Thinklogical

TLX160 Matrix Switch
Security Target

Document Version 1.7

Prepared by Thinklogical

Table of Contents

1 Security Target Introduction

1.1 Security Target and TOE Identification

Security Target Title: Thinklogical TLX160 Matrix Switch

Security Target

ST Author: Thinklogical

TOE Identification: TLX160 Matrix Switch Chassis (TLX-MSC-000160 Rev B)

Assessment

NOTE: Base Chassis “Thinklogical KVM Matrix Switch (TLX160 Matrix Switch Rev B)” consists of the following:

TLX160 Matrix Switch Module Controller Card, (TLX-MSM-C00160 Rev B) – qty 1
Software revision is SFT-TLX160-15 [TLX160 FIRMWARE VERSION V 5.10.03]
FPGA Firmware revision is FLX-C00160-002 [TLX160 FIRMWARE VERSION 0x100F]
iMX6 Processor Board, (DCSA000081 Rev C) - qty 1
TLX160 Matrix Switch Module Fan Tray, (TLX-MSM-F00160 Rev B) – qty 1
TLX160 Matrix Switch Module Power Supply, (TLX-MSM-P00160 OEM / No Rev) – qty 2

NOTE: The Assessment for the TOE will include the following so as to configure the system for redundancy.

Additional TLX160 Matrix Switch Module Controller Card, (TLX-MSM-C00160 Rev B) – qty 1
Software revision is SFT-TLX160-15 [TLX160 FIRMWARE VERSION V 5.10.03]
FPGA Firmware revision is FLX-C00160-002 [TLX160 FIRMWARE VERSION 0x100F]
Additional iMX6 Processor Board, (DCSA000081 Rev C) - qty 1

TLX160 Matrix Switch Data Input and Output Card, 10 Ports, SFP+, 10G
Multi-Mode (TLX-MSD-M00010 Rev A), Single Mode (TLX-MSD-S00010 Rev A),
Unpopulated (TLX-MSD-000010 Rev A)

TLX160 Matrix Switch Data Input and Output Card, 10 Ports, SFP+, 6G
Multi-Mode (TLX-MSD-MV0010 Rev A), Single Mode (TLX-MSD-SV0010 Rev A)

Common Criteria Version: 3.1 Revision 5

Assurance Level: EAL4 + ALC_FLR.2

PP Identification: None

1.2 Security Target Overview

Thinklogical TLX160 Matrix Switch is a fiber optic switch that uses multi-mode or single-mode fiber optics to transmit and receive a digital video pulse stream without alteration or interpretation of the original signal. Embedded keyboard, mouse, USB 1.1, USB 2.0 (high speed up to 480 Mbps), and audio signals are also transmitted. The TLX160 provides reliability and signal integrity with high performance 6.25Gbps and 10.3125Gbps capability. Scalable up to 160 x 160 bi-directional ports, this highly robust KVM Matrix Switch is used with Thinklogical™ Velocity extender series and the Thinklogical™ TLX extender series.

The Switch includes pluggable cards which allow changing the number of supported ports in groups of 10.

The TOE provides remote connections from a set of shared computers to a set of shared peripherals. The switching capability of the TOE is used to connect ports on a particular computer to a particular peripheral set. The corresponding electronic signal from a computer port is transformed into an optical signal by the Velocity and or TLX extender, transmitted through an optical fiber, switched by the KVM Matrix Switch to another optical fiber, and then transformed back to an electronic form by the Velocity and or TLX extender. The resulting signal is used by the shared peripherals.

The TOE provides a capability to dynamically change the switching configuration to connect a particular computer to a particular peripheral set.

The TOE enforces secure separation of information flows corresponding to different switched connections. The corresponding Data Separation Security Policy is the main security feature of the TOE.

The following table outlines the required non-TOE systems or (devices) and their security requirements.

Table 1: System Security Requirements

Device	**Requirement**
Management Device	The management device will be in a secure location and manage TOE by either the LAN or the Serial (RS232) connections that are physically secure.
TLX Transmitter Extender	The TLX transmitter extender will be in a secure location
TLX Receiver Extender	The TLX receive extender will be in a secure location
Velocity Transmitter Extender	The Velocity transmitter extender will be in a secure location
Velocity Receiver Extender	The Velocity receive extender will be in a secure location

1.3 Common Criteria Conformance

Common Criteria Version: 3.1 Revision 5

Common Criteria: Part 2 and Part 3 conformant.

