IHSE Secure Isolator Devices

Firmware Version 44404-E7E7

Security Target

Evaluation Assurance Level (EAL): EAL4+

Doc No: 2175-001-D102
Version: 0.5
6 October 2021

IHSE GmbH
Benzstraße 1
88094 Oberteuringen
Germany

Prepared by:
EWA-Canada, An Intertek Company
1223 Michael Street North, Suite 200
Ottawa, Ontario, Canada
K1J 7T2

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:	IHSE Secure Isolator Devices Firmware Version 44404-E7E7 Security Target
ST Version:	0.5
ST Date:	6 October 2021

1.3 TOE REFERENCE

TOE Identification: IHSE Secure Isolator Devices Firmware Version 44404-E7E7

TOE Developer: IHSE GmbH

TOE Type: Keyboard, Video, Mouse and Audio Isolator Devices (Other Devices and Systems)

1.4 TOE OVERVIEW

The IHSE Isolator devices ensure unidirectional flow of data between peripheral devices and a secure connected computer.

The following security features are provided by the IHSE Isolator devices:

- Video Security
  - The display is isolated through a dedicated, read-only, Extended Display Identification Data (EDID) emulation function
  - Access to the monitor's EDID is blocked
  - Access to the Monitor Control Command Set (MCCS commands) is blocked
  - DisplayPort and High-Definition Multimedia Interface (HDMI) video options are supported
- Keyboard and Mouse Security
  - The keyboard and mouse are isolated by dedicated, Universal Serial Bus (USB) device emulation
  - 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
- Audio Security
  - One-way computer to speaker sound flow is enforced through unidirectional optical data diodes
- Hardware Anti-Tampering
  - Special holographic tampering evident labels on the product's enclosure provide a clear visual indication if the product has been opened or compromised
- Self Test
  - The microcontroller firmware is subject to self test following power up

IHSE Isolator devices use isolated microcontrollers to emulate connected peripherals in order to prevent display signaling, keyboard signaling, and power signaling attacks.

Figure 1 is a simplified block diagram showing the TOE keyboard and mouse data path. A Host Emulator (HE) communicates with the user keyboard via the USB protocol. The Host Emulator converts user key strokes into unidirectional serial data. An isolated Device Emulator (DE) is connected to the data switch on one side and to the computer on the other side. Each key stroke is converted by the selected DE into a bi-directional stream to communicate with the computer. Figure 2 shows an extended isolator. It shows the receive (RX) and transmit (TX) functions.

