High Sec Labs FV11H-M, FV11D-M, FV11PH-M, FV11HH-MM, FV11PP-MM, FV11HP-MM, FV11PH-MM Video Isolators
Firmware Version 44000-E7E7

Security Target

Doc No: 2149-001-D102A7
Version: 1.1
14 January 2026

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
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, Protection Profile (PP) and PP Modules.

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 Functional Requirements, specifies the security functional requirements that must be satisfied by the TOE and the IT environment.

Section 7, Security Assurance Requirements, specifies the security assurance requirements that must be satisfied by the TOE and the IT environment.

Section 8, Security Requirements Rationale, provides a rationale for the selection of functional and assurance requirements.

Section 9, TOE Summary Specification, describes the security functions that are included in the TOE to enable it to meet the IT security functional requirements.

Section 10, Terminology and Acronyms, defines the acronyms and terminology used in this ST.

Section 11, References, provides a list of documents referenced in this ST.

1.2 SECURITY TARGET REFERENCE

ST Title:	High Sec Labs FV11H-M, FV11D-M, FV11PH-M, FV11HH-MM, FV11PP-MM, FV11HP-MM, FV11PH-MM Video Isolators Firmware Version 44000-E7E7 Security Target
ST Version:	1.1
ST Date:	14 January 2026

1.3 TOE REFERENCE

TOE Identification:	High Sec Labs FV11H-M, FV11D-M, FV11PH-M, FV11HH-MM, FV11PP-MM, FV11HP-MM, FV11PH-MM Video Isolators Firmware Version 44000-E7E7
TOE Developer:	High Sec Labs Ltd.
TOE Type:	Peripheral Sharing Device (Other Devices and Systems)

1.4 TOE OVERVIEW

The High Sec Labs (HSL) Video Isolators ensure unidirectional video between a connected computer and a display.

The following security features are provided by the HSL Peripheral Sharing Devices:

- Video Security
    - Computer video input interfaces are isolated through the use of separate electronic components, power and ground domains
    - The display is isolated by 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
    - DisplayPort, High-Definition Multimedia Interface (HDMI), and Digital Visual Interface (DVI)-D video peripherals are supported as follows:
        - The FV11D-M device supports a DVI-D video display
        - The FV11H-M, FV11PH-M, FV11HH-MM and FV11PH-MM devices support an HDMI video display
        - The FV11PH-M, FV11PP-MM and FV11HP-MM devices support a DisplayPort video display

  - DisplayPort, High-Definition Multimedia Interface (HDMI), and Digital Visual Interface (DVI)-D video input is supported as follows:
    - The FV11D-M device supports DVI-D video input
    - The FV11H-M, FV11PH-M, FV11HH-MM and FV11HP-MM devices support HDMI video input
    - The FV11PH-M, FV11PH-MM and FV11PP-MM devices support DisplayPort video input
- 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

High Sec Labs secure peripheral sharing devices use isolated microcontrollers to emulate connected peripherals in order to prevent display signaling and power signaling attacks.

The TOE is a combined software and hardware TOE. A mapping showing the applicable Security Functional Requirements (SFRs) for each device is included in Annex B.

1.4.1 TOE Environment

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

Component	Description
Connected Computer	1 general purpose computer
User display	Standard computer display (HDMI 2.0, DVI-D, DisplayPort 1.1, 1.2 or 1.3)
HSL KVM Cables	Video cable (DisplayPort, DVI-D, HDMI)

Table 1 – Non-TOE Hardware and Software

1.5 TOE DESCRIPTION

1.5.1 Evaluated Configuration

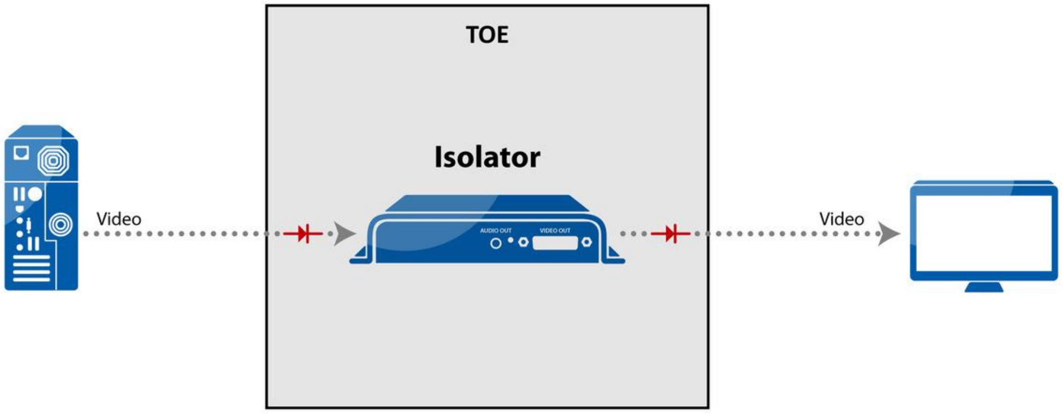

Figure 1 – Isolator Evaluated Configuration

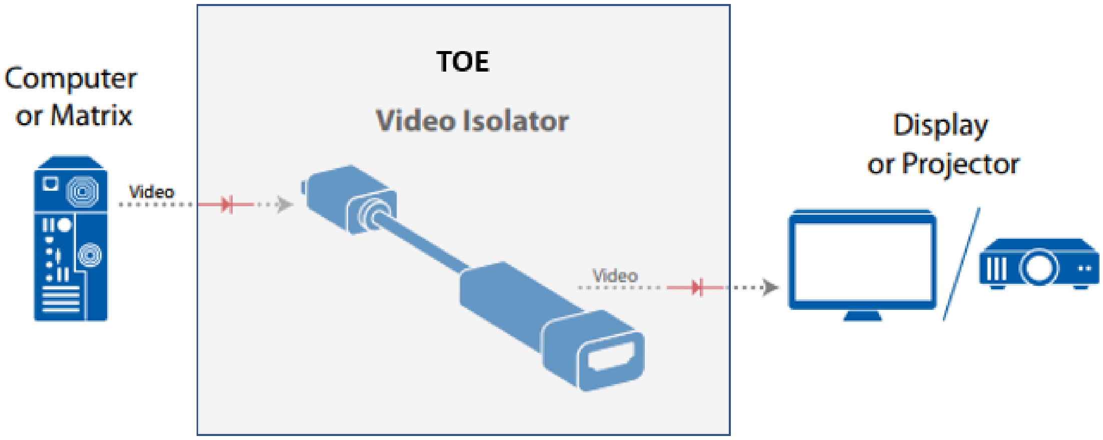

Figure 2 – Mini Isolator Evaluated Configuration

In the evaluated configuration, the isolator is connected to the computer and to the video display device to ensure unidirectional communications. The video input may be DisplayPort, HDMI or DVI-D.

