HSL Secure KVM Combiner Switches

Firmware Version 44403-E7E7

Security Target

Evaluation Assurance Level (EAL): EAL4+

Doc No: 2128-000-D102
Version: 1.1
17 July 2020

High Sec Labs Ltd.
29 HaEshel St
Caesarea,
Israel 3079510

Prepared by:
EWA-Canada, An Intertek Company
1223 Michael Street North, Suite 200
Ottawa, Ontario, Canada
K1J7T2

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 SECURITY TARGET INTRODUCTION

This Security Target (ST) defines the scope of the evaluation in terms of the assumptions made, the intended environment for the Target of Evaluation (TOE), the Information Technology (IT) security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the TOE satisfies its IT security requirements. This document forms the baseline for the Common Criteria (CC) evaluation.

1.1 DOCUMENT ORGANIZATION

Section 1, ST Introduction, provides the Security Target reference, the Target of Evaluation reference, the TOE overview and the TOE description.

Section 2, Conformance Claims, describes how the ST conforms to the Common Criteria and Packages. The ST does not conform to a Protection Profile.

Section 3, Security Problem Definition, describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.

Section 4, Security Objectives, defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment in response to the problem defined by the security problem definition.

Section 5, Extended Components Definition, defines the extended components which are then detailed in Section 6.

Section 6, Security Requirements, specifies the security functional and assurance requirements that must be satisfied by the TOE and the IT environment.

Section 7, TOE Summary Specification, describes the security functions that are included in the TOE to enable it to meet the IT security functional requirements.

Section 8 Terminology and Acronyms, defines the acronyms and terminology used in this ST.

1.2 SECURITY TARGET REFERENCE

ST Title:	HSL Secure KVM Combiner Switches Firmware Version 44403-E7E7 Security Target
ST Version:	1.1
ST Date:	17 July 2020

1.3 TOE REFERENCE

TOE Identification: HSL Secure KVM Combiner Switches Firmware Version 44403-E7E7

TOE Developer: High Sec Labs Ltd.

TOE Type: Keyboard, Video, Mouse (KVM) Switches (Other Devices and Systems)

1.4 TOE OVERVIEW

HSL Secure Combiner Switches allow users to share keyboard and mouse functionality between a number of connected computers while viewing the video from multiple sources simultaneously. Security features ensure isolation between computers and peripherals[1] to prevent data leakage between connected systems.

The following security features are provided by the HSL Secure Combiner Switches:

- Video Security
    - Computer video input interfaces are isolated through the use of different electronic components, power and ground domains
    - The display is isolated by a dedicated, read-only, Extended Display Identification Data (EDID) emulation for each computer
    - Access to the monitor's EDID is blocked
    - Access to the Monitor Control Command Set (MCCS commands) is blocked
- Keyboard and Mouse Security
    - The keyboard and mouse are isolated by dedicated, Universal Serial Bus (USB) device emulation for each computer
    - One-way, peripheral-to-computer data flow is enforced through unidirectional optical data diodes
    - Communication from computer-to-keyboard/mouse is blocked
    - Non HID (Human Interface Device) data transactions are blocked
- Hardware Anti-Tampering Indication
    - Special holographic tampering evident labels on the product's enclosure provide a clear visual indication if the product has been opened or compromised

[1] 'Peripherals' or 'peripheral devices' refer to auxiliary devices that are intended to be connected to a computer, but are not an essential part of the computer. E.g. monitor, keyboard or mouse.

The TOE is a combined software and hardware TOE.

1.4.1 TOE Environment

The following operating system and computer hardware components are required for operation of the TOE in the evaluated configuration.

Component	Operating System	Hardware
Connected computers (up to 8 for TC82PHG-3T devices, and up to 16 for the TC162PHG-3T devices)	Windows Server 2008 R2	General purpose computing hardware supporting DisplayPort or High-Definition Multimedia Interface (HDMI) (supporting Ultra-high-definition (UHD) 4K resolution up to 3840 x 2160) video and USB type B mouse and keyboard connections
Video monitor (up to 2 monitors)	Not applicable	HDMI 1.4 or DisplayPort 1.1, 1.2
Keyboard	Not applicable	USB Type A
Mouse	Not applicable	USB Type A

Table 1 – Non-TOE Hardware and Software

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

The TOE is made up of the TC82PHG-3T and TC162PHG-3T model secure KVM combiner switches.

Table 2 provides a comparison of the devices. Figure 1 provides the evaluated configuration.

Device	Part Number	Number of Ports	Supported Display Type
TC82PHG-3T 8:2 Secure Combiner	CGA13355	8	HDMI
TC82PHG-3T 8:2 Secure Combiner Gen II	CGA17473	8	HDMI/DisplayPort
TC162PHG-3T 16:2 Secure Combiner	CGA13354	16	HDMI
TC162PHG-3T 16:2 Secure Combiner Gen II	CGA18237	16	HDMI/DisplayPort

Table 2 – TOE Device Comparison

The TOE firmware version is 44403-E7E7, and is broken down as described in Table 3.

Product Version	System Controller Board Firmware Version	Video Controller Board Firmware Version	Keyboard Host Emulator Firmware Version	DPP Firmware Version	Device Emulator Firmware Version		Video Hardware Version	System Controller Board Version
Version	4	4	4	0	4	-	E7	E7