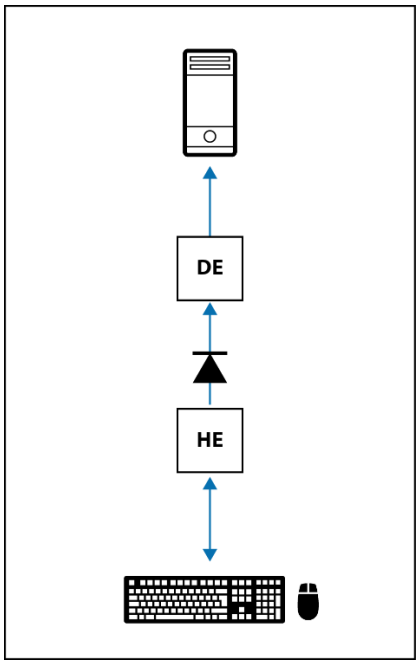

Figure 1 – Simplified Isolator Diagram

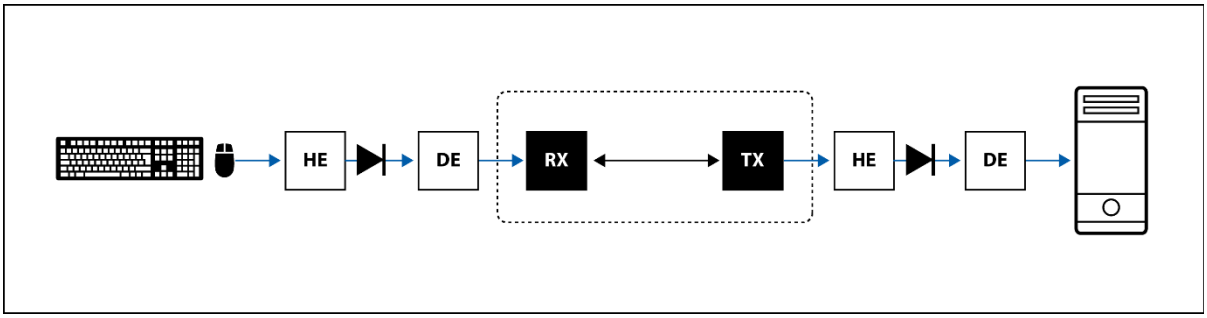

Figure 2 – Extended Isolator Diagram

The TOE is a combined software and hardware TOE.

1.4.1 TOE Environment

The following components are required for operation of the TOE in the evaluated configuration.

Component	Description
Connected Computer	General purpose computer
Keyboard	General purpose USB keyboard
Mouse	General purpose USB mouse
Audio output device	Analog audio output device (speakers or headphones)
User display	Standard computer display (HDMI 2.0, or DisplayPort 1.1, 1.2 or 1.3)
IHSE Cables	USB Type-A to USB Type-B (keyboard and mouse) Video cable (DisplayPort, or HDMI) 3.5mm stereo cable (Audio cable)

Table 1 – Non-TOE Hardware and Software

1.5 TOE DESCRIPTION

1.5.1 Evaluated Configuration

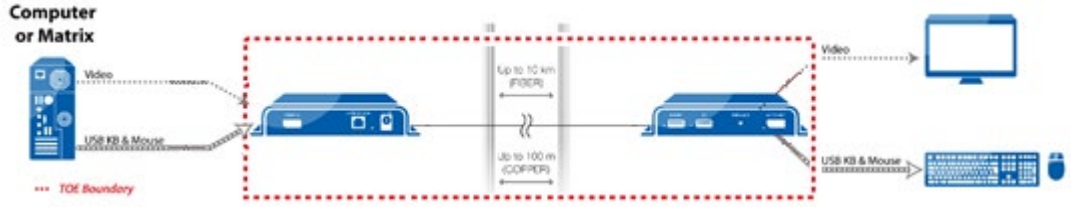

Figure 3 – Isolator Evaluated Configuration

In the evaluated configuration, the isolator device is connected to the computer and to the video, audio, keyboard and mouse peripherals to ensure unidirectional communications. The audio connection to speakers or headphones is not shown in the diagram.

1.5.2 Physical Scope

The TOE consists of the devices shown in Table 2.

Family	Description	Part Number	Model	Tamper Evident labels	Analog Audio	Video in	Video out	Number of supported displays	Keyboard and Mouse
Isolator devices supporting DisplayPort and HDMI video, Keyboard and Mouse and Audio	Copper HD KVMA Isolated Secure Extender	CGA20108	K487-1PHCA-N	Yes	Yes	DisplayPort /HDMI	DisplayPort /HDMI	1	Yes
	Fiber HD KVMA Isolated Secure Extender	CGA20109	K487-1PHSA-N	Yes	Yes	DisplayPort /HDMI	DisplayPort /HDMI	1	Yes
	Copper HD KVMA Isolated Redundant Secure Extender	CGA20408	K487-1PHCRA-N	Yes	Yes	DisplayPort /HDMI	DisplayPort /HDMI	1	Yes
	Fiber HD KVMA Isolated Redundant Secure Extender	CGA20409	K487-1PHSRA-N	Yes	Yes	DisplayPort /HDMI	DisplayPort /HDMI	1	Yes
	Copper UHD KVMA Isolated Secure Extender	CGA20110	K497-1PHCA-N	Yes	Yes	DisplayPort /HDMI	DisplayPort /HDMI	1	Yes
	Fiber UHD KVMA Isolated Secure Extender	CGA20111	K497-1PHSA-N	Yes	Yes	DisplayPort /HDMI	DisplayPort /HDMI	1	Yes
	Copper UHD KVMA Isolated Redundant Secure Extender	CGA20410	K497-1PHCRA-N	Yes	Yes	DisplayPort /HDMI	DisplayPort /HDMI	1	Yes
	Fiber UHD KVMA Isolated Redundant Secure Extender	CGA20411	K497-1PHSRA-N	Yes	Yes	DisplayPort /HDMI	DisplayPort /HDMI	1	Yes