For this evaluation, the TOE was tested according to the PP requirements using devices supporting DP 1.1a, DP 1.2 (for some tests), HDMI 1.4, USB 2.0, and CCID Revision 1.1 (for UA). The TOE supports DP 1.3 and HDMI 2.0 subject to the limitations stated in the TSS. These limitations are due to the PP mandated blocking of specific parts of the protocols.

1.5.2 Physical Scope

The TOE consists of the devices shown in Table 2.

Family Description	Part Number	Model	Tamper Evident labels	Video in	Video out
Single Port video isolator devices	CGA14746	FV11H-M	Yes	HDMI	HDMI
	CGA14744	FV11D-M	Yes	DVI-D	DVI-D
	CGA19442	FV11PH-M	Yes	DP/HDMI	DP/HDMI
	CGA26978	FV11HH-MM	Yes	HDMI	HDMI
	CGA26979	FV11HP-MM	Yes	HDMI	DP
	CGA26980	FV11PH-MM	Yes	DP	HDMI
	CGA26981	FV11PP-MM	Yes	DP	DP

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 trusted carrier, such as Fed-Ex, that provide a tracking service for all shipments.

1.5.2.2 TOE Guidance

The TOE includes the following guidance documentation:

- HSL QUICK SETUP GUIDE Secure KVM Isolators, HLT34088 Rev. 2.0

Guidance may be downloaded from the High Sec Labs website (https://highseclabs.com/quick-start-guides/) in .pdf format.

The following guidance is available upon request by emailing support@highseclabs.com:

- High Sec Labs FV11H-M, FV11D-M, FV11PH-M, FV11HH-MM, FV11PP-MM, FV11HP-MM, FV11PH-MM Firmware Version 44000-E7E7 Peripheral Sharing Devices Common Criteria Guidance Supplement, Version 1.0

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 video. The TOE ensures that only authorized peripheral devices may be used.
Protection of the TSF[1]	The TOE ensures a secure state in the case of failure, provides only restricted access, and performs self-testing. The TOE provides passive detection of physical attack.

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 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 PP-CONFIGURATION CONFORMANCE CLAIM

This ST claims exact conformance with the National Information Assurance Partnership (NIAP) PP-Configuration for Peripheral Sharing Device and Video/Display Devices, 19 July 2019 [CFG_PSD-VI_V1.0]

This PP-Configuration includes the following components:

- Base-PP: Protection Profile for Peripheral Sharing Device, Version 4.0 [PP_PSD_V4.0]
- PP-Module: PP-Module for Video/Display Devices, Version 1.0 [MOD_VI_V1.0]

2.3 TECHNICAL DECISIONS

The Technical Decisions in Table 4 apply to the PP and the modules and have been accounted for in the ST and in the evaluation.

TD	Name	PP affected	Relevant Y/N
TD0506	Missing Steps to disconnect and reconnect display	[MOD_VI_V1.0]	Y
TD0514	Correction to MOD VI FDP_APC_EXT.1 Test 3 Step 6	[MOD_VI_V1.0]	Y

TD	Name	PP affected	Relevant Y/N
TD0518	Typographical errors in dependency Table	[PP_PSD_V4.0]	N FPT_STM.1 is not claimed in the ST
TD0539	Incorrect selection trigger in FTA_CIN_EXT.1 in MOD_VI_V1.0	[MOD_VI_V1.0]	Y
TD0583	FPT_PHP.3 modified for remote controllers	[PP_PSD_V4.0]	Y
TD0584	Update to FDP_APC_EXT.1 Video Tests	[MOD_VI_V.10]	Y
TD0593	Equivalency Arguments for PSD	[MOD_VI_V1.0]	Y
TD0681	PSD purging of EDID data upon disconnect	[MOD_VI_V1.0]	Y
TD0686	DisplayPort CEC Testing	[MOD_VI_V1.0]	Y
TD0804	Clarification regarding Extenders in PSD Evaluations	[PP_PSD_V4.0]	Y
TD0842	Alternate Conversion Option for FDP_IPC_EXT.1	[MOD_VI_V1.0]	Y
TD0844	Addition of Assurance Package for Flaw Remediation V1.0 Conformance Claim	[PP_PSD_V4.0]	N No ALC_FLR SARs are claimed in the ST
TD0942	Updated EDID Read Requirements	[MOD_VI_V1.0]	Y

Table 4 – Applicable Technical Decisions

2.4 PACKAGE CLAIM

This Security Target does not claim conformance to any package.

2.5 CONFORMANCE RATIONALE

The TOE Video Isolator devices are inherently consistent with the Compliant Targets of Evaluation described in the [PP_PSD_V4.0] and in the PP-Module for Video/Display Devices, Version 1.0 [MOD_VI_1.0], and with the PP-Configuration for Peripheral Sharing Device and Video/Display Devices [CFG_PSD-VI_V1.0].

The security problem definition, statement of security objectives and statement of security requirements in this ST conform exactly to the security problem definition, statement of security objectives and statement of security requirements contained in [PP_PSD_V4.0] and the PP-Module for Video/Display Devices, Version 1.0 [MOD_VI_1.0].

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 5 lists the threats described in Section 3.1 of the [PP_PSD_V4.0]. Mitigation to the threats is through the objectives identified in Section 4.1, Security Objectives for the TOE.

Threat	Description
T.DATA_LEAK	A connection via the PSD[2] between one or more computers may allow unauthorized data flow through the PSD or its connected peripherals.
T.SIGNAL_LEAK	A connection via the PSD between one or more computers may allow unauthorized data flow through bit-by-bit signaling.
T.RESIDUAL_LEAK	A PSD may leak (partial, residual, or echo) user data between the intended connected computer and another unintended connected computer.
T.UNINTENDED_USE	A PSD may connect the user to a computer other than the one to which the user intended to connect.
T.UNAUTHORIZED_DEVICES	The use of an unauthorized peripheral device with a specific PSD peripheral port may allow unauthorized data flows between connected devices or enable an attack on the PSD or its connected computers.
T.LOGICAL_TAMPER	An attached device (computer or peripheral) with malware, or otherwise under the control of a malicious user, could modify or overwrite code or data stored in the PSD's volatile or non-volatile memory to allow unauthorized information flows.
T.PHYSICAL_TAMPER	A malicious user or human agent could physically modify the PSD to allow unauthorized information flows.

[2] Peripheral Sharing Device

Threat	Description
T.REPLACEMENT	A malicious human agent could replace the PSD during shipping, storage, or use with an alternate device that does not enforce the PSD security policies.
T.FAILED	Detectable failure of a PSD may cause an unauthorized information flow or weakening of PSD security functions.

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 6.

Assumptions	Description
A.NO_TEMPEST	Computers and peripheral devices connected to the PSD are not TEMPEST approved. The TSF may or may not isolate the ground of the keyboard and mouse computer interfaces (the USB ground). The Operational Environment is assumed not to support TEMPEST red-black ground isolation.
A.PHYSICAL	The environment provides physical security commensurate with the value of the TOE and the data it processes and contains.
A.NO_WIRELESS_DEVICES	The environment includes no wireless peripheral devices.
A.TRUSTED_ADMIN	PSD Administrators and users are trusted to follow and apply all guidance in a trusted manner.
A.TRUSTED_CONFIG	Personnel configuring the PSD and its operational environment follow the applicable security configuration guidance.
A.USER_ALLOWED_ACCESS	All PSD users are allowed to interact with all connected computers. It is not the role of the PSD to prevent or otherwise control user access to connected computers. Computers or their connected network shall have the required means to authenticate the user and to control access to their various resources.

