intended to be used in order to be able to provide security functionality. It includes information about the physical, personnel, and connectivity aspects of the environment. The operational environment must be managed in accordance with the provided guidance documentation. The following subsections define specific conditions that are assumed to exist in an environment where the TOE is deployed.

3.3.1 Assumptions on Physical Aspects of the Operational Environment:

The TOE is intended for application in areas that have physical control and monitoring. It is assumed that the following physical conditions will exist:

Table 3 - Assumptions on Physical Aspects of the Operational Environment	
Assumption	Description
A.PHYSICAL	The TOE is physically secure.

3.3.2 Assumptions on Personnel Aspects of the Operational Environment

Table 4 - Assumptions on Personnel Aspects of the Operational Environment	
Assumption	Description
A.NO_EVIL	The AUTHORIZED USER is non-hostile and follows all usage guidance.
A.MANAGE	The TOE is installed and managed in accordance with the manufacturer's directions.
A.ACCESS	An AUTHORIZED USER possesses the necessary privileges to access the information transferred by the TOE. USERS are AUTHORIZED USERS.

3.3.3 Assumptions on Connectivity aspects of the Operational Environment:

There are no assumptions regarding the connectivity aspect of the operational environment.

4 Security Objectives

4.1 Security Objectives for the TOE

Table 5 - Security Objectives for the TOE		
#	TOE Objective	Description
1	O.CONF	The TOE shall not violate the confidentiality of information which it processes. Information generated within any PERIPHERAL GROUP COMPUTER CONNECTION shall not be accessible by any other PERIPHERAL GROUP with a different GROUP ID.
2	O.INDICATE	The AUTHORIZED USER shall receive an unambiguous indication of which SWITCHED COMPUTER has been selected.
3	O.ROM	TOE software/firmware shall be protected against unauthorized modification. Embedded software must be contained in mask-programmed or one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly.
4	O.SELECT	An explicit action by the AUTHORIZED USER shall be used to select the COMPUTER to which the shared set of PERIPHERAL DEVICES is CONNECTED Single push button, multiple push button, or rotary selection methods are used by most (if not all) current market products. Automatic switching based on scanning shall not be used as a selection mechanism.
5	O.SWITCH	All DEVICES in a SHARED PERIPHERAL GROUP shall be CONNECTED to at most one SWITCHED COMPUTER at a time.
6	O.USBDETECT[5]	The TOE shall detect any USB connection that is not a pointing device or keyboard and will perform no interaction with that device after the initial identification.
7	O.PAIR_PROTECT	The KVM portion of the TOE shall establish a permanent unique pairing with a given remote control; if a different pairing is attempted, the KVM portion of the TOE will detect the violation, ignore commands from the remote control, and instruct the remote to display an error message.

4.1.1 Rationale for the Security Objectives for the TOE

4.1.1.1 Mappings of TOE Security Objectives to Threats and OSP

The following table shows the mapping of security objectives for the TOE to threats countered by that objective, and the OSP enforced by that objective.

[5] The objective was modified to remove “display” from the types of devices detected; there are no USB displays allowed.

Table 6 - Mapping of TOE Security Objectives to Threats and OSP							
		Threats					OSP
#	TOE Objective	T.INVALIDUSB	T.RESIDUAL	T.ROM_PROG	T.SPOOF	T.TRANSFER	P.RC_PAIRING_PROTECTION
1	O.CONF		X			X	
2	O.INDICATE				X		
3	O.ROM			X			
4	O.SELECT			X			
5	O.SWITCH					X	
6	O.USBDETECT	X					
7	O.PAIR_PROTECT						X

4.1.1.2 Security Objectives Rationale for Threats

This section presents the rationale that justifies that the security objectives for the TOE are suitable to counter all threats to be countered by the TOE.

O.CONF

O.CONF will counter the threats T.RESIDUAL and T.TRANSFER by limiting access to information generated within a group to members of that group. If the PERIPHERALS can be CONNECTED to more than one COMPUTER at any given instant, then a channel may exist which would allow transfer of information from one to the other. This is particularly important for DEVICES with bi-directional communications channels such as KEYBOARD and POINTING DEVICES. Since many PERIPHERALS now have embedded microprocessors or microcontrollers, significant amounts of information may be transferred from one COMPUTER system to another, resulting in compromise of sensitive information. An example of this is transfer via the buffering mechanism in many KEYBOARDS.

Further, the purpose of the TOE is to share a set of PERIPHERALS among multiple COMPUTERS. Information transferred to/from one SWITCHED COMPUTER is not to be shared with any other COMPUTER

O.INDICATE

O.INDICATE helps mitigate the threat T.SPOOF, by ensuring the USER receives positive confirmation of SWITCHED COMPUTER selection.