Table 3 – Firmware Version Numbering Structure

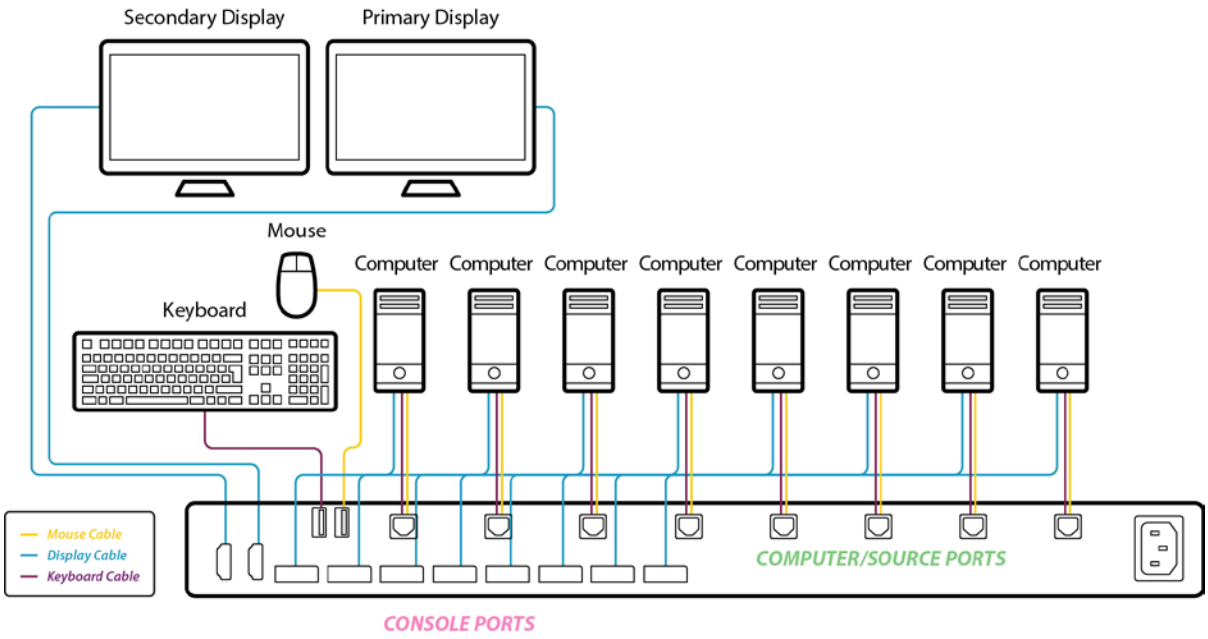

Figure 1 – TOE Diagram

In the evaluated configuration, the TOE is connected to two video displays, a keyboard and mouse on the console side and up to 16 computers on the connected computer side.

1.5.1.1 TOE Delivery

The TOE is delivered as a single package including the KVM combiner hardware and software and the cables required to connect to the computers. The TOE is delivered to the customer via trusted courier.

1.5.1.2 TOE Guidance

The TOE includes the following guidance documentation:

- HighSecLabs Secure 8/16 Port Combiner User Manual, Doc No. HDC18240, Rev 1.0
- HSL Secure KVM Combiner Switches Common Criteria Guidance Supplement, Version: 1.0, 2 August 2019

The TOE documentation is available as a .pdf from the HighSecLabs website.

1.5.2 Logical Scope

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security function classes described in Section 6. Table 3 summarizes the logical scope of the TOE.

Functional Classes	Description
User Data Protection	The TOE ensures that only authorized device types may be successfully connected to the TOE. The TOE ensures that user data only flows from the peripheral devices to the selected computer, and video data flows only from the connected computer to the display.
Security Management	The TOE ensures that no user is able to modify the security attributes used to determine authorized peripheral devices and to provide data isolation between connected computers. Only switching between connected computers is permitted.
Protection of the TSF	The TOE provides clear indications of tampering attempts.
TOE Access	The TOE provides a visual indication showing which channel is associated with each displayed window.

Table 4 – Logical Scope of the TOE

1.5.3 Functionality Excluded from the Evaluated Configuration

The following features, although supported, were not tested as part ofthis evaluation:

- For the purposes of this evaluation, Windows Server 2008 R2 host machines were used. However, the use of other operating systems does not affect the security functionality provided by the TOE devices.
- Touch screens. Although all of the claimed TOE functionality is supported using touch screens, this option was not tested in the evaluated configuration.

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This Security Target claims to be conformant to Version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

As follows:

- CC Part 2 extended
- CC Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017 has been taken into account.

2.2 PROTECTION PROFILE CONFORMANCE CLAIM

This ST does not claim conformance of the TOE with any Protection Profile (PP).

2.3 PACKAGE CLAIM

This Security Target claims conformance to Evaluation Assurance Level 4 augmented with ALC_FLR.3 Systematic flaw remediation.

2.4 CONFORMANCE RATIONALE

This ST does not claim conformance of the TOE with any PP, therefore a conformance rationale is not applicable.

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 4 lists the threats addressed by the TOE. Potential threat agents are unauthorized or malicious users, and poor design. The threat agents are assumed to have an enhanced-basic attack potential and are assumed to have access to all publicly available information about the TOE and potential methods of attacking the TOE, a proficient level of expertise, standard equipment, and minimal time to attack the TOE without detection. It is expected that the TOE will be protected to the extent necessary to ensure that TOE devices remain connected and minimize the window of opportunity available for attack. Unauthorized persons have basic knowledge of TOE operations, and a moderate level of skill.

Mitigation of the threats is through the objectives identified in Section 4.1, Security Objectives for the TOE.

Threat	Description
T.DATA_LEAK	An unauthorized user may be able to access data that is transmitted via an unauthorized data transfer through the TOE or its connected peripherals.
T.PHYSICAL_TAMPER	A malicious user could physically tamper with or modify the TOE to allow unauthorized information flows between connected devices.
T.SWITCHING	A poorly designed TOE could result in a situation where a user is connected to a computer other than the one to which the user intended to connect, resulting in an unintended flow of data.
T.UNAUTH	A malicious user could tamper with the security attributes that determine allowed peripheral devices and allowed data flows, resulting in the use of unauthorized peripheral devices that may allow unauthorized data flows between connected devices, or an attack on the TOE or its connected computers.
T.UNAUTH_DEVICE	A malicious user could connect an unauthorized peripheral device to the TOE, and that device could cause information to flow between connected devices in an unauthorized manner, or could enable an attack on the TOE or its connected computers.

Table 5 – Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

There are no Organizational Security Policies applicable to this TOE.

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 5.

Assumptions	Description
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data that passes through the TOE, is assumed to be provided by the environment.
A.TRUSTED_CONFIG	Personnel installing and configuring the TOE and its operational environment will follow the applicable guidance.
A.TRUSTED_USER	TOE users are trusted to follow and apply all guidance and security procedures in a reliable manner.
A.USER_IDENT	The operational environment is responsible for the identification and authentication of users. This determines physical access to the TOE, and access to the connected computers and their applications and resources.

Table 6 – Assumptions

4 SECURITY OBJECTIVES

The purpose of the security objectives is to address the security concerns and to show which security concerns are addressed by the TOE, and which are addressed by the environment. Threats may be addressed by the TOE or the security environment or both. Therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE
- Security objectives for the environment

4.1 SECURITY OBJECTIVES FOR THE TOE

This section identifies and describes the security objectives that are to be addressed by the TOE.

Security Objective	Description
O.CHANNEL_ISOLATION	User data must be routed by the TOE only to the computer selected by the user. The TOE must provide isolation between the data flowing from the peripheral device to the selected computer and any non-selected computer.
O.NO_DATA_RETENTION	The TOE shall not retain user data after the channel is switched or the TOE is powered down.
O.PERIPHERAL_DEVICE	The TOE shall ensure that only approved peripheral device types may be used with the TOE.
O.STATIC_ATTRIBUTES	The TSF will provide TOE users with the security management functionality to switch between connected computers. The TOE will protect all other security attributes from being altered by the TOE users.
O.TAMPER_INDICATION	The TOE shall be labeled with at least one visible tamper-evident marking that clearly indicates when tampering has been detected.

Table 7 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section identifies and describes the security objectives that are to be addressed by the IT environment or by non-technical or procedural means.

Security Objective	Description
OE.AUTH	The operational environment will ensure that users are identified and authenticated prior to gaining physical access to the TOE, or access to the applications and resources of the connected computers.
OE.INSTALL	The operational environment will ensure that appropriately trained and trusted personnel are available to correctly install and configure the TOE.
OE.PERSON	TOE users will follow TOE guidance and the security procedures of the operational environment in which the TOE is installed.
OE.PHYSICAL	The operational environment will provide physical security commensurate with the value of the TOE and the data that passes through the TOE.

