Assurance Activity Report for

High Sec Labs SK41D-4TR KVM Firmware Version 44404-E7E7

High Sec Labs SK41D-4TR KVM Firmware Version 44404-E7E7 Security Target, Version 1.7 September 14, 2021

Protection Profile for Peripheral Sharing Device, Version: 4.0
PP-Module for Keyboard/Mouse Devices, Version 1.0
PP-Module for Video/Display Devices, Version 1.0

AAR Version 1.3, September 14, 2021

Evaluated by:

intertek
acumen
security

2400 Research Blvd, Suite 395
Rockville, MD 20850

Prepared for:

NIAP

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

The Developer of the TOE:
High Sec Labs

The Author of the Security Target:
EWA-Canada, An Intertek Company

The TOE Evaluation was Sponsored by:
High Sec Labs

Evaluation Personnel:
Acumen Security
Kenneth Lasoski
Joshua Gola

Common Criteria Version
Common Criteria Version 3.1 Revision 5

Common Evaluation Methodology Version
CEM Version 3.1 Revision 5

Revision History

VERSION	DATE	CHANGES
1.0	7/13/2021	Initial release
1.1	8/11/2021	Updates in response to validator ECRs
1.2	9/2/2021	Updates in response to validator ECRs
1.3	9/14/2021	Updates in response to validator ECRs

Contents

`

1 TOE Overview

The High Sec Labs (HSL) SK41D-4TR Keyboard, Video, Mouse (KVM) switch allows users to share keyboard, video, and mouse peripherals between a number of connected computers. Security features ensure isolation between computers and peripherals to prevent data leakage between connected systems.

- 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
  - Digital Visual Interface (DVI)-D video is supported

- Keyboard and Mouse Security
  - The keyboard and mouse are isolated by dedicated, USB device emulation for each computer
  - One-way, peripheral-to-computer data flow is enforced through unidirectional optical
  - data diodes
  - Communication from computer-to-keyboard/mouse is blocked
  - Non-HID (Human Interface Device) data transactions are blocked

- Hardware Anti-Tampering
  - Any attempt to open the product enclosure will activate an antitampering system, making the product inoperable and indicating tampering via blinking Light Emitting Diodes (LEDs)
  - Special holographic tampering evident labels on the product’s enclosure provide a clear visual indication if the product has been opened or compromised

The High Sec Labs SK41D-4TR KVM uses multiple isolated microcontrollers (one microcontroller per connected computer) to emulate connected peripherals in order to prevent an unauthorized data flow through bit-by-bit signaling.

2 Assurance Activities Identification

The Assurance Activities contained within this document include all those defined within the Protection Profile for Peripheral Sharing Device, Version: 4.0 and the following PP modules:

- PP-Module for Keyboard/Mouse Devices, Version 1.0
- PP-Module for Video/Display Devices, Version 1.0

SFRs have been selected in accordance with PP-Configuration for Peripheral Sharing Device, Keyboard/Mouse Devices, and Video/Display Devices, 19 July 2019 and on the selections within the PP and modules.

3 Test Equivalency Justification

3.1 Architectural Description

The High Sec Labs' SK41D-4TR KVM TOE can be connected to four computers. The video input and output format is DVI-D, and a single display is connected to the KVM. The TOE uses ruggedized 32 pin connectors (MIL Spec MIL-DTL-38999) that support both DVI-D and USB 2.0 protocols. The KVM is used with a wired remote control.

In the ST, Table 4 indicates the device name/model to be tested. No other models are included in the TOE.

4 Test Bed Descriptions

4.1 Test Bed # 1

Below is a diagram of the components included in the test bed:

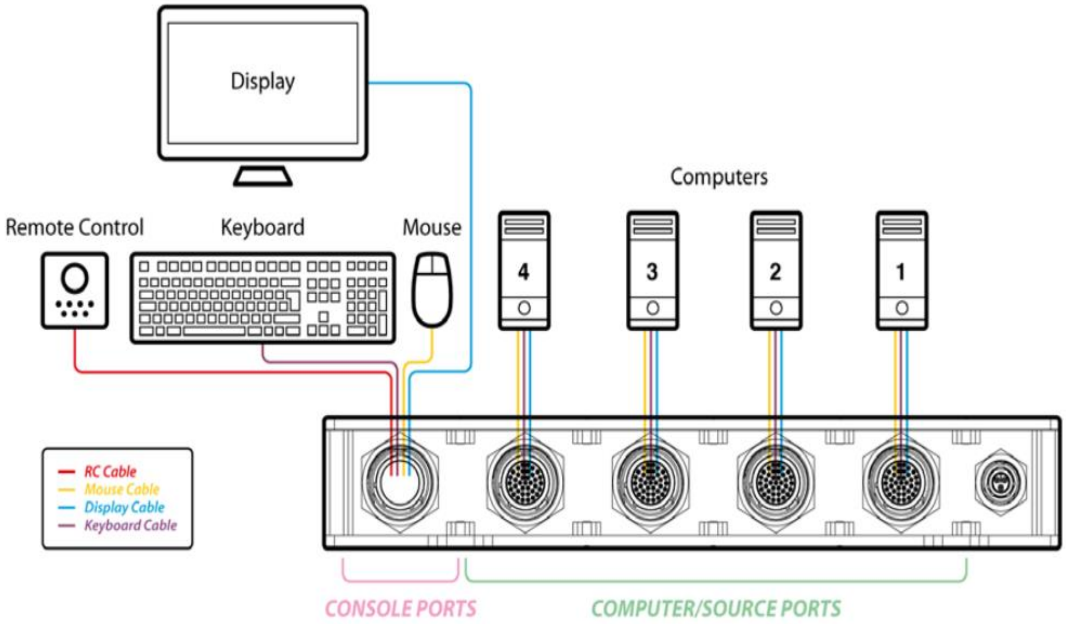


Diagram of the TOE, with how to connect cables and required equipment

4.1.1 Test Equipment

The following equipment was used in the testing of the TOE:

Test Equipment
Dell Keyboard
HP Deskjet 1112 USB Printer
Dr. Meter DC Power Supply HY3005F-3
RIGOL DG1022A Waveform Audio Signal Generator
RIGOL DG1022A Waveform Audio Signal Generator
QuantumData 882E Video Test Generator (DisplayPort)
QuantumData 980 Video Test Generator (HDMI)
TELEDYNE LECROY USB-TMS2-M01-X USB Sniffer
UNIGRAF DPA-400 DisplayPort Aux Channel Monitor
Tektronix TBS1104 Oscilloscope
Fluke 117 True RMS Digital Multimeter
Custom USB Dummy Load
Edifier R980T Multimedia Speaker
PS/2 to USB Adapter
Perixx PeriMice-201 II Optical PS/2 Mouse
MPOW BH323A 3.5mm Headset with USB Connector
Identiv SCR3310 USB UA Device with Power LED
TCL 40” LED Smart TV With Audio Return Channel (ARC)

Test Equipment
BYEASY USB 4 Port Hub
Logitech V-U-0018 USB Camera
Steelseries Rival 100 USB Gaming Mouse
Custom BADUSB
Netum USB Barcode Reader
Wireless LAN Dongle
Keweisi USB Detector
3.5mm Microphone
Dell P2319H Monitor (High Resolution Monitor #1)
Asus PA238 Monitor (High Resolution Monitor #2)
Dell Wired Keyboard KB216t
UGREEN VGA to HDMI Adapter
Dell 1907FPc Monitor (Low Resolution Monitor)
Dell Wired Mouse M-UAR DEL 7
Cable Matters VGA to DisplayPort Adapter

Cables

Cable
3.5mm Audio Splitter
Spliced HDMI Cable
Spliced 3.5mm Cable
Spliced USB Type-B Cable
Spliced DisplayPort Cable
Spliced USB Type-C Cable
Spliced USB Type-A Cable

Computers

Name and Hardware	OS	Version	Function
Computer #1 HP ProDesk 600 G4	Windows 10	10.0.19041	Test Workstation – This computer will be connected to the KVM and provide keyboard, mouse and video when needed.
Computer #2 HP ProDesk 600 G4	Windows 10	10.0.19041	Test Workstation – This computer will be connected to the KVM and provide keyboard, mouse and video when needed.
Lab PC Dell Vostro Desktop	Windows 10	10.0.19041	Lab Workstation – This computer will be external to the TOE and be used in

Name and Hardware	OS	Version	Function
			measuring the KVM's data output.

Software

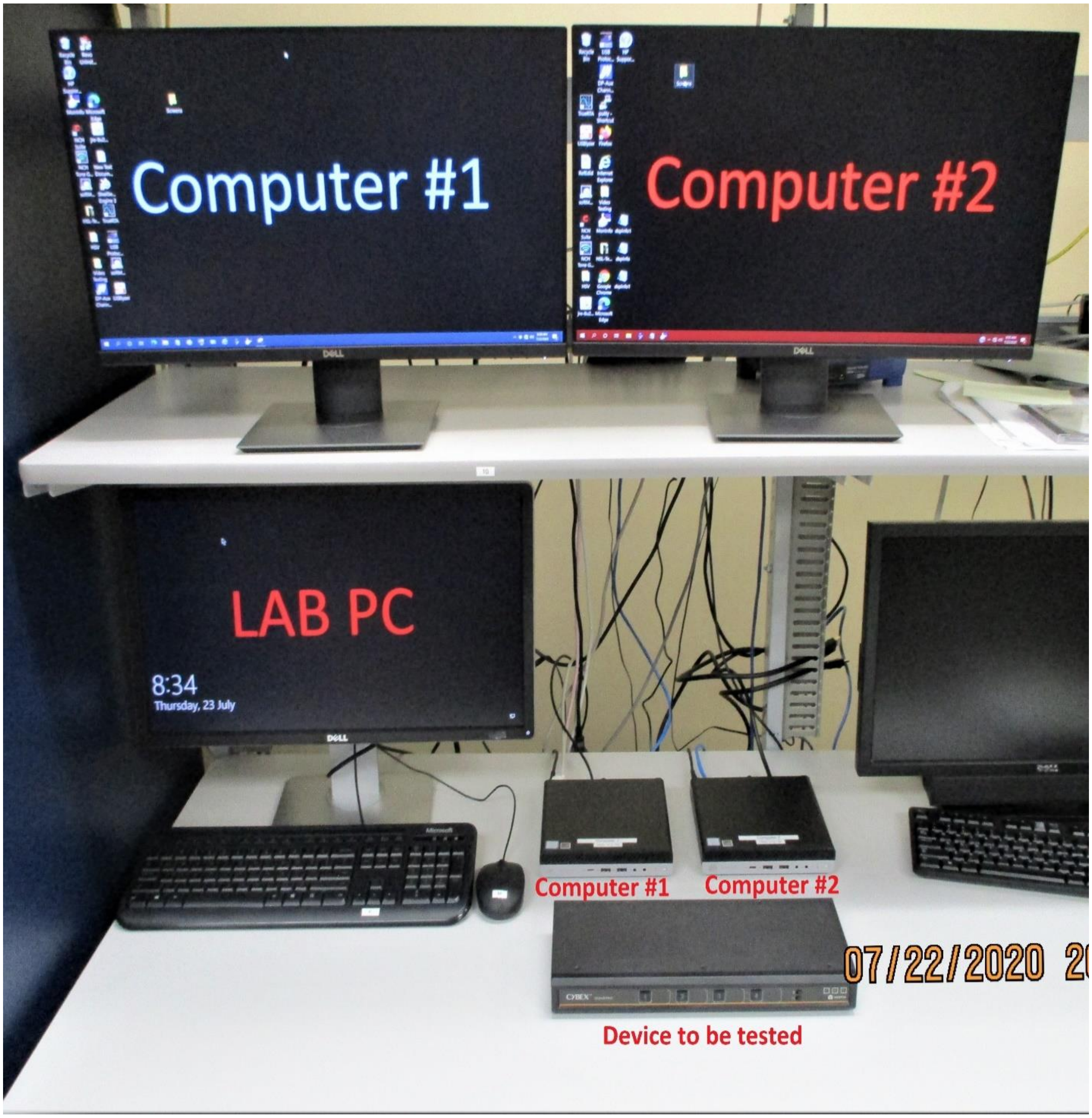
Name	Version
DisplayPort Aux Channel Monitor	2.0
Monitor Asset Manager	2.91.0.1043
SoftMCCS (Monitor Control Console Software)	2.5.0.1087
TrueRTA (Real Time Audio Spectrum Analyzer)	3.5.6
Teledyne Lecroy USB Protocol Suite™	7.60
USBlyzer (USB Analyzer Software)	2.1
Microsoft Device Manager	10.0.19041
Microsoft Notepad	10.0.19041

4.1.2 Test Time & Location

All testing was carried out on-site in Ottawa, Ontario by Acumen Security personnel. Initial receipt and inspection of the TOE occurred in March 2020. The general timeline for testing spanned from March 2020 to August 2021, with periods of inactivity in-between. Much of the testing for the TOE was achieved during the October and November 2020 timeframes as well as August of 2021. For the entire duration of the testing, the TOE was in a physically protected, access controlled, designated test lab with no unattended entry/exit ways. Only individuals authorized by High Sec Labs and Acumen Security, Inc. were allowed access to the rooms where the devices were kept stored. At the start of each day, the test bed was verified to ensure that it was not compromised. This was achieved by inspecting the tamper seals, enclosures, and cabling for signs of tampering. All evaluation documentation was always kept with the evaluator. In addition, all the necessary precautions and safety protocols were followed.

4.1.3 Test Environment

The following test environment is in use throughout the testing process. Each device will be tested using one Lab workstation, and two test workstations. This will ensure throughout the testing process that at least two ports per TOE can be tested simultaneously. As the TOE has four ports, the evaluator has tested two computer ports at a time, then moved the test computers over to two other ports and repeated this process until all switch port combinations have been tested. The evaluator confirms that all computer ports on the switch (#1, #2, #3 and #4) were all tested. No activity was observed on any non-connected PC.



The photograph above shows the environment where all the devices will be tested. The evaluator used two test computers (Computer #1 and #2) as well as a Lab PC. The device being tested was connected to one or both computers, as well as the lab PC to conduct testing.

4.1.4 Configuration Information

The following devices were tested:

Product: SK41D-4TR

- Name: HighSecLabs™ 4 Ports Secure Ruggedized DVI-D KVM Switch
- Number of Ports: 4 Ports

- Display Type: DVI-D

Product: WR40-4R

- Name: HighSecLabs™ WR40-4R Remote Control
- Number of Buttons: 1 Button
- Connection Type: Ruggedized 32 Pin

5 Detailed Test Cases (TSS, Isolation Document, and Guidance Activities)

The following is a list of the documents consulted:

- High Sec Labs SK41D-4TR KVM Firmware Version 44404-E7E7 Peripheral Sharing Devices Security Target, Version 1.7, September 14, 2021
- High Sec Labs SK41D-4TR KVM Firmware Version 44404-E7E7 Peripheral Sharing Devices Isolation Document, Version 0.3, October 7, 2020
- High Sec Labs SK41D-4TR KVM Firmware Version 44404-E7E7 Common Criteria Guidance Supplement, Version 0.5, September 14, 2021
- HSL Quick Installation Guide 4 Ports Secure Ruggedized DVI-D KVM Switch, HDC23220 Rev 1.2
- HSL Administrator Guide, HDC19968, Rev. C

5.1 TSS, Isolation Document, and Guidance Activities (Auditing)

5.1.1 FAU_GEN.1

5.1.1.1 FAU_GEN.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.1.2 FAU_GEN.1 TSS 1

Objective	The evaluator shall verify that the TSS describes the audit functionality including which events are audited, what information is saved in each record type, how the records are stored, the conditions in which audit records are overwritten, and the means by which the audit records may be read. Although the TOE may provide an interface for an administrator to view the audit records, this is not a requirement.
Evaluator Findings	The evaluator examined Section 7.1 titled 'Security Audit' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that the 'Security Audit' section of the TSS describes in detail the audit functions, including both the RAM logs and the one-time programming (OTP) logs. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.1.3 FAU_GEN.1 Guidance 1

Objective	The evaluator shall verify that the operational guidance provides instructions on how the audit logs can be viewed as well as any information needed to interpret the audit logs.
Evaluator Findings	The evaluator examined [ADMIN] to determine the verdict of this evaluation activity. "This Administrator Guide provides all the details you'll need to receive log and audit data from your new product." In addition, in the 'Administrator Configuration' section, it states "The product enables authorized administrators to download event log files and audit

	the product history as well as have access to advanced settings. This function is available only to authenticated administrators." Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.2 FDP_APC_EXT.1/KM

5.1.2.1 FDP_APC_EXT.1/KM Isolation Document 1

Objective	The evaluator shall examine the Isolation Document and verify it describes how the TOE ensures that no data or electrical signals flow between connected computers in both cases (powered on, powered off).
Evaluator Findings	The Isolation document , Section 2 'Design Description" states "This section also describes the operation of each of the main components in the data paths, including how the component works, how isolation is kept, and how power source or power loading may affect isolation between these data paths." Section 2.3 'MAIN COMPONENTS IN THE DATA PATH' has this statement "There is no means for the power source to affect isolation. Isolation is maintained when the power is off." Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.2.2 FDP_APC_EXT.1/KM TSS 1

Objective	There are no TSS EAs for this component beyond what the PSD PP requires.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.2.3 FDP_APC_EXT.1/KM Guidance 1

Objective	There are no guidance EAs for this component beyond what the PSD PP requires.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.3 FDP_APC_EXT.1/VI

5.1.3.1 FDP_APC_EXT.1/VI Isolation Document 1

Objective	The evaluator shall examine the Isolation Document and verify it describes how the TOE ensures that no data or electrical signals flow between connected computers in both cases (powered on, powered off).