Assurance Level: EAL4 + ALC_FLR.2

1.4 Conventions

The notation, formatting, and conventions used in this ST are consistent with version 3.1 of the Common Criteria (CC). The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Deleted words are denoted by strikethrough text.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *italicized* text.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [Assignment_value].

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration_number).

The CC paradigm also allows protection profile (PP) and security target authors extended components. In this ST, extended components will be indicated with the "_EXT" following the component name.

Assumptions: TOE secure usage assumptions are given names beginning with "A."-- e.g., A.ACCESS.

Threats: Threats are given names beginning with "T."-- e.g., T.COMINT.

Policies: Organizational Security Policies are given names beginning with "P."-- e.g., P.CRYPTOGRAPHY.

Objectives: Security objectives for the TOE and the TOE environment are given names beginning with "O." and "OE.", respectively,—e.g., O.CRYPTOGRAPHY and OE.INSTAL.

User Roles: User Roles are confined to three different types as follows: Administrator, Operator, System user. Details can be found in Section 8.

2 TOE Description

2.1 System Type and Overview

The TOE is a single matrix routing system, which provides connection of 160 optical inputs to any or all of the 160 optical outputs. The TOE consists of 16 Data Input/Output Cards having 10 optical input and Output ports each. The TOE supports any combination of legacy Velocity VX based IO cards or TLX IO cards. The 16 data Input and Output Cards installed can be used to connect any of the 160 inputs, in one direction, to any output or multiple outputs. Any combination of Transmitter Port – forward channel to Receiver Port – forward channel or Receiver Port –back channel to Transmitter Port back channel are supported. Each of the 16 data Input and Output Cards connect to a 160 x 160 switch on the backplane. The TOE allows for remote operation of shared computers using sets of shared peripherals, dynamically connecting (switching) physical ports on a particular computer to a particular shared peripheral set.

The TOE consists of the following hardware devices:

1. Thinklogical KVM Matrix Switch (TLX160 Matrix Switch Rev B)

2. 16 Data Input/Output Cards in any combination of the following:

   TLX160 Matrix Switch Data Input and Output Card, 10 Ports, SFP+, 10G Multi-Mode (TLX-MSD-M00010 Rev A)

   TLX160 Matrix Switch Data Input and Output Card, 10 Ports, SFP+, 10G Single Mode (TLX-MSD-S00010 Rev A)

   TLX160 Matrix Switch Data Input and Output Card, 10 Ports, SFP+, 6G Multi-Mode (TLX-MSD-MV0010 Rev A)

   TLX160 Matrix Switch Data Input and Output Card, 10 Ports, SFP+, 6G Single Mode (TLX-MSD-SV0010 Rev A)

Each Transmitter and Receiver Port Group is composed of two ports: T port and R port. Two optical cables are then required to connect a Velocity and or TLX Transmitter or Receiver Extender to a Transmitter or Receiver Port Group on the Switch. One cable is used to transmit data from the Extender to the Switch; the other cable is used to transmit data from the Switch to the Extender. As a result, a bi-directional connection is established, where data can flow in both directions.
All data types, including video, audio and serial data are converted to an optical form and transmitted in a single optical cable.
The purpose of the Switch is to establish logical connections between Transmitter and Receiver Port Groups, while preserving Data Separation Security Function Policy (SFP).

Data Separation Security Function Policy (SFP) states that data shall flow between Transmitter Port group A and Receiver Port group B if and only if a deliberate logical connection has been established to connect A to B. There shall be no data flow between any pair of Transmitter Port Groups or Receiver Port Groups. There shall be no data flow between Transmitter Port Groups or Receiver Port Groups and any other physical port on the Switch.

The use of a restrict or partition table in the system overrides any deliberate logical connection established between Transmitter Port A and Receiver Port B since the restrict policy disallows connection of a higher priority input to a lower priority output and the partition policy disallows connection of an input from one partition going to the output of another partition.

The use of a P2P table in the system overrides any deliberate multicast logical connection established between more than one transmitter port group. The P2P policy disallows an input from ever being able to go to more than one output.