Table 8 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

The following table maps the security objectives to the assumptions, threats, and organizational policies identified for the TOE.

	T.DATA_LEAK	T.PHYSICAL_TAMPER	T.SWITCHING	T.UNAUTH	T.UNAUTH_DEVICE	A.PHYSICAL	A.TRUSTED_CONFIG	A.TRUSTED_USER	A.USER_IDENT
O.CHANNEL_ISOLATION	X		X						
O.NO_DATA_RETENTION	X		X						
O.PERIPHERAL_DEVICE					X				
O.STATIC_ATTRIBUTES	X			X					
O.TAMPER_INDICATION		X							
OE.AUTH									X
OE.INSTALL							X		
OE.PERSON		X						X	
OE.PHYSICAL		X				X			

Table 9 – Mapping Between Objectives, Threats, and Assumptions

4.3.1 Security Objectives Rationale Related to Threats

The security objectives rationale related to threats traces the security objectives for the TOE and the Operational Environment back to the threats addressed by the TOE.

Threat: **T.DATA_LEAK**	An unauthorized user may be able to access data that is transmitted via an unauthorized data transfer through the TOE or its connected peripherals.	
Objectives:	O.CHANNEL_ISOLATION	User data must be routed by the TOE only to the computer selected by the user. The TOE must provide isolation between the data flowing from the peripheral device to the selected computer and any non-selected computer.
	O.NO_DATA_RETENTION	The TOE shall not retain user data after the channel is switched or the TOE is powered down.
	O.STATIC_ATTRIBUTES	The TSF will provide TOE users with the security management functionality to switch between connected computers. The TOE will protect all other security attributes from being altered by the TOE users.
Rationale:	O.CHANNEL_ISOLATION mitigates this threat by ensuring that data flows only to the user-selected computer, and is therefore unavailable to an unauthorized user. O.NO_DATA_RETENTION mitigates this threat by ensuring that data is not retained by the TOE, from where it could be mistakenly sent to a non-selected connected computer. O.STATIC_ATTRIBUTES mitigates this threat by ensuring that the security attributes that determine allowed peripherals and data flows cannot be altered to allow an unauthorized data transfer.	

Threat: **T.PHYSICAL_TAMPER**	A malicious user could physically tamper with or modify the TOE to allow unauthorized information flows between connected devices.	
Objectives:	O.TAMPER_INDICATION	The TOE shall be labeled with at least one visible tamper-evident marking that clearly indicates when tampering has been detected.
	OE.PERSON	TOE users will follow the security procedures of the operational environment in which the TOE is installed.

Rationale:	OE.PHYSICAL	The operational environment will provide physical security commensurate with the value of the TOE and the data that passes through the TOE.
	O.TAMPER_INDICATION mitigates this threat by ensuring that tampering with the TOE will result in a clear indication of that activity. OE.PHYSICAL ensures that the operational environment protects against potential malicious users by providing appropriate physical security. OE.PERSON mitigates this threat by ensuring that users with access to the TOE follow the security procedures for the operational environment.	

Threat: T.SWITCHING	A poorly designed TOE could result in a situation where a user is connected to a computer other than the one to which the user intended to connect, resulting in an unintended flow of data.	
Objectives:	O.CHANNEL _ISOLATION	User data must be routed by the TOE only to the computer selected by the user. The TOE must provide isolation between the data flowing from the peripheral device to the selected computer and any non-selected computer.
	O.NO_DATA _RETENTION	The TOE shall not retain user data after the channel is switched or the TOE is powered down.
Rationale:	O.CHANNEL_ISOLATION mitigates this threat by ensuring that user data is sent only to the intended connected computer. O.NO_DATA_RETENTION mitigates this threat by ensuring that no data is retained by the TOE, from where it could be mistakenly sent to an unselected connected computer.	

Threat: T.UNAUTH	A malicious user could tamper with the security attributes that determine allowed peripheral devices and allowed data flows, resulting in the use of unauthorized peripheral devices that may allow unauthorized data flows between connected devices, or an attack on the TOE or its connected computers.	
Objectives:	O.STATIC _ATTRIBUTES	The TSF will provide TOE users with the security management functionality to switch between connected computers. The TOE will protect all other security attributes from being altered by the TOE users.

Rationale:	O.STATIC_ATTRIBUTES mitigates this threat by ensuring that the security attributes that determine allowed peripheral devices and allowed data flows may not be altered by TOE users.

Threat: **T.UNAUTH_DEVICE**	A malicious user could connect an unauthorized peripheral device to the TOE, and that device could cause information to flow between connected devices in an unauthorized manner, or could enable an attack on the TOE or its connected computers.	
Objectives:	O.PERIPHERAL_DEVICE	The TOE shall ensure that only approved peripheral device types may be used with the TOE.
Rationale:	O.PERIPHERAL_DEVICE mitigates this threat by ensuring that only permitted peripheral devices may be connected to the TOE.	

4.3.2 Security Objectives Rationale Related to Assumptions

The security objectives rationale related to assumptions traces the security objectives for the operational environment back to the assumptions for the TOE's operational environment.

Assumption: **A.PHYSICAL**	Physical security, commensurate with the value of the TOE and the data that passes through the TOE, is assumed to be provided by the environment.	
Objectives:	OE.PHYSICAL	The operational environment will provide physical security commensurate with the value of the TOE and the data that passes through the TOE.
Rationale:	OE.PHYSICAL supports this assumption by protecting the TOE and the data that passes through the TOE from physical attack.	

Assumption: **A.TRUSTED_CONFIG**	Personnel installing and configuring the TOE and its operational environment will follow the applicable guidance.	
Objectives:	OE.INSTALL	The operational environment will ensure that appropriately trained and trusted personnel are available to correctly install and configure the TOE.
Rationale:	OE.INSTALL supports this assumption by ensuring that trained and trusted individuals are available to install and configure the TOE.	

Assumption: **A.TRUSTED_USER**	TOE users are trusted to follow and apply all guidance and security procedures in a reliable manner.	
Objectives:	OE.PERSON	TOE users will follow TOE guidance and the security procedures of the operational environment in which the TOE is installed.
Rationale:	OE.PERSON supports this assumption by ensuring that TOE users follow security procedures and guidance.	

Assumption: **A.USER_IDENT**	The operational environment is responsible for the identification and authentication of users. This determines physical access to the TOE, and access to the connected computers and their applications and resources.	
Objectives:	OE.AUTH	The operational environment will ensure that users are identified and authenticated prior to gaining physical access to the TOE, or access to the applications and resources of the connected computers.
Rationale:	OE.AUTH supports this assumption by ensuring that the operational environment identifies and authenticates TOE users.	