Table 2 – TOE Peripheral Sharing Devices and Features

1.5.2.1 TOE Delivery

The TOE, together with its corresponding cables are delivered to the customer via a trusted carrier, such as Fed-Ex, that provides a tracking service for all shipments.

1.5.2.2 TOE Guidance

The TOE includes the following guidance documentation:

- QUICK SETUP Draco vario Secure Extender K487-1PHCA-N, K487-1PHCRA-N, K487-1PHSA-N, K487-1PHSRA-N Document no.: q487_0001 Rev.: 0001
- QUICK SETUP Draco vario Secure Extender K497-1PHCA-N, K497-1PHCRA-N, K497-1PHSA-N, K497-1PHSRA-N Document no.: q497_0001 Rev.:0001

Guidance may be downloaded from the IHSE website (www.ihse.com) in .pdf format.

1.5.3 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 enforces unidirectional data flow for keyboard and mouse, display, and audio output. The TOE ensures that only authorized peripheral devices may be used.
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.
Protection of the TSF[1]	The TOE provides passive detection of physical attack and performs self-testing.

Table 3 – Logical Scope of the TOE

[1] TOE Security Functionality

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 conformant
- 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.DATA_PATH	A poorly designed TOE could result in a situation where a user is connected to a computer function other than the one to which the user intended to connect, resulting in an unintended flow of data.
T.PHYSICAL_TAMPER	A malicious user could physically tamper with or modify the TOE to allow unauthorized information flows between connected devices.
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 4 – 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 for the TOE, the peripheral devices and all cabling.
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 5 – 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.

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 appropriate computer interface. The TOE must provide isolation of the data flowing from the peripheral device to the connected computer.
O.PERIPHERAL_DEVICE	The TOE shall ensure that only approved peripheral device types may be used with the TOE.
O.STATIC_ATTRIBUTES	The TOE will protect all security attributes from being altered by the TOE users.
O.SELF_TEST	The TOE shall perform self-tests following power up.
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 6 – 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 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 7 – 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.DATA_PATH	T.PHYSICAL_TAMPER	T.UNAUTH	T.UNAUTH_DEVICE	A.PHYSICAL	A.TRUSTED_CONFIG	A.TRUSTED_USER	A.USER_IDENT
O.CHANNEL_ISOLATION	X	X							
O.PERIPHERAL_DEVICE					X				
O.STATIC_ATTRIBUTES	X			X					
O.SELF_TEST		X							
O.TAMPER_INDICATION			X						
OE.AUTH									X
OE.INSTALL							X		
OE.PERSON			X					X	
OE.PHYSICAL			X			X			

Table 8 – 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 appropriate computer interface. The TOE must provide isolation of the data flowing from the peripheral device to the connected computer.
	O.STATIC _ATTRIBUTES	The TOE will protect all security attributes from being altered by the TOE users.
Rationale:	O.CHANNEL_ISOLATION mitigates this threat by ensuring that data flows only to the appropriate interfaces of the connected computer, and is therefore unavailable to an unauthorized user. 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.DATA_PATH**	A poorly designed TOE could result in a situation where a user is connected to a computer function 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 appropriate computer interface. The TOE must provide isolation of the data flowing from the peripheral device to the connected computer.
	O.SELF_TEST	The TOE shall perform self-tests following power up.
Rationale:	O.CHANNEL_ISOLATION mitigates this threat by ensuring that user data is sent only to the appropriate interfaces of the connected computer. O.SELF_TEST mitigates the threat of failures leading to compromise of the security functions through self-test of its own functionality.	