Assumptions	Description
A.NO_SPECIAL_ANALOG_CAPABILITIES	The computers connected to the TOE are not equipped with special analog data collection cards or peripherals such as analog to digital interface, high performance audio interface, digital signal processing function, or analog video capture function.

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, and traces each Security Functional Requirement (SFR) back to a security objective of the TOE.

<table>
<tr><th>Security Objective</th><th>Description</th></tr>
<tr><td><b>O.COMPUTER _INTERFACE _ISOLATION</b></td><td>The PSD shall prevent unauthorized data flow to ensure that the PSD and its connected peripheral devices cannot be exploited in an attempt to leak data. The TOE-Computer interface shall be isolated from all other PSD-Computer interfaces while TOE is powered.
Addressed by:<table><tr><td>MOD_VI</td><td>FDP_APC_EXT.1/VI, FDP_PDC_EXT.1</td></tr></table></td></tr>
<tr><td><b>O.COMPUTER _INTERFACE _ISOLATION _TOE_UNPOWERED</b></td><td>The PSD shall not allow data to transit a PSD-Computer interface while the PSD is unpowered.
Addressed by:<table><tr><td>MOD_VI</td><td>FDP_APC_EXT.1/VI, FDP_PDC_EXT.1</td></tr></table></td></tr>
<tr><td><b>O.USER_DATA _ISOLATION</b></td><td>The PSD shall route user data, such as keyboard entries, only to the computer selected by the user. The PSD shall provide isolation between the data flowing from the peripheral device to the selected computer and any non-selected computer.
Addressed by:<table><tr><td>MOD_VI</td><td>FDP_APC_EXT.1/VI, FDP_PDC_EXT.1</td></tr></table></td></tr>
</table>

<table>
<tr><th>Security Objective</th><th>Description</th></tr>
<tr><td><b>O.NO_USER _DATA_RETENTION</b></td><td>The PSD shall not retain user data in non-volatile memory after power up or, if supported, factory reset.
Addressed by:<table><tr><td>PP_PSD</td><td>FDP_RIP_EXT.1</td></tr></table></td></tr>
<tr><td><b>O.NO_OTHER _EXTERNAL _INTERFACES</b></td><td>The PSD shall not have any external interfaces other than those implemented by the TSF.
Addressed by:<table><tr><td>PP_PSD</td><td>FDP_PDC_EXT.1</td></tr></table></td></tr>
<tr><td><b>O.LEAK _PREVENTION _SWITCHING</b></td><td>The PSD shall ensure that there are no switching mechanisms that allow signal data leakage between connected computers.
Addressed by:<table><tr><td>PP_PSD</td><td>FDP_SWI_EXT.1, FDP_SWI_EXT.2</td></tr></table></td></tr>
<tr><td><b>O.AUTHORIZED _USAGE</b></td><td>The TOE shall explicitly prohibit or ignore unauthorized switching mechanisms, either because it supports only one connected computer or because it allows only authorized mechanisms to switch between connected computers. Authorized switching mechanisms shall require express user action restricted to console buttons, console switches, console touch screen, wired remote control, and peripheral devices using a guard. Unauthorized switching mechanisms include keyboard shortcuts, also known as “hotkeys,” automatic port scanning, control through a connected computer, and control through keyboard shortcuts. Where applicable, the results of the switching activity shall be indicated by the TSF so that it is clear to the user that the switching mechanism was engaged as intended.
A conformant TOE may also provide a management function to configure some aspects of the TSF. If the TOE provides this functionality, it shall ensure that whatever management functions it provides can only be performed by authorized administrators and that an audit trail of management activities is generated.
Addressed by:<table><tr><td>PP_PSD</td><td>FDP_SWI_EXT.1, FDP_SWI_EXT.2</td></tr><tr><td>MOD_VI</td><td>FDP_CDS_EXT.1</td></tr></table></td></tr>
</table>

Security Objective	Description		
O.PERIPHERAL _PORTS_ISOLATION	The PSD shall ensure that data does not flow between peripheral devices connected to different PSD interfaces. Addressed by:	MOD_VI	FDP_APC_EXT.1/VI, FDP_PDC_EXT.1
O.REJECT _UNAUTHORIZED _PERIPHERAL	The PSD shall reject unauthorized peripheral device types and protocols. Addressed by:	PP_PSD	FDP_PDC_EXT.1
		MOD_VI	FDP_PDC_EXT.2/VI, FDP_PDC_EXT.3/VI, FDP_IPC_EXT.1, FDP_SPR_EXT.1/DP, SPR_EXT.1/DVI-D, FDP_SPR_EXT.1/HDMI, FDP_SPR_EXT.1/USB
O.REJECT _UNAUTHORIZED _ENDPOINTS	The PSD shall reject unauthorized peripheral devices connected via a Universal Serial Bus (USB) hub. Addressed by:	PP_PSD	FDP_PDC_EXT.1
O.NO_TOE_ACCESS	The PSD firmware, software, and memory shall not be accessible via its external ports. Addressed by:	PP_PSD	FPT_NTA_EXT.1
O.TAMPER _EVIDENT _LABEL	The PSD shall be identifiable as authentic by the user and the user must be made aware of any procedures or other such information to accomplish authentication. This feature must be available upon receipt of the PSD and continue to be available during the PSD deployment. The PSD shall be labeled with at least one visible unique identifying tamper-evident marking that can be used to authenticate the device. The PSD manufacturer must maintain a complete list of manufactured PSD articles and their respective identification markings' unique identifiers. Addressed by:	PP_PSD	FPT_PHP.1