5 EXTENDED COMPONENTS DEFINITION

5.1 SECURITY FUNCTIONAL REQUIREMENTS

This section specifies the extended Security Functional Requirements (SFRs) used in this ST. The following extended SFR has been created to address additional security features of the TOE:

- Visual indication rule (FTA_VIR_EXT.1)

5.1.1 Family FTA_VIR_EXT: Visual indications

Visual indications provide a means of ensuring that users are aware which connected computer is being displayed at any given time. Since visual indication is a means of accessing the TOE, this family has been made part of the TOE Access Class. Although there are similarities between this family and the TOE access banners family, the visual indications are not presented in the form of a banner or advisory. Therefore, a new family was required. A similar SFR exists in various versions of the Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile. However, since the extended component definition of this SFR (EXT_VIR.1) does not closely follow CC guidelines in that it does not belong to any class, a new family and SFR were created to ensure that this functionality could be included in this ST. The Visual indications family was modeled after FTA_TAB: TOE Access Banners. The Visual indication rule SFR was loosely modeled after FTA_TAB.1: Default TOE access banners.

Family Behaviour

This family defines the requirements for providing a means of displaying which computer is connected to which set of peripheral devices.

Component Levelling

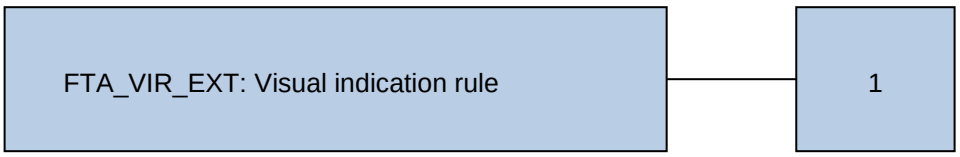

Figure 2 – FTA_VIR_EXT: Visual indication rule Component Levelling

Management

There are no management activities foreseen.

Audit

There are no auditable events foreseen.

5.1.1.1 FTA_VIR_EXT.1 Visual indication rule

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_VIR_EXT.1.1 A visual method of indicating which computer is connected to the shared set of peripheral devices shall be provided, and this method shall be persistent for the duration of the connection.

5.2 SECURITY ASSURANCE REQUIREMENTS

This ST does not include extended Security Assurance Requirements.

6 SECURITY REQUIREMENTS

Section 6 provides security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC, and an Evaluation Assurance Level (EAL) that contains assurance components from Part 3 of the CC.

6.1 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations, when performed on requirements that derive from CC Part 2, are identified in this ST in the following manner:

- Selection: Indicated by surrounding brackets, e.g., [selected item].
- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*].
- Refinement: Refined components are identified by using **bold** for additional information, or ~~strikeout~~ for deleted text.
- Iteration: Indicated by assigning a number in parenthesis to the end of the functional component identifier as well as by modifying the functional component title to distinguish between iterations, e.g., 'FDP_ACC.1(1), Subset access control (administrators)' and 'FDP_ACC.1(2) Subset access control (devices)'.

6.2 SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC and extended components defined in Section 5, summarized in Table 9.

Class	Identifier	Name
User Data Protection (FDP)	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
	FDP_RIP.1	Subset residual information protection

Class	Identifier	Name
Security Management (FMT)	FMT_MSA.1(1)	Management of security attributes (Peripherals)
	FMT_MSA.1(2)	Management of security attributes (User data)
	FMT_MSA.3(1)	Static attribute initialisation (Peripherals)
	FMT_MSA.3(2)	Static attribute initialisation (User data)
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_PHP.1	Passive detection of physical attack
TOE Access (FTA)	FTA_VIR_EXT.1	Visual indication rule

Table 10 – Summary of Security Functional Requirements

6.2.1 User Data Protection (FDP)

6.2.1.1 FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [*Peripheral Device SFP*] on
[*Subjects: Peripheral devices*
Objects: Console ports
Operations: allow connection, disallow connection].

6.2.1.2 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [*Peripheral Device SFP*] to objects based on the following:
[*Subjects: peripheral devices*
Subject attributes: peripheral device type
Objects: Console ports
Object attributes: none].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*the TOE queries the connected peripheral device upon initial connection or upon TOE power up and allows the connection if the peripheral device is an authorized device as listed in Table 10*].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*none*].

Console Port	Authorized Device	Authorized Protocols
Keyboard	Any USB HID device	USB
Mouse	Any USB HID device	USB
Display	Video display or projector	DisplayPort, HDMI

Table 11 – Authorized Peripheral Devices

6.2.1.3 FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [*User Data Isolation SFP*] on
[*Subjects: TOE computer interfaces, TOE peripheral device interfaces*
Information: User data
Operations: data flow].

6.2.1.4 FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [*User Data Isolation SFP*] based on the following types of subject and information security attributes:
[*Subjects: TOE computer interfaces*
Subject attributes: user selected computer interface
Subjects: TOE peripheral device interfaces
Subject attributes: none
Information: User data
Information attributes: none].

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: [
1. user data is permitted to flow from the HID peripheral device interface to the TOE computer interface for the selected computer;
2. video signals are permitted to flow from the connected computers to the display].

FDP_IFF.1.3 The TSF shall enforce the [*no additional rules*].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [*no additional rules*].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [
1. the TOE will deny user data information flow from a peripheral device

to a non-selected computer interface
2. the TOE will deny user data information flow from one connected computer to another connected computer].

6.2.1.5 FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [deallocation of the resource from] the following objects: [*a TOE computer interface*].

Application Note: Deallocation of the resource is deemed to take place:

- Immediately after the TOE is switched to another selected computer
- On start-up of the TOE

6.2.2 Security Management (FMT)

6.2.2.1 FMT_MSA.1(1) Management of security attributes (Peripherals)

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(1) The TSF shall enforce the [*Peripheral Device SFP*] to restrict the ability to [modify] the security attributes [*peripheral device type*] to [*no TOE users*].

6.2.2.2 FMT_MSA.1(2) Management of security attributes (User data)

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1(2) The TSF shall enforce the [*User Data Isolation SFP*] to restrict the ability to [[*change*]] the security attributes [*selected computer interface*] to [*users with physical access to the TOE-attached peripherals*].

6.2.2.3 FMT_MSA.3(1) Static attribute initialisation (Peripherals)

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1(1) The TSF shall enforce the [*Peripheral Device SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(1) The TSF shall allow ~~the~~ [*no user*] to specify alternative initial values to override the default values when an object or information is created.

6.2.2.4 FMT_MSA.3(2) Static attribute initialisation (User data)

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1(2) The TSF shall enforce the [*User Data Isolation SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(2) The TSF shall allow ~~the~~ [*no user*] to specify alternative initial values to override the default values when an object or information is created.

6.2.2.5 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [*switch between connected computers*].

6.2.2.6 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [*user*].

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

6.2.3 Protection of the TSF (FPT)

6.2.3.1 FPT_PHP.1 Passive detection of physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

6.2.4 TOE Access (FTA)

6.2.4.1 FTA_VIR_EXT.1 Visual indication rule

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_VIR_EXT.1.1 A visual method of indicating which computer is connected to the shared set of peripheral devices shall be provided, and this method shall be persistent for the duration of the connection.