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.
	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:	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.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 TOE will protect all 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 ST does not include extended Security Functional Requirements.

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 (SFRs) 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
Security Management (FMT)	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles

Class	Identifier	Name
Protection of the TSF (FPT)	FPT_PHP.1	Passive detection of physical attack
	FPT_TST.1	TSF testing

Table 9 – 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*[2]] 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	USB HID device	USB
Mouse	USB HID device	USB

[2] Security Function Policy

Console Port	Authorized Device	Authorized Protocols
Display	Video display or projector	DisplayPort, HDMI
Audio Output	Speakers or headphones	Analog audio

Table 10 – 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: none
Subjects: TOE peripheral device interfaces
Subject attributes: peripheral device type
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*;
2. *video signals are permitted to flow from the connected computer to the display; and*
3. *analog audio signals are permitted to flow from the connected computer to the speaker/headphone peripheral device*].

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: [*any data flow not specifically allowed will be denied*].

6.2.2 Security Management (FMT)

6.2.2.1 FMT_MSA.1 Management of security attributes

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 The TSF shall enforce the [*Peripheral Device SFP, User Data Isolation SFP*] to restrict the ability to [modify] the security attributes [*peripheral device type*] to [*no users*].

6.2.2.2 FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

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

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

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

6.2.2.3 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: [*none*].

6.2.2.4 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.

6.2.3.2 FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests [during initial start-up] to demonstrate the correct operation of [the TSF].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [TSF data].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of [TSF].

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[3] 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

[3] Configuration Management

Assurance Class	Assurance Components	
	Identifier	**Name**
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
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 11 – 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.PERIPHERAL_DEVICE	O.STATIC_ATTRIBUTES	O.SELF_TEST	O.TAMPER_INDICATION
FDP_ACC.1		X			
FDP_ACF.1		X			
FDP_IFC.1	X				
FDP_IFF.1	X				
FMT_MSA.1			X		
FMT_MSA.3			X		
FMT_SMF.1			X		
FMT_SMR.1			X		
FPT_PHP.1					X
FPT_TST.1				X	

Table 12 – 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 appropriate computer interface. The TOE must provide isolation of the data flowing from the peripheral device to the connected 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 appropriate computer interface.	

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 TOE will protect all security attributes from being altered by the TOE users.	
Security Functional Requirements:	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Rationale:	FMT_MSA.1 ensures that no users can modify the list of acceptable peripheral device types. FMT_MSA.3 provides restrictive default values for these types, and does not allow these values to be changed. FMT_SMF.1 ensures that the TSF prevents users from changing the values that determine the security configuration. FMT_SMR.1 provides the TOE user role.	

Objective: **O.SELF_TEST**	The TOE shall perform self-tests following power up.	
Security Functional Requirements:	FPT_TST.1	TSF testing
Rationale:	FPT_TST.1 ensures that the TOE performs a self test on power up.	

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	✓	
FDP_IFC.1	FDP_IFF.1	✓	
FDP_IFF.1	FDP_IFC.1	✓	
	FMT_MSA.3	✓	
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	✓	Satisfied by FDP_ACC.1 and FDP_IFC.1
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	Satisfied by FMT_MSA.1
	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	

SFR	Dependency	Dependency Satisfied	Rationale
FPT_TST.1	None	N/A	

Table 13 – 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. They are enforced by the data flows described in the following sections.

7.1.1 Data Flow

7.1.1.1 Video Functionality

Video data flow is comprised of unidirectional Extended Display Identification Data (EDID) and video data flow paths. Figure 4 shows a data flow during the display EDID read function.