O.ROM

O.ROM helps mitigates the threat, T.ROM_PROG, by ensuring that the ROMs used in the TSF to hold embedded TSF data are not physically able to be re-programmed. Thus, even if an interface does exist to the ROM containing the embedded TSF code, high confidence can be obtained that that code (stored in the ROM) will remain unchanged.

O.SELECT

O.SELECT helps mitigates the threat, T.ROM_PROG, by ensuring that the USER must take positive action to select the current SWITCHED COMPUTER.

O.SWITCH

O.SWITCH helps mitigates the threat, T.TRANSFER, by ensuring all DEVICES in a SHARED PERIPHERAL GROUP are CONNECTED to at most one SWITCHED COMPUTER at a time. The purpose of the TOE is to share a set of PERIPHERALS among multiple COMPUTERS. It makes no sense to have, for example, video CONNECTED to one COMPUTER while a POINTING DEVICE is CONNECTED to another COMPUTER.

O.USBDETECT

O.USBDETECT will help counter the threat T.INVALIDUSB by detecting the unauthorized connection so that all information from it can be ignored.

O.PAIR_PROTECT

O.PAIR_PROTECT will enforce the OSP P.RC_PAIRING_PROTECTION by establishing a permanent unique association (pairing) between a given remote control and the KVM portion of the TOE; and if a different pairing is attempted, the KVM portion of the TSF will detect the violation, ignore commands from the remote control, and instruct the remote to display an error message.

4.2 Security Objectives for the TOE Operational Environmental

Table 7 - Security Objectives for the TOE Operational Environmental		
#	Objective	Description
1	OE.ACCESS	The AUTHORIZED USER shall possess the necessary privileges to access the information transferred by the TOE. USERS are AUTHORIZED USERS.
2	OE.MANAGE	The TOE shall be installed and managed in accordance with the manufacturer's directions.
3	OE.NOEVIL	The AUTHORIZED USER shall be non-hostile and follow all usage guidance.
4	OE.PHYSICAL	The TOE shall be physically secure.

4.2.1 Rationale for the Security Objectives for the TOE Operational Environment

4.2.1.1 Mappings of Security Objectives to Threats, OSP, and Assumptions

Table 8 - Mapping of TOE Operational Environment Security Objectives to Assumptions, shows the mapping of security objectives for the TOE operational environment to threats countered by that objective, the OSP enforced by that objective, and/or the assumption upheld by that objective.

Table 8 - Mapping of TOE Operational Environment Security Objectives to Assumptions					
		Assumptions			
#	TOE Objective	A.ACCESS	A.MANAGE	A. NOEVIL	A.PHYSICAL
1	OE.ACCESS	X			
2	OE.MANAGE		X		
3	OE.NOEVIL			X	
4	OE.PHYSICAL				X

4.2.1.2 IT Security Objectives Rationale for Assumptions

This section presents the rationale that justifies the security objectives for the TOE operational environment are upheld by that objective.

OE.ACCESS

By ensuring all authorized users are trustworthy individuals, having background investigations commensurate with the level of data being protected, have undergone appropriate training, and follow all user guidance, the assumption A.ACCESS is addressed.

OE.MANAGE

By ensuring the TOE shall be installed and managed in accordance with the manufacturer's directions, the assumption A.MANAGE is addressed.

OE.NOEVIL

By ensuring the AUTHORIZED USER shall be non-hostile and follow all usage guidance, the assumption A. NOEVIL is addressed.

OE.PHYSICAL

By ensuring the TOE is protected from physical attack (e.g., theft, modification, destruction, or eavesdropping), the assumption A.PHYSICAL is addressed. Physical attack could include unauthorized intruders into the TOE environment, but it does not include physical destructive actions that might be taken by an individual that is authorized to access the TOE environment.

5 Extended Components Definition

This section provides definition of the extended security functional and assurance requirements; the components that are CC Part 2 extended (if present), and CC Part 3 extended (if present), i.e., NIAP interpreted requirements, and extended requirements.

5.1 Extended Security Function Requirements Definitions

This section defines the extended security functional requirements for the TOE defined in this Security Target, i.e., additional extended defined requirements found in this ST are defined in the PSS PP [11] and are included by reference. The security functional requirement components in this security target are CC Part 2 extended.

Table 9 - TOE Security Functional Requirements CC Part 2 Extended				
#	SFR	Description	Dependencies	Hierarchical to
1	FPT_PAR_EXP.1	Device pairing	None	None

5.1.1 Class FPT: Protection of the TSF

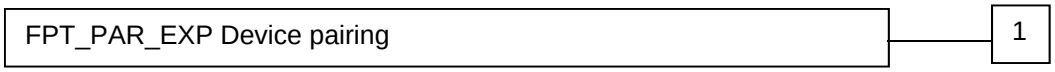
5.1.1.1 Device pairing (FPT_PAR_EXP)

Family Behavior

This family identifies the parts of the TOE that require permanent associations, the ability to detect if the association is violated, and the actions taken if the association is violated.