Evaluator Findings	The evaluator examined the Isolation Document. The Isolation Document includes a figure, (Figure 1) that illustrate the possible data flows. There follows a table, Table 1 Data Flow Description, that provides an explanation of the data flows. Figures 2, 3, 4 and 5 which characterize the data flows for various TOE configurations (i.e. combiner, switches, etc.), are part of the isolation justification and indicate the methods used to maintain the data separation. The 'Main Components in the Data Path' section provides an explanation of all data flow isolation. The 'Power Isolation' section discusses power isolation. The 'Isolation Means Justification' describes the isolation enforcement policy for various aspects of the TOE. Figure 8 shows the physical characteristics. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.3.2 FDP_APC_EXT.1/VI TSS 1

Objective	There are no EAs for this component beyond what the PSD PP requires.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.3.3 FDP_APC_EXT.1/VI Guidance 1

Objective	There are no guidance EAs for this component beyond what the PSD PP requires.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.4 FDP_CDS_EXT.1

5.1.4.1 FDP_CDS_EXT.1 Isolation Document

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.4.2 FDP_CDS_EXT.1 TSS

Objective	The evaluator shall examine the TSS and verify that it describes how many connected displays may be supported at a time.
Evaluator Findings	The evaluator examined the ST. The 'Evaluated Configuration' section indicates that one display is supported. The 'Video Switching Functionality' section of the TSS indicates that the TOE supports a single display. This information is consistent with the claims in FDP_CDS_EXT.1(1). Based on these findings, this evaluation activity is considered satisfied.

Verdict	Pass

5.1.4.3 FDP_CDS_EXT.1 Guidance

Objective	The evaluator shall examine the operational user guidance and verify that it describes how many displays are supported by the TOE.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The CC Guidance Supplement section titled 'Number of Supported Displays' indicates that the TOE supports a single display. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.5 FDP_FIL_EXT.1/KM

5.1.5.1 FDP_FIL_EXT.1/KM Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this SFR.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.5.2 FDP_FIL_EXT.1/KM TSS 1

Objective	The evaluator shall examine the TSS and verify that it describes whether the PSD has configurable or fixed device filtering. [Conditional - If "configurable" is selected in FDP_FIL_EXT.1.1/KM, then:] the evaluator shall examine the TSS and verify that it describes the process of configuring the TOE for whitelisting and blacklisting KM peripheral devices, including information on how this function is restricted to administrators. The evaluator shall verify that the TSS does not allow TOE device filtering configurations that permit unauthorized devices on KM interfaces.
Evaluator Findings	The evaluator examined Section 7.2.2.3 titled 'Keyboard and Mouse Compatible Device Types' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that the selection is fixed. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.5.3 FDP_FIL_EXT.1/KM Guidance 1

Objective	[Conditional - If "configurable" is selected in FDP_FIL_EXT.1.1/KM, then:] the evaluator shall examine the guidance documentation and verify that it describes the process of configuring the TOE for whitelisting and blacklisting KM peripheral devices and the administrative privileges required to do this.

Evaluator Findings	The evaluator examined the ST to determine that ‘Configurable’ has not been selected. Therefore, this evaluation activity is not applicable.
Verdict	Not Applicable/Pass

5.1.6 FDP_PDC_EXT.1

5.1.6.1 FDP_PDC_EXT.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.6.2 FDP_PDC_EXT.1 TSS 1

Objective	The evaluator shall verify that the TSS describes the interfaces between the PSD and computers and the PSD and peripherals and ensure that the TOE does not contain wireless connections for these interfaces.
Evaluator Findings	The evaluator confirmed that the ST indicates that there are no wireless peripherals allowed in this configuration. The ‘Keyboard and Mouse Compatible Device Types’ section indicates that the TOE does not support a wireless connection to a mouse, keyboard or USB hub. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.6.3 FDP_PDC_EXT.1 TSS 2

Objective	The evaluator shall verify that the list of peripheral devices and interfaces supported by the TOE does not include any prohibited peripheral devices or interface protocols specified in Appendix E.
Evaluator Findings	The evaluator examined the section titled ‘User Data Protection’ in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section describes the allowed peripheral devices and protocols in ‘Keyboard and Mouse Compatible Device Types’ and ‘Video Compatible Device Types’. The TOE does not allow non-compliant devices or interface protocols specified in Appendix E. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.6.4 FDP_PDC_EXT.1 TSS 3

Objective	The evaluator shall verify that the list of peripheral devices and interfaces supported by the TOE does not include any prohibited peripheral devices or interface protocols specified in Appendix E.

Evaluator Findings	The evaluator examined the section titled ‘Keyboard and Mouse Compatible Device Types’ and the ‘Video Compatible Device Types’ in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section describes the allowed peripheral devices and protocols in Compatible Device. The TOE does not allow non-compliant devices. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.6.5 FDP_PDC_EXT.1 TSS 4

Objective	The evaluator shall verify that the TSS describes all external physical interfaces implemented by the TOE, and that there are no external interfaces that are not claimed by the TSF.
Evaluator Findings	The evaluator examined the section titled ‘User Data Protection’ in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section describes all physical interfaces to the peripheral devices in ‘Keyboard and Mouse Compatible Device Types’ and ‘Video Compatible Device Types’. The TOE is compliant to the PSD PP Appendix E and does not describe any unclaimed external interfaces. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.6.6 FDP_PDC_EXT.1 Guidance 1

Objective	The evaluator shall verify that the operational user guidance provides clear direction for the connection of computers and peripheral devices to the TOE.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The evaluator examined the Quick Installation Guide to confirm that it provides clear instructions describing how to connect peripheral devices to the TOE. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.6.7 FDP_PDC_EXT.1 Guidance 2

Objective	The evaluator shall verify that the operational user guidance provides clear direction for the usage and connection of TOE interfaces, including general information for computer, power, and peripheral devices.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The evaluator examined the user guidance documentation. The product guidance documents provide clear instructions on how to connect peripheral devices, power and computers. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.6.8 FDP_PDC_EXT.1 Guidance 3

Objective	The evaluator shall determine if interfaces that receive or transmit data to or from the TOE present a risk that these interfaces could be misused to import or export user data.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The product guidance documents provide connectivity details. The CC Guidance Supplement provides additional instructions on usage, including environmental requirements required to alleviate the risk of data loss. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.6.9 FDP_PDC_EXT.1 Guidance 4

Objective	The evaluator shall verify that the operational user guidance describes the visual or auditory indications provided to a user when the TOE rejects the connection of a device.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The product guides discuss the acceptance/rejection of a device. When no device is detected, the LED is off. When the TOE rejects a device, an LED on the port blinks green. When the TOE accepts a device, the LED is solid green. There are no audible indications. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.6.10 FDP_PDC_EXT.1 Guidance 1-KM, VI

Objective	The evaluator shall verify that the operational user guidance describes devices authorized for use with the TOE in accordance with the authorized peripheral device connections.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The product guidance documents indicate the peripheral device type interfaces of the TOE devices. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.7 FDP_PDC_EXT.2/KM

5.1.7.1 FDP_PDC_EXT.2/KM Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this SFR.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.7.2 FDP_PDC_EXT.2/KM TSS 1

Objective	TSS evaluation activities for this SFR are performed under FDP_PDC_EXT.1 above.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.7.3 FDP_PDC_EXT.2/KM Guidance 1

Objective	Guidance evaluation activities for this SFR are performed under FDP_PDC_EXT.1 above.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.8 FDP_PDC_EXT.2/VI

5.1.8.1 FDP_PDC_EXT.2/VI Isolation Document 1

Objective	There are no Isolation Document EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.8.2 FDP_PDC_EXT.2/VI TSS 1

Objective	TSS evaluation activities for this SFR are performed under FDP_PDC_EXT.1 above.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.8.3 FDP_PDC_EXT.2/VI Guidance 1

Objective	Guidance evaluation activities for this SFR are performed under FDP_PDC_EXT.1 above.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.9 FDP_PDC_EXT.3/KM

5.1.9.1 FDP_PDC_EXT.3/KM Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this SFR.
Evaluator Findings	Not Applicable

Verdict	Not Applicable/Pass

5.1.9.2 FDP_PDC_EXT.3/KM TSS 1

Objective	The evaluator shall examine the TSS and verify it describes which types of peripheral devices that the PSD supports.
Evaluator Findings	The evaluator examined the section titled 'User Data Protection' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that the TSS describes which peripherals are used in the 'Keyboard and Mouse Compatible Device Types' and 'Video Compatible Device Types' sections. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.9.3 FDP_PDC_EXT.3/KM TSS 2

Objective	The evaluator shall examine the TSS to verify that keyboard or mouse device functions are emulated from the TOE to the connected computer.
Evaluator Findings	The evaluator examined the section titled 'Keyboard and Mouse Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that 'Keyboard and Mouse Switching Functionality' section indicates that the keyboard and mouse function are emulated by the TOE. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.9.4 FDP_PDC_EXT.3/KM Guidance 1

Objective	There are no guidance EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.10 FDP_PDC_EXT.3/VI

5.1.10.1 FDP_PDC_EXT.3/VI Isolation Document 1

Objective	There are no Isolation Document EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.10.2 FDP_PDC_EXT.3/VI TSS 1

Objective	TSS evaluation activities for this SFR are performed under FDP_PDC_EXT.1 above.

Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.10.3 FDP_PDC_EXT.3/VI Guidance 1

Objective	Guidance evaluation activities for this SFR are performed under FDP_PDC_EXT.1 above.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.11 FDP_RDR_EXT.1

5.1.11.1 FDP_RDR_EXT.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.11.2 FDP_RDR_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to verify that it describes how the TSF identifies and rejects a device that attempts to enumerate again as a different device.
Evaluator Findings	The evaluator examined the section titled ‘Keyboard and Mouse Switching Functionality’ in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section discusses Keyboard and Mouse Enumeration and indicates that 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. This section also states that 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. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.11.3 FDP_RDR_EXT.1 Guidance 1

Objective	There are no guidance EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.12 FDP_RIP_EXT.1

5.1.12.1 FDP_RIP_EXT.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.12.2 FDP_RIP_EXT.1 TSS 1

Objective	The evaluator shall verify that the TSS includes a Letter of Volatility that provides the following information: • Which TOE components have non-volatile memory, the non-volatile memory technology, manufacturer/part number, and memory sizes; • Any data and data types that the TOE may store on each one of these components; • Whether or not each one of these parts is used to store user data and how this data may remain in the TOE after power down; and • Whether the specific component may be independently powered by something other than the TOE (e.g., by a connected computer). Note that user configuration and TOE settings are not considered user data for purposes of this requirement.
Evaluator Findings	The evaluator examined Annex A titled 'Letter of Volatility' in the Security Target to determine the verdict of this evaluation activity. The Letter of Volatility is provided as Annex A in the Security Target. The evaluator confirmed that this section lists each component, its function, manufacture and part number, the type of data stored and whether the storage is volatile, or non-volatile. It also indicates the power source. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.12.3 FDP_RIP_EXT.1 TSS 2

Objective	The evaluator shall verify that the Letter of Volatility provides assurance that user data is not stored in TOE non-volatile memory or storage.
Evaluator Findings	The evaluator examined the section titled 'Letter of Volatility' in the Security Target to determine the verdict of this evaluation activity. The Letter of Volatility is provided as Annex A in the Security Target. The evaluator confirmed that this section indicates that user data is not stored in non-volatile memory or storage. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.12.4 FDP_RIP_EXT.1 Guidance 1

Objective	There are no guidance Evaluation Activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.13 FDP_RIP.1/KM

5.1.13.1 FDP_RIP.1/KM Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.13.2 FDP_RIP.1/KM TSS 1

Objective	The evaluator shall verify that the TSS indicates whether or not the TOE has user data buffers.
Evaluator Findings	Section 7.2.2.1 'Keyboard and Mouse Enumeration', discusses the Serial Random Access Memory (SRAM). 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 KVM, and when the user switches channels. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.13.3 FDP_RIP.1/KM TSS 2

Objective	The evaluator shall verify that the TSS describes how all keyboard data stored in volatile memory is deleted upon switching computers.
Evaluator Findings	The evaluator examined the section titled 'Keyboard and Mouse Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that data is erased during power off of the KVM, and when the user switches channels. When the TOE switches from one computer to another, the system controller ensures that the keyboard and mouse stacks are deleted, and that any data received from the keyboard in the first 100 milliseconds following switching is deleted. This is done to ensure that any data buffered in the keyboard microcontroller is not passed to the newly selected computer. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.13.4 FDP_RIP.1/KM Guidance 1

Objective	There are no guidance EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.14 FDP_RIP_EXT.2

5.1.14.1 FDP_RIP_EXT.2 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.14.2 FDP_RIP_EXT.2 TSS 1

Objective	The evaluator shall verify that the TSS describes the TOE's reaction to memory purge or restore factory defaults.
Evaluator Findings	The evaluator examined the section titled 'Residual Information Protection' in the Security Target to determine the verdict of this evaluation activity. When the Reset to Factory Default command is issued, the following actions take place: • All peripheral devices are logically disconnected from the selected computer • The front panel LEDs blink together • The TOE resets, purging the appropriate data • The TOE performs a normal power up and self-test sequence When the device completes the reboot, the peripherals are connected to channel #1 and all default settings are restored. The data in the critical logs, and the primary administrator username and password data are maintained in the OTP Memory of the System Controller. All other data is purged. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.14.3 FDP_RIP_EXT.2 TSS 2

Objective	The evaluator shall verify that the Letter of Volatility included in the TSS describes the effect that the TOE Restore Factory Default function has on each component listed in the Letter of Volatility.
Evaluator Findings	The evaluator examined the section titled 'Letter of Volatility' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that the 'Letter of Volatility' indicates the effect of the restore to factory default function on each component. Based on these findings, this evaluation activity is considered satisfied.