<table>
<tr><th>Security Objective</th><th>Description</th></tr>
<tr><td><b>O.ANTI_TAMPERING</b></td><td>The PSD shall be physically enclosed so that any attempts to open or otherwise access the internals or modify the connections of the PSD would be evident, and optionally thwarted through disablement of the TOE. Note: This applies to a wired remote control as well as the main chassis of the PSD.
Addressed by:<table><tr><td>PP_PSD</td><td>FPT_PHP.1</td></tr></table></td></tr>
<tr><td><b>O.SELF_TEST</b></td><td>The PSD shall perform self-tests following power up or powered reset.
Addressed by:<table><tr><td>PP_PSD</td><td>FPT_TST.1</td></tr></table></td></tr>
<tr><td><b>O.SELF_TEST _FAIL_TOE _DISABLE</b></td><td>The PSD shall enter a secure state upon detection of a critical failure.
Addressed by:<table><tr><td>PP_PSD</td><td>FPT_FLS_EXT.1, FPT_TST_EXT.1</td></tr></table></td></tr>
<tr><td><b>O.SELF_TEST _FAIL_INDICATION</b></td><td>The PSD shall provide clear and visible user indications in the case of a self-test failure.
Addressed by:<table><tr><td>PP_PSD</td><td>FPT_TST_EXT.1</td></tr></table></td></tr>
<tr><td><b>O.PROTECTED _EDID</b></td><td>The TOE shall read the connected display Extended Display Identification Data (EDID) once during the TOE power up or reboot sequence and prevent any EDID channel write transactions that connected computers initiate.
Addressed by:<table><tr><td>MOD_VI</td><td>FDP_PDC_EXT.2/VI, FDP_SPR_EXT.1/DP, FDP_SPR_EXT.1/DVI-D, FDP_SPR_EXT.1/HDMI, FDP_SPR_EXT.1/USB</td></tr></table></td></tr>
<tr><td><b>O.UNIDIRECTIONAL _VIDEO</b></td><td>The TOE shall enforce unidirectional video data flow from the connected computer video interface to the display interface only.
Addressed by:<table><tr><td>MOD_VI</td><td>FDP_UDF_EXT.1/VI</td></tr></table></td></tr>
</table>

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.NO_TEMPEST	The operational environment will not use TEMPEST approved equipment.
OE.PHYSICAL	The operational environment will provide physical security, commensurate with the value of the PSD and the data that transits it.
OE.NO_WIRELESS_DEVICES	The operational environment will not include wireless keyboards, mice, audio, user authentication, or video devices.
OE.TRUSTED_ADMIN	The operational environment will ensure that trusted PSD Administrators and users are appropriately trained.
OE.TRUSTED_CONFIG	The operational environment will ensure that administrators configuring the PSD and its operational environment follow the applicable security configuration guidance.
OE.NO_SPECIAL_ANALOG _CAPABILITIES	The operational environment will not have special analog data collection cards or peripherals such as analog to digital interface, high performance audio interface, or a component with digital signal processing or analog video capture functions.

Table 8 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

The security objectives rationale describes how the assumptions and threats map to the security objectives.

Threat or Assumption	Security Objective(s)	Rationale
T.DATA_LEAK	O.COMPUTER _INTERFACE _ISOLATION	Isolation of computer interfaces prevents data from leaking between them without authorization.
	O.COMPUTER _INTERFACE _ISOLATION _TOE_UNPOWERED	Maintaining interface isolation while the TOE is in an unpowered state ensures that data cannot leak between computer interfaces.
	O.USER_DATA _ISOLATION	The TOE's routing of data only to the selected computer ensures that it will not leak to any others.
	O.NO_OTHER _EXTERNAL _INTERFACES	The absence of additional external interfaces ensures that there is no unexpected method by which data can be leaked.
	O.PERIPHERAL_PORTS _ISOLATION	Isolation of peripheral ports prevents data from leaking between them without authorization.
	O.PROTECTED_EDID	The TOE's protection of the EDID interface prevents its use as a vector for unauthorized data leakage via this channel.
	O.UNIDIRECTIONAL _VIDEO	The TOE's enforcement of unidirectional output for video data protects against data leakage via connected computers by ensuring that no video data can be input to a connected computer through this interface.
T.SIGNAL_LEAK	O.COMPUTER _INTERFACE _ISOLATION	Isolation of computer interfaces prevents data leakage through bit-wise signaling because there is no mechanism by which the signal data can be communicated.
	O.NO_OTHER _EXTERNAL _INTERFACES	The absence of additional external interfaces ensures that there is no unexpected method by which data can be leaked through bitwise signaling.

Threat or Assumption	Security Objective(s)	Rationale
	O.LEAK_PREVENTION _SWITCHING	The TOE’s use of switching methods that are not susceptible to signal leakage helps mitigate the signal leak threat.
	O.PROTECTED_EDID	The TOE’s protection of the EDID interface prevents its use as a vector for bit-by-bit signal leakage via this channel.
	O.UNIDIRECTIONAL _VIDEO	The TOE’s enforcement of unidirectional output for video data protects against signaling leakage via connected computers by ensuring that no video data can be input to a connected computer through this interface.
T.RESIDUAL _LEAK	O.NO_USER_DATA _RETENTION	The TOE’s lack of data retention ensures that a residual data leak is not possible.
	O.PROTECTED_EDID	The TOE’s protection of the EDID interface prevents the leakage of residual data by ensuring that no such data can be written to EDID memory.
T.UNINTENDED _USE	O.AUTHORIZED _USAGE	The TOE’s support for only switching mechanisms that require explicit user action to engage ensures that a user has sufficient information to avoid interacting with an unintended computer.
T.UNAUTHORIZED _DEVICES	O.REJECT _UNAUTHORIZED _ENDPOINTS	The TOE’s ability to reject unauthorized endpoints mitigates the threat of unauthorized devices being used to communicate with connected computers.
	O.REJECT _UNAUTHORIZED _PERIPHERAL	The TOE’s ability to reject unauthorized peripherals mitigates the threat of unauthorized devices being used to communicate with connected computers.
	O.UNIDIRECTIONAL _VIDEO	The TOE’s limitation of supported video protocol interfaces prevents the connection of unauthorized devices.

Threat or Assumption	Security Objective(s)	Rationale
T.LOGICAL _TAMPER	O.NO_TOE_ACCESS	The TOE’s prevention of logical access to its firmware, software, and memory mitigates the threat of logical tampering.
T.PHYSICAL _TAMPER	O.ANTI_TAMPERING	The TOE mitigates the threat of physical tampering through use of an enclosure that provides tamper detection functionality.
	O.TAMPER_EVIDENT _LABEL	The TOE mitigates the threat of physical tampering through use of tamper evident labels that reveal physical tampering attempts.
T.REPLACEMENT	O.TAMPER_EVIDENT _LABEL	The TOE’s use of a tamper evident label that provides authenticity of the device mitigates the threat that it is substituted for a replacement device during the acquisition process.
T.FAILED	O.SELF_TEST	The TOE mitigates the threat of failures leading to compromise of security functions through self-tests of its own functionality.
	O.SELF_TEST_FAIL _TOE_DISABLE	The TOE mitigates the threat of failures leading to compromise of security functions by disabling all data flows in the event a failure is detected.
	O.SELF_TEST_FAIL _INDICATION	The TOE mitigates the threat of failures leading to compromise of security functions by providing users with a clear indication when it is in a failure state and should not be trusted.
A.NO_TEMPEST	OE.NO_TEMPEST	If the TOE’s operational environment does not include TEMPEST approved equipment, then the assumption is satisfied.
A.NO_PHYSICAL	OE.PHYSICAL	If the TOE’s operational environment provides physical security, then the assumption is satisfied.
A.NO_WIRELESS _DEVICES	OE.NO_WIRELESS _DEVICES	If the TOE’s operational environment does not include wireless peripherals, then the assumption is satisfied.