The TOE connections are first controlled by restrict and priority tables, then controlled by the P2P table and then, if not in conflict with the restrict table or partition table or P2P table, over the serial RS-232/console interface or a wired 10/100/1000BASE-TX LAN connection. The connection over the serial RS-232/console interface or a wired 10/100/1000BASE-TX LAN can be from a management interface/control CPU that is required to be in a secure location and secure network.

The control CPU has no control software on it to setup or break connections or to modify the .csv partition or restrict table files. Instead, the control CPU acts as a terminal emulator on the system controller interfaces as described below.

The connection over the wired 10/100/1000BASE-TX LAN can also be from a management interface/control CPU which has a TLS/ https (FIPS 140) compliant web browser. If the System controller has Thinklogical software called ADM (Thinklogical Administrator) loaded onto it, the System controller will be able to serve up encrypted web pages for only the Administrator to manage the Matrix switch through a secure GUI interface. An Operator or user will not be able to access the ADM.

This control CPU is required to be in a physically secure location and on a secure network.

Access to the system controller interfaces is defined by the user type which is described in section 8 User Roles. Also, refer to Figure 2b below for a Typical TOE installation with user access.

Please note:
For all API interfaces, the command API is described in the document:
Manual_TLX_Matrix_Switch_ASCII_API_V5
For Matrix Switch control card - TLX_Matrix_Switch_ADM_Rev_C.

1) Control CPU connected to API RS-232 port

There is no proprietary software installed or running on the control CPU. The control CPU acts solely as a “Terminal Emulator” when connected to the API RS232 port.

A control CPU connected to the RS232 port does not need to be authenticated and has no access to the system controller operating/file system.

The control CPU can access the API as a “Terminal Emulator” however, there are no API commands that exist which allow any user to log into or access the operating/file system to then affect the .csv files.

Further, the control CPU can generate API commands to setup and break connections but only those allowed in the Restrict and Partition tables.

2) Control CPU connected to Console Port

There is no proprietary software installed or running on the control CPU. The control CPU acts solely as a “Terminal Emulator” when connected to the Console port.

A control CPU connected to the Console port requires two levels of authentication to gain access to the operating/file system and to the .csv files. Please refer to section 8 User Roles for more information.

To gain access to the .csv files, which resides on the TOE system controller card, the following security levels are in place that must be met.

1) An Operator login is required consisting of a user name and password.
2) Then an Administrator login is required consisting of user name and password.
3) The .csv tables can then be accessed and altered but cannot take effect until the system is rebooted.

3) Control CPU connected to Network Interface Port 17567

There is no proprietary software installed or running on the control CPU. The control CPU acts solely as a “Terminal Emulator” when connected to the Network Interface Port 17567.

A control CPU connected to the Network Interface Port 17567 port does not need to be authenticate and has no access to the system controller operating/file system.

The control CPU can access the API as a “Terminal Emulator” however, there are no API commands that exist which allow any user to log into or access the operating/file system to then affect the .csv files.

Further, the control CPU can generate API commands to setup and break connections but only those allowed in the Restrict and Partition tables.

4) Control CPU connected to Network Interface SSH Port 22

There is no proprietary software installed or running on the control CPU. The control CPU acts solely as a “Terminal Emulator” when connected to the Network Interface SSH Port 22

A control CPU connected to the Network Interface SSH Port 22 requires two levels of authentication to gain access to the operating/file system and to the .csv files. Please refer to section 8 User Roles for more information.

To gain access to the .csv files, which resides on the TOE system controller card, the following security levels are in place that must be met.

1) An Operator login is required consisting of a user name and password.
2) Then an Administrator login is required consisting of user name and password.
3) The .csv tables can then be accessed and altered but cannot take effect until the system is rebooted.

5) System control card ADM network interface as webserver HTTPS Port 60087

The System control card ADM can be accessed via a web browser from any control CPU computer on the same network as the System controller ADM web server or via a direct connection.

The System control card ADM port number is **60087**. The administrator can access the ADM web server by setting the browser’s URL to the system controller IP address (for example: https://192.168.13.9**:60087)** to load the login page. Then the Administrator will need to login with username and password to access the system controller administration pages. The Administrator will not be able to access the system controller API, through TLADM, for connection configuration and breakdown.