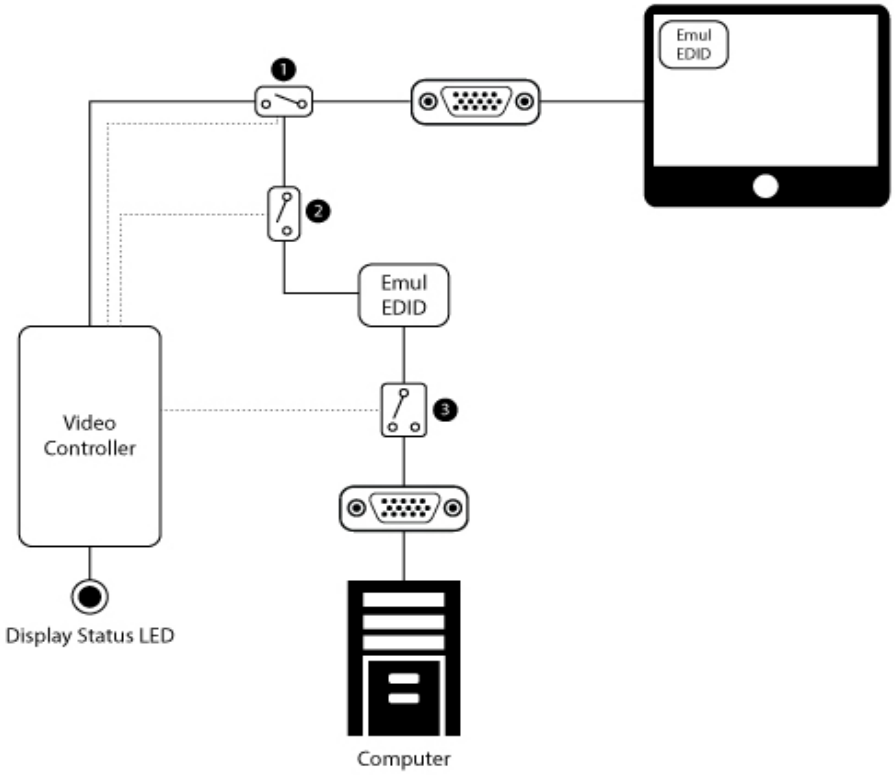

Figure 4 – Display EDID Read Function

An EDID read event occurs as the TOE is being powered up or when forcing an EDID read using 'Command Mode'. The video controller reads the EDID content from the display device to verify that it is valid and usable. For this, Switch 1 is

closed, and Switch 2 and Switch 3 are open. If data is not valid, TOE operation will cease and wait for the display peripheral to be changed.

In the next step, Switch 1 and Switch 3 are open, and Switch 2 is closed. The video controller writes the EDID content into the emulated EDID Electrically Erasable Programmable Read-Only Memory (EEPROM) chip.

The video controller uses the I2C lines to write to the emulated EDID EEPROM chip. Once the write operation is complete, the video controller switches to normal operating mode. In this mode, Switch 1 and Switch 2 are closed, and Switch 3 is open.

In the normal operation mode, the Emulated EDID EEPROM chip is switched to the computer to enable reading of the EDID information. The write protect switch (Switch 2) is switched to protected mode (i.e. it is closed) to prevent any attempt to write to the EEPROM or to transmit MCCS commands. In this mode, the power to the emulated EDID EEPROM is received from the computer through the video cable. During TOE normal operation, any attempt by the connected computer to affect the EDID channel is blocked by the architecture.

The EDID function is emulated by an independent emulation EEPROM chip. This chip reads content from the connected display once during TOE power up. Any subsequent change to the display peripheral will be ignored.

The EDID read event can also be initiated using 'Command Mode' and the Capture Key. The procedures for initiating the EDID read event are described in the Quick Start Guides. Following initiation of the EDID read, the procedures are the same.

The TOE will reject any display device that does not present valid EDID content. A Light Emitting Diode (LED) on the rear panel of the TOE will indicate a rejected display device.