Verdict	Pass

5.1.14.4 FDP_RIP_EXT.2 Guidance 1

Objective	The evaluator shall check that the operational user guidance provides a method to purge TOE memory or to restore factory default settings.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'Selected Channel at Startup' section of the CC Guidance Supplement states that Channel 1 is selected by default after a factory reset. The [ADMIN] has instructions on how to reset the TOE to factory defaults in the 'Warnings and Precautions" section. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.15 FDP_SPR_EXT.1/DVI-D

5.1.15.1 FDP_SPR_EXT.1/DVI-D TSS

Objective	The evaluator shall examine the TSS and verify that it describes that the various sub-protocols are allowed or blocked by the TOE as described by the SFR.
Evaluator Findings	Section 7.2.1.2 of the TSS describes the sub-protocols used by the TOE. All others are blocked.
Verdict	Pass

5.1.15.2 FDP_SPR_EXT.1/DVI-D Isolation Document 1

Objective	There are no Isolation Document EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.16 FDP_SWI_EXT.1

5.1.16.1 FDP_SWI_EXT.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.16.2 FDP_SWI_EXT.1 TSS 1

Objective	If the ST includes the selection the "TOE supports only one connected computer", the evaluator shall verify that the TSS indicates that the TOE supports only one connected computer.
Evaluator Findings	The evaluator examined FDP_SWI_EXT.1 in the 'Security Functional Requirements' section of the Security Target. The selection 'switching can be initiated only through express user action' has been made. Since 'TOE supports only one connected computer' is not selected, this evaluation activity is considered not applicable.
Verdict	Not Applicable/Pass

5.1.16.3 FDP_SWI_EXT.1 TSS 2

Objective	If the ST includes the selection "switching can be initiated only through express user action", the evaluator shall verify that the TSS describes the TOE supported switching mechanisms and that those mechanisms can be initiated only through express user action.
Evaluator Findings	The evaluator examined the section titled 'System Controller', Section 7.2.1, of the Security Target to determine the verdict of this evaluation activity. The TSS has been written for multiple connected computers and explains how the user is able to conduct the switching. The System Controller section describes the switching mechanism. All devices may be switched using the front panel buttons. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.16.4 FDP_SWI_EXT.1 Guidance 1

Objective	If the ST includes the selection "switching can be initiated only through express user action", the evaluator shall verify that the operational user guidance describes the TOE supported switching mechanisms.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The switching mechanisms are described in the Quick Install Guide [23220]. This guide includes instructions on how the user performs switching. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.17 FDP_SWI_EXT.2

5.1.17.1 FDP_SWI_EXT.2 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.17.2 FDP_SWI_EXT.2 TSS 1

Objective	The evaluator shall verify that the TSS describes the TOE supported switching mechanisms. The evaluator shall verify that the TSS does not include automatic port scanning, control through a connected computer, and control through keyboard shortcuts as TOE supported switching mechanisms. The evaluator shall verify that the described switching mechanisms can be initiated only through express user action according to the selections.
Evaluator Findings	The evaluator examined the section titled 'System Controller' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that all devices may be switched using the front panel buttons or wired remote control device. Switching can only be initiated through express user action. The TSS does not include automatic port scanning, control through a connected computer, and control through keyboard shortcuts as TOE supported switching mechanisms. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.17.3 FDP_SWI_EXT.2 Guidance 1

Objective	The evaluator shall verify that the operational user guidance describes the TOE supported switching mechanisms. The evaluator shall verify that the operational user guidance does not include automatic port scanning, control through a connected computer, and control through keyboard shortcuts as TOE supported switching mechanisms.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The switching mechanisms are described in the Quick Install Guide [23220]. The guide includes instructions on how the user performs switching and does not include automatic port scanning, control through a connected computer, and control through keyboard shortcuts. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.18 FDP_SWI_EXT.3

5.1.18.1 FDP_SWI_EXT.3 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.18.2 FDP_SWI_EXT.3 TSS 1

Objective	The evaluator shall verify that the TSS does not indicate that keyboard and mouse devices may be switched independently to different connected computers.
Evaluator Findings	The evaluator examined the section titled 'Keyboard and Mouse Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator

	confirmed that this section discusses keyboard and mouse switching. The 'TOE Access' section indicates that the TOE user switches between computers by pressing the corresponding front panel button on the device. The TSS states "Once a channel is selected, the combined mouse and keyboard data stream is passed through an optical data diode and routed to the specific host channel device emulator. The optical data diode is an opto-coupler designed to physically prevent reverse data flow. The keyboard and mouse can only be switched together." Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.18.3 FDP_SWI_EXT.3 Guidance 1

Objective	The evaluator shall verify that the guidance does not describe how to switch the keyboard and mouse devices independently to different connected computers.
Evaluator Findings	The keyboard and mouse are switched together – never independently. The Administrator Guide and Quick Installation Guide documents were checked. The evaluator verified that they did not have any instructions regarding switching the keyboard and mouse separately.
Verdict	Pass

5.1.19 FDP_UDF_EXT.1/KM

5.1.19.1 FDP_UDF_EXT.1/KM Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.19.2 FDP_UDF_EXT.1/KM TSS 1

Objective	The evaluator shall examine the TSS to verify that it describes if and how keyboard Caps Lock, Num Lock, and Scroll Lock indications are displayed by the TOE and to verify that keyboard internal LEDs are not changed by a connected computer.
Evaluator Findings	The evaluator examined the section titled 'Keyboard and Mouse Switching Functionality' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section explains how the flows to the keyboard/mouse are unidirectional. It states that 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. It also indicates that 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. Based on these findings, this evaluation activity is considered satisfied.

Verdict	Pass

5.1.19.3 FDP_UDF_EXT.1/KM TSS 2

Objective	The evaluator shall examine the TSS to verify that keyboard and mouse functions are unidirectional from the TOE keyboard/mouse peripheral interface to the TOE keyboard/mouse computer interface.
Evaluator Findings	The evaluator examined the section titled ‘Keyboard and Mouse Switching Functionality’ in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section explains how the flows to the keyboard/mouse are unidirectional. It states that 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. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.1.19.4 FDP_UDF_EXT.1/KM Guidance 1

Objective	There are no guidance EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.20 FDP_UDF_EXT.1/VI

5.1.20.1 FDP_UDF_EXT.1/VI Isolation Document 1

Objective	There are no Isolation Document EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.20.2 FDP_UDF_EXT.1/VI TSS 1

Objective	There are no TSS EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.1.20.3 FDP_UDF_EXT.1/VI Guidance 1

Objective	There are no guidance EAs for this component.

Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.2 TSS, Isolation Document, and Guidance Activities (Identification and Authentication)

5.2.1 FIA_UAU.2

This SFR is evaluated by the Evaluation Activities in FMT_MOF.1 below.

5.2.2 FIA_UID.2

This SFR is evaluated by the Evaluation Activities in FMT_MOF.1 below.

5.3 TSS, Isolation Document, and Guidance Activities (Security Management)

5.3.1 FMT_MOF.1

5.3.1.1 FMT_MOF.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.3.1.2 FMT_MOF.1 TSS 1

Objective	The evaluator shall verify that the TSS describes the mechanism for preventing non-administrators from accessing the administrative functions stated above.
Evaluator Findings	The evaluator examined the section titled 'Identification and Authentication and Security Management' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section states that there is a single administrator role. In order to access administrative functions, the user must have an administrator username and password. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.3.1.3 FMT_MOF.1 TSS 2

Objective	If the TSF provides multiple administrative roles, the evaluator shall verify that the authorized behavior for each separate administrative role is described.
Evaluator Findings	The evaluator examined the section titled 'Identification and Authentication and Security Management' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section states that there is a single administrator role. An account with this role may be used to perform the following administrative tasks: • Manage administrator accounts (change password, create administrator account) • Reset to factory defaults – note that this does not reset the username and password of the primary administrator, and does not reset the critical logs

	Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.3.1.4 FMT_MOF.1 TSS 3

Objective	The evaluator shall check the TSS to verify that it describes at least the following: a) Administrator name limitations and syntax requirements; b) Administrator password limitations and syntax requirements; c) Restoring lost name or password; d) Initial setting of administrator credentials; e) Logon success, fail limitations, and logging; and f) All functions identified in the above assignment.
Evaluator Findings	The evaluator examined the section titled ‘Identification and Authentication and Security Management’ in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section describes the administrator account username and password limitations. For these accounts, usernames must be between 8 and 11 characters in length, and may be made up of uppercase and lowercase letters. The primary administrator has a default password which is changed on first use. This account does not revert to default but maintains the administrator’s account when an RFD is performed. The administrator’s password must be between 8 and 15 characters in length and may contain uppercase letters, lowercase letters, numbers or any of the following special characters: ‘!’, ‘@’, ‘#’, ‘$’, ‘%’, ‘^’, ‘&’, ‘*’, ‘(’, ‘)’, ‘-’, or ‘_’. The password must contain at least one uppercase letter, one lowercase letter, one number and one special character. Lost passwords are irrecoverable. The user is locked out after three failed login attempts. The user may cycle the device power and try again. All password related events are logged. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.3.1.5 FMT_MOF.1 Guidance 1

Objective	The evaluator shall check the user and administrative guidance to verify that the administrative functions described above are only available to identified administrators. If the TSF provides multiple administrative roles, the evaluator shall verify that the authorized behavior for each separate administrative role is described.
Evaluator Findings	The evaluator examined the administrator guidance [Admin] to determine the verdict of this evaluation activity. All of the available administrative functions are described in the Section ***Administrator Configuration***. This manual is intended only for use by the administrator. A user must be in possession of an administrative username and password in order to access the functionality described in this guide. Only one administrative role is supported.

	Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.3.2 FMT_SMF.1

5.3.2.1 FMT_SMF.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.3.2.2 FMT_SMF.1 TSS 1

Objective	The evaluator shall check to ensure the TSS describes the management functions available to the administrators and user TOE configurations and how they are used by the TOE.
Evaluator Findings	The evaluator examined the section titled 'Identification and Authentication and Security Management' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section states that there is a single administrator role. An account with this role may be used to perform the following administrative tasks: • Manage administrator accounts (change password, create administrator account) • Reset to factory defaults – note that this does not reset the username and password of the primary administrator, and does not reset the critical logs Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.3.2.3 FMT_SMF.1 Guidance 1

Objective	The evaluator shall check that every management function mandated in the ST for this requirement is described in the operational user guidance and that the description contains the information required to perform the management duties associated with each management function.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The Administrator Guide contains instructions on how to perform administrative functions. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.3.3 FMT_SMR.1

Refer to the Evaluation Activities of FMT_MOF.1.1 above.

5.4 TSS, Isolation Document, and Guidance Activities (Protection of the TSF)

5.4.1 FPT_FLS_EXT.1

Not Applicable. This SFR is evaluated in conjunction with FPT_TST.1.

5.4.2 FPT_NTA_EXT.1

5.4.2.1 FPT_NTA_EXT.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.4.2.2 FPT_NTA_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure that the TSS documents that connected computers and peripherals do not have access to TOE software, firmware, and TOE memory, except as described above.
Evaluator Findings	The evaluator examined the section titled ‘No Access to TOE’ in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that firmware is executed on SRAM with the appropriate protections to prevent external access and tampering of code or stacks. Firmware cannot be read or rewritten using JTAG tools. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.4.2.3 FPT_NTA_EXT.1 Guidance 1

Objective	The evaluator shall check the operational user guidance to ensure any configurations required to comply with this SFR are defined.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The ‘Secure Operation’ section 4 of the CC Guidance Supplement provides a description of the firmware and its accessibility. No additional configuration is required to comply with this SFR. The Quick Install Guide includes a warning that there is active tamper detection in the device and that tamper evident seals are used on the device. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.4.3 FPT_PHP.1

5.4.3.1 FPT_PHP.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.4.3.2 FPT_PHP.1 TSS 1

Objective	The evaluator shall verify that the TSS indicates that the TOE provides unambiguous detection of physical tampering of the TOE enclosure and TOE remote controller (if applicable). The evaluator shall verify that the TSS provides information that describes how the TOE indicates that it has been tampered with.
Evaluator Findings	The evaluator examined the section titled 'Passive Detection of Physical Tampering' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that the tamper evident seals are described in this section. If a seal is removed, the word VOID appears to indicate the TOE has been tampered with. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.4.3.3 FPT_PHP.1 Guidance 1

Objective	The evaluator shall verify that the operational user guidance describes the mechanism by which the TOE provides unambiguous detection of physical tampering and provides the user with instructions for verifying that the TOE has not been tampered with.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The product guidance documents for the KVM switches direct users to contact Technical Support if the enclosure appears to have been tampered with. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.4.4 FPT_PHP.3

5.4.4.1 FPT_PHP.3 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.4.4.2 FPT_PHP.3 TSS 1

Objective	The evaluator shall verify that the TSS describes the TOE's reaction to opening the device enclosure or damaging/exhausting the anti-tampering battery associated with the enclosure.
Evaluator Findings	The evaluator examined the section titled 'Resistance to Physical Attack' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section discusses the TOE's response to a tamper event. If the enclosure is opened, the anti-tamper circuitry causes a fuse on the system controller to melt and renders the TOE inoperable. Additionally, if the self-test detects that the battery is depleted or failing, the anti-tampering function will be triggered. Based on these findings, this evaluation activity is considered satisfied. The same applies to the remote control device. When the anti-

	tampering mechanism on the remote control is triggered, the device becomes permanently disabled.
Verdict	Pass

5.4.4.3 FPT_PHP.3 Guidance 1

Objective	The evaluator shall examine the operational user guidance and verify that the guidance provides users with information on how to recognize a device where the anti-tampering functionality has been activated.
Evaluator Findings	The evaluator examined the guidance document to verify it contains a warning that discusses the anti-tamper circuitry. The port LEDs flash sequentially after a tamper event has occurred. Users are instructed to contact Technical Support when the tamper event occurs. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.4.4.4 FPT_PHP.3 Guidance 2

Objective	The evaluator shall verify that the operational user guidance warns the user of the actions that will cause the anti-tampering functionality to disable the device.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The Quick Install guide contains a warning that discusses the anti-tamper circuitry. Users are instructed that if the enclosure appears to have been tampered with, or if all the port LEDs flash sequentially, they are to contact Technical Support. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.4.5 FPT_STM.1

5.4.5.1 FPT_STM.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.4.5.2 FPT_STM.1 TSS 1

Objective	The evaluator shall check to ensure the TSS describes how the TOE provides reliable timestamps.
Evaluator Findings	The evaluator examined the section titled ‘Reliable Timestamps’ in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section states that the devices have a real-time clock powered by a battery and the time is set during

	production. This section also provides appropriate warnings to the administrator regarding the time zone setting. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.4.5.3 FPT_STM.1 Guidance 1

Objective	The evaluator shall check that the operational user guidance describes how the TOE provides reliable timestamps and if there are any management functions for configuring the time.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'Timestamps' section of the CC Guidance Supplement states that each device includes a real-time clock powered by a battery. The time is set during production. There are no management functions that allow configuration of time. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.4.6 FPT_TST.1

5.4.6.1 FPT_TST.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.4.6.2 FPT_TST.1 TSS 1

Objective	The evaluator shall verify that the TSS describes the self- tests that are performed on start up or on reset (if "upon reset button activation" is selected). The evaluator shall verify that the self-tests cover at least the following: a) a test of the user interface – in particular, tests of the user control mechanism (e.g., checking that the front panel push-buttons are not jammed); and b) if "active anti-tamper functionality" is selected, a test of any antitampering mechanism (e.g., checking that the backup battery is functional).
Evaluator Findings	The evaluator examined the section titled 'TSF Testing' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section discusses the self-test and what it encompasses: • Verification of the front panel push-buttons • Verification of the active anti-tampering functionality, including the continued functionality of the backup battery (where applicable) • Verification of the integrity of the microcontroller firmware

	• Verification of computer port isolation. This is tested by sending test packets to various interfaces and attempting to detect this traffic at all other interfaces Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.4.6.3 FPT_TST.1 TSS 2

Objective	The evaluator shall verify that the TSS describes how the TOE ensures a shutdown upon a self-test failure or a failed anti-tampering function, if present. If there are instances when a shutdown does not occur (e.g., a failure is deemed non-security relevant), those cases are identified and a rationale is provided explaining why the TOE's ability to enforce its security policies is not affected.
Evaluator Findings	The evaluator examined the section titled 'TSF Testing' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that if the self test fails, the front panel LEDs blink and the TOE makes a clicking sound. The TOE disables the PSD switching functionality, and enters a disabled state. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.4.6.4 FPT_TST.1TSS 3

Objective	The evaluator shall check the TSS to verify that it describes the TOE behavior in case of self-test failure. The evaluator shall verify that the described TOE behavior includes shutting down the PSD functionality once the failure is detected.
Evaluator Findings	The evaluator examined the section titled 'TSF Testing' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that if the self test fails, the front panel LEDs blink and the TOE makes a clicking sound. The TOE disables the PSD switching functionality, and enters a disabled state. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.4.6.5 FPT_TST.1 TSS 4

Objective	The evaluator shall examine the TSS to verify that it describes how users verify the integrity of the selections in FPT_TST.1.2 and FPT_TST.1.3. This method can include restarting the TOE, a dedicated self-test, or some other method.
Evaluator Findings	The evaluator examined the section titled 'TSF Testing' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that the TOE can be rebooted to rerun the self test to clear the error. All errors are logged. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.4.6.6 FPT_TST.1 Guidance 1

Objective	The evaluators shall verify that the operational user guidance describes how users verify the integrity of the selections in FPT_TST.1.2 and FPT_TST.1.3. This method can include restarting the TOE, a dedicated self-test, or some other method.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'Self Tests' section of the CC Guidance Supplement provides instructions on how to initiate a self-test, and how to exit self-test mode. In the case of a failure, users are directed to contact Technical Support. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.4.7 FPT_TST_EXT.1

5.4.7.1 FPT_TST_EXT.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

5.4.7.2 FPT_TST_EXT.1 TSS 1

Objective	The evaluator shall check the TSS to verify that it describes the TOE behavior in case of self-test failure. The evaluator shall verify that the described TOE behavior includes shutting down the PSD functionality once the failure is detected.
Evaluator Findings	The evaluator examined the section titled 'TSF Testing' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section states that the TOE front panel LEDs blink and there is a clicking noise made by the TOE when a self-test fails. The TOE disables the PSD switching functionality and remains in a disabled state until the TOE is rebooted and the self-test passes. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.4.7.3 FPT_TST_EXT.1 Guidance 1

Objective	The evaluator shall verify that the operational user guidance: a) describes how the results of self-tests are indicated to the user; b) provides the user with a clear indication of how to recognize a failed selftest; and c) details the appropriate actions to be completed in the event of a failed self-test.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'Self Tests' section of the CC Guidance Supplement describes a self-test failure and explains what the operator has to do if there is a failure. The channel indicators on the front panel

	light up sequentially and peripheral port interfaces are disabled during the self-test and following a failed self-test. In the event of a failed self-test, users are directed to contact HSL Technical Support. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.4.7.4 FPT_TST_EXT.1 Guidance 2