Threat or Assumption	**Security Objective(s)**	**Rationale**
A.TRUSTED_ADMIN	OE.TRUSTED _ADMIN	If the TOE’s operational environment ensures that only trusted administrators will manage the TSF, then the assumption is satisfied.
A.TRUSTED _CONFIG	OE.TRUSTED _CONFIG	If TOE administrators follow the provided security configuration guidance, then the assumption is satisfied.
A.USER_ALLOWED _ACCESS	OE.PHYSICAL	If the TOE’s operational environment provides physical access to connected computers, then the assumption is satisfied.
A.NO_SPECIAL _ANALOG _CAPABILITIES	OE.NO_SPECIAL _ANALOG _CAPABILITIES	If administrators in the TOE’s operational environment take care to ensure that computers with special analog data collection interfaces are not connected to the TOE, then the assumption that such components are not present is satisfied.

Table 9 – Security Objectives Rationale

5 EXTENDED COMPONENTS DEFINITION

The extended components definition is presented in Appendix C of the Protection Profile for Peripheral Sharing Device [PP_PSD_V4.0] and in the module for display devices [MOD_VI_V1.0].

The families to which these components belong are identified in the following table:

Functional Class	Functional Families	Protection Profile Module
User Data Protection (FDP)	FDP_APC_EXT Active PSD Connections	[PP_PSD_V4.0]
	FDP_CDS_EXT Connected Displays Supported	[MOD_VI_V1.0]
	FDP_IPC_EXT Internal Protocol Conversion	[MOD_VI_V1.0]
	FDP_PDC_EXT Peripheral Device Connection	[PP_PSD_V4.0] [MOD_VI_V1.0]
	FDP_RIP_EXT Residual Information Protection	[PP_PSD_V4.0]
	FDP_SPR_EXT Sub-Protocol Rules	[MOD_VI_V1.0]
	FDP_SWI_EXT PSD Switching	[PP_PSD_V4.0]
	FDP_UDF_EXT Unidirectional Data Flow	[MOD_VI_V1.0]
Protection of the TSF (FPT)	FPT_FLS_EXT Failure with Preservation of Secure State	[PP_PSD_V4.0]
	FPT_NTA_EXT No Access to TOE	[PP_PSD_V4.0]
	FPT_TST_EXT TSF Testing	[PP_PSD_V4.0]

Table 10 – Functional Families of Extended Components

6 SECURITY FUNCTIONAL REQUIREMENTS

Section 6 provides security functional and assurance requirements that must be satisfied by a compliant TOE.

6.1 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. This is defined in the PP as:

- Assignment: Indicated by surrounding brackets and underline, e.g., [assigned item].
- Selection: Indicated by surrounding brackets and italics, e.g., [*selected item*].
- Refinement: Refined components are identified by using **[bold surrounded by brackets]** for additional information, or ~~[strikeout surrounded by brackets]~~ for deleted text.
- Iteration: Iteration operations for iterations within the Protection Profile and associated modules are identified with a slash ('/') and an identifier (e.g. "/VI").

Extended SFRs are identified by the inclusion of "EXT" in the SFR name.

The CC operations already performed in the PP and PP modules are reproduced in plain text and not denoted in this ST. The requirements have been copied from the PP and PP modules and any remaining operations have been completed herein. Refer to the PP and PP modules to identify those operations.

6.2 SECURITY FUNCTIONAL REQUIREMENTS

Section 6.2 details the security functional requirements that apply to all TOE devices.

Class	Identifier	Name	Source	Applicable Devices
User Data Protection (FDP)	FDP_APC_EXT.1/VI	Active PSD Connections	[MOD_VI_V1.0]	All
	FDP_CDS_EXT.1	Connected Displays Supported	[MOD_VI_V1.0]	All
	FDP_IPC_EXT.1	Internal Protocol Conversion	[MOD_VI_V1.0]	FV11PH-M, FV11PH-MM

Class	Identifier	Name	Source	Applicable Devices
	FDP_PDC_EXT.1	Peripheral Device Connection	[PP_PSD_V4.0] [MOD_VI_V1.0][3]	All
	FDP_PDC_EXT.2/VI	Authorized Devices (Video Output)	[MOD_VI_V1.0]	All
	FDP_PDC_EXT.3/VI(1)	Authorized Connection Protocols (Video Output) (1)	[MOD_VI_V1.0]	FV11D-M
	FDP_PDC_EXT.3/VI(2)	Authorized Connection Protocols (Video Output) (2)	[MOD_VI_V1.0]	FV11H-M, FV11HH-MM
	FDP_PDC_EXT.3/VI(3)	Authorized Connection Protocols (Video Output) (3)	[MOD_VI_V1.0]	FV11PH-M, FV11PH-MM, FV11HP-MM
	FDP_PDC_EXT.3/VI(4)	Authorized Connection Protocols (Video Output) (4)	[MOD_VI_V1.0]	FV11PP-MM
	FDP_RIP_EXT.1	Residual Information Protection	[PP_PSD_V4.0]	All
	FDP_SPR_EXT.1/DVI-D	Sub-Protocol Rules (DVI-D Protocol)	[MOD_VI_V1.0]	FV11D-M
	FDP_SPR_EXT.1/HDMI	Sub-Protocol Rules (HDMI Protocol)	[MOD_VI_V1.0]	FV11H-M, FV11PH-M, FV11HH-MM, FV11PH-MM, FV11HP-MM
	FDP_SPR_EXT.1/DP	Sub-Protocol Rules (DP Protocol)	[MOD_VI_V1.0]	FV11PH-M, FV11PP-MM, FV11PH-MM, FV11HP-MM
	FDP_SWI_EXT.1	PSD Switching	[PP_PSD_V4.0]	All
	FDP_UDF_EXT.1/VI	Unidirectional Data Flow (Video Output)	[MOD_VI_V1.0]	All

[3] There is no modification to this SFR in the [MOD_VI_V1.0]. However, there are additions to the Peripheral Device Connections associated with this SFR and additional evaluation activities.

Class	Identifier	Name	Source	Applicable Devices
Protection of the TSF (FPT)	FPT_FLS_EXT.1	Failure with Preservation of Secure State	[PP_PSD_V4.0]	All
	FPT_NTA_EXT.1	No Access to TOE	[PP_PSD_V4.0]	All
	FPT_PHP.1	Passive Detection of Physical Attack	[PP_PSD_V4.0]	All
	FPT_TST.1	TSF Testing	[PP_PSD_V4.0]	All
	FPT_TST_EXT.1	TSF Testing	[PP_PSD_V4.0]	All

Table 11 – Summary of Security Functional Requirements

6.2.1 User Data Protection (FDP)

6.2.1.1 FDP_APC_EXT.1/VI Active PSD Connections

FDP_APC_EXT.1.1/VI The TSF shall route user data only from the interfaces selected by the user.

FDP_APC_EXT.1.2/VI The TSF shall ensure that no data or electrical signals flow between connected computers whether the TOE is powered on or powered off.

FDP_APC_EXT.1.3/VI The TSF shall ensure that no data transits the TOE when the TOE is powered off.