6.3 SECURITY ASSURANCE REQUIREMENTS

The assurance requirements are summarized in Table 11.

Assurance Class	Assurance Components	
	Identifier	**Name**
Development (ADV)	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance Documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support (ALC)	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
	ALC_FLR.3	Systematic flaw remediation
Security Target Evaluation (ASE)	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

Assurance Class	Assurance Components	
	Identifier	**Name**
Tests (ATE)	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment (AVA)	AVA_VAN.3	Focused vulnerability analysis

Table 12 – Security Assurance Requirements

6.4 SECURITY REQUIREMENTS RATIONALE

6.4.1 Security Functional Requirements Rationale

The following Table provides a mapping between the Security Functional Requirements (SFRs) and Security Objectives.

	O.CHANNEL_ISOLATION	O.NO_DATA_RETENTION	O.PERIPHERAL_ISOLATION	O.STATIC_ATTRIBUTES	O.TAMPER_INDICATION
FDP_ACC.1			X		
FDP_ACF.1			X		
FDP_IFC.1	X				
FDP_IFF.1	X				
FDP_RIP.1		X			
FMT_MSA.1(1)				X	
FMT_MSA.1(2)				X	

	O.CHANNEL_ISOLATION	O.NO_DATA_RETENTION	O.PERIPHERAL_ISOLATION	O.STATIC_ATTRIBUTES	O.TAMPER_INDICATION
FMT_MSA.3(1)				X	
FMT_MSA.3(2)				X	
FMT_SMF.1				X	
FMT_SMR.1				X	
FPT_PHP.1					X
FTA_VIR_EXT.1				X	

Table 13 – Mapping of SFRs to Security Objectives

6.4.2 SFR Rationale Related to Security Objectives

The following rationale traces each SFR back to the Security Objectives for the TOE.

Objective: **O.CHANNEL_ISOLATION**	User data must be routed by the TOE only to the computer selected by the user. The TOE must provide isolation between the data flowing from the peripheral device to the selected computer and any non-selected computer.	
Security Functional Requirements:	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
Rationale:	FDP_IFC.1 and FDP_IFF.1 ensure that the only permitted user data flow is from the peripheral device to the selected computer.	

Objective: **O.NO_DATA_RETENTION**	The TOE shall not retain user data after the channel is switched or the TOE is powered down.	
Security Functional Requirements:	FDP_RIP.1	Subset residual information protection
Rationale:	FDP_RIP.1 ensures that user data from one connected computer	

	becomes unavailable when the peripherals are switched to another connected computer.

Objective: **O.PERIPHERAL_DEVICE**	The TOE shall ensure that only approved peripheral device types may be used with the TOE.	
Security Functional Requirements:	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
Rationale:	FDP_ACC.1 and FDP_ACF.1 ensure that only authorized peripheral device types may be connected to the TOE.	

Objective: **O.STATIC_ATTRIBUTES**	The TSF will provide TOE users with the security management functionality to switch between connected computers. The TOE will protect all other security attributes from being altered by the TOE users.	
Security Functional Requirements:	FMT_MSA.1(1)	Management of security attributes (Peripherals)
	FMT_MSA.1(2)	Management of security attributes (User data)
	FMT_MSA.3(1)	Static attribute initialisation (Peripherals)
	FMT_MSA.3(2)	Static attribute initialisation (User data)
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
	FTA_VIR_EXT.1	Visual indication rule
Rationale:	FMT_MSA.1(1) ensures that no users can modify the list of acceptable peripheral device types. FMT_MSA.3(1) provides restrictive default values for these types, and does not allow these values to be changed. FMT_MSA.1(2) ensures that only users with physical access to the peripherals attached to the TOE are able to switch connected computers. FMT_MSA.3(2) provides restrictive default values for the selected types, and does not allow these values to be changed. FMT_SMF.1 ensures that the TSF provides TOE users with the capability to switch between connected computers. FMT_SMR.1 provides for a single user role for the TOE. FTA_VIR_EXT.1 ensures that the user is able to identify the active channel when switching between connected computers.	

Objective: **O.TAMPER_INDICATION**	The TOE shall be labeled with at least one visible tamper-evident marking that clearly indicates when tampering has been detected.	
Security Functional Requirements:	FPT_PHP.1	Passive detection of physical attack
Rationale:	FPT_PHP.1 ensures that the TSF provides unambiguous detection of physical tampering.	

6.4.3 Dependency Rationale

Table 13 identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependency	Dependency Satisfied	Rationale
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	Satisfied by FMT_MSA.3(1)
FDP_IFC.1	FDP_IFF.1	✓	
FDP_IFF.1	FDP_IFC.1	✓	
	FMT_MSA.3	✓	Satisfied by FMT_MSA.3(2)
FDP_RIP.1	None	N/A	
FMT_MSA.1(1)	FDP_ACC.1 or FDP_IFC.1	✓	Satisfied by FDP_ACC.1
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1(2)	FDP_ACC.1 or FDP_IFC.1	✓	Satisfied by FDP_IFC.1
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.3(1)	FMT_MSA.1	✓	Satisfied by FMT_MSA.1(1)
	FMT_SMR.1	✓	
FMT_MSA.3(2)	FMT_MSA.1	✓	Satisfied by FMT_MSA.1(2)

SFR	Dependency	Dependency Satisfied	Rationale
	FMT_SMR.1	✓	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	Users are identified and authenticated by the operational environment. This dependency is satisfied by the operational environment in accordance with OE.AUTH.
FPT_PHP.1	None	N/A	
FTA_VIR_EXT.1	None	N/A	

Table 14 – Functional Requirement Dependencies

6.4.4 Security Assurance Requirements Rationale

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 4 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Systematic Flaw Remediation (ALC_FLR.3). EAL 4 was chosen for competitive reasons. The developer is claiming the ALC_FLR.3 augmentation since the current practices and procedures exceed the minimum requirements for EAL 4.

7 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

7.1 USER DATA PROTECTION

There are two SFPs that are enforced by the TOE.

7.1.1 Peripheral Device SFP

The TOE supports the following peripheral devices on the TOE console ports. If a device that does not support the authorized protocols is plugged into a console port, that device will not be correctly enumerated and therefore will not function.

TOE Console Port	Authorized Protocols	Authorized Devices
Keyboard	USB Type A HID	Any wired keyboard and keypad
Mouse/ Pointing Device	USB Type A HID	Any wired mouse, trackball or touch screen
Display	HDMI 1.4 DisplayPort 1.1, 1.2	Monitor, projector

Table 15 – Authorized Peripheral Devices

USB hub and composite devices that include at least one end point that enumerates as a USB HID is accepted as an authorized device on the keyboard and mouse ports. Any functionality that does not enumerate as HID will not be available.