Objective	The evaluator shall verify that the operational user guidance provides adequate information on TOE self-test failures, their causes, and their indications.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The 'Self Tests' section of the CC Guidance Supplement describes a self-test failure. The document indicates that self-test failures may be caused by an unexpected input at power up, or by a failure in the device integrity. Self-test failures are indicated by blinking LEDs. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.5 TSS, Isolation Document, and Guidance Activities (TOE Access)

5.5.1 FTA_CIN_EXT.1

5.5.1.1 FTA_CIN_EXT.1 Isolation Document 1

Objective	There are no Isolation Document evaluation activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

5.5.1.2 FTA_CIN_EXT.1 TSS 1

Objective	The evaluator shall verify that the TSS describes how the TOE behaves on power up and on reset, if applicable, regarding which computer interfaces are active, if any.
Evaluator Findings	The evaluator examined the section titled 'TOE Access' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section indicates that on power up or power up following reset, all peripherals are connected to channel #1, and the corresponding push button LED will be illuminated. This is true for the remote control as well, with the indicator for which button is selected being illuminated. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.5.1.3 FTA_CIN_EXT.1 TSS 2

Objective	The evaluator shall verify that the TSS documents the behavior of all indicators when each switching mechanism is in use, and that no conflicting information is displayed by any indicators.
Evaluator Findings	The evaluator examined the section titled 'TOE Access' in the Security Target to determine the verdict of this evaluation activity. The evaluator confirmed that this section describes the switching functionality. The description and figure show how the selected channel is indicated and that no conflicting information is displayed. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.5.1.4 FTA_CIN_EXT.1 Guidance 1

Objective	The evaluator shall verify that the operational user guidance notes which computer connection is active on TOE power up or on recovery from reset, if applicable. If a reset option is available, use of this feature must be described in the operational user guidance.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The evaluator examined the CC Guidance Supplement and the Administrator Guide. The 'Selected Channel at Startup' section of the CC Guidance Supplement indicates that Channel 1 is selected by default when the device is started or reset. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

5.5.1.5 FTA_CIN_EXT.1 Guidance 2

Objective	The evaluator shall verify that the operational user guidance documents the behavior of all indicators when each switching mechanism is in use, and that no conflicting information is displayed by any indicators.
Evaluator Findings	The evaluator examined the guidance to determine the verdict of this evaluation activity. The evaluator examined the product Quick Installation Guide. These guides describe the behavior of the TOE indicators. This document provides a description of the channel indicators and a description of the indicator behavior when the switching mechanism is in use. This behavior ensures that no conflicting information is displayed by the indicators. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

6 Detailed Test Cases (Test Activities)

6.1 FAU_GEN.1 Test 1

Item	*Data/Description*
Test ID	*FAU_GEN.1 – Test 1*
Objective	The evaluator shall perform each of the auditable functions to succeed, and where possible, to fail. The evaluator shall use the means described in the TSS to access the audit records and verify that each of the events has been recorded, with all the of the expected information. The evaluator shall perform the following tests: 1. Set up the TOE to enable administrator access per applicable TOE administrative guidance. Verify that the TOE is in factory default format. 2. Attempt to set the initial administrator username and password. 3. Log into the TOE using administrative credentials and password. 4. Under the main operation page, select option "6" then "1" for critical one-time programming (OTP) logs. 5. Ensure tampering events logs are recorded by the TOE. 6. Ensure self-test failure logs are recorded by the TOE. 7. Ensure peripheral device rejection logs are recorded by the TOE 8. Ensure reset to factory default event logs are recorded by the TOE. 9. Ensure changes to the primary administrator password logs are recorded by the TOE. 10. Under the main operations page, select option "6" then "2" for random access memory (RAM) logs. 11. Ensure peripheral device acceptance logs are recorded by the TOE. 12. Ensure non-security related configuration change logs are recorded by the TOE. 13. Ensure administrator login logs are recorded by the TOE. 14. Ensure administrator logout logs are recorded by the TOE. 15. Ensure creation and removal of administrator account logs are recorded by the TOE. 16. Ensure administrator password change logs are recorded by the TOE. 17. Ensure password lock event logs are recorded by the TOE. 18. Ensure the powerup log is recorded by the TOE.
Notes	• The TOE initiates the startup of all audit event functionality automatically immediately on power-on. Shutdown of the TOE is immediate upon on removing the power cable. Thus, auditing is implicit on the powerup event. • The evaluator confirms that the test execution steps were performed on the TOE.
Testbed	#1
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor.

Test Execution Steps	1. TOE was set to enable administrator access; TOE is in factory default format. 2. Initial administrator username and password was set. 3. Logged into the TOE using administrative credentials and password. 4. Critical one-time programming logs were presented with different administrative function options. 5. Tampering event logs were recorded and present in the TOE logs. 6. Self-test failure logs were recorded and present in the TOE logs. 7. Peripheral device rejection logs were recorded and present in the TOE logs. 8. Reset to factory default event logs were recorded and present in the TOE logs. 9. Changes to the primary administrator password logs were recorded and present in the TOE logs. 10. Random access memory logs were presented with different administrative function options. 11. Peripheral device acceptance logs were recorded and present in the TOE logs. 12. Non-security related configuration change logs were recorded and present in the TOE logs. 13. Administrator login logs were recorded and present in the TOE logs. 14. Administrator logout logs were recorded and present in the TOE logs. 15. Creation and removal of administrator account logs were recorded and present in the TOE logs. 16. Administrator password change logs were recorded and present in the TOE logs. 17. Password lock event logs were recorded and present in the TOE logs. 18. Power up event logs were recorded and present in the TOE logs.
Pass/Fail Explanation	The evaluator confirms they accessed the audit records and verified that each of the events listed in FAU_GEN.1 have been recorded, with all the of the expected information.
Units Tested	SK41D-4TR
Result	PASS

6.2 FDP_APC_EXT.1

Objective	There are no tests for FDP_APC_EXT.1
Pass/Fail Explanation	Not Applicable
Verdict	Not Applicable/PASS

6.3 FDP_APC_EXT.1/KM Test 1

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1/KM – Test 1*
Objective	For tests that use the USB sniffer or USB analyzer software, the evaluator verifies whether traffic is sent or not sent by inspection of the passing USB transactions and ensuring they do not contain USB data payloads other than any expected traffic, as well as USB NAK transactions or system messages. To avoid clutter during USB traffic capture, the evaluator may filter NAK transactions and system messages.

The evaluator shall perform the following tests:

Test 1-KM – KM Switching methods

[Conditional: Perform this test if “switching can be initiated only through express user action” is selected in FDP_SWI_EXT.1.1 in the PSD PP]

While performing this test, ensure that switching is always initiated through express user action.

This test verifies the functionality of the TOE’s KM switching methods.

Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect an authorized peripheral device for each peripheral device type selected in FDP_PDC_EXT.3.1/KM. Run an instance of a text editor on each connected computer.

Step 2: Connect a display to each computer in order to see all computers at the same time, turn on the TOE, and enter text or move the cursor to verify which connected computer is selected.

Step 3: For each switching method selected in FDP_SWI_EXT.2.2, switch selected computers in accordance with the operational user guidance, and verify that it succeeds.

Step 4: For each peripheral device type selected in FDP_PDC_EXT.3.1/KM, attempt to switch the device to more than one computer at once and verify that the TOE ignores all such commands or otherwise prevents the operation from executing.

Step 5: [Conditional: If “keyboard” is selected in FDP_PDC_EXT.3.1/KM, then] attempt to control the computer selection using the following standard keyboard shortcuts, where ‘#’ represents a computer channel number, and verify that the selected computer is not switched:

- Control - Control - # - Enter
- Shift - Shift - #
- Num Lock - Minus - #
- Scroll Lock - Scroll Lock - #
- Scroll Lock - Scroll Lock - Function #
- Scroll Lock - Scroll Lock - arrow (up or down)
- Scroll Lock - Scroll Lock - # - enter
- Control - Shift - Alt - # - Enter
- Alt - Control - Shift - #

Step 6: [Conditional: If “mouse” is selected in FDP_PDC_EXT.3.1/KM, then] attempt to switch to other connected computers using the pointing device and verify that it does not succeed.

Step 7: [Conditional: If “peripheral devices using a guard” is selected in FDP_SWI_EXT.2.2, then] attempt to switch to other connected computers using

	the peripheral device and guard by only performing some of the steps outlined in the operational user guidance, and verify that it does not succeed.
Notes	• The evaluator has tested computer ports #1 and #2, then moved the test computers over to ports #3 and #4. The evaluator confirms that all computer ports on the switch (#1, #2, #3 and #4) were all tested. • The evaluator has tested two computer ports at a time, then moved the test computers over to two other ports and repeated this process until all switch port combinations have been tested. The evaluator confirms that all computer ports on the switch (#1, #2, #3 and #4) were all tested. No activity was observed on any non-connected PC. • Testing was performed using both the TOE front panel and then the WR40-4R remote control.
Testbed	#1
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Notepad, Dell P2319H Monitor.
Test Execution Steps	1. TOE was configured and a text editor was running on each connected computer. 2. User was able to see each computer at the same time. TOE was powered on and user was able to verify selected computer with cursor. 3. User was able to switch between selected computers. 4. The TOE did prevent the user from switching to more than one computer at once. 5. The TOE did not respond to such standard keyboard shortcuts. 6. User was not able to switch between computers using the pointing device.
Pass/Fail Explanation	The functionality of the TOE’s KM switching methods has been tested successfully. The evaluator has confirmed that the TOE prevents the user from switching between more than one computer at once.
Units Tested	SK41D-4TR / WR40-4R
Result	PASS

6.4 FDP_APC_EXT.1/KM Test 2

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1/KM – Test 2*
Objective	Test 2-KM – Positive and Negative Keyboard and Mouse Data Flow Rules Testing This test verifies the functionality for correct data flows of a mouse and keyboard during different power states of the selected computer. Step 1: Continue with the test setup from Test 1 and for each connected computer, connect a USB sniffer between it and the TOE or open the USB analyzer software. Perform steps 2-12 with each connected computer as the selected computer. Step 2: Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that the expected results are observed on the selected computer and that the expected traffic is sent and captured using the USB analyzer.

	[Conditional: Perform steps 3-10 if “switching can be initiated only through express user action” is selected in FDP_SWI_EXT.1.1 in the PSD PP.] Step 3: [If “mouse” is selected in FDP_PDC_EXT.3.1/KM, then] switch the TOE to each connected computer, and use the mouse to position the mouse cursor at the center of each display. Switch the TOE back to the originally selected computer. Step 4: [If “keyboard is selected in FDP_PDC_EXT.3.1/KM, then] use the keyboard to enter text into the text editor. [If “mouse” is selected in FDP_PDC_EXT.3.1/KM, then] use the mouse to move the cursor to the bottom right corner of the display. Step 5: Switch to each connected computer and verify that the actions taken in Step 4 did not occur on any of the non-selected computers. Step 6: Switch to the originally selected computer. Continue exercising the functions of the peripheral device(s) and examine the USB protocol analyzers on each one of the non-selected computers and verify that no traffic is sent. Step 7: Disconnect and reconnect the TOE interface cables connected to the selected computer. Examine the USB protocol analyzers on each one of the non-selected computers and verify that no traffic is sent. Step 8: Reboot the selected computer. Examine the USB protocol analyzers on each one of the nonselected computers and verify that no traffic is sent. Step 9: Enter sleep or suspend mode in the selected computer. Examine the USB protocol analyzers on each one of the non-selected computers to verify that no traffic is sent. Step 10: Exit sleep or suspend mode on the selected computer. Examine the USB protocol analyzers on each of the non-selected computers to verify that no traffic is sent. Ensure that any text in the Text Editor application is deleted. Step 11: Perform step 12 when the TOE is off and then in a failure state. Step 12: Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that no results are observed on the selected computer and that no traffic is captured using the USB analyzer.
Notes	• The evaluator has tested two computer ports at a time, then moved the test computers over to two other ports and repeated this process until all switch port combinations have been tested. The evaluator confirms that all computer ports on the switch (#1, #2, #3 and #4) were all tested. No activity was observed on any non-connected PC. • Testing was performed using both the TOE front panel and then the WR40-4R remote control.
Testbed	#1
Test Equipment Used	Teledyne Lecroy USB sniffer, USBlyzer, Notepad, Dell Wired Keyboard, Dell Wired Mouse, Teledyne Lecroy USB Protocol Suite, Dell P2319H Monitor.

Test Execution Steps	1. USB analyzer was connected between PC and TOE, USB analyzer software was running on the computer. 2. USB traffic was seen on the selected computer. 3. The mouse curser was placed in the center of the display. 4. The mouse curser was placed in the bottom right corner of the display. 5. The mouse curser did not move from its original place when switching between computers. 6. No USB traffic was seen on the non-selected computers. 7. No USB traffic was seen on the non-selected computers. 8. No USB traffic was seen on the non-selected computers. 9. No USB traffic was seen on the non-selected computers. 10. No USB traffic was seen on the non-selected computers. Text in editor was deleted. 11. TOE was powered off, then in a failure state. 12. No USB traffic was seen on the non-selected and selected computers.
Pass/Fail Explanation	Correct data flows of a mouse and keyboard during different power states of the selected computer has been tested. The evaluator has confirmed that data flow is transmitted to the correct computers at the accurate times.
Units Tested	SK41D-4TR
Result	PASS

6.5 FDP_APC_EXT.1/KM Test 3

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1/KM – Test 3*
Objective	Test 3-KM – Flow Isolation and Unidirectional Rule This test verifies that the TOE properly enforces unidirectional flow and isolation. Step 1: Ensure the TOE and the Operational Environment are configured in accordance with the operational guidance. Perform steps 2-12 with each connected computer as the selected computer. Step 2: Ensure the TOE is powered on and connect a display directly to the selected computer. Open a real-time hardware information console on the selected computer. [If “mouse” is selected in FDP_PDC_EXT.3.1/KM, then perform steps 3-4] Step 3: Connect a gaming mouse with programmable LEDs directly to the selected computer and attempt to configure the LEDs using the mouse application running on the selected computer. Verify that the mouse programmable LEDs change state. Step 4: Disconnect the gaming mouse from the selected computer and connect it to the TOE mouse peripheral device port through the USB sniffer. Attempt to configure the LEDs using the mouse application running on the selected computer. Verify that the mouse programmable LEDs do not change state and that no traffic is sent and captured by the USB sniffer while the evaluator is not moving the mouse. [If “keyboard” is selected in FDP_PDC_EXT.3.1/KM, then perform step 5]

	Step 5: Connect a keyboard to the peripheral device interface through the USB sniffer. Use a keyboard emulation software application running on the selected computer to turn the keyboard Num Lock, Caps Lock, and Scroll Lock LEDs on and off. Verify that the LEDs on the keyboard do not change state and that no traffic is sent and captured by the USB sniffer. Step 6: Power down the TOE and disconnect the peripheral interface USB cable from the TOE to the selected computer and the peripheral devices from the TOE. Step 7: Power up the TOE and ensure the selected computer has not changed (this should have no effect on the selected computer because it was disconnected in the previous step). Reconnect the peripheral devices disconnected in step 6 to the TOE. Step 8: [If “mouse” is selected in FDP_PDC_EXT.3.1/KM, then] check that immediately following the connection, the mouse LEDs are illuminated (indicating that the peripheral devices are powered on, although the selected computer is not connected). [If “keyboard” is selected in FDP_PDC_EXT.3.1/KM, then] check that immediately following the connection, the Num Lock, Caps Lock, and Scroll Lock keyboard LEDs are blinking momentarily and then stay off (indicating that the keyboard is powered on, although the selected computer is not connected). Step 9: Turn the TOE off and disconnect the peripheral devices connected in step 6. Step 10: Reconnect the first computer interface USB cable to the TOE. Step 11: Turn on the TOE and check the computer real-time hardware information console for the presence of the peripheral devices connected in step 6 and disconnected in step 9. The presence of the TOE peripheral devices in the information console when the peripheral devices are not connected to the TOE indicates that the TOE emulates the KM devices. Step 12: [Conditional] If the TOE keyboard and mouse do not appear in the listed devices, repeat the following steps for both mouse and keyboard to simulate USB traffic: • Connect a USB generator to the TOE peripheral device interface port. • Configure the USB generator to enumerate as a generic HID mouse/keyboard device and then to generate a random stream of mouse/keyboard report packets. • Connect a USB sniffer device between the TOE computer interface and the USB port on the first computer to capture the USB traffic between the TOE and the first computer. Turn on the TOE and verify that no packets cross the TOE following the device enumeration.
Notes	• The evaluator has tested computer ports #1 and #2, then moved the test computers over to ports #3 and #4. The evaluator confirms that all computer ports on the switch (#1, #2, #3 and #4) were all tested. • The evaluator has tested two computer ports at a time, then moved the test computers over to two other ports and repeated this process until all switch port combinations have been tested. The evaluator confirms that all computer

	ports on the switch (#1, #2, #3 and #4) were all tested. No activity was observed on any non-connected PC. - Testing was performed using both the TOE front panel and then the WR40-4R remote control.
Testbed	#1
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Device Manager, Steelseries Rival 100 Gaming Mouse, Teledyne Lecroy USB Sniffer, Teledyne Lecroy USB Protocol Suite, Dell P2319H Monitor.
Test Execution Steps	1. TOE was configured correctly. 2. TOE was powered on; selected computer had display connected. Hardware information console was open on computer. 3. Mouse programmable LED did change state. 4. Mouse programmable LED did not change state, no USB traffic was generated. 5. Keyboard LEDs did not change state and no USB traffic was generated. 6. TOE was powered off; peripheral cable was unplugged. 7. TOE was powered on; peripheral cable was reconnected. 8. Mouse: LEDs are illuminated. Keyboard: LEDs blinked momentarily then stayed off. 9. TOE was powered off; peripherals were disconnected. 10. USB cable was reconnected. 11. Hardware management console indicated emulated peripheral devices. 12. No packets were captured following the device enumeration.
Pass/Fail Explanation	Unidirectional flow and isolation of USB traffic has been tested. The evaluator has confirmed that USB traffic is enforced properly and in a single direction.
Units Tested	SK41D-4TR
Result	PASS

6.6 FDP_APC_EXT.1/KM Test 4

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1/KM – Test 4*
Objective	*[Conditional: Perform this test if "switching can be initiated only through express user action" is selected in FDP_SWI_EXT.1.1 in the PSD PP]* This test verifies correct data flow while the TOE is powered on or powered off. 1. Ensure the TOE and the Operational Environment are configured in accordance with the operational guidance. Connect a display directly to each connected computer. Perform steps 2-10 for each connected computer. 2. Connect a USB sniffer between a non-selected TOE KM computer interface and its computer. Run USB protocol analyzer software on all remaining computers. 3. Turn on the TOE and observe the TOE enumeration data flow in the protocol analyzer connected to the selected computer and is not in any other USB protocol analyzers or the USB sniffer. 4. Ensure the TOE is switched to the first computer. 5. Reboot the first computer. Verify that no USB traffic is captured on all non-selected computer USB protocol analyzers.