The TOE supports DisplayPort versions 1.1, 1.2 and 1.3, and HDMI 2.0:

- For DisplayPort connections, the TOE video function filters the AUX channel by converting it to I2C EDID only. DisplayPort video is converted into an HDMI video stream, and the I2C EDID lines connected to the emulated EDID EEPROM functions as shown in the figures above. This allows EDID to be passed from the display to the computer (as described above), and allows Hot-Plug Detection (HPD) and Link Training information to pass through the TOE. AUX channel threats are mitigated through the conversion from DisplayPort to HDMI protocols. Traffic types including USB, Ethernet, MCCS, and EDID write from the computer to the display are blocked by the TOE. High-bandwidth Digital Content Protection (HDCP) and Consumer Electronics Control (CEC) functions are not connected
- For HDMI connections, EDID information is allowed to pass from the display to the computer, as described above. HPD information is also allowed to pass. Other protocols, including Audio Return Channel (ARC), EDID from the computer to the display, HDMI Ethernet and Audio Return

Channel (HEAC), and HDMI Ethernet Channel (HEC) are blocked. HDCP and Consumer Electronics Control (CEC) functions are not connected

The TOE video function blocks MCCS write transactions through the emulated EDID EEPROM. The emulated EEPROM supports only EDID read transactions.

Following a failed self-test, or when the TOE is powered off, all video input signals are isolated from the video output interface by the active video re-driver. The Emulated EDID EEPROM may still operate since it is powered by the computer.

The TOE accepts any DisplayPort or HDMI display device at the video peripheral ports. Only USB Type A connections are permitted. The TOE does not support a wireless connection to a video display.

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

7.1.1.2 Keyboard and Mouse Functionality

The TOE determines whether or not a peripheral device that has been plugged into the keyboard and mouse peripheral ports is allowed to operate with the TOE. The TOE uses optical data diodes to enforce a unidirectional data flow from the user peripherals to the coupled hosts, and uses isolated device emulators to prevent data leakage through the peripheral switching circuitry.

The Serial Random Access Memory (SRAM) in the host and device emulator circuitry stores USB Host stack parameters and up to the last 4 key codes. User data may be briefly retained; however, there are no data buffers. Data is erased during power off of the device.

The TOE supports USB Type A HIDs on keyboard and mouse ports. The USB bidirectional communication protocol is converted into a unidirectional proprietary protocol, and is then converted back into the USB bidirectional protocol to communicate with the coupled computer hosts.

A USB keyboard is connected to the TOE keyboard host emulator through the console keyboard port. The keyboard host emulator is a microcontroller which enumerates the connected keyboard and verifies that it is a permitted device type. Once the keyboard has been verified, the USB keyboard sends scan codes, which are generated when the user types. These scan codes are converted by the keyboard host emulator into a proprietary protocol data stream that is combined with the data stream from the mouse host emulator.

Similarly, the USB mouse is connected to the TOE mouse host emulator through the USB mouse port. The mouse host emulator is a microcontroller which enumerates the connected mouse and verifies that it is a permitted device type. Once the mouse device has been verified, it sends serial data generated by mouse movement and button use. The mouse serial data is converted by the mouse host emulator into a proprietary protocol data stream that is combined with the data stream from the keyboard host emulator.

The combined data stream is passed through the channel select lines to the connected computer. The combined mouse and keyboard data stream is passed

through an optical data diode to the host device emulator. The optical data diode is an opto-coupler designed to physically prevent reverse data flow.

Device emulators are USB enabled microcontrollers that are programmed to emulate a standard USB keyboard and mouse composite device. The combined data stream is converted back to bidirectional data before reaching the selected host computer.

Since the keyboard and mouse function are emulated by the TOE, the connected computer is not able to send data to the keyboard that would allow it to indicate that Caps Lock, Num Lock or Scroll Lock are set.

The TOE accepts only USB HIDs at the keyboard and mouse peripheral ports. Only USB Type A connections are permitted. The TOE does not support a wireless connection to a mouse, keyboard or USB hub.

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

7.1.1.3 Audio Data Flow

The TOE audio data flow path is unidirectional and includes filtering by design.