TOE Security Functional Requirements addressed: FDP_ACC.1, FDP_ACF.1

7.1.2 User Data Isolation SFP

The allowed data flows between the connected computer and the peripheral devices are described in Sections 7.1.2.1 and 7.1.2.2 below.

TOE Security Functional Requirements addressed: FDP_IFC.1, FDP_IFF.1, FDP_RIP.1.

7.1.2.1 Video Data Flow

The video data flows consist of EDID read and write functions, and unidirectional video from the connected computer to the monitor. The data flow is shown in the following figures. The figures show only four connected computers for simplicity; however, the data flows apply to all 8 or 16 connected computer ports.

In Figure 3, the TOE video controller function reads the connected display EDID Electrically Erasable Programmable Read-Only Memory (EEPROM) content from the connected monitor through the closed isolation switch. No video is displayed on the monitor since the multiplexer (Video Mux) is switched to the isolation state. This mode of operation only occurs during power up. The EDID is not read from the monitor at any other time. The video controller reads the EDID content to verify that it is valid and usable. If the data is found to be invalid, this function will stop and wait for the next Hot Plug event before continuing on.

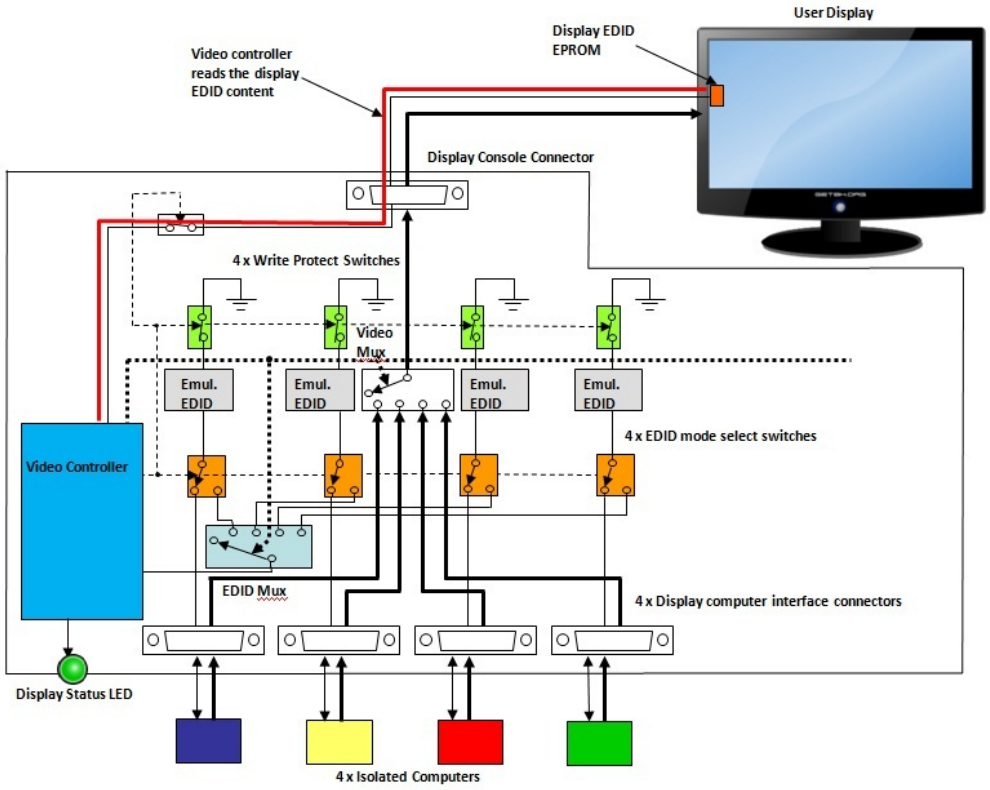

Figure 3 – Video Data Flow during EDID Read

Figure 4 shows the video controller writing the EDID content into the emulated EDID EEPROM chip for the first connected computer. The thick lines show the native video connections. The thin lines show I²C lines. The EDID multiplexer (labeled EDID Mux) couples the I²C lines to the EDID mode switch (orange) for the first connected computer. The first EDID mode switch switches the video controller I²C lines to the first emulated EDID EEPROM chip (gray). The chip write protect switch (green) opens to enable writing. The video controller uses the I²C lines to write to the first emulated EDID EEPROM chip. Once the write operation is complete and verified, the video controller function switches the EDID multiplexer to the next channel and the operation is repeated until all of the EDID EEPROM chips are programmed. Once this write operation is complete, the video controller switches to the normal operation mode.

In the EDID Write mode, the emulated EDID EEPROM chips are switched to their respective computers to allow the EDID information to be read. The write

protect switches (shown in green) are then switched back to protected mode to prevent any attempt to write the EEPROM or transmit MCCS commands.

In the EDID write mode, each connected computer interface is completely independent. The power to each emulated EDID EEPROM is received from its respective computer through the video cable. The main video multiplexer is then switched to the user selected computer to enable the video display for that computer.