	6. Generate intensive USB HID traffic by moving the mouse at high speed and/or holding down the keyboard space key at the same time. Verify that no new USB traffic is captured on all non-selected computer USB protocol analyzers. 7. Perform steps 8 and 9 for each TOE keyboard/mouse peripheral interface. 8. Connect a USB dummy load into the TOE KM peripheral device interface. Verify that no new USB traffic is captured on all non-selected computer USB protocol analyzers. Remove the plug after the step is completed. 9. Connect a switchable 5-volt power supply with any compatible USB plug into the TOE KM peripheral device interface. Modulate the 5-volt supply (i.e., cycle on and off) manually at various speeds from approximately one cycle per five seconds to one cycle per second. Verify that no new USB traffic is captured on all non-selected computer USB analyzers. 10. Turn off the TOE. Verify that no new traffic is captured.
Notes	• The evaluator has tested computer ports #1 and #2, then moved the test computers over to ports #3 and #4. The evaluator confirms that all computer ports on the switch (#1, #2, #3 and #4) were all tested. • The evaluator has tested two computer ports at a time, then moved the test computers over to two other ports and repeated this process until all switch port combinations have been tested. The evaluator confirms that all computer ports on the switch (#1, #2, #3 and #4) were all tested. No activity was observed on any non-connected PC. • Testing was performed using both the TOE front panel and then the WR40-4R remote control. • TD0507 applied.
Testbed	#1
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Teledyne Lecroy USB Sniffer, USBlyzer, HSL USB Dummy Load, Dr. Meter DC Power Supply, Teledyne Lecroy USB Protocol Suite, Dell P2319H Monitor, Spliced USB Type-A Cable.
Test Execution Steps	1. TOE was configured, display was connected to each computer. 2. USB analyzer software was running, USB sniffer was properly implemented. 3. USB traffic was only being captured on selected computer. 4. First computer was selected via TOE. 5. No USB traffic was captured on all non-selected computers. 6. No USB traffic was captured on all non-selected computers. 7. Performed steps 8 and 9 for each KM interface. 8. No USB traffic was captured on all non-selected computers. 9. No USB traffic was captured on all non-selected computers. 10. No USB traffic was captured on all non-selected computers.
Pass/Fail Explanation	Correct data flow while the TOE is powered on or powered off has been tested. The evaluator confirms that USB traffic is only captured on selected authorized computers.
Units Tested	SK41D-4TR
Result	PASS

6.7 FDP_APC_EXT.1/KM Test 5

Item	*Data/Description*

Test ID	*FDP_APC_EXT.1/KM – Test 5*
Objective	Test 5-KM – No Flow between Connected Computers over Time This test verifies that the TOE does not send data to different computers connected to the same interface at different times. Repeat this test for each TOE KM computer port. Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect an authorized peripheral device for each peripheral device type selected in FDP_PDC_EXT.3.1/KM. Connect two computers to a different display and run an instance of a text editor and USB analyzer software on each computer. Step 2: Connect the first computer to the TOE and ensure it is selected and that no other computers are connected. Step 3: Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that the expected results are observed on the selected computer and that the expected traffic is sent and captured using the USB analyzer. Step 4: Disconnect the first computer. Generate intensive USB HID traffic by moving the mouse at high speed and/or holding down the keyboard space key at the same time. Step 5: Cease generation of the USB HID traffic, connect the second computer to the same port and ensure it is selected. Step 6: Verify that no results from the previous use of the peripheral device are observed on the selected computer and that no traffic is sent and captured using the USB analyzer. Step 7: Reboot the TOE and repeat step 6. Step 8: Turn off the TOE and repeat step 6. Step 9: Restart the TOE and repeat step 6. Step 10: Exercise the functions of the peripheral device type selected in FDP_PDC_EXT.3.1/KM and verify that the expected results are observed on the selected computer and that the expected traffic is sent and captured using the USB analyzer.
Notes	• The evaluator has tested computer ports #1 and #2, then moved the test computers over to ports #3 and #4. The evaluator confirms that all computer ports on the switch (#1, #2, #3 and #4) were all tested. • The evaluator has tested two computer ports at a time, then moved the test computers over to two other ports and repeated this process until all switch port combinations have been tested. The evaluator confirms that all computer ports on the switch (#1, #2, #3 and #4) were all tested. No activity was observed on any non-connected PC. • Testing was performed using both the TOE front panel and then the WR40-4R remote control.
Testbed	#1
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Notepad, USBlyzer, Dell P2319H Monitor.

Test Execution Steps	1. Authorized peripheral devices were connected, display was connected to each computer, text editor and USB analyzer was running on each computer. 2. Only the first computer was connected and selected. 3. USB traffic was captured on selected computer. 4. Computer was disconnected; USB traffic was generated. 5. Second computer was connected to first computers port. 6. No USB traffic leaked over from the first computer. 7. TOE was rebooted. No USB data was captured. 8. TOE was powered off. No USB data was captured. 9. TOE was rebooted. No USB data was captured. 10. Expected USB traffic was generated on selected computer.
Pass/Fail Explanation	Data flow through the same interface has been observed and tested. The evaluator confirms that the TOE does not send data to different computers connected to the same interface at different times.
Units Tested	SK41D-4TR
Result	PASS

6.8 FDP_APC_EXT.1/VI Test 1

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1/VI – Test 1*
Objective	Test 1-VI: Video Source Selection and Identification, TOE Off and Failure States TD (TD0539 is applied) This test verifies the TOE switching function operates properly and will stop the video output display when in an OFF or FAILURE state. Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Step 2: Play a different video with embedded audio on a number of computers for each TOE computer video interface. Step 3: Connect each computer to a TOE computer video interface. Step 4: Connect a display to each TOE display interface. Step 5: Turn on the TOE. Step 6: For each connected computer, ensure it is selected and verify that the video and its accompanying audio from the selected computer(s) are received on the proper display(s). Step 7: [Conditional: if the TOE claims the Combiner Use Case then] verify that video generated by the TOE has clear identification marking or text to properly identify the source computer shown. Step 8: Turn off the TOE and verify that no video appears on any connected display. Step 9: Power on the TOE and cause the TOE to enter a failure state. Verify that the TOE provides the user with a visual indication of failure and that no usable video appears on any connected display.

	Step 10: Repeat steps 3 to 9 for each unique display protocol and port type supported by the TOE.
Notes	• The evaluator has tested two computer ports at a time, then moved the test computers over to two other ports and repeated this process until all switch port combinations have been tested. The evaluator confirms that all computer ports on the switch (#1, #2, #3 and #4) were all tested. No activity was observed on any non-connected PC. • Testing was performed using both the TOE front panel and then the WR40-4R remote control. • TD0539 Applied.
Testbed	#1
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Edifier Multimedia Speaker, Dell P2319H Monitor.
Test Execution Steps	1. The TOE was configured. 2. Different videos were playing on multiple computers. 3. Each computer was connected to a TOE computer video interface. 4. Display was connected to each TOE display interface. 5. TOE was powered on. 6. Selected computer is the one that is shown. 7. “one connected display” is selected in FDP_CDS_EXT.1.1; correct source computer is shown. 8. No video appeared on any connected display. 9. Visual indication of a failure state was present. No usable video appeared on any connected display.
Pass/Fail Explanation	The evaluator confirms that the TOE switching function operates properly and will stop the video output display when in an OFF or FAILURE state.
Units Tested	SK41D-4TR
Result	PASS

6.9 FDP_APC_EXT.1/VI Test 2

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1/VI – Test 2*
Objective	Test 2-VI: Computer Video Interface Isolation [Conditional: perform this test if “switching can be initiated only through express user action” is selected in FDP_SWI_EXT.1.1 in the PSD PP.] This test verifies that the TOE does not transfer data to any non-selected computer video interface. Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect only the first computer interface cable to one computer. Turn on the TOE. Step 2: Switch the TOE primary display to computer #1. Step 3: Observe the primary display to verify that the selected computer is the one that is shown.

	Step 4: Remove the non-selected computer video interface cables from the TOE and connect the oscilloscope probe to the TOE #2 computer video interface to verify that no SYNC signal is passed through the TOE. Based on the connection interface protocol, this is performed as follows: 1. Video Graphics Array (VGA) – single ended probe on pins 13 and then 14; 2. High-Definition Multimedia Interface (HDMI) – connect pin 19 to a 3.3V power supply via a 100 Ohm resistor to provide Hot Plug Detect (HPD) signal; Check for signals - differential probe between pins 10 (+) and 12 (-); 3. Digital Visual Interface (DVI)-I – connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - single ended probe on pins 8 and C4. Differential probe between pins 23 (+) and 24 (-); 4. DVI-D - connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 23 (+) and 24 (-); 5. DisplayPort - connect pin 18 to a 3.3V power supply via 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 3 (-) and 1 (+) and between 10 (-) and 12 (+); 6. USB Type-C with DisplayPort as Alternate Function – connect pin A8 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals – Differential probe between pins A2 and A3, A10 and A11; B2 and B3, and B10 and B11. Step 5: Repeat steps 3 and 4 while selecting other TOE connected computers. Verify that no SYNC signal is present. Step 6: Repeat steps 3 to 5 with the TOE unpowered. Verify that no SYNC signal is present. Step 7: With the probe connected to the TOE computer #2 video interface, disconnect / reconnect the computer #1 video cable. Power up the TOE and select computer #1. Attempt to detect the change in the oscilloscope at each one of the TOE #2 computer video interface pins. No changes shall be detected. Step 8: Repeat step 7 for each one of the other TOE computer video interfaces. Step 9: Repeat steps 7 and 8, but instead of disconnecting / reconnecting the computer, disconnect and reconnect the display. Step 10: Repeat steps 7 and 8, but instead of disconnecting / reconnecting the computer, reboot the selected computer. Step 11: Repeat steps 2 to 10 with each connected computer. Step 12: [Conditional: if “multiple connected displays” is selected in FDP_CDS_EXT.1.1 then] repeat steps 3 to 10 with each other display connected to the TOE. Step 13: Repeat this test for each unique display protocol and port type supported by the TOE.
Notes	• The evaluator has tested two computer ports at a time, then moved the test computers over to two other ports and repeated this process until all switch port combinations have been tested. The evaluator confirms that all computer ports on the switch (#1, #2, #3 and #4) were all tested. No activity was observed on any non-connected PC.

	- USB connections present on the TOE only allow HID devices not video protocols. - Testing was performed using both the TOE front panel and then the WR40-4R remote control.
Testbed	#1
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Tektronix Oscilloscope, Dr. Meter DC Power Supply, Dell P2319H Monitor, Spliced HDMI Cable, Spliced DisplayPort Cable, Spliced USB Type-C Cable.
Test Execution Steps	1. First computer interface cable was connected to one computer. TOE was powered on. 2. TOE primary display was on computer #1. 3. The selected computer is the one that is shown. 4. No SYNC signal was passed through the TOE. 5. No SYNC signal was present. 6. No SYNC signal was present. 7. No change in oscilloscope was detected. 8. No change detected in any other interface. 9. No change detected in any of the interfaces when disconnecting and reconnecting the display. 10. No change detected in any of the interfaces when rebooting the selected computer. 11. All tests passed for each connected computer. 12. All tests passed for secondary display. 13. Test were repeated for each unique display protocol.
Pass/Fail Explanation	The evaluator confirms that the TOE does not transfer data to any non-selected computer video interface.
Units Tested	SK41D-4TR
Result	PASS

6.10 FDP_APC_EXT.1/VI Test 3

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1/VI – Test 3*
Objective	3-VI - Unauthorized Sub-protocols Note that in the following steps only native video protocol cables shall be used. No conversion from other video protocols is allowed in these tests except as directed in FDP_IPC_EXT.1.1. This test verifies that unauthorized sub-protocols are blocked. Perform this test for each of the selections in FDP_PDC_EXT.3.1/VI and FDP_IPC_EXT.1.1. In the following steps the evaluator shall establish a verified test setup that passes video signals across the TOE. Step 1: Connect at least one computer with a native video protocol output to the TOE computer #1 video input interface. Step 2: Connect at least one display with native video protocol to the TOE display output.

	Step 3: Power up the TOE and ensure the connected computer is selected. Step 4: Verify that the video image is visible and stable on the user display. In the following steps the evaluator shall verify that the test setup properly blocks the unauthorized video sub-protocol traffic. Step 5: Open the Monitor Control Command Set (MCCS) control console program on the computer and attempt to change the display contrast and brightness. Verify that the display does not change its contrast and brightness accordingly. Step 6: Disconnect the video cable connecting the display and the TOE and connect the display directly to the computer. Verify that the video image is visible and stable on the user display. Step 7: Attempt to change the display contrast and brightness. Verify that the display does change its contrast and brightness accordingly. Step 8: Connect the following testing device based on the display video protocol being tested at the peripheral display interface: 1. DisplayPort – DisplayPort AUX channel analyzer in series between the display and the TOE 2. HDMI – HDMI sink test device 3. USB Type-C with DisplayPort as Alternate Function – USB sniffer in series between the display and the TOE 4. VGA – VGA sink test device 5. DVI-I/DVI-D – DVI sink test device Step 9: Attempt to change the display contrast and brightness. Verify that the testing device does not capture any MCCS commands. Step 10: Replace the computer with a source generator for each selected protocol at the computer video interface. If DVI-I or DVI-D is selected, use an HDMI source generator. Step 11: Run an EDID write transaction at the generator and verify in the testing device that no EDID traffic is captured. Step 12: [Conditional, if DisplayPort, DVI-D, DVI-I, HDMI, or USB Type-C is the selected protocol being tested at the computer video interface, then] run Consumer Electronics Control (CEC) and High-bandwidth Digital Content Protection (HDCP) tests or commands at the generator and verify in the testing device that no CEC or HDCP traffic is captured. Step 13: [Conditional, if DVI-D, DVI-I, or HDMI is the selected protocol being tested at the computer video interface, then] run Audio Return Channel (ARC), HDMI Ethernet and Audio Return Channel (HEAC), and HDMI Ethernet Channel (HEC) tests or commands at the generator and verify in the testing device that no ARC, HEAC, or HEC traffic is captured. Step 14: [Conditional: If "[HDMI] protocol" is selected in FDP_IPC_EXT.1.2, then] perform steps 15 and 16 for both pin 13 (CEC) and 14 (UTILITY).