The requirements for device pairing ensure that interchangeable components used to control TSF behavior cannot be used to control other TOE's behaviors.

Component leveling



User Notes
The need arises for device pairing when remote control devices used to control the controlled portion of a TSF could potentially be used to control the behavior of other TOEs, which may allow an unauthorized user to control TOE functions. By requiring that a permanent association be established between the remote control and the controlled portion of the TSF, a remote control cannot be used to control other TOEs initialized with a different remote control.

FPT_PAR_EXP.1 Device pairing identifies the parts of the TOE that require permanent associations, the ability to detect violations, and the actions taken if the association is violated.

Management: FPT_PAR_EXP.1

There are no management activities foreseen.

Audit: FPT_PAR_EXP.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: detection of association violation.

FPT_PAR_EXP.1 Device pairing

Hierarchical to:	No other components
Dependencies:	None
FPT_PAR_EXP.1.1	The [assignment: TOE component] of the TSF shall be able to permanently associate the following TOE components: [assignment: TOE components].
Application note:	*Device pairing must establish the permanent association between the TOE components named in the assignment during the first use of these components.*
FPT_PAR_EXP.1.2	The [assignment: TOE component] of the TSF shall be able to detect if the association is violated.
Application note:	*Violation of the permanent association refers to the attempted use of a different component that may allow an unauthorized user to access the TSF.*
FPT_PAR_EXP.1.3	The [assignment: TOE component] of the TSF shall perform the following actions if this association is violated: [assignment: action(s) taken].

5.2 Extended Security Assurance Requirement Definitions

There are no extended Security Assurance Requirements defined in this Security Target.

5.3 Rationale for Extended Security Requirements

This section presents the rationale for the inclusion of the extended requirements found in this Security Target.

5.3.1 Rationale for Extended Security Function Requirements

The following rational is presented for the extended security function requirements defined in this security target.

FPT_PAR_EXP.1 Device pairing

This SFR is extended because Part 2 of the Common Criteria does not address the requirements to establish permanent associations between parts of the TOE. This TOE requires components that allow the TOE be remotely controlled; therefore, it is potentially possible an unauthorized user attempt to control the TSF using a different remote control.

5.3.2 Rationale for Extended Security Assurance Requirements

There are no extended Security Assurance Requirements defined in this ST; therefore, no rational is presented.

6 Security requirements

This section describes the security functional and assurance requirements for the TOE; those that are CC Part 2 conformant, CC Part 2 extended, and CC Part 3 conformant.

6.1 Security Function Requirements

This section describes the functional requirements for the TOE. The security functional requirement components in this security target are CC Part 2 conformant or CC Part 2 extended as defined in Section 2, “Conformance Claims.”

Table 10 - TOE Security Functional Requirements

#	SFR	Description	Dependencies	Hierarchical to	Operations
1	FDP_IFC.1	Subset Information Flow Control	FDP_IFF.1	None	---
2	FDP_IFF.1	Simple Security Attributes	FDP_IFC.1 FMT_MSA.3	None	---
3	FMT_MSA.1	Management of Security Attributes	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1]	None	---
4	FMT_MSA.3	Static Attribute Initialization	FMT_MSA.1 FMT_SMR.1	None	A
5	FPT_PAR_EXT.1	Device pairing	None	None	A
6	EXT_VIR.1	Visual Indication Rule	None	None	---
7	EXT_IUC.1	Invalid USB Connection	None	None	R
8	EXT_ROM.1	Read-Only ROMs	None	None	---

6.1.1 Class FDP: User data protection

6.1.1.1 Information flow control policy (FDP_IFC)

6.1.1.1.1 FDP_IFC.1 (Subset Information Flow Control)

FDP_IFC.1.1 The TSF shall enforce the Data Separation SFP on the set of peripheral port groups, and the bi-directional flow of peripheral data between the shared peripherals and the switched computers.

6.1.1.2 Information flow control functions (FDP_IFF)

6.1.1.2.1 FDP_IFF.1 (Simple Security Attributes)

FDP_IFF.1.1 The TSF shall enforce the Data Separation SFP based on the following types of subject and information security attributes: peripheral port groups (subjects), peripheral data, and peripheral port group ids (attributes).

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

Switching Rule: peripheral data can flow to a peripheral port group with a given ID only if it was received from a peripheral port group with the same ID.

FDP_IFF.1.3 The TSF shall enforce the No additional information flow control SFP rules.