There is no proprietary software installed or running on the browser control CPU. The browser control CPU acts solely as an “https web client” when connected to the network interface https port 60087.

For the physical interfaces mentioned above, the diagrams below shows all the logical interface running on them.

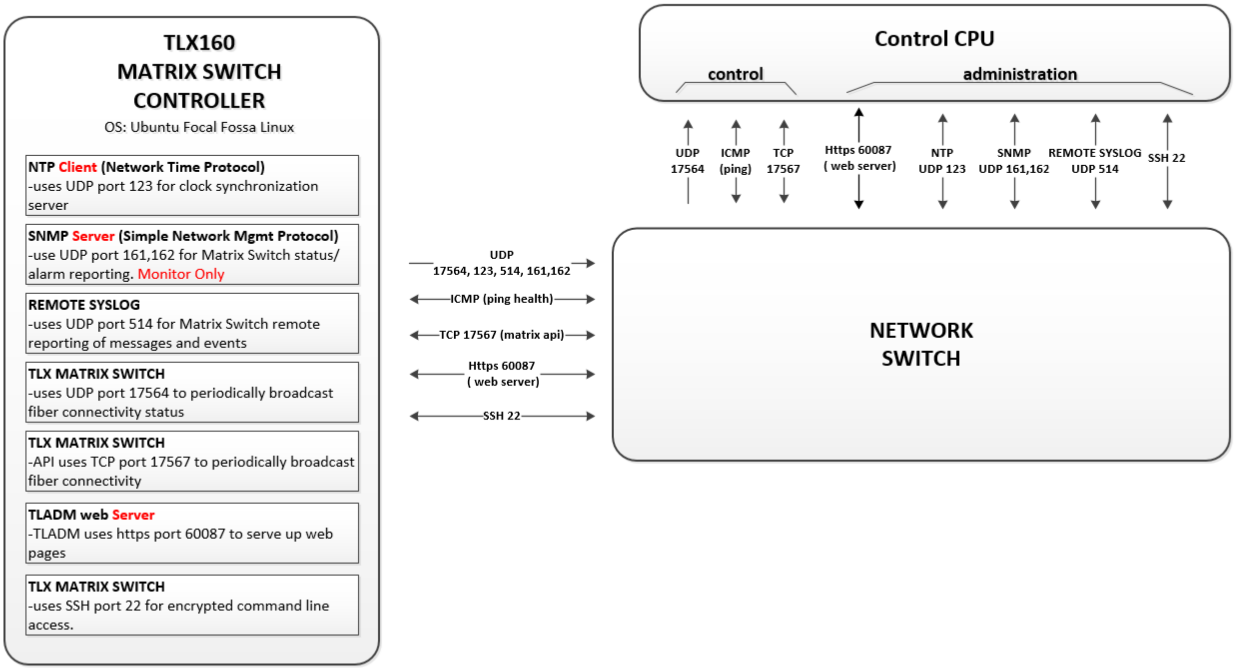
TLX160
MATRIX SWITCH
CONTROLLER
OS: Ubuntu Focal Fossa Linux
NTP Client (Network Time Protocol)
-uses UDP port 123 for clock synchronization server
SNMP Server (Simple Network Mgmt Protocol)
-use UDP port 161,162 for Matrix Switch status/ alarm reporting. Monitor Only
REMOTE SYSLOG
-uses UDP port 514 for Matrix Switch remote reporting of messages and events
TLX MATRIX SWITCH
-uses UDP port 17564 to periodically broadcast fiber connectivity status
TLX MATRIX SWITCH
-API uses TCP port 17567 to periodically broadcast fiber connectivity
TLADM web Server
-TLADM uses https port 60087 to serve up web pages
TLX MATRIX SWITCH
-uses SSH port 22 for encrypted command line access.
UDP
17564, 123, 514, 161,162
ICMP (ping health)
TCP 17567 (matrix api)
Https 60087
(web server)
SSH 22
Control CPU
control
administration
UDP
17564
ICMP
(ping)
TCP
17567
Https 60087
(web server)
NTP
UDP 123
SNMP
UDP 161,162
REMOTE SYSLOG
UDP 514
SSH 22
NETWORK
SWITCH