Unidirectional flow data diodes prevent audio data flow from an audio device to a selected computer. The audio interface is electrically isolated from other interfaces, and from other TOE circuitry. An analog to digital and digital to analog conversion is performed to filter out high frequencies. These features ensure that the audio filtration specification requirements are met.

The TOE does not supply power to the analog audio output interface, and cannot be configured to do so. Therefore, it cannot be used to supply power to an unauthorized device on that interface.

When the TOE is powered off, an audio isolation relay is open, thereby isolating the audio input from the computer interface from all other circuitry and interfaces. Following a failed self-test, the TOE will de-energize this audio isolation relay to isolate the audio input. The audio subsystem does not store, convert or delay audio data flows.

The TOE accepts analog headphones or analog speakers connected via a 1/8” (3.5mm) audio jack at the audio peripheral port. The TOE does not support a wireless connection to an audio output device.

The use of analog microphone or line-in audio devices is strictly prohibited as indicated in the user guidance. The TOE will reject a microphone through the following two methods:

- There is an analog audio data diode that forces data to flow only from a computer to an audio peripheral device
- There is a microphone Direct Current (DC) bias barrier that blocks an electret microphone DC bias if the TOE is deliberately or inadvertently connected to the microphone input jack of a connected computer

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

7.1.2 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
Audio	Analog audio through a 3.5 mm jack	Audio output devices such as speakers and headphones

Table 14 – 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

7.1.3 User Data Isolation SFP

The allowed data flows between the connected computer and the peripheral devices are described in Section 7.1.1.

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

7.2 SECURITY MANAGEMENT

7.2.1 Security Attributes

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.

The device type is determined by the signals from the peripheral device (e.g. USB HID). This cannot be changed by the user. No user can modify the device type attribute to cause the data from one peripheral device type to be directed to the computer port for a different device type. Therefore, the default values are considered to be restrictive.

TOE Security Functional Requirements addressed: FMT_MSA.1, FMT_MSA.3.

7.2.2 Security Management and Roles

The TOE provides for a single role 'user'. The TOE configuration cannot be changed. This ensures that that keyboard, video, mouse and audio data is directed as per the default configuration, and this cannot be changed by the user.

TOE Security Functional Requirements addressed: FMT_SMF.1, FMT_SMR.1.

7.3 PROTECTION OF THE TSF

7.3.1 Tamper Evidence

The TOE enclosure was designed specifically to prevent physical tampering. It features a stainless-steel welded chassis and panels that prevent external access through bending or brute force.

Additionally, each device is fitted with one or more holographic Tampering Evident Labels placed at critical locations on the TOE enclosure. If the label is removed, the word 'VOID' appears on both the label and the product surface.

TOE Security Functional Requirements addressed: FPT_PHP.1.

7.3.2 TSF Testing

The TOE performs a self-test at initial start-up. The self-test runs independently at each microcontroller and performs a verification of the integrity of the microcontroller firmware.

If the self-test fails, the LED on the front panel blinks to indicate the failure. The TOE remains in a disabled state until the self-test is rerun and passes.

TOE Security Functional Requirements addressed: FPT_TST.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.
I²C	I²C is a synchronous, serial protocol used to connect low-speed devices such as microcontrollers, EEPROMs, and other similar peripherals in embedded systems.
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 15 – Terminology

8.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
ARC	Audio Return Channel
CC	Common Criteria
CEC	Consumer Electronics Control
CM	Configuration Management
DC	Direct Current
DE	Device Emulator
EAL	Evaluation Assurance Level
EDID	Extended Display Identification Data
EEPROM	Electrically Erasable Programmable Read-Only Memory
HDCP	High-bandwidth Digital Content Protection
HDMI	High-Definition Multimedia Interface
HE	Host Emulator
HEC	HDMI Ethernet Channel
HID	Human Interface Device

Acronym	Definition
HPD	Hot-Plug Detection
IT	Information Technology
LED	Light Emitting Diode
MCCS	Monitor Control Command Set
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirement
SRAM	Serial Random Access Memory
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
USB	Universal Serial Bus

Table 16 – Acronyms