	Step 15: Turn off the TOE. Use a multi-meter to measure the resistance-to-ground of the pin at the TOE HDMI peripheral interface and verify it is greater than 2 Mega-ohms. Step 16: Attach a single ended oscilloscope probe between the pin and the ground, turn on the TOE, and verify that no changes between 0.0v and 0.2v and between 3.0v and 3.3v are detected. Step 17: [Conditional: if VGA is not the selected protocol being tested, then] disconnect all devices. Connect the display to a TOE computer video interface and the oscilloscope to the TOE display interface in order to verify that no HPD signal is passed by measuring a signal voltage of less than 1.0V. Based on the selected protocol being tested, this is performed as follows: 1. HDMI – connect scope to pin 19 and verify no HPD signal is detected; 2. DVI-D/DVI-I – connect scope to pin 16 and verify no HPD signal is detected; 3. DisplayPort - connect scope to pin 18 and verify no HPD signal is detected; 4. USB Type-C with DisplayPort as Alternate Function – connect scope to pin A8 and B8 and verify no HPD signal is detected. Step 18: Repeat this test for each of the selections in FDP_PDC_EXT.3.1/VI and FDP_IPC_EXT.1.2.
Notes	• The evaluator has tested two computer ports at a time, then moved the test computers over to two other ports and repeated this process until all switch port combinations have been tested. The evaluator confirms that all computer ports on the switch (#1, #2, #3 and #4) were all tested. No activity was observed on any non-connected PC. • Testing was performed using both the TOE front panel and then the WR40-4R remote control. • USB connections present on the TOE only allow HID devices not video protocols. • TD0514 and TD0584 are both applied.
Testbed	#1
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, SoftMCCS, DisplayPort Aux Channel Monitor, Unigraf DPA-400 DisplayPort Aux Channel Monitor, QuantumData 882E Video Test Generator, Fluke True RMS Digital Multimeter, Tektronix Oscilloscope, QuantumData 980 Video Test Generator, TCL 40” Smart TV with ARC, Spliced HDMI Cable, Spliced DisplayPort Cable, Spliced USB Type-C Cable, Dell P2319H Monitor.
Test Execution Steps	1. Computer was connected to at least one computer with native video protocol output. 2. At least one display with native video protocol was connected to TOE display output. 3. TOE was powered up. Connected video was selected. 4. Image was visible and stable on the user display. 5. Display contrast and brightness did not change. 6. Video image was visible and stable on user display. 7. Contrast and brightness did change accordingly. 8. Connected testing device based on display video protocol.

	9. MCCS commands were not captured. 10. HDMI source generator was connected. 11. No EDID traffic was captured. 12. No CEC or HDCP traffic was captured. 13. No ARC, HEAC, or HEC traffic was captured. 14. Preformed steps 15 and 16 for both pins 13 (CEC) and 14 (UTILITY). 15. Multi-meter reads greater than 2 Mega-ohms. 16. No charges between 0.0v and 0.2v and between 3.0 and 3.3v were detected. 17. No HPD signal was passed by measuring a signal voltage of less than 1.0 v. 18. Test repeated for selections in FDP_PDC_EXT.3.1/VI and FDP_IPC_EXT.1.2.
Pass/Fail Explanation	The evaluator has confirmed that the TOE successfully blocks unauthorized sub-protocols.
Units Tested	SK41D-4TR
Result	PASS

6.11 FDP_APC_EXT.1/VI Test 4

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1/VI – Test 4*
Objective	Test 4-VI - Video and EDID Channel Unidirectional Rule This test verifies that the TOE video path is unidirectional from the computer video interface to the display interface with the exception of EDID, which may be read from the display once at power up and then may be read by the connected computers. The evaluator should have at least two high-resolution displays of different models and one low-resolution display for each TOE-supported video protocol. In the following steps the evaluator should attempt to read display EDID after the TOE completed its self-test / power up. The TOE should not read the new display EDID. Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Connect a computer and a high-resolution display to the TOE. Step 2: Ensure the TOE is on, computer #1 is selected, and verify that the display shows video from computer #1 as expected. Step 3: Turn off the TOE. Disconnect the user display from the TOE. Step 4: Connect the low-resolution display to the TOE and turn on the TOE. After the video is shown on the display, turn off the TOE and disconnect the low-resolution display. Step 5: Turn on the TOE. After the TOE has completed the self-test, connect the second high-resolution display of a different model to the TOE. The TOE may fail to generate video on the user display (i.e., no EDID is read at the TOE power up). If the display is showing video, then run the EDID reading and parsing software on

	computer #1 and check that there is no active EDID (i.e., the computer is using a default generic display or reading older display settings from the registry). Step 6: Perform steps 7-11 for each TOE computer video interface. Step 7: Power off the TOE and disconnect the computer #1 video output and the display. Connect the display cable to the TOE computer #1 video interface. Connect the computer #1 video cable to the TOE display interface. This configuration will attempt to force video data through the TOE in the reverse direction. Step 8: Power up the TOE again. Step 9: Check that the video is not visible in the display. Step 10: Perform steps 11 while the TOE is powered on and powered off. Step 11: Remove the display cable from the TOE and connect the oscilloscope to verify that no SYNC signal is passed through the TOE. Based on the video protocols supported, this is performed as follows: 1. VGA – single ended probe on pins 13 and 14; 2. HDMI – connect pin 19 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - differential probe between pins 10 (+) and 12 (-); 3. DVI-I – connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - single ended probe on pins 8 and C4. Differential probe between pins 23 (+) and 24 (-); 4. DVI-D - connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 23 (+) and 24 (-); 5. DisplayPort - connect pin 18 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals - Differential probe between pins 3 (-) and 1 (+) and between 10 (-) and 12 (+); 6. USB Type-C with DisplayPort as Alternate Function – connect pin A8 to a 3.3V power supply via a 100 Ohm resistor to provide HPD signal; Check for signals – Differential probe between pins A2 and A3, A10 and A11; B2 and B3, and B10 and B11.
Notes	• The evaluator has tested two computer ports at a time, then moved the test computers over to two other ports and repeated this process until all switch port combinations have been tested. The evaluator confirms that all computer ports on the switch (#1, #2, #3 and #4) were all tested. No activity was observed on any non-connected PC. • Testing was performed using both the TOE front panel and then the WR40-4R remote control. • USB connections present on the TOE only allow HID devices not video protocols. • TD0506 is applied.
Testbed	#1

Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor, Asus PA238 Monitor, Dell 1907FPc Monitor, Tektronix Oscilloscope, Dr. Meter DC Power Supply, Spliced HDMI Cable, Spliced DisplayPort Cable, Spliced USB Type-C Cable.
Test Execution Steps	1. Computer and high-resolution display were connected to the TOE. 2. Display shows video from computer #1. 3. TOE was powered off. Display was disconnected from TOE. 4. Video was shown on the display, TOE was turned off. 5. TOE fails to generate video on the user display. 6. Steps 7 - 11 performed for DVI-D only. 7. Connected computer #1 video output to the TOE display port, and display cable to the computer#1 video interface. 8. TOE was powered up. 9. No video was visible in the display. 10. TOE was powered off. 11. No SYNC signal was passed through the TOE.
Pass/Fail Explanation	The evaluator confirms the TOE video path is unidirectional from the computer video interface to the display interface except for EDID.
Units Tested	SK41D-4TR
Result	PASS

6.12 FDP_APC_EXT.1/VI Test 5

Item	*Data/Description*
Test ID	*FDP_APC_EXT.1/VI – Test 5*
Objective	Test 5-VI – No Flow between Connected Computers over Time This test verifies that the TOE does not send data to different computers connected to the same TOE video interface over time. Repeat this test for each TOE Video port. Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Run EDID reading and parsing software on two computers and connect a display to the TOE. Step 2: Connect computer #1 to the TOE, ensure the TOE is on, computer #1 is selected, no other computers are connected, and verify that the display shows video from computer #1 as expected. Step 3: Capture the TOE EDID content in the software on computer #1 and save as a file with a name that indicates capture time. Step 4: Disconnect computer #1 and connect an I2C programmer to the same port. Attempt to write the characters “FFFF” over the entire EDID address range. Step 5: Disconnect the I2C programmer, reconnect computer #1 to the same port, and repeat step 3. Step 6: Reboot the TOE and repeat step 3. Step 7: Turn off the TOE and repeat step 3. Step 8. Restart the TOE and repeat step 3.

	Step 9: Disconnect computer #1 and repeat steps 2 to 8 with computer #2 on the same port. Step 10: Repeat steps 2 to 9 for a total of 20 EDID file captures. Step 11: Collect all 20 captured EDID files, compare them bit-by-bit, and verify that they are all identical excluding null captures recorded in Step 7.
Notes	• The evaluator has tested two computer ports at a time, then moved the test computers over to two other ports and repeated this process until all switch port combinations have been tested. The evaluator confirms that all computer ports on the switch (#1, #2, #3 and #4) were all tested. No activity was observed on any non-connected PC. • Testing was performed using both the TOE front panel and then the WR40-4R remote control. • TD0584 applied.
Testbed	#1
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Monitor Asset Manager, QuantumData 980 Video Test Generator, QuantumData 882E Video Test Generator, Dell P2319H Monitor.
Test Execution Steps	1. TOE was configured correctly. 2. Display showed video from computer #1. 3. EDID content saved on computer #1. 4. EDID address change failed. 5. Reconnected computer #1 to the same port as the I2C programmer. 6. TOE was rebooted. 7. TOE was turned off. 8. TOE was restarted. 9. Replaced computer #1 with computer #2. 10. 20 EDID files were captured. 11. Verified all 20 EDID files were identical.
Pass/Fail Explanation	The evaluator confirms that that the TOE does not send data to different computers connected to the same TOE video interface over time.
Units Tested	SK41D-4TR
Result	PASS

6.13 FDP_FIL_EXT.1/KM Test 1

Item	*Data/Description*
Test ID	*FDP_FIL_EXT.1/KM – Test 1*
Objective	Perform the test steps in FDP_PDC_EXT.1 with all devices on the PSD KM blacklist and verify that they are rejected as expected. 1. Ensure the TOE is powered off and connected to a computer. Run USB analyzer software on the connected computer and connect a USB sniffer to the TOE keyboard/mouse peripheral interface. Open the real-time hardware information console. 2. Attempt to connect the unauthorized device to the USB sniffer: • USB audio headset

	• USB camera • USB printer • USB user authentication device connected to a TOE keyboard/mouse peripheral interface • USB wireless LAN dongle 3. Power on the TOE. Verify the device is rejected. 4. Ensure the unauthorized device is disconnected from the USB sniffer, then attempt to connect it to the USB sniffer again. 5. Verify the device is rejected. 6. Repeat steps 1 through 5 with a USB hub connected between the USB device and USB sniffer and observe that the results are identical. 7. Repeat steps 1-6 with a composite device with non-HID device classes and verify that the non-HID functions are rejected, or the entire device is rejected.
Notes	• The evaluator has tested two computer ports at a time, then moved the test computers over to two other ports and repeated this process until all switch port combinations have been tested. The evaluator confirms that all computer ports on the switch (#1, #2, #3 and #4) were all tested. No activity was observed on any non-connected PC. • Testing was performed using both the TOE front panel and then the WR40-4R remote control.
Testbed	#1
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, USBlyzer, Teledyne Lecroy USB Sniffer, Device Manager, MPOW Headset with USB Connector, Logitech USB Camera, HP Deskjet USB Printer, Identiv USB UA Device, Wireless LAN Dongle, BYEASY USB Hub, Dell Keyboard with Smart Card Reader, Teledyne Lecroy USB Protocol Suite, Dell P2319H Monitor.
Test Execution Steps	1. TOE was powered off. USB analyzer software was running, and USB sniffer was connected. 2. User connected each device to the USB sniffer. 3. TOE was powered on. Device was rejected. 4. Device disconnect then reconnected. 5. Device was rejected. 6. Devices remain rejected through USB hub. 7. Device was rejected.
Pass/Fail Explanation	All devices on the PSD KM blacklist were tested and are rejected as expected. The evaluator confirms that the blacklist in place rejects all devices found in step 2.
Units Tested	SK41D-4TR
Result	PASS

6.14 FDP_FIL_EXT.1/KM Test 2

Objective	[Conditional: Perform this only if "configurable" is selected in FDP_FIL_EXT.1.1/KM] In the following steps the evaluator shall verify that whitelisted and blacklisted devices are treated correctly. Step 1: Ensure the TOE and the Operational Environment are configured in accordance with the operational guidance.

	Step 2: Connect to the TOE KM peripheral device interface a composite device which contains a HID class and a non-HID class. Step 3: Configure the TOE KM CDF to whitelist the composite device. Step 4: Verify that the HID-class part is accepted and that the non-HID class part is rejected through realtime device console and USB sniffer capture, or that the entire device is rejected. Step 5: Configure the TOE KM CDF to blacklist the device. Step 6: Verify that both the HID-class part and the non-HID class part is rejected through real-time device console and USB sniffer capture.
Evaluator Findings	"Configurable" has not been selected. Therefore, this evaluation activity is not applicable.
Verdict	Not Applicable/Pass

6.15 FDP_PDC_EXT.1 Test 1

Item	*Data/Description*
Test ID	*FDP_PDC_EXT.1 – Test 1*
Objective	The evaluator shall check the TOE and its supplied cables and accessories to ensure that there are no external wired interfaces other than the computer interfaces, peripheral device interfaces, and power interfaces.
Notes	• The evaluator confirms that the test execution steps were performed on all the units detailed in the units tested section. The same execution output was observed for each model tested.
Testbed	#1
Test Equipment Used	N/A
Test Execution Steps	1. Check the supplied cables and accessories to ensure there are no external wired interfaces other than the computer interfaces, peripheral device interfaces, and power interfaces.
Pass/Fail Explanation	The evaluator confirms that all supplied cables and accessories contain no external wired interfaces. This excludes computer interfaces, peripheral device interfaces, and power interfaces.
Units Tested	SK4ID-4TR / WR40-4R
Result	PASS

6.16 FDP_PDC_EXT.1 Test 2

Item	*Data/Description*
Test ID	*FDP_PDC_EXT.1 – Test 2*
Objective	The evaluator shall check the TOE for radio frequency certification information to ensure that the TOE does not support wireless interfaces.
Notes	• The evaluator confirms that the test execution steps were performed on all the units detailed in the units tested section. The same execution output was observed for each model tested.
Testbed	#1

Test Equipment Used	N/A	
Test Execution Steps	1. Check the TOE for radio frequency certification information to ensure that the TOE does not support wireless interfaces.	
Pass/Fail Explanation	The evaluator has checked the TOE for radio frequency certification information and verifies the TOE does not support wireless interfaces.	
Units Tested	SK4ID-4TR	WR40-4R
Result	PASS	

6.17 FDP_PDC_EXT.1 - Test 3

Item	*Data/Description*
Test ID	*FDP_PDC_EXT.1 – Test 3*
Objective	The evaluator shall verify that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the Peripheral Device Connections (Appendix E). For this test, verify device rejection through TOE user indication in accordance with the operational user guidance, an immediate cessation of traffic following device detection or enumeration, or incompatibility of the device interface with the peripheral interface, and through no such device appearing in the real-time hardware information console. Step 1: Ensure the TOE is powered off. Open a real-time hardware information console on the connected computer. Step 2: Attempt to connect a USB mass storage device to the TOE peripheral interface. Step 3: Power on the TOE. Verify the device is rejected. Step 4: Ensure the USB mass storage device is disconnected, and then attempt to connect it to the TOE peripheral interface again. Step 5: Verify the device is rejected. Step 6: Power off the TOE. Connect an unauthorized USB device to a USB hub, and attempt to connect the USB hub to the TOE peripheral interface. Step 7: Power on the TOE. Verify the device is rejected. Step 8: Ensure the USB hub is disconnected, and then attempt to connect it to the TOE peripheral interface again. Step 9: Verify the device is rejected. Step 10: Power off the TOE. Attempt to connect any Personal System/2 (PS/2) device directly to the TOE peripheral interface. Step 11: Power on the TOE. Verify the device is rejected. Step 12: Ensure the PS/2 device is disconnected, and then attempt to connect it directly to the TOE peripheral interface again. Step 13: Verify the device is rejected.