Figure 1. TLX160 Standard System logical interfaces

The Thinklogical TLX160 Matrix Switch is depicted in **Figure 1a.**

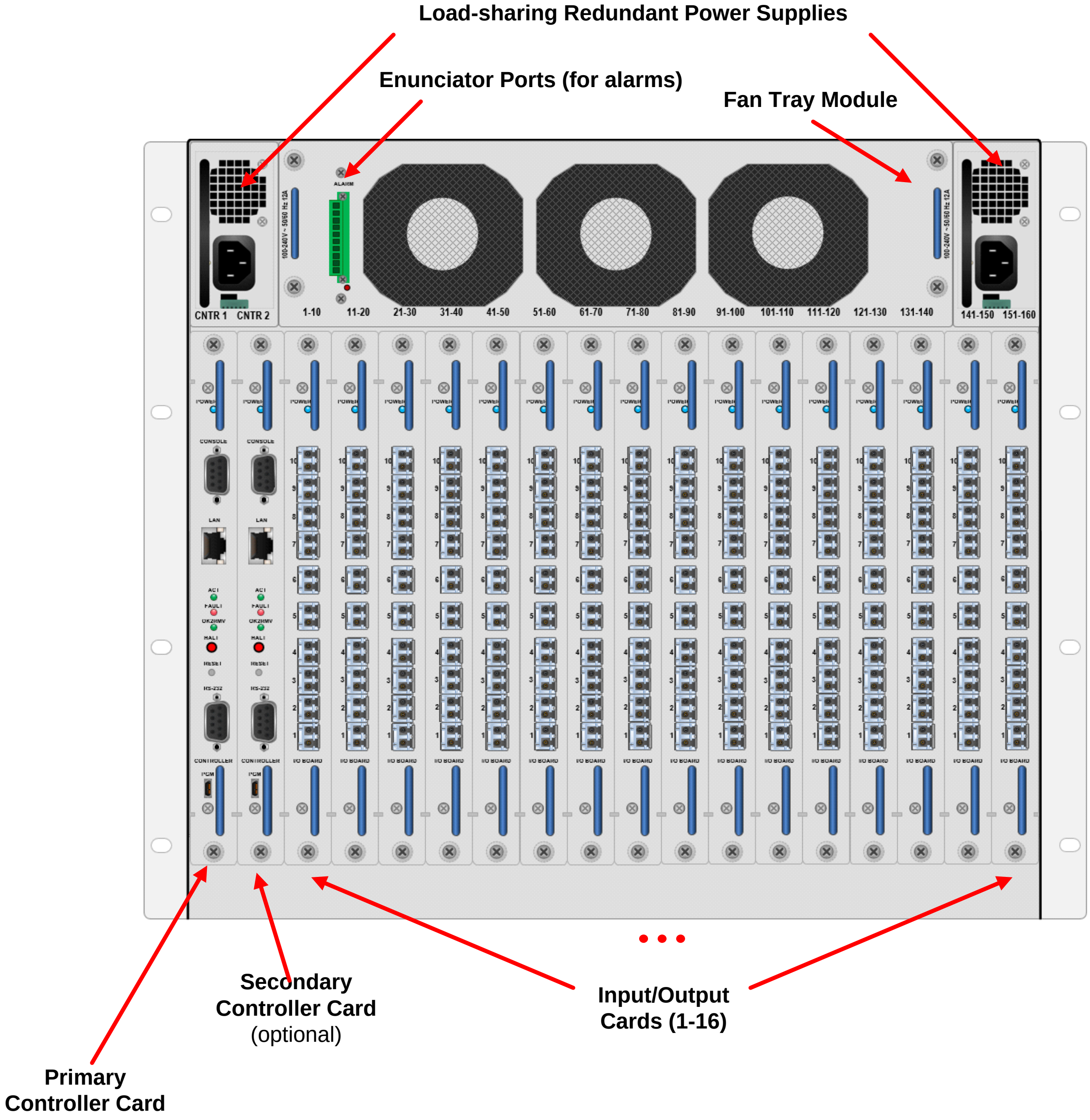

Figure 2a. Thinklogical TLX160 Matrix Switch