FDP_IFF.1.4 The TSF shall provide the following: No additional SFP capabilities.

FDP_IFF.1.5	The TSF shall explicitly authorize an information flow based on the following rules: No additional rules.
FDP_IFF.1.6	The TSF shall explicitly deny an information flow based on the following rules: No additional rules.

6.1.2 CLASS FMT: Security Management

6.1.2.1 FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1	The TSF shall enforce the Data Separation SFP to restrict the ability to modify the security attributes peripheral port group ids to the user.
PP Application Note:	*An authorized user shall perform an explicit action to select the computer to which the shared set of peripheral devices is connected, thus effectively modifying the group id associated with the peripheral devices.*

6.1.2.2 FMT_MSA.3 (Static Attribute Initialization)

FMT_MSA.3.1	The TSF shall enforce the Data Separation SFP to provide restrictive default values for security attributes that are used to enforce the SFP.
PP Application Note:	*On start-up, one and only one attached computer shall be selected.*
FMT_MSA.3.2	The TSF shall allow the none to specify alternative initial values to override the default values when an object or information is created.

6.1.3 Class FPT: Protection of the TSF

6.1.3.1 FPT_PAR_EXT.1 Device pairing

FPT_PAR_EXP.1.1	The ***KVM component*** of the TSF shall be able to permanently associate the following TOE components: ***remote control***.
Application note:	*Device pairing must establish the permanent association between the TOE components named in the assignment during the first use of these components.*
FPT_PAR_EXP.1.2	The ***KVM component*** of the TSF shall be able to detect if the association is violated.
Application note:	*Violation of the permanent association refers to the attempted use of a different component that may allow an unauthorized user to access the TSF.*
FPT_PAR_EXP.1.3	The ***KVM component*** of the TSF shall perform the following actions if this association is violated: ***Ignore commands from the remote control and instruct the remote control to display an error message on the remote control's LCD.***

6.1.4 Class EXT: Extended Requirements

6.1.4.1 EXT_VIR.1 (Visual Indication Rule)

EXT_VIR.1.1	A visual method of indicating which computer is connected to the shared set of peripheral devices shall be provided that is persistent for the duration of the connection.
PP Application Note:	*Does not require tactile indicators, but does not preclude their presence.*

6.1.4.2 EXT_IUC.1 (invalid USB Connection)

EXT_IUC.1.1 **Refinement:** All USB devices connected to the Peripheral switch shall be interrogated to ensure that they are valid (pointing device, keyboard). No further interaction with non-valid devices shall be performed.[6]

6.1.4.3 EXT_ROM.1 Read-Only ROMs

EXT_ROM.1.1 TSF software embedded in TSF ROMs must be contained in mask-programmed or one-time-programmable read-only memory permanently attached (non-socketed) to a circuit assembly.

[6] The SFR was refined to remove “display” from the types of devices detected; there are no USB displays allowed.

6.2 Security Assurance Requirements for the TOE

This Security Target is Evaluation Assurance Level 2 (EAL 2) as shown in Table 11 – Assurance Requirements below. The security assurance requirements for the TOE consist of the following components that are CC Part 3 conformant and CC Part 3 conformant as summarized in Table 11 below and detailed in the following subsections. These requirements are included by reference.

Table 11 – Assurance Requirements

Assurance Class	Assurance Component	Assurance Components Description
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
Life-cycle Support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
Security Target	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.1	Analysis of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

6.3 Security Requirements Rationale

6.3.1 Security Function Requirements Rationale

Table 12 - TOE SFR/SAR to Objective Mapping satisfies the requirement to trace each SFR back to the security objectives for the TOE.

Table 12 - TOE SFR/SAR to Objective Mapping								
		TOE Objective						
#	SFR/SAR	O.CONF	O.INDICATE	O.ROM	O.SELECT	O.SWITCH	O.USBDETECT	O.PAIR_PROTECT
1	FDP_IFC.1	X						
2	FDP_IFF.1	X				X		
3	FMT_MSA.1				X			
4	FMT_MSA.3				X			
5	FPT_PAR_EXT.1							X
6	EXT_VIR.1		X					
7	EXT_IUC.1						X	
8	EXT_ROM.1			X				
	ADV_ARC.1							
	ADV_FSP.2							
	ADV_TDS.1							
	AGD_OPE.1							
	AGD_PRE.1							
	ALC_CMC.2							
	ALC_CMS.2							
	ALC_DEL.1							
	ALC_FLR.2							
	ATE_COV.1							
	ATE_FUN.1							
	ATE_IND.2							
	AVA_VAN.2							

6.3.1.1 Security Function Requirements Rationale

The following paragraphs present the rationale that demonstrate that the SFRs meet all security objectives for the TOE.