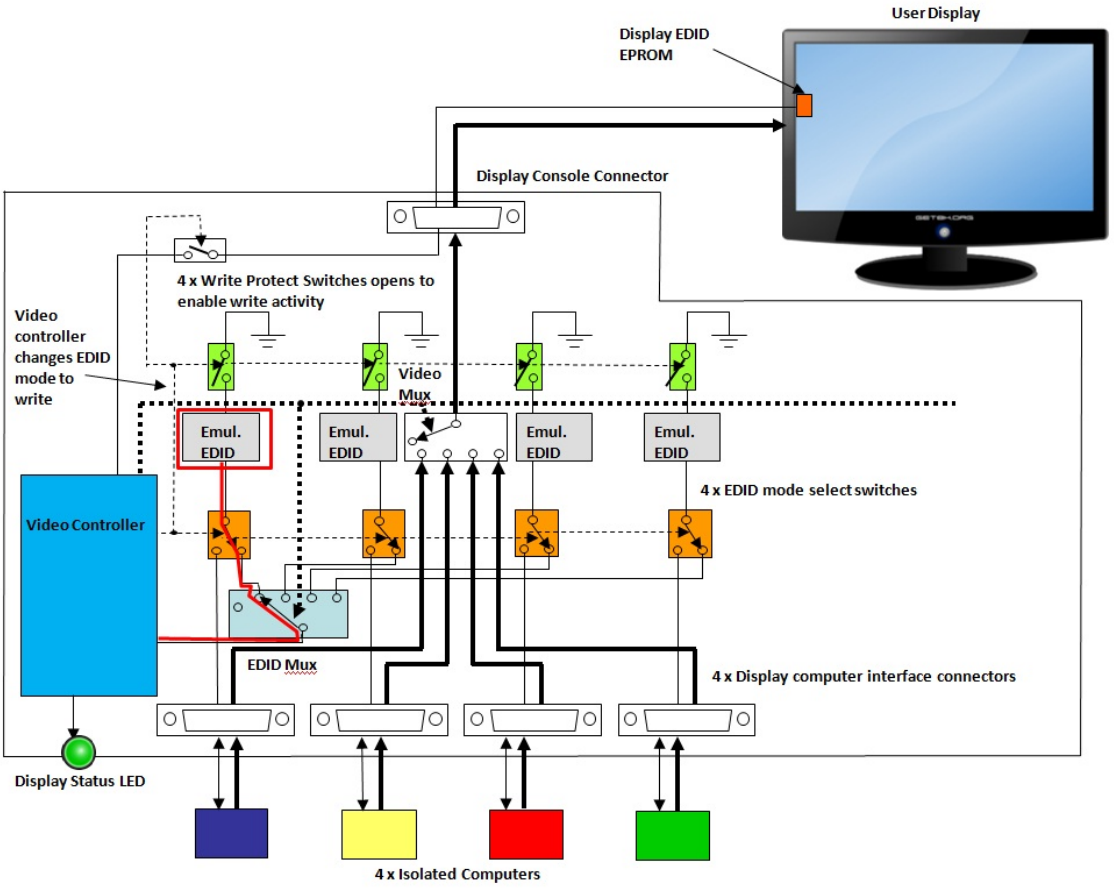

Figure 4 – Video Data Flow during EDID Write

Normal operation is shown in Figure 5. The connected computers have no means to affect the EDID channel.

The following security features are enforced by the video data flow:

a. The video input interfaces are isolated from one another. Isolation is achieved through the use of separate power and ground planes, and separate electronic components and separate emulated EDID chips for each channel;
b. The EDID function is emulated by an independent emulated EDID EEPROM chip for each connected computer channel. These chips receive their content from the connected monitor during TOE power up;
c. The TOE will reject any display device with non-valid EDID content;

d. The TOE supports HDMI 1.4, DisplayPort 1.1 and DisplayPort 1.2 video source input from connected computers. The video function effectively filters out the AUX channel by converting it to I²C EDID only. The DisplayPort video is converted into an HDMI video stream. The I²C EDID lines are connected to the corresponding emulated EDID EEPROM functions as shown in the figures above. Threats to the AUX channel are mitigated through the conversion from DisplayPort to HDMI. Unauthorized protocols such as USB, Ethernet, MCCS and EDID write are blocked since the emulated EEPROM only supports valid EDID read requests from the connected computers;
e. The TOE video function blocks MCCS write transactions through the emulated EDID EEPROMs. Emulated EEPROMs only supports EDID read transactions. The write protect switch prevents connected computers from writing to the Emulated EDID EEPROMs;
f. When the TOE is powered off, or following failure of a self-test, all video signals are isolated. The emulated EDID EEPROMs may still operate since they receive power from their respective connected computers, however, the isolation function continues to be enforced; and
g. Although only one connected computer interface is active at a time, the monitor will continue to display the video from the connected computers in accordance with the user's configuration. The active computer is always indicated by the buttons on the KVM device, and on the screen.

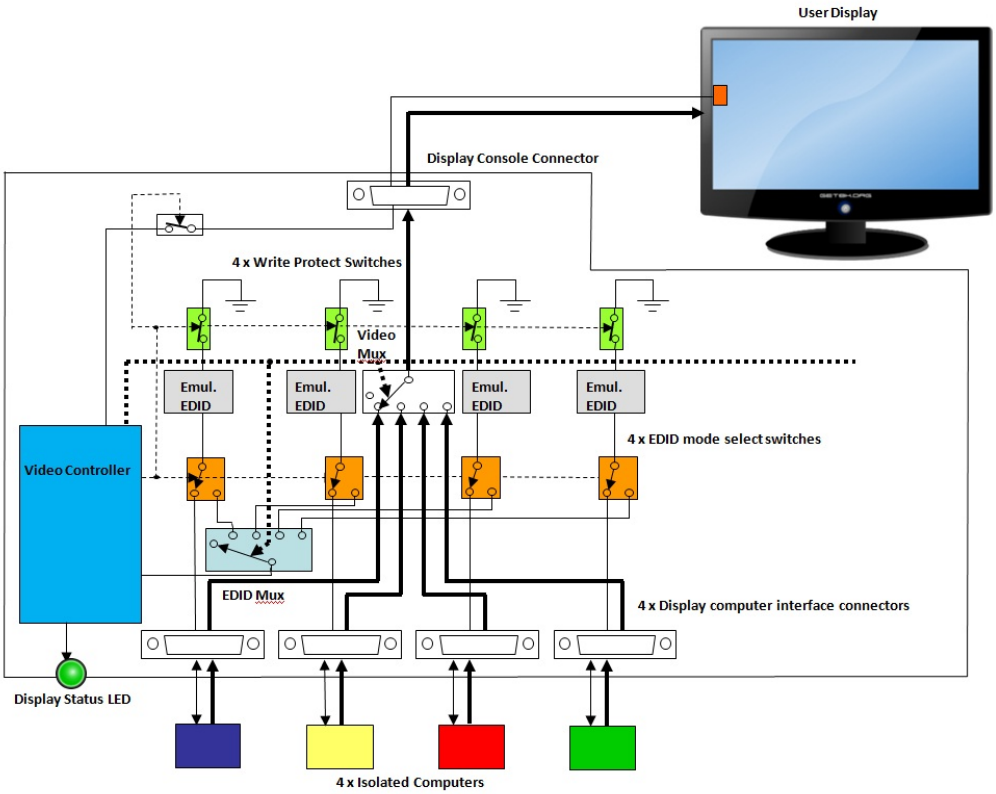

Figure 5 – Video Data Flow during Normal Operation

7.1.2.2 Keyboard and Mouse Data Flow

Isolation between the connected computers is enforced using one way data diodes and device emulators as shown in Figure 6. This diagram shows only two connected computers for simplicity. However, the functionality applies to all connected computer ports. The device emulators are microcontrollers that receive a serial stream representing the keyboard and mouse commands on one side, and interact with the connected computer via the USB bus on the other side. The use of isolated device emulators ensures that connected computers cannot interact physically or logically with shared TOE or peripheral resources. Each device emulator is powered by its respective connected computer. Power domains of different computer interfaces are independent and isolated using unidirectional data diodes.

The TOE implements a host emulator to interface with the keyboard and mouse peripheral devices, thereby isolating the peripherals from the internal circuitry and from the connected computers.

Data transmission from the host emulator to the device emulators is limited to basic HID transactions through the use of a serial protocol between the TOE host emulator and the device emulators. Only the limited data supported by the serial protocol is able to flow between the emulators.

Optical data diodes are used to enforce the unidirectional data flow of serial data between the TOE host emulator and the device emulators. Optical data diodes are included for each device emulator channel to ensure that each channel is physically and logically isolated from the other channels, and from other TOE functionality. This also prevents data flow from the device emulators to the host emulator and on to the peripheral devices.

A peripheral switch multiplexer ensures the selection of just one keyboard / mouse serial data source at any given time. The multiplexer has positions for each connected computer port, plus an addition position for isolation. The isolation position is used when the self-test has failed, and effectively disables the data flow from the keyboard and mouse.