Notes	• The TOE does not contain any PS/2 input, therefore any attempt to directly connect a PS/2 interface to the TOE will result in the device being rejected.
Testbed	#1
Test Equipment Used	Device Manager, BYEASY USB Hub, PS/2 to USB Adapter, Perixx PS/2 Optical Mouse, HSL BADUSB, Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor.
Test Execution Steps	1. TOE was powered off. A real-time hardware information console application was running on the connected computer. 2. Connected a USB mass storage to the TOE peripheral interface. 3. TOE was powered on; the device was rejected. 4. Disconnected the USB mass storage device, connected it to the TOE peripheral interface. 5. The device was rejected. 6. TOE was powered off. Connected an unauthorized USB device to USB hub, connected it to the TOE peripheral interface again. 7. TOE was powered on; the device was rejected. 8. Disconnected the USB hub, connected it to the TOE peripheral interface. 9. The device was rejected. 10. TOE was powered on. Attempted to connect a PS/2 device directly to the TOE peripheral interface. 11. TOE was powered on; the device was rejected (The PS/2 device cannot be connected as the TOE contains no PS/2 ports). 12. PS/2 device was already disconnected; attempted to connect it to the TOE peripheral interface. 13. The device was rejected (The PS/2 device cannot be connected as the TOE contains no PS/2 ports).
Pass/Fail Explanation	The evaluator confirms that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the Peripheral Device Connections (Appendix E)
Units Tested	SK4ID-4TR / WR40-4R
Result	PASS

6.18 FDP_PDC_EXT.1 Test 1-KM

Item	*Data/Description*
Test ID	*FDP_PDC_EXT.1/KM – Test 1*
Objective	Test 1-KM: The evaluator shall verify that the TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the unauthorized peripheral device connections. For this test, verify device rejection through TOE user indication in accordance with the operational user guidance, an immediate cessation of traffic following device detection or enumeration, no traffic captured on the USB sniffer or analyzer software other than NAK transactions or system messages, or incompatibility of

	the device interface with the peripheral interface. Also verify device rejection through examination of the USB sniffer or analyzer software for no traffic captured other than NAK transactions or system messages and through examination of the real-time hardware console for no display of new USB devices (recognized or not recognized). Repeat this test for each keyboard/mouse TOE peripheral interface. Perform steps 1-6 for each of the following unauthorized devices: • USB audio headset • USB camera • USB printer • USB user authentication device connected to a TOE keyboard/mouse peripheral interface • USB wireless LAN dongle Step 1: Ensure the TOE is powered off and connected to a computer. Run USB analyzer software on the connected computer and connect a USB sniffer to the TOE keyboard/mouse peripheral interface. Open the real-time hardware information console. Step 2: Attempt to connect the unauthorized device to the USB sniffer. Step 3: Power on the TOE. Verify the device is rejected. Step 4: Ensure the unauthorized device is disconnected from the USB sniffer, then attempt to connect it to the USB sniffer again. Step 5: Verify the device is rejected. Step 6: Repeat steps 1 through 5 with a USB hub connected between the USB device and USB sniffer and observe that the results are identical. Step 7: Repeat steps 1-6 with a composite device with non-HID device classes and verify that the non-HID functions are rejected or the entire device is rejected.
Notes	• The evaluator has tested two computer ports at a time, then moved the test computers over to two other ports and repeated this process until all switch port combinations have been tested. The evaluator confirms that all computer ports on the switch (#1, #2, #3 and #4) were all tested. No activity was observed on any non-connected PC. • Testing was performed using both the TOE front panel and then the WR40-4R remote control.
Testbed	#1
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, USBlyzer, Teledyne Lecroy USB Sniffer, MPOW Headset with USB Connector, Logitech USB Camera, HP Deskjet USB Printer, Identiv USB UA Device, Wireless LAN Dongle, BYEASY USB Hub, Dell Keyboard with Smart Card Reader, Teledyne Lecroy USB Protocol Suite, Dell P2319H Monitor, Device Manager.
Test Execution Steps	1. TOE was powered off. USB analyzer software was running, and USB sniffer was connected.

	2. User connected each unauthorized device to the USB sniffer. 3. TOE was powered on. Device was rejected. 4. Device disconnect then reconnected. 5. Device was rejected. 6. Devices remained rejected through USB hub. 7. Device was rejected.
Pass/Fail Explanation	TOE ports properly reject unauthorized devices and devices with unauthorized protocols as per the unauthorized peripheral device connections. The Evaluator confirms that the devices listed in step 2 were all properly rejected.
Units Tested	SK4ID-4TR
Result	PASS

6.19 FDP_PDC_EXT.1 Test 2-KM

Item	*Data/Description*
Test ID	*FDP_PDC_EXT.1/KM – Test 2*
Objective	Test 2-KM: The evaluator shall verify that the TOE KM ports do not reject authorized devices and devices with authorized protocols as per the authorized peripheral device connections. Repeat this test for each of the following four device types: • Barcode reader; • Keyboard or Keypad; • Mouse, Touchscreen, Trackpad, or Trackball; and • PS/2 to USB adapter (with a connected PS/2 keyboard or mouse). Step 1: Configure the TOE and the Operational Environment in accordance with the operational guidance. Run an instance of a text editor on a connected computer. Step 2: Ensure the TOE is powered off. Step 3: Connect the authorized device to the TOE peripheral interface. Step 4: Power on the TOE. Verify the TOE user indication described in the operational user guidance is not present. Step 5: Ensure the connected computer is selected and send inputs using the authorized devices. Verify that the input is received into the text editor or on the screen of the connected computer. Step 6: Disconnect the authorized device, and then reconnect it to the TOE KM peripheral device interface. Step 7: Verify the TOE user indication described in the operational user guidance is not present. Step 8: Send inputs using the authorized devices. Verify that the input is received into the text editor or on the screen of the connected computer.

Notes	• The evaluator has tested two computer ports at a time, then moved the test computers over to two other ports and repeated this process until all switch port combinations have been tested. The evaluator confirms that all computer ports on the switch (#1, #2, #3 and #4) were all tested. No activity was observed on any non-connected PC. • Testing was performed using both the TOE front panel and then the WR40-4R remote control.
Testbed	#1
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Notepad, Netum USB Barcode Reader, PS/2 to USB Adapter, Perixx Optical PS/2 Mouse, Dell P2319H Monitor.
Test Execution Steps	1. TOE was configured, text editor application was running on connected computer. 2. TOE was powered off. 3. User connected each authorized device throughout test. 4. TOE was powered on. User indication was not present. 5. Input from authorized device is present via text editor. 6. Authorized device was connected to TOE KM port. 7. User indication was not present. 8. Input from the authorized device was present via text editor.
Pass/Fail Explanation	The TOE KM ports do not reject authorized devices and devices with authorized protocols as per the authorized peripheral device connections. The evaluator has confirmed that authorized devices were accepted by the TOE.
Units Tested	SK4ID-4TR
Result	PASS

6.20 FDP_PDC_EXT.1 Test 1-VI

Item	*Data/Description*
Test ID	*FDP_PDC_EXT.1 – Test 1*
Objective	Test 1-VI: The evaluator shall verify that the TOE ports do not reject authorized devices and devices with authorized protocols as per the Peripheral Device Connections appendix in MOD_VI_V1.0. Repeat this test for each of the selected protocols in FDP_PDC_EXT.3.1/VI: Step 1: Connect the authorized device with an authorized protocol directly to a computer. Display any image on the device. Disconnect the device from the computer. Step 2: Configure the TOE and the Operational Environment in accordance with the operational guidance. Step 3: Ensure the TOE is powered off. Step 4: Connect the authorized device with an authorized protocol to the TOE peripheral interface. Step 5: Power on the TOE and verify the TOE user indication described in the operational user guidance is not present.

	Step 6: Ensure the connected computer is selected and verify that the device displays the same image as in step 1. Step 7: Disconnect the authorized device, then reconnect it to the TOE peripheral interface. Step 8: Verify the TOE user indication described in the operational user guidance is not present. Step 9: Verify that the device displays the same image as in step 1 and 6.
Notes	• The evaluator has tested two computer ports at a time, then moved the test computers over to two other ports and repeated this process until all switch port combinations have been tested. The evaluator confirms that all computer ports on the switch (#1, #2, #3 and #4) were all tested. No activity was observed on any non-connected PC. • Testing was performed using both the TOE front panel and then the WR40-4R remote control.
Testbed	#1
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor.
Test Execution Steps	1. Authorized device with authorized protocol was connected directly to computer. 2. TOE was configured in accordance with the operational guidance. 3. TOE was fully powered off. 4. Authorized device with an authorized protocol was connected to TOE peripheral interface. 5. User indication was not present. 6. Same image as step 1 is displayed. 7. Authorized device reconnected to the TOE peripheral interface. 8. User indication was not present. 9. Same image as step 1 and 6 is present.
Pass/Fail Explanation	The evaluator confirms that the TOE ports do not reject authorized devices and devices with authorized protocols as per the Peripheral Device Connections appendix in MOD_VI_V1.0.
Units Tested	SK4ID-4TR / WR40-4R
Result	PASS

6.21 FDP_PDC_EXT.2/KM Test 1

Objective	Testing of this component is performed through evaluation of FDP_PDC_EXT.1 Test 2 as specified in section 2.2.2.2 above. (See FDP_PDC_EXT.1.)
Evaluator Findings	Not Applicable. See FDP_PDC_EXT.1.
Verdict	Not Applicable/Pass

6.22 FDP_PDC_EXT.2/VI Test 1

Objective	Testing of this component is performed through evaluation of FDP_PDC_EXT.1 as specified in section 2.2.1.2 above. (See FDP_PDC_EXT.1.)

Evaluator Findings	Not Applicable. See FDP_PDC_EXT.1.
Verdict	Not Applicable/Pass

6.23 FDP_PDC_EXT.3/KM Test 1

Objective	Test activities for this SFR are covered under FDP_APC_EXT.1 tests 1-KM and 3-KM.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

6.24 FDP_PDC_EXT.3/VI Test 1

Objective	Testing of this component is performed through evaluation of FDP_APC_EXT.1 as specified in section 2.2.1.1 above.
Evaluator Findings	Not Applicable. See FDP_APC_EXT.1/VI/
Verdict	Not Applicable/Pass

6.25 FDP_RDR_EXT.1 Test 1

Item	*Data/Description*
Test ID	*FDP_RDR_EXT.1 – Test 1*
Objective	The evaluator shall use a BadUSB, programmable keyboard, and/or USB Rubber Ducky as a malicious USB device to perform the following test: Step 1: Ensure the TOE and the Operational Environment are configured in accordance with the operational guidance. Ensure the TOE is powered off and connect a USB sniffer between the TOE and a computer. Open the real-time hardware information console. Step 2: Configure the malicious USB device as a HID-class device and to re-enumerate as a mass storage device. Step 3: Connect the malicious USB device to the TOE KM peripheral interface. Step 4: Power on the TOE and activate the re-enumeration after 1 minute. Step 5: Verify device rejection per TOE guidance, the cessation of traffic passed in the USB sniffer, and the absence of the device and any new devices in the information console. Step 6: Remove the malicious USB device and reconfigure as a HID-class device and to re-enumerate as a mass storage device. Step 7: Connect the malicious USB device to the TOE KM peripheral interface and activate the reenumeration after 1 minute.

	Step 8: Verify device rejection per TOE guidance, the cessation of traffic passed in the USB sniffer, and the absence of the device and any new devices in the information console.
Notes	• The evaluator has tested two computer ports at a time, then moved the test computers over to two other ports and repeated this process until all switch port combinations have been tested. The evaluator confirms that all computer ports on the switch (#1, #2, #3 and #4) were all tested. No activity was observed on any non-connected PC. • Testing was performed using both the TOE front panel and then the WR40-4R remote control.
Testbed	#1
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Teledyne Lecroy USB Sniffer, Device Manager, HSL BADUSB, Teledyne Lecroy USB Protocol Suite, Dell P2319H Monitor.
Test Execution Steps	1. TOE was powered off. USB sniffer was configured correctly, and hardware information console was open. 2. USB device was configured correctly. 3. USB Device was connected to peripheral interface. 4. TOE was powered on. 5. Device did not appear in hardware information console. 6. USB device was configured correctly. 7. USB Device was connected to peripheral interface. 8. Device did not appear in hardware information console.
Pass/Fail Explanation	The evaluator configured the USB device, verified device rejection and verified the TOE is properly enforcing security protocols.
Units Tested	SK41D-4TR
Result	PASS

6.26 FDP_RIP_EXT.1 Test 1

Objective	There are no test Evaluation Activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

6.27 FDP_RIP.1/KM Test 1

Objective	There are no test EAs for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

6.28 FDP_RIP_EXT.2 Test 1

Item	*Data/Description*
Test ID	*FDP_RIP_EXT.2 – Test 1*

Objective	Step 1: Perform the TOE memory purge or restore factory defaults according to the guidance and verify that the TOE enters a desirable secure state. Step 2: The evaluator shall check that the log record is not deleted if a logging function is supported by the TOE.
Notes	• Testing was performed using both the TOE front panel and then the WR40-4R remote control.
Testbed	#1
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor.
Test Execution Steps	1. Log into the TOE using administrative credentials and password. 2. Under the main operation page, select option "5" for reset to factory defaults. 3. The TOE will begin the process of resetting to factory defaults.
Expected Output	1. Logged into TOE using administrative credentials and password. 2. Select the correct menu to bring up reset to factory defaults. 3. The TOE will begin the process of resetting to factory defaults.
Execution Output	1. The evaluator performed a reset to factory defaults according to guidance and verified that the TOE entered a secure state. 2. The evaluator confirmed that the One-time programmable, critical, and non-critical logging functions were not deleted as a result of the memory purge.
Pass/Fail Explanation	The evaluator confirms that the TOE provides a restore factory default setting feature and correctly restores the state of the TOE.
Units Tested	SK41D-4TR
Result	PASS

6.29 FDP_SWI_EXT.1 Test 1

Objective	There are no test Evaluation Activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

6.30 FDP_UDF_EXT.1/KM Test 1

Objective	Test activities for this SFR are covered under FDP_APC_EXT.1 test 3-KM.
Evaluator Findings	Not Applicable
Verdict	Not Applicable

6.31 FDP_UDF_EXT.1/VI Test 1

Objective	This component is evaluated through evaluation of FDP_APC_EXT.1 as specified in section 2.2.1.1 above.
Evaluator Findings	Not Applicable. See FDP_APC_EXT.1.
Verdict	Not Applicable/Pass

6.32 FMT_MOF.1 Test 1

Item	*Data/Description*
Test ID	*FMT_MOF.1 – Test 1*
Objective	Step 1: Set up the TOE to enable administrator access per applicable TOE administrative guidance. Verify that the TOE is in factory default format. Step 2: Attempt to set the initial administrator user name and password. Step 3: Logon as a valid administrator and perform all authorized administrative functions to assure the logon was successful. Step 4: Log off from the TOE. Step 5: Attempt to logon with an incorrect administrator name. Verify that the logon is failing as expected and that administrative functions are unavailable. Step 6: Attempt to access administrative functions while there is no logged on administrator. Verify that all attempts fail. Step 7: If the TOE provides multiple administrative roles, repeat this test for each defined role to ensure that the authorizations for each role are consistent with what is described in the operational guidance.
Notes	• Testing was performed using both the TOE front panel and then the WR40-4R remote control.
Testbed	#1
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor.
Test Execution Steps	1. TOE was set to enable administrator access; TOE was in factory default format. 2. Initial administrator username and password was set. 3. Logged in as an administrator and performed all authorized administrative functions. 4. Logged off from the TOE. 5. Attempted to logon with incorrect administrator name. Administrative functions were unavailable, and logon fails. 6. Attempted to access administrator functions with no logged-on administrator, attempts to do so fail. 7. Repeated the test using multiple administrator roles. The authorizations for each role were consistent with that is described in the operational guidance.
Pass/Fail Explanation	The evaluator confirms that the administrative functions described in FMT_MOF.1.1 are only available to identified administrator.

Units Tested	SK41D-4TR
Result	PASS

6.33 FMT_SMF.1 Test 1

Item	*Data/Description*
Test ID	*FMT_SMF.1 – Test 1*
Objective	The evaluator shall test the TOE's ability to provide the management functions by configuring the TOE and testing each option assigned from above. The evaluator is expected to test these functions in all the ways in which the ST and guidance documentation state the configuration can be managed.
Notes	• Testing was performed using both the TOE front panel and then the WR40-4R remote control.
Testbed	#1
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor.
Test Execution Steps	1. Logged into TOE using administrative credentials and password 2. The evaluator was presented with different administrative function options. 3. The "reset to factory default" management function was present and resets the TOE to factory default settings. 4. The evaluator was presented with different administrative function options. 5. The "create administrate account" management function was present and created an administrative account on the TOE. 6. The evaluator was presented with different administrative function options. 7. The "change password" management function was present and changed the password for the selected administrator.
Pass/Fail Explanation	The evaluator confirms that the TOE provides management functions described in the ST and guidance documents and has tested each option accordingly.
Units Tested	SK41D-4TR
Result	PASS

6.34 FPT_NTA_EXT.1 Test 1

Objective	There are no test Evaluation Activities for this component.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

6.35 FPT_PHP.1 Test 1

Item	*Data/Description*
Test ID	*FPT_PHP.1 – Test 1*
Objective	The evaluator shall verify, for each tamper evident seal or label affixed to the TOE enclosure and TOE remote controller (if applicable), that any attempts to open the enclosure or remove the seal results in the seal being damaged in a manner that is consistent with the operational user guidance.