O.CONF

FDP_ETC.1[7]

FDP_IFC.1: This captures the policy that no information flows between different PERIPHERAL PORT GROUP IDs.

FDP_IFF.1: This requirement identifies the security ATTRIBUTES needed to detail the operation of a switch and the rules allowing information transfer. This requirement is a dependency of FDP_IFC.1.

FDP_ITC.1: [8]

[7] The ST author removed this SFR from the rationale for O.CONF; there is no such SFR defined in this ST or defined in Section 5.1, “Target of Evaluation Security Requirements” of the PSS PP.

[8] The ST author removed this SFR from the rationale for O.CONF; there is no such SFR defined in this ST or defined in Section 5.1, “Target of Evaluation Security Requirements” of the PSS PP.

O.INDICATE

EXT_VIR.1: There must be some positive feedback from the TOE to the USER to indicate which SWITCHED COMPUTER is currently CONNECTED. [9]

O.ROM

EXT_ROM.1 implements the O.ROM objective directly. While there might be other ways to protect embedded TSF code on a ROM (programmable or not), the requirement stipulates an easily-verifiable implementation that ensures that the TSF code will not be overwritten or modified.

O.SELECT

FMT_MSA.1: This restricts the ability to change selected PERIPHERAL PORT GROUP IDS to the AUTHORIZED USER. This requirement is a dependency of FMT_MSA.3.
FMT_MSA.3: The TOE assumes a default PERIPHERAL PORT GROUP selection based on a physical switch position or a manufacturer's specified sequence for choosing among the CONNECTED COMPUTERS (CONNECTED here implies powered on). This requirement is a dependency of FDP_IFF.1.

O.SWITCH

FDP_IFF.1: This requirement identifies the security ATTRIBUTES needed to detail the operation of a switch and the rules allowing information transfer. This requirement is a dependency of FDP_IFC.1.

O.USBDETECT

EXT_IUC.1: Upon detection of an invalid USB connection, the switch will disable the connection and notify the user.

O.PAIR_PROTECT

FPT_PAR_EXT.1 : The KVM portion of the TOE shall establish a unique logical pairing with a given remote control; if a different pairing is attempted, the KVM portion of the TOE will ignore commands from the remote control, and instruct the remote control to display an error message.

6.3.1.2 Security requirement dependency analysis

Table 13 - SFR Component Dependency Mapping maps the dependencies that exist for each SFR. If the column labeled "satisfied" shows a dependency that has not been resolved, the rationale is provided in the text following the table, why this dependency does not apply for the TOE.

Table 13 - SFR Component Dependency Mapping

#	Component	Dependencies	Satisfied [Component #]
1	FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
2	FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 FMT_MSA.3
3	FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_IFC.1 No No
4	FMT_MSA.3	FDP_MSA.1 FMT_SMR.1	FDP_MSA.1 No
6	FPT_PAR_EXT.1	None	None
7	EXT_VIR.1	None	None
8	EXT_IUC.1	None	None
9	EXT_ROM.1	None	None

[9] Part 2 of the Common Criteria does not provide a component appropriate to express the requirement for visual indication

6.3.1.2.1 Rationale for unsatisfied dependencies:

Each functional requirement, including extended requirements was analyzed to determine that all dependencies were satisfied. All requirements were then analyzed to determine that no additional dependencies were introduced as a result of completing each operation. With the exception of dependencies related to FMT_MOF.1 (Management of security functions behavior), FMT_SMR.1 (Security Roles) and FMT_SMF.1 (Specification of Management Functions).

FMT_SMR.1

The TOE is not required to associate USERS with roles; hence, there is only one "role", that of USER. This deleted requirement, a dependency of FMT_MSA.1 and FMT_MSA.3, allows the TOE to operate normally in the absence of any formal roles.

FMT_SMF.1

The TOE is not required to manage functions in the conventional sense, the user "manages" the selection of the Peripheral Port Group Ids, which does not require a management function be defined; therefore, this dependency is not required for the secure operation of the TOE.

6.3.2 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the Common Criteria EAL2 assurance package.

The EAL chosen is based on the statement of the security environment (threats, organizational policies, assumptions) and the security objectives defined in this ST. The sufficiency of the EAL chosen is justified based on those aspects of the environment that have impact upon the assurance needed in the TOE

Given the amount of assurance deemed necessary to meet the security environment and objectives of the TOE and the intent of EAL 2, EAL 2 is an appropriate level of assurance for the TOE described in this ST. Therefore, EAL2 is an appropriate level of assurance for the TOE.

Table 14 shows the matrix of Security Assurance requirements; the ST assurance levels are shown in **BOLD** text, which clearly demonstrates that this Security Target meets EAL2.