FDP_APC_EXT.1.4/VI The TSF shall ensure that no data transits the TOE when the TOE is in a failure state.

6.2.1.2 FDP_CDS_EXT.1 Connected Displays Supported

FDP_CDS_EXT.1.1 The TSF shall support [*one connected display*] at a time.

6.2.1.3 FDP_IPC_EXT.1 Internal Protocol Conversion

FDP_IPC_EXT.1.1 The TSF shall convert the DisplayPort protocol at the [*DisplayPort peripheral display interface(s), DisplayPort computer video interface*] into the HDMI protocol within the TOE.

FDP_IPC_EXT.1.2 The TSF shall output the [*HDMI*] protocol from inside the TOE to [*computer video interface, peripheral display interface(s)*] as [*DisplayPort protocol, HDMI protocol*].

Application Note: TD0842 applies to this SFR definition. FDP_IPC_EXT.1 applies to models FV11PH-M, FV11HP-MM, FV11PH-MM, and FV11PP-MM.

6.2.1.4 FDP_PDC_EXT.1 Peripheral Device Connection

FDP_PDC_EXT.1.1 The TSF shall reject connections with unauthorized devices upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

FDP_PDC_EXT.1.2 The TSF shall reject connections with devices presenting unauthorized interface protocols upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

FDP_PDC_EXT.1.3 The TOE shall have no external interfaces other than those claimed by the TSF.

FDP_PDC_EXT.1.4 The TOE shall not have wireless interfaces.

FDP_PDC_EXT.1.5 The TOE shall provide a visual or auditory indication to the User when a peripheral is rejected.

6.2.1.5 FDP_PDC_EXT.2/VI Peripheral Device Connection (Video Output)

FDP_PDC_EXT.2.1/VI The TSF shall allow connections with authorized devices as defined in Appendix E **[of [MOD_VI_V1.0]]** and [

- *no other devices*

] upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

FDP_PDC_EXT.2.2/VI The TSF shall allow connections with authorized devices presenting authorized interface protocols as defined in Appendix E **[of [MOD_VI_V1.0]]** and [

- *no other devices*

] upon TOE power up and upon connection of a peripheral device to a powered-on TOE.

6.2.1.6 FDP_PDC_EXT.3/VI(1) Authorized Connection Protocols (Video Output) (1)

FDP_PDC_EXT.3.1/VI(1) The TSF shall have interfaces for the [*DVI-D*] protocols.

FDP_PDC_EXT.3.2/VI(1) The TSF shall apply the following rules to the supported protocols: [*the TSF shall use a fixed EDID file stored within the TSF to send to each of the host computers, the TSF shall read the connected display EDID information once during power-on or reboot [when prompted by user intervention]*[.

Application Note: TD0942 applies to this SFR definition. FDP_PDC_EXT.3/VI(1) applies to model FV11D-M.

6.2.1.7 FDP_PDC_EXT.3/VI(2) Authorized Connection Protocols (Video Output) (2)

FDP_PDC_EXT.3.1/VI(2) The TSF shall have interfaces for the [*HDMI*] protocols.

FDP_PDC_EXT.3.2/VI(2) The TSF shall apply the following rules to the supported protocols: [*the TSF shall use a fixed EDID file stored within the TSF to send to each of the host computers, the TSF shall read the connected display EDID information once during power-on or reboot [when prompted by user intervention]]*.

Application Note: TD0942 applies to this SFR definition. FDP_PDC_EXT.3/VI(2) applies to models FV11H-M and FV11HH-MM. Only the FV11H-M has the ability to read the connected display EDID information.

6.2.1.8 FDP_PDC_EXT.3/VI(3) Authorized Connection Protocols (Video Output) (3)

FDP_PDC_EXT.3.1/VI(3) The TSF shall have interfaces for the [*HDMI, DisplayPort*] protocols.

FDP_PDC_EXT.3.2/VI(3) The TSF shall apply the following rules to the supported protocols: [*the TSF shall use a fixed EDID file stored within the TSF to send to each of the host computers, the TSF shall read the connected display EDID information once during power-on or reboot [when prompted by user intervention]]*.

Application Note: TD0942 applies to this SFR definition. FDP_PDC_EXT.3/VI(3) applies to models FV11PH-M, FV11HP-MM and FV11PH-MM. Only the FV11PH-M has the ability to read the connected display EDID information.

6.2.1.9 FDP_PDC_EXT.3/VI(4) Authorized Connection Protocols (Video Output) (4)

FDP_PDC_EXT.3.1/VI(4) The TSF shall have interfaces for the [*DisplayPort*] protocols.

FDP_PDC_EXT.3.2/VI(4) The TSF shall apply the following rules to the supported protocols: [*the TSF shall use a fixed EDID file stored within the TSF to send to each of the host computers*].

Application Note: TD0942 applies to this SFR definition. FDP_PDC_EXT.3/VI(4) applies to model FV11PP-MM.

6.2.1.10 FDP_RIP_EXT.1 Residual Information Protection

FDP_RIP_EXT.1.1 The TSF shall ensure that no user data is written to TOE non-volatile memory or storage.

6.2.1.11 FDP_SPR_EXT.1/DVI-D Sub-Protocol Rules (DVI-D Protocol)

FDP_SPR_EXT.1.1/DVI-D The TSF shall apply the following rules for the DVI-D protocol:

- block the following video/display sub-protocols:
    - ARC,
    - CEC,

  - EDID from computer to display,
  - HDCP,
  - HEAC,
  - HEC,
  - MCCS
- allow the following video/display sub-protocols:
  - EDID from display to computer,
  - HPD from display to computer.

Application Note: FDP_SPR_EXT.1/DVI-D applies to model FV11D-M.

6.2.1.12 FDP_SPR_EXT.1/HDMI Sub-Protocol Rules (HDMI Protocol)

FDP_SPR_EXT.1.1/HDMI The TSF shall apply the following rules for the HDMI protocol:

- block the following video/display sub-protocols:
  - ARC
  - CEC,
  - EDID from computer to display,
  - HDCP,
  - HEAC,
  - HEC,
  - MCCS
- allow the following video/display sub-protocols:
  - EDID from display to computer,
  - HPD from display to computer.

Application Note: FDP_SPR_EXT.1/HDMI applies to the following models: FV11H-M, FV11PH-M, FV11HH-MM, FV11HP-MM and FV11PH-MM.

6.2.1.13 FDP_SPR_EXT.1/DP Sub-Protocol Rules (DisplayPort Protocol)

FDP_SPR_EXT.1.1/DP The TSF shall apply the following rules for the DisplayPort protocol:

- block the following video/display sub-protocols:
  - CEC,
  - EDID from computer to display,
  - HDCP,
  - MCCS
- allow the following video/display sub-protocols:
  - EDID from display to computer,
  - HPD from display to computer,
  - Link Training.

Application Note: FDP_SPR_EXT.1/DP applies to the following models: FV11PH-M, FV11PP-MM, FV11HP-MM and FV11PH-MM.