Notes	• The evaluator confirms that the test execution steps were performed on all the units detailed in the units tested section. The same execution output was observed for each model tested.	
Testbed	#1	
Test Equipment Used	N/A	
Test Execution Steps	1. Removed the tamper evident seals from the TOE.	
Pass/Fail Explanation	The evaluator confirms that any attempt to open the enclosure or remove the seal results in the seal being damaged in a manner that is consistent with the operational user guidance.	
Units Tested	SK41D-4TR	WR40-4R
Result	PASS	PASS

6.36 FPT_PHP.1 Test 2

Item	*Data/Description*	
Test ID	*FPT_PHP.1 – Test 2*	
Objective	The evaluator shall verify that it is not possible to administratively disable or otherwise prevent the display of any tampering indicators.	
Notes	• The evaluator confirms that the test execution steps were performed on all the units detailed in the units tested section. The same execution output was observed for each model tested.	
Testbed	#1	
Test Equipment Used	N/A	
Test Execution Steps	1. Attempt to remove the tamper evident seals from the TOE without damaging the tampering indicators.	
Pass/Fail Explanation	The evaluator confirms that it is not possible to administratively disable or otherwise prevent the display of any tampering indicators.	
Units Tested	SK41D-4TR	WR40-4R
Result	PASS	PASS

6.37 FPT_PHP.3 Test 1

Item	*Data/Description*
Test ID	*FPT_PHP.3 – Test 1*
Objective	In the following testing the evaluator shall attempt to gain physical access to the TOE internal circuitry (enough access to allow the insertion of tools to tamper with the internal circuitry). The TOE anti- tampering function is expected to trigger, causing an irreversible change to the TOE functionality. The evaluator then shall verify that the anti-tampering triggering provides the expected user indications and also disables the TOE. TOE disabling means that the user would not be able to use the TOE for any purpose – all peripheral devices and computers are isolated. Note that it is obvious that if the TOE was physically tampered with, then the attacker may easily circumvent the tamper indication means (for example cut the relevant TOE front panel wires). Nevertheless, the following test verifies that the

	user would be unable to ignore the TOE tampering indications and resume normal work. The evaluator shall perform the following steps: Step 1: [conditional: this step is applicable for TOEs having a remote controller] The evaluator shall attempt to open the PSD remote controller enclosure enough to gain access to its internal circuitry and observe that the TOE is both permanently disabled and provides the proper indication that it has been tampered with in accordance with the operational user guidance. Step 2: The evaluator shall attempt to open the PSD enclosure enough to gain access to its internal circuitry and observe that the TOE is both permanently disabled and provides the proper indication that it has been tampered with in accordance with the operational user guidance. Step 3: The evaluator shall attempt to access the TOE settings to reset the tampering state and verify that it is not possible to recover from the tampered state. Step 4: The evaluator shall acquire a copy of the TOE that has been previously tampered with. Step 5: The evaluator shall power on the TOE and verify that the tampering indicator is displayed.
Notes	• Testing was performed using both the TOE and then the WR40-4R remote control. • TD0583 applied. • Testing of the WR40-4R remote control was completed with and without the unit connected to SK41D-4TR switch. Testing was also completed with the remote control powered on and then the remote control disconnected from the power source. The remote-control anti-tampering functionality is independently powered by the anti-tampering battery contained within the device (base unit or remote). Therefore, any triggering of the anti-tampering switch on the remote will result in rendering the remote control unusable regardless of power state (Connected to SK41D-4TR or WR40-4R independently tested). The evaluator confirms the result for each different test scenario all result in a PASS.
Testbed	#1
Test Equipment Used	N/A

Test Execution Steps	1. Remote controller displayed proper indications that unit has been tampered with. 2. Removed tamper proof seals from PSD, the seals showed “VOID” to indicate the unit had been tampered with. Once PSD had been opened the anti-tampering mechanism released and rendered the unit permanently disabled. 3. Attempted to reset the tampering state, could not recover the PSD from tampered state. 4. Evaluator has acquired a copy of the TOE that has been previously tampered with. 5. Tampering indicator on TOE is displayed, unit is rendered permanently disabled.	
Pass/Fail Explanation	The evaluator confirms that the anti-tampering triggering provides the expected user indications and disables the TOE.	
Units Tested	SK41D-4TR	WR40-4R
Result	PASS	PASS

6.38 FPT_STM.1

Objective	There are no tests for FPT_STM.1
Pass/Fail Explanation	Tested with FAU_GEN.1
Verdict	Not Applicable/PASS

6.39 FPT_TST.1 Test 1

Item	*Data/Description*
Test ID	*FPT_TST.1 – Test 1*
Objective	The evaluator shall trigger the conditions specified in the TSS that are used to initiate TSF self-testing and verify that successful completion of the selftests can be determined by following the corresponding steps in the operational guidance. 1. The TOE must be powered off, ensure the power cable is removed from the TOE before proceeding. 2. The evaluator will connect the power cable to the TOE and observe the TOE performs a start-up self-test diagnostic for the following criteria: o Verification of the front panel push buttons o Verification of the active anti-tampering functionality o Verification of the integrity of the microcontroller firmware o Verification of computer port isolation 3. Upon completion of the self-testing diagnostic the TOE will power on into operational mode and channel 1 will be selected by default.

Notes	• The evaluator has tested two computer ports at a time, then moved the test computers over to two other ports and repeated this process until all switch port combinations have been tested. The evaluator confirms that all computer ports on the switch (#1, #2, #3 and #4) were all tested. No activity was observed on any non-connected PC. • Testing was performed using both the TOE front panel and then the WR40-4R remote control
Testbed	#1
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor.
Test Execution Steps	1. The TOE was powered off, the power cable was removed from the TOE before proceeding. 2. The evaluator connected the power cable to the TOE and observed the TOE perform a start-up self-test diagnostic for the following criteria: o Verification of the front panel push buttons o Verification of the active anti-tampering functionality o Verification of the integrity of the microcontroller firmware o Verification of computer port isolation 3. Upon completion of the self-testing diagnostic the TOE powered into operational mode and channel 1 was selected by default.
Pass/Fail Explanation	The evaluator confirms that that successful completion of the self-tests can be determined by following the corresponding steps in operational guidance.
Units Tested	SK41D-4TR / WR40-4R
Result	PASS

6.40 FPT_TST_EXT.1 Test 1

Item	*Data/Description*
Test ID	*FPT_TST_EXT.1 – Test 1*
Objective	The evaluator shall cause a TOE self-test failure and verify that the TOE responds by disabling normal functions and provides proper indications to the user. 1. The TOE must be powered off, ensure the power cable is removed from the TOE before proceeding. 2. Firmly press any of the front panel buttons on the TOE while simultaneously plugging in the power cable. This will cause the unit to enter a Self-test failure mode where the TOE will be powered on, but unusable. The front panel lights will continue to cycle between the computers connected but the TOE remains inoperable. 3. The evaluator shall ensure no video/keyboard/mouse is being output from the TOE while it is in self-test failure state.
Notes	• The evaluator has tested two computer ports at a time, then moved the test computers over to two other ports and repeated this process until all switch port combinations have been tested. The evaluator confirms that all computer ports on the switch (#1, #2, #3 and #4) were all tested. No activity was observed on any non-connected PC. • Testing was performed using both the TOE front panel and then the WR40-4R remote control

Testbed	#1
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor.
Test Execution Steps	1. TOE was powered off; cable was unplugged from back of TOE. 2. The TOE powered on in self-test failure mode, providing visual indication by cycling through the LED computer channels on the front panel display 3. No video, keyboard or mouse was usable or visible while TOE was in self-test failure state.
Pass/Fail Explanation	The evaluator confirms that the TOE does perform a self-test failure and that the TOE responds by disabling normal functions and provides proper indications to the user.
Units Tested	SK41D-4TR
Result	PASS

6.41 FTA_CIN_EXT.1 Test 1

Item	*Data/Description*
Test ID	*FTA_CIN_EXT.1 – Test 1*
Objective	Step 1: The evaluator shall configure the TOE and its operational environment in accordance with the operational user guidance. Step 2: The evaluator shall select a connected computer and power down the TOE, then power up the TOE and verify that the expected selected computer is indicated in accordance with the TSS and that the connection is active. Step 3: The evaluator shall repeat this process for every possible selected TOE configuration. Step 4: [Conditional] If "upon reset button activation" is selected in FPT_TST.1.1, then the evaluator shall repeat this process for each TOE configuration using the reset function rather than power-down and powerup. Step 5: The evaluator shall verify that the TOE selected computer indications are always on (i.e., continuous) and fully visible to the TOE user. Step 6: [Conditional] If the TOE allows peripherals to have active interfaces with different computers at the same time, the evaluator shall verify that each permutation has its own selection indications. Step 7: [Conditional] If "a screen with dimming function" is selected, the evaluator shall verify that indications are visible at minimum brightness settings in standard room illumination conditions. Step 8: [Conditional] If "multiple indicators which never display conflicting information" is selected, the evaluator shall verify that either all indicators reflect the same status at all times, or the indicator for the most recently used switching mechanism displays the correct switching status and that all other indicators display the correct status or no status.

Notes	• The evaluator has tested two computer ports at a time, then moved the test computers over to two other ports and repeated this process until all switch port combinations have been tested. The evaluator confirms that all computer ports on the switch (#1, #2, #3 and #4) were all tested. No activity was observed on any non-connected PC. • Testing was performed using both the TOE front panel and then the WR40-4R remote control
Testbed	#1
Test Equipment Used	Dell Wired Keyboard, Dell Wired Mouse, Dell P2319H Monitor.
Test Execution Steps	1. The TOE and its operational environment have been configured in accordance with the operational user guidance. 2. A computer was selected, then the TOE was powered down. The TOE was then powered up and the evaluator verified that the expected selected computer was indicated in accordance with the TSS and that the connection was active. 3. This process was repeated for every possible selected TOE configuration. 4. "U*pon reset button activation*" was not selected in FPT_TST.1.1, therefore this step was not tested. 5. The selected computer indications on the TOE were always on and fully visible to the TOE user. 6. The TOE allowed peripherals to have active indications with different computers at the same time. 7. The TOEs indicators were visible at minimum brightness settings in standard room illumination conditions. 8. The indicators always reflect the same status, or the indicator for the most recently used switching mechanism displays the correct switching status and that all other indicators display the correct status or no status.
Pass/Fail Explanation	The evaluator confirms the TOE properly indicates which computer connection is active on TOE power up. The evaluator also verifies the behavior of all indicators when each switching mechanism is in use, and that no conflicting information is displayed by any indicators.
Units Tested	SK41D-4TR / WR40-4R
Result	PASS

7 Security Assurance Requirements

7.1 ADV_FSP.1 Basic Functional Specification

7.1.1 ADV_FSP.1

7.1.1.1 ADV_FSP.1 Activity 1

Objective	There are no specific Evaluation Activities associated with these SARs. The Evaluation Activities listed in this PP are associated with the applicable SFRs; since these are directly associated with the SFRs, the tracing element ADV_FSP.1.2D is implicitly already done, and no additional documentation is necessary. The functional specification documentation is provided to support the evaluation activities described in Section 5.2 and other activities described for AGD, and ATE SARs. The requirements on the content of the functional specification information are implicitly assessed by virtue of the other Evaluation Activities being performed. If the evaluator is unable to perform an activity because there is insufficient interface information, then an adequate functional specification has not been provided.
Evaluator Findings	Sufficient interface information was available to perform the evaluation activities.
Verdict	Pass

7.2 AGD_OPE.1 Operational User Guidance

7.2.1 AGD_OPE.1

7.2.1.1 AGD_OPE.1 Activity 1

Objective	The operational user guidance does not have to be contained in a single document. Guidance to users and Administrators can be spread among documents or web pages. The developer should review the Evaluation Activities contained in Section 5.2 of this PP to ascertain the specifics of the guidance for which the evaluator will be checking. This will provide the necessary information for the preparation of acceptable guidance.
Evaluator Findings	The evaluator examined the guidance documents to perform this evaluation. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

7.3 AGD_PRE.1 Preparative Procedures

7.3.1 AGD_PRE.1

7.3.1.1 AGD_PRE.1 Activity 1

Objective	As with the operational user guidance, the developer should look to the Evaluation Activities contained in Section 5.2 of this PP to determine the required content with respect to preparative procedures.
Evaluator Findings	The evaluator examined the guidance documents to perform this evaluation. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

7.4 ALC Assurance Activities

7.4.1 ALC_CMC.1

7.4.1.1 ALC_CMC.1 Activity 1

Objective	The "evaluation evidence required by the SARs" in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring that the TOE is specifically identified and that this identification is consistent in the ST and in the AGD guidance, the evaluator implicitly confirms the information required by this component.
Evaluator Findings	The ST was used to determine the identification of the TOE. This was also corroborated by the identification in the TOE user guidance documents. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

7.4.2 ALC_CMS.1

7.4.2.1 ALC_CMS.1 Activity 1

Objective	Given the scope of the TOE and its associated evaluation evidence requirements, this component's Evaluation Activities are covered by the Evaluation Activities listed for ALC_CMC.1.
Evaluator Findings	Not Applicable
Verdict	Not Applicable/Pass

7.5 ATE_IND.1 Independent Testing – Conformance

7.5.1 ATE_IND.1

7.5.1.1 ATE_IND.1 Activity 1

Objective	The evaluator shall prepare a test plan and report documenting the testing aspects of the system. The test plan covers all of the testing actions contained in the CEM and the body of this PP's Evaluation Activities. While it is not necessary to have one test case per test listed in an Evaluation Activity, the evaluator must document in the test plan that each applicable testing requirement in the PP is covered. The test plan identifies the platforms to be tested, and for those platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification must address the differences between the tested platforms and the untested platforms and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no affect; rationale must be provided. If all platforms claimed in the ST are tested, then no rationale is necessary. The test plan describes the composition of each platform to be tested and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluator is expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test equipment or tools. For each piece of equipment or tool, an argument (not just an

	assertion) should be provided that the equipment or tool will not adversely affect the performance of the functionality by the TOE and its platform. The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include expected results. The test report (which could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a "fail" and "pass" result (and the supporting details), and not just the "pass" result.
Evaluator Findings	The evaluator created a test plan and executed all the tests in the test plan. The results of all the testing are included in the test plan. Based on this document, this evaluation activity is considered satisfied.
Verdict	Pass

7.6 AVA_VAN.1 Vulnerability Survey

7.6.1 AVA_VAN.1

7.6.1.1 AVA_VAN.1 Activity 1

Objective	As with ATE_IND, the evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to determine the vulnerabilities that have been found in peripheral sharing devices and the implemented communication protocols in general, as well as those that pertain to the particular TOE. The evaluator documents the sources consulted and the vulnerabilities found in the report. For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability. If exploiting the vulnerability requires expert skills and an electron microscope, for instance, then a test would not be suitable and an appropriate justification would be formulated.
Evaluator Findings	The evaluators documented their analysis and testing of potential vulnerabilities with respect to this requirement. Public searches were performed against all keywords found within the Security Target and AGD that may be applicable to specific TOE components. This included several combinations of the following words websites are several combinations of the following words: SK41D-4TR, WR40-4R, HighSecLabs, Firmware 44404-E7E7, NAK transaction, SYNC Signal, HPD signal, EDID traffic, ARC Signal, HDCP signal and USB HID traffic and STMicroelectronics 32-Bit. The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below. 1. Check National Vulnerability Database: https://nvd.nist.gov/vuln/search 2. Check High Security Labs Support: http://www.highseclabs.com/support/ Check Common Vulnerabilities and Exposures: https://google.com The search was performed on August 27, 2021.

	The evaluation team found no vulnerabilities were applicable to the TOE version or hardware. Based on these findings, this evaluation activity is considered satisfied.
Verdict	Pass

8 Conclusion

The testing shows that all test cases required for conformance have passed testing.

9 Evaluation Evidence

- [ASE] High Sec Labs SK41D-4TR KVM Firmware Version 44404-E7E7 Security Target, v1.7, September 14, 2021
- [Isol] High Sec Labs SK41D-4TR KVM Firmware Version 44404-E7E7 Isolation Document, Version 0.3, October 7, 2020
- [CC_Supp] High Sec Labs SK41D-4TR KVM Firmware Version 44404-E7E7 Common Criteria Guidance Supplement, Version 0.5, September 14, 2021
- [23220] HSL Quick Installation Guide 4 Ports Secure Ruggedized DVI-D KVM Switch, HDC23220 Rev 1.2
- [Admin] HSL Administrator Guide, HDC19968, Rev. C
- [Testplan] Test Report for SK41D-4TR KVM Firmware Version 44404-E7E7, version 1.2, August 27, 2021

10 References

- [PP_PSD_V4.0] Protection Profile for Peripheral Sharing Device, July 19, 2019
- [MOD_KM_V1.0] PP-Module for Keyboard/Mouse Devices, July 19, 2019
- [MOD_VI_V1.0] PP-Module for Video/Display Devices, July 19, 2019
- [CFG_PSD_KM-VI_v1.0] PP-Configuration for Peripheral Sharing Device, Keyboard/Mouse Devices and Video/Display Devices, July 19, 2019

End of Document