Table 14 - Evaluation assurance level summary

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		**1**	1	1	1	1	1
	ADV_FSP	1	**2**	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		**1**	2	3	4	5	6
Guidance Documents	AGD_OPE	1	**1**	1	1	1	1	1
	AGD_PRE	1	**1**	1	1	1	1	1
Life-cycle Support	ALC_CMC	1	**2**	3	4	4	5	5
	ALC_CMS	1	**2**	3	4	5	5	5
	ALC_DEL		**1**	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	**1**	1	1	1	1	1
	ASE_ECD	1	**1**	1	1	1	1	1
	ASE_INT	1	**1**	1	1	1	1	1
	ASE_OBJ	1	**2**	2	2	2	2	2

Table 14 - Evaluation assurance level summary								
Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
	ASE_REQ	1	**2**	2	2	2	2	2
	ASE_SPD		**1**	1	1	1	1	1
	ASE_TSS	1	**1**	1	1	1	1	1
Tests	ATE_COV		**1**	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		**1**	1	1	1	2	2
	ATE_IND	1	**2**	2	2	2	2	3
Vulnerability Assessment	AVA_VAN	1	**2**	2	3	4	5	5

6.3.2.1.1 Security requirement dependency analysis

Table 15 - SAR Component Dependency Mapping, maps the dependencies that exist for each SAR to demonstrate all SAR dependencies are satisfied.

Table 15 - SAR Component Dependency Mapping		
Component	Dependencies	Satisfied
ADV_ARC.1	ADV_FSP.1 ADV_TDS.1	Yes – ADV_FSP.2 Yes – ADV_TDS.1
ADV_FSP.2	ADV_TDS.1	Yes – ADV_TDS.1
ADV_TDS.1	ADV_FSP.2	Yes - ADV_FSP.2
AGD_OPE.1	ADV_FSP.1	Yes - ADV_FSP.2
AGD_PRE.1	None	--
ALC_CMC.2	ALC_CMS.1	Yes – ALC_CMS.2
ALC_CMS.2	None	--
ALC_DEL.1	None	--
ALC_FLR.2	None	--
ATE_COV.2	ADV_FSP.2 ATE_FUN.1	Yes – ADV_FSP.2 Yes - ATE_FUN.1
ATE_FUN.1	ATE_COV.1	Yes - ATE_COV.1
ATE_IND.2	ADV_FSP.2 AGD_OPE.1 AGD_PRE.1 ATE_COV.1 ATE_FUN.1	Yes – ADV_FSP.2 Yes – AGD_OPE.1 Yes – AGD_PRE.1 Yes – ATE_COV.1 Yes - ATE_FUN.1
AVA_VAN.2	ADV_ARC.1 ADV_FSP.2 ADV_TDS.1 AGD_OPE.1 AGD_PRE.1	Yes - ADV_ARC.1 Yes - ADV_FSP.2 Yes - ADV_TDS.1 Yes – AGD_OPE.1 Yes - AGD_PRE.1

7 TOE Summary Specification

7.1 Implementation description of TOE SFRs

This section provides evaluators and potential consumers of the TOE with a high-level description of each SFR, thereby enabling them to gain a general understanding of how the TOE is implemented. These descriptions are intentionally not overly detailed, thereby disclosing no proprietary information. These sections refer to SFRs defined in Section 6, Security requirements.

7.2 TOE Security Functions

The TOE consists of the following Security Functions:

- User data protection
- Security Management
- Extended Requirements
- Protection of the TSF

7.2.1 User data protection

The TOE implements the Data Separation SFP information flow control policy to ensure information can flow only between the Shared Peripheral Group and the selected computer. This function is implemented using a hardware Multiplexers/DeMultiplexer (Mux/DeMux) to switch between the Shared Peripheral Group and the switched computers; the Mux/DeMux is controlled by the switches on the Remote Control. The Multiplexer/Demultiplxer is specifically designed such that only one computer is connected to the Shared Peripheral Group at one time and that there is no path for information flow between computers. Additionally, there is no memory in the Mux/DeMux so that there can be no residual data when switching between computers, therefore, no data can be transferred between computers. **FDP_IFC.1, FDP_IFF.1**

7.2.2 Security Management

The TOE provides a manual interface for management functions. This interface consists of switches and indicators as listed below:

- The Remote Control has the following LCD and LED[10] indicators:
  - A small LCD screen provides operating state and error state information for the user.
  - Four (4) LEDs for the KVM switch used to indicate which computer is connected to the set of peripheral devices connected to the KVM.
  - Four (4) LEDs to indicate the power status of each computer and are provided for user convenience; they provide the same function as the LEDs in front of the computers. A ON LED indicates the computer has power, an OFF LED indicates the computer is off and a blinking LED indicates that the computer is sleeping.
  - One (1) LED to indicate the state of the enable button; when the user presses the enable button, this LED turns on. It indicates that the computers can be turned on/off from the Remote Control. Use of the enable button avoids accidentally turning the computer on/off.
- Upon intrusion, all LEDs will blink to get user attention and the LCD will display “INTRUSION DETECTED” as described in Table 16 – LCD Display Messages.
- The Remote Control has the following switches for management:
  - Four (4) switches to control which computer is connected to the Shared Peripheral Group
    - These buttons are labeled 1 to 4 (Computer Module 1 to Computer Module 4)
  - Four (4) power on/off switches, one for each computer module
    - One (1) dual function switch for Master Power and power enable/disable mode

[10] The color of all KVM and power LEDs on the Remote Control can be programmed to cyan, red, green, yellow, or blue; prior to programming the default color of all KVM LEDs is cyan, all power LEDs is blue and enable LED is always blue. Programming details are found in User guidance [1].

- Pressing this button once will toggle it between enable and disable modes
- In disable mode, the enable LED will be off and the four power on/off switches don't work. This is to avoid accidently powering on and off the modules.
- Note that the KVM buttons always work regardless whether the power buttons are in enable or disable mode.
- In enable mode, the enable LED will be on. Pressing this button again will
  - Turn on the entire stack if all computers are off
  - Turn off the entire stack if all computer are on
  - Wake up the sleeping computer and turn on computers in the stack if they are in different power modes (mix of sleep, off and on).
- In enable mode, the enable LED will be on. Press and hold this button for more than 4 seconds will force all computers to turn off.
- In enable mode, the enable LED will be on. Pressing power on/off switch above will turn on/off the corresponding computer or wake the corresponding sleeping computer up.
- In enable mode, the enable LED will be on. Press and hold the power button above for more than 4 seconds will force the corresponding compute off.

- If the Master Power button is idle (not use) for more than 10 seconds, firmware will disable it. This is done to avoid accidentally powering on and off the entire stack. The user will need to press it once to enable it again.

o One (1) LED color programming switch
  o The LED color-programming switch allows user to program the color of the LEDs on the Remote Control.

The user manages the Shared Peripheral Group connection to the desired computer using the manual switches provided. Each computer has a corresponding switch that when pressed at the same time as the enable switch, turns on/off that computer. The enable switch is used to prevent accidental turning off the computers and as a master power switch. **FMT_MSA.1**

When TOE power is applied, the TOE switches the Shared Peripheral Group to computer 1 by default. This cannot be changed. **FMT_MSA.3**

7.2.3 Protection of the TSF

The TOE requires that a user's remote control be paired with their assigned KVM to prevent other users from using a different remote control to access a KVM to which they are not authorized. The pairing of the remote control and the KVM is performed during initial activation; e.g., during setup, the user is required to pull a security tab on the remote control. When the security tab is pulled, the serial number of the remote control is sent to the KVM where it is stored in a one-time programmable memory device; after writing the serial number to memory, the memory device is permanently changed to read-only. Each time a remote control is connected to the KVM, the serial number is transmitted to the KVM where it is validated. If the serial number is not correct, the KVM instructs the remote to display the error message "RC NOT MATCHED" on the LCD, and any command sent from the Remote Control to the KVM is ignored. If the KVM malfunctions after pairing, the system must be returned to NCS for replacement of the KVM.

The Remote Control security tab works as follows:

- When the security tab is intact, the pairing feature is disabled. The Remote Control can work with any unpaired KVM.
- When the security tab is pulled, the pairing feature is activated. The KVM will learn the serial number of the Remote Control and the KVM will only work with that remote (pairing).
- Once this feature is activated, the KVM will ignore any Remote Control that doesn't have the matched serial number.

FPT_PAR_EXT.1

7.2.4 Extended Requirements

The TOE provides a LED indicator light above the push button switch on the Remote control that indicates to the user which computer is connected to the Shared Peripheral Group; the LED remains on as long as the indicated computer is connected to the Shared Peripheral Group. These LEDs are described in Section 7.2.2, Security Management. **EXT_VIR.1**

The TOE also supports operational and error message display on a small LCD on the remote control. This LCD displays short messages intended to be self-explanatory for both normal and error indications. The messages that can be displayed are listed in Table 16 – LCD Display Messages.