6.2.1.14 FDP_SWI_EXT.1 PSD Switching

FDP_SWI_EXT.1.1 The TSF shall ensure that [*the TOE supports only one connected computer*].

6.2.1.15 FDP_UDF_EXT.1/VI Unidirectional Data Flow (Video Output)

FDP_UDF_EXT.1.1/VI The TSF shall ensure video data transits the TOE unidirectionally from the TOE computer video interface to the TOE peripheral device display interface.

6.2.2 Protection of the TSF (FPT)

6.2.2.1 FPT_FLS_EXT.1 Failure with Preservation of Secure State

FPT_FLS_EXT.1.1 The TSF shall preserve a secure state when the following types of failures occur: failure of the power-on self-test and [*no other failures*].

6.2.2.2 FPT_NTA_EXT.1 No Access to TOE

FPT_NTA_EXT.1.1 TOE firmware, software, and memory shall not be accessible via the TOE’s external ports, with the following exceptions: [*the **Extended Display Identification Data** (EDID) memory of Video TOEs may be accessible from connected computers; the configuration data, settings, and logging data that may be accessible by authorized administrators*].

6.2.2.3 FPT_PHP.1 Passive Detection of Physical Attack

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.

6.2.2.4 FPT_TST.1 TSF Testing

FPT_TST.1.1 The TSF shall run a suite of self-tests during initial start-up and at the conditions *[no other conditions]* to demonstrate the correct operation of user control functions and *[no other functions]*.

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

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

6.2.2.5 FPT_TST_EXT.1 TSF Testing

FPT_TST_EXT.1.1 The TSF shall respond to a self-test failure by providing users with a [*visual*] indication of failure and by shutdown of normal TSF functions.

7 SECURITY ASSURANCE REQUIREMENTS

The assurance requirements are summarized in Table 12.

Assurance Class	**Assurance Components**	
	Identifier	**Name**
Development (ADV)	ADV_FSP.1	Basic Functional Specification
Guidance Documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support (ALC)	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM Coverage
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_IND.1	Independent Testing - Conformance
Vulnerability Assessment (AVA)	AVA_VAN.1	Vulnerability Survey

Table 12 – Security Assurance Requirements

8 SECURITY REQUIREMENTS RATIONALE

8.1 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

Table 7 provides a mapping between the SFRs and Security Objectives.

8.2 DEPENDENCY RATIONALE

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

SFR	Dependencies	Rationale Statement
FDP_APC_EXT.1/VI	None	N/A
FDP_CDS_EXT.1	None	N/A
FDP_IPC_EXT.1	FDP_PDC_EXT.2	Included
FDP_PDC_EXT.1	None	N/A
FDP_PDC_EXT.2/VI	FDP_PDC_EXT.1	Included
FDP_PDC_EXT.3/VI(1)	FDP_PDC_EXT.1	Included
FDP_PDC_EXT.3/VI(2)	FDP_PDC_EXT.1	Included
FDP_PDC_EXT.3/VI(3)	FDP_PDC_EXT.1	Included
FDP_PDC_EXT.3/VI(4)	FDP_PDC_EXT.1	Included
FDP_RIP_EXT.1	None	N/A
FDP_SPR_EXT.1/DP	FDP_PDC_EXT.3	Included
FDP_SPR_EXT.1/DVI-D	FDP_PDC_EXT.3	Included
FDP_SPR_EXT.1/HDMI	FDP_PDC_EXT.3	Included
FDP_SWI_EXT.1	None	N/A
FDP_UDF_EXT.1/VI	FDP_APC_EXT.1	Included
FPT_FLS_EXT.1	FPT_TST.1 FPT_PHP.3	Included Included only if anti-tamper is selected in FPT_FLS_EXT.1.1
FPT_NTA_EXT.1	None	N/A

SFR	Dependencies	Rationale Statement
FPT_PHP.1	None	N/A
FPT_TST.1	None	N/A
FPT_TST_EXT.1	FPT_TST.1	Included

Table 13 – Functional Requirement Dependencies

8.3 SECURITY ASSURANCE REQUIREMENTS RATIONALE

The TOE assurance requirements for this ST consist of the requirements indicated in the [PP_PSD_V4.0].

9 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements. Unless otherwise stated, the description applies to all devices.

9.1 USER DATA PROTECTION

9.1.1 PSD Switching

The TOE supports only one connected computer.

TOE Security Functional Requirements addressed: FDP_SWI_EXT.1.

9.1.1.1 Active PSD Connections

The TOE ensures that data flows only between the connected computer and the display peripheral. No data transits the TOE when the TOE is powered off, or when the TOE is in a failure state. A failure state occurs when the TOE fails a self-test when powering on.

TOE Security Functional Requirements addressed: FDP_APC_EXT.1/VI.

9.1.1.2 Connected Computer Interfaces

The TOE is connected to the computer video port using a video cable supporting DisplayPort, HDMI or DVI-D.

There are no wireless interfaces or additional external interfaces

TOE Security Functional Requirements addressed: FDP_PDC_EXT.1.

9.1.1.3 Residual Information Protection

The Letter of Volatility is included as Annex A.

TOE Security Functional Requirements addressed: FDP_RIP_EXT.1.

9.1.2 Video Functionality

Video data flow is comprised of unidirectional Extended Display Identification Data (EDID) and video data flow path and goes from the TOE computer video interface to the TOE peripheral device display interface. Figure 3 shows a data flow during the display EDID read function.

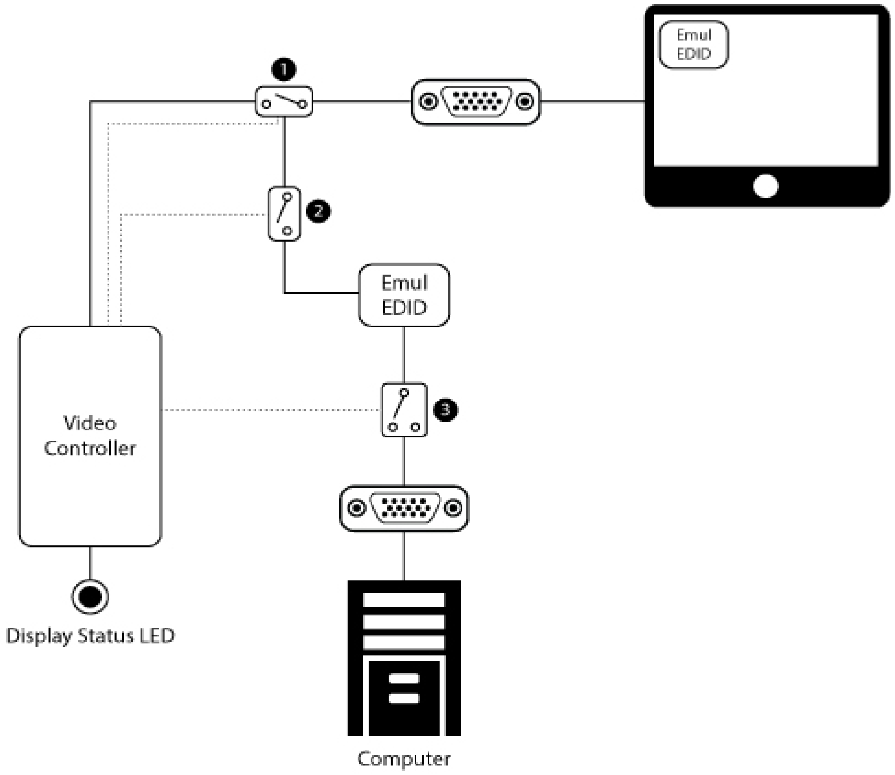

Figure 3 – Display EDID Read Function

An EDID read event only occurs when the user clicks the EDID LOCK button. 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 Inter-Integrated Circuit (I^2C) 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 normal 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 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, DVI-D and HDMI 2.0:

- For DisplayPort connections, the TOE video function filters the AUX channel by converting it to I^{2}C EDID only. DisplayPort video is converted into an HDMI video stream, and the I^{2}C 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.
    - DisplayPort is supported for video input and video output on the FV11PH-M and FV11PP-MM device.
    - DisplayPort is supported for video input on the FV11PH-MM device.
    - DisplayPort is supported for video output on the FV11HP-MM device.
- For DVI-D 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), HDMI Ethernet Channel (HEC) and MCCS are blocked. HDCP and Consumer Electronics Control (CEC) functions are not connected.
    - DVI-D is supported for video input and video output on the FV11D-M device.
- 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.
    - HDMI is supported for video input and video output on the FV11H-M, FV11PH-M, and FV11HH-MM devices.

  - HDMI is supported for video input on the FV11HP-MM device.
  - HDMI is supported for video output on the FV11PH-MM device.

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.

TOE Security Functional Requirements addressed: FDP_IPC_EXT.1, FDP_SPR_EXT.1/DP, FDP_SPR_EXT.1/DVI-D, FDP_SPR_EXT.1/HDMI.

9.1.2.1 Video Compatible Device Types

The TOE accepts any DisplayPort, DVI-D or HDMI display device at the video peripheral ports as shown in Table 2. The TOE does not support a wireless connection to a video display.

The TOE utilizes a fixed EDID file installed on the device during production and stored within non-volatile memory in the TOE. The TOE does not provide an interface to modify the fixed EDID file stored on the device. On the FV11H-M, FV11D-M, FV11PH-M Isolator models, the user can click the EDID LOCK button on the device to run an EDID capture from the display.

TOE Security Functional Requirements addressed: FDP_PDC_EXT.1, FDP_PDC_EXT.2/VI, FDP_PDC_EXT.3/VI(1), FDP_PDC_EXT.3/VI(2), FDP_PDC_EXT.3/VI(3), FDP_PDC_EXT.3/VI(4).

9.2 PROTECTION OF THE TSF

9.2.1 No Access to TOE

Connected computers do not have access to TOE firmware or memory, with the following exceptions:

- EDID data is accessible to connected computers from the TOE.

All of the TOE microcontrollers run from internal protected flash memory. Firmware cannot be updated from an external source. Firmware cannot be read or rewritten through the use of Joint Test Action Group (JTAG) tools. Firmware is executed on Static Random Access Memory (SRAM) with the appropriate protections to prevent external access and tampering of code or stacks.

TOE Security Functional Requirements addressed: FPT_NTA_EXT.1.

9.2.2 Passive Anti-tampering Functionality

The Isolator 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.

The Mini Isolator features a plastic welded chassis.

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.

9.2.3 TSF Testing

The TOE performs a self-test at initial start-up. The self-test runs independently at each microcontroller and performs a verification check 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_FLS_EXT.1, FPT_TST.1, FPT_TST_EXT.1.

10TERMINOLOGY AND ACRONYMS

10.1 TERMINOLOGY

The following terminology is used in this ST:

Term	Description
AUX	AUX refers to the auxiliary channel, particularly as it applies to the DisplayPort protocol.
VI	VI refers to the requirements for Video/Display Devices.

Table 14 – Terminology

10.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
ARC	Audio Return Channel
CC	Common Criteria
CEC	Consumer Electronics Control
DVI	Digital Visual Interface
EDID	Extended Display Identification Data
EEPROM	Electrically Erasable Programmable Read-Only Memory
HDCP	High-bandwidth Digital Content Protection
HDMI	High-Definition Multimedia Interface
HEAC	HDMI Ethernet and Audio Return Channel
HEC	HDMI Ethernet Channel
HPD	Hot-Plug Detection
HSL	High Sec Labs
I^2C	Inter-Integrated Circuit
IT	Information Technology
JTAG	Joint Test Action Group
LED	Light Emitting Diode
MCCS	Monitor Control Command Set

Acronym	Definition
PP	Protection Profile
PSD	Peripheral Sharing Device
SFR	Security Functional Requirement
SRAM	Static Random Access Memory
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
USB	Universal Serial Bus

Table 15 – Acronyms

11 REFERENCES

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation – • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017 • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017 • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004, Version 3.1 Revision 5, April 2017
[PP_PSD_V4.0]	Protection Profile for Peripheral Sharing Device, Version: 4.0, 2019-07-19
[MOD_VI_1.0]	PP-Module for Video/Display Devices, Version 1.0, 19 July 2019
[CFG_PSD-VI_V1.0]	PP-Configuration for Peripheral Sharing Device and Video/Display Devices, 19 July 2019

Table 16 – References

ANNEX A – LETTER OF VOLATILITY

The table below provides volatility information and memory types for the High Sec Labs Peripheral Sharing Devices. User data is not retained in any TOE device when the power is turned off.

Product Model	Number in each product	Function, Manufacturer and Part Number	Storage Type	Size	Power Source (if not the TOE)	Volatility	Contains User Data
Isolators: FV11H-M FV11D-M FV11PH-M FV11HH-MM FV11HP-MM FV11PH-MM FV11PP-MM	1	Video Controller: ST Microelectronics STM32F070C6T6	Embedded SRAM[1]	6KB	Connected computer	Volatile	No user data
			Embedded Flash[2]	32KB		Non-Volatile	No user data
			Embedded EEPROM	4KB		Non-Volatile	No user data
	1	EDID Emulators: ST Microelectronics M24C02-WMN6TP	EEPROM[3]	2KB		Non-Volatile	No user data

Notes:

[1] SRAM stores USB Host stack parameters and up to the last 4 key-codes. Data is erased during power off of the device. Device emulators receive power from the individual connected computers and therefore devices are powered on as long as the associated computer is powered on and connected.

[2] Flash storage is used to store firmware code. It contains no user data. Flash storage is permanently locked by fuses after initial programming to prevent rewriting. It is an integral part of the ST Microcontroller together with SRAM and EEPROM.

[3] EEPROM is used to store operational parameters, such as display Plug & Play, and contains no user data.