The keyboard and mouse data flow is not combined with or connected to any other TOE data flow. The keyboard and mouse functions are completely isolated from all other switching functions, such as audio or video. The keyboard and mouse are always switched together. The keyboard and mouse host emulators only enumerate USB HID (Human Interface Devices). No other devices or endpoints are supported on the keyboard or mouse interfaces, and will be rejected. USB hub and composite devices that include an HID interface will only enumerate the HID component of the composite device. The keyboard and mouse console ports are interchangeable since both enumerate HIDs.

When power to the TOE is lost, the optical data diodes are powered off and no data flow is possible between the keyboard and mouse peripheral devices and computer interfaces.

When the user switches from one computer to another, the system controller function ensures that the keyboard and mouse stacks are deleted and that the

first 100 milliseconds of commands received from the keyboard after switching are ignored (deleted). This is done to delete the accumulation of cached commands from the previous channel in the keyboard microcontroller buffer.

Since traffic cannot flow from the connected computer to the keyboard or mouse, it is not possible to display indications such as CAP LOCK and NUM LOCK on the keyboard.

In accordance with the user guidance, wireless keyboards and mice are not permitted in the evaluated configuration.

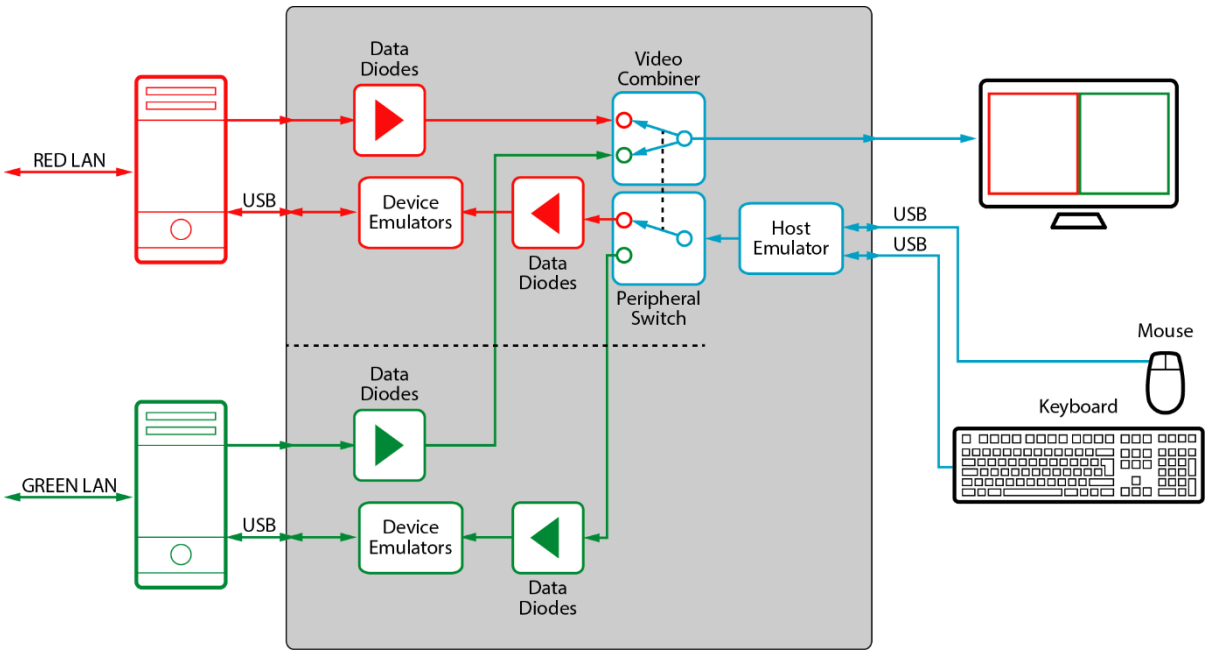

Figure 6 – Keyboard and Mouse Data Flow

TOE Security Functional Requirements addressed: FDP_ACC.1, FDP_ACF.1, FDP_IFC.1(1), FDP_IFF.1(1)

7.2 SECURITY MANAGEMENT

The TOE provides for a single user role called ‘user’. The only security management functionality available to the user is the ability to switch between connected computers. It should be noted that users are also able to change the size and location of the windows that represent the various connected computers on their screens. However, this is not considered to be a security management function.

The default accepted peripheral device type attributes are restrictive in that they are limited to the values indicated in Table 10. No user is able to change the default values.

Switching may only be done by the user with physical access to the peripherals attached to the TOE KVM device. The default values are considered restrictive in that the TOE defaults to the first connected computer on power up. No user is able to change this default behaviour.

TOE Security Functional Requirements addressed: FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.3(1), FMT_MSA.3(2), FMT_SMF.1, FMT_SMR.1.

7.3 PROTECTION OF THE TSF

7.3.1 Tamper Evidence

The TOE enclosure is designed to prevent physical tampering. It features a stainless steel welded chassis and panels that prevent external access through bending or brute force. Additionally, the TOE is equipped with holographic Tampering Evident Labels located in critical areas of the TOE enclosure. Any attempt to access the TOE internal circuitry causes permanent visible damage to one or more labels.

TOE Security Functional Requirements addressed: FPT_PHP.1

7.4 TOE ACCESS

7.4.1 Visual Indication Rule

For each video source, the screen displays a corresponding window. The border around each window is displayed in a different colour for ease of identification. A legend appears at the bottom of the screen showing which colour corresponds to which channel.

TOE Security Functional Requirements addressed: FTA_VIR_EXT.1

8 TERMINOLOGY AND ACRONYMS

8.1 TERMINOLOGY

The following terminology is used in this ST:

Term	Description
AUX	This refers to an auxiliary channel.
Combiner	A combiner is a type of KVM device that allows a user to share keyboard and mouse functionality between a number of connected computers while viewing the video from multiple sources simultaneously.
I²C	I²C is a synchronous, serial protocol used to connect low-speed devices such as microcontrollers, EEPROMs, and other similar peripherals in embedded systems.
Mux	This refers to a multiplexer.
Peripheral devices	'Peripherals' or 'peripheral devices' refer to auxiliary devices that are intended to be connected to a computer, but are not an essential part of the computer. In the context of this ST, a peripheral device is a monitor (also called a display), or a USB HID such as a keyboard or mouse.

Table 16 – Terminology

8.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
CC	Common Criteria
CM	Configuration Management
EAL	Evaluation Assurance Level
EDID	Extended Display Identification Data
EEPROM	Electrically Erasable Programmable Read-Only Memory
HDMI	High-Definition Multimedia Interface
HID	Human Interface Device
HSL	HighSecLabs
IT	Information Technology
MCCS	Monitor Control Command Set

Acronym	Definition
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
UHD	Ultra-high-definition
USB	Universal Serial Bus
KVM	Keyboard, Video, Mouse

Table 17 – Acronyms