Table 16 – LCD Display Messages	
Situation	Message displayed
Display current FW version of the secure Remote Control and secure KVM. Secure Remote Control on top line and secure KVM on bottom line. This information is only available at power up	RC 1.0.0 KVM 1.0.0
When a USB device that is not a keyboard or mouse is connected to the KVM	NON KB/M CONNECTED
When the paring of Remote Control and KVM is activated	PAIRING ACTIVATED
After pairing is activated, if a non-paired Remote Control is connected to the KVM	RC NOT MATCHED
When the Remote Control cannot communicate with the Master Controller in the KVM via the USB bus for whatever reasons	CONNECTION FAILED
If the KVM switch has been tampered	INTRUSION DETECTED
KVM is switched to Computer 1	COMPUTER 1 SELECTED
KVM is switched to Computer 2	COMPUTER 2 SELECTED
KVM is switched to Computer 3	COMPUTER 3 SELECTED
KVM is switched to Remote Computer	COMPUTER 4 SELECTED
When KVM cannot switch as commanded by user (for whatever reason)	KVM ERROR TRY AGAIN
When enable button is pressed	POWER BUTTON ENABLE
When enable button is activated and power button 1 is pressed	TURN ON (or OFF) COMPUTER 1
When enable button is activated and power button 2 is pressed	TURN ON (or OFF) COMPUTER 2
When enable button is activated and power button 3 is pressed	TURN ON (or OFF) COMPUTER 3
When enable button is activated and power button 4 is pressed	TURN ON (or OFF) COMPUTER 4
When enable (a.k.a. master power) button is pressed twice and all computers are off or in sleep mode (Enable button can be used to power on all computers at once)	TURN ON ALL COMPUTERS
When enable (a.k.a. master power) button is pressed twice and all computers are on (Enable button can be used to turn off all computers at once)	TURN OFF ALL COMPUTERS
When the Remote Control is in LED programming mode	LED CONFIG PRESS KVMs
When the safety lock on the stack is activated (unsafe condition)	SYSTEM UNLOCKED

The TOE detects when a USB device is connected to the Shared Peripheral Group Ports and verifies the validity of the device; to be a valid device it may only be a pointing device or a keyboard device. This security function is implemented as follows:
When a USB device is plugged in, the microcontroller reads the class, subclass and protocol information of the device as defined in the USB standard. By reading this information, the microcontroller identifies if the USB device is a USB keyboard, USB mouse (pointing device) or something else. If it is a USB keyboard or mouse, the microcontroller switches the MUX to connect the keyboard or mouse to the KVM. If it is something else, the microcontroller will not switch the MUX. As a result, the undesired USB device is not connected to the KVM.

When the USB device, valid or invalid, is unplugged and another device is plugged in, the microcontroller will be interrupted and the procedure above repeats. **EXT_IUC.1**

The USB standards used are:

- USB Specification
  - Version 2.0, April 27, 2000
- USB HID (Human Interface Device) Usage table,
  - Version 1.12, October 28, 2004
- USB Device Class Definition for Human Interface Device (HID) Firmware Specification,
  - Version 1.11, June 27, 2001.

The TOE prevents any program modifications to the firmware by using a one-time programmable device that has security settings set to execute-only after programming; this is implemented by writing two (2) bits in the flash memory control register when programming is complete. Execute-only means the block may only be executed and may not be read, written or erased. This mode is used to protect code. Execute-only protection prevents both modification and visibility to a protected flash block.

To prevent a change to the security settings of the device, once the final security configuration is decided, the security settings are permanently written to the device by performing a commit sequence.

All programmable devices in the TOE are permanently attached (soldered) to the PCB board.
EXT_ROM.1

Acronyms

Table 17 - TOE Related Abbreviations and Acronyms	
Abbreviations/ Acronyms	Description
KVM	Keyboard-Video-Mouse
PPG	Peripheral Port Group
PSS	Peripheral Sharing Switch
PSU	Power Supply Unit

Table 18 - CC Related Abbreviations and Acronyms	
Abbreviations/ Acronyms	Description
CAC	Common Access Card
CAP	Composed Assurance Package
CC	Common Criteria
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security
DAC	Discretionary Access Control
DOD	Department of Defense
DOD	See DOD
EAL	Evaluation Assurance Level
IT	Information Technology
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

8 References

Table 19 - TOE Guidance Documentation		
Reference	Description	Part Number
[1]	STRATUS CM 4110 and 4120 User Guide	1026482
[2]	STRATUS MCS Multiple Client Station with Secure KVM Quick Start Guide	1025278
[3]	Download Instructions for Straus CM 4110 and 4120 User Guide	1026489

Table 20 - Common Criteria v3.1 References			
Reference	Description	Version	Date
[7]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCMB-2009-07-001	V3.1 R3	July 2009
[8]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components CCMB-2009-07-002	V3.1 R3	July 2009
[9]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components CCMB-2009-07-003	V3.1 R3	July 2009
[10]	Common Criteria for Information Technology Security Evaluation Evaluation Methodology CCMB-2009-07-004	V3.1 R3	July 2009

Table 21 – Supporting Documents			
Reference	Description	Version	Date
[11]	Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile	2.1	September 7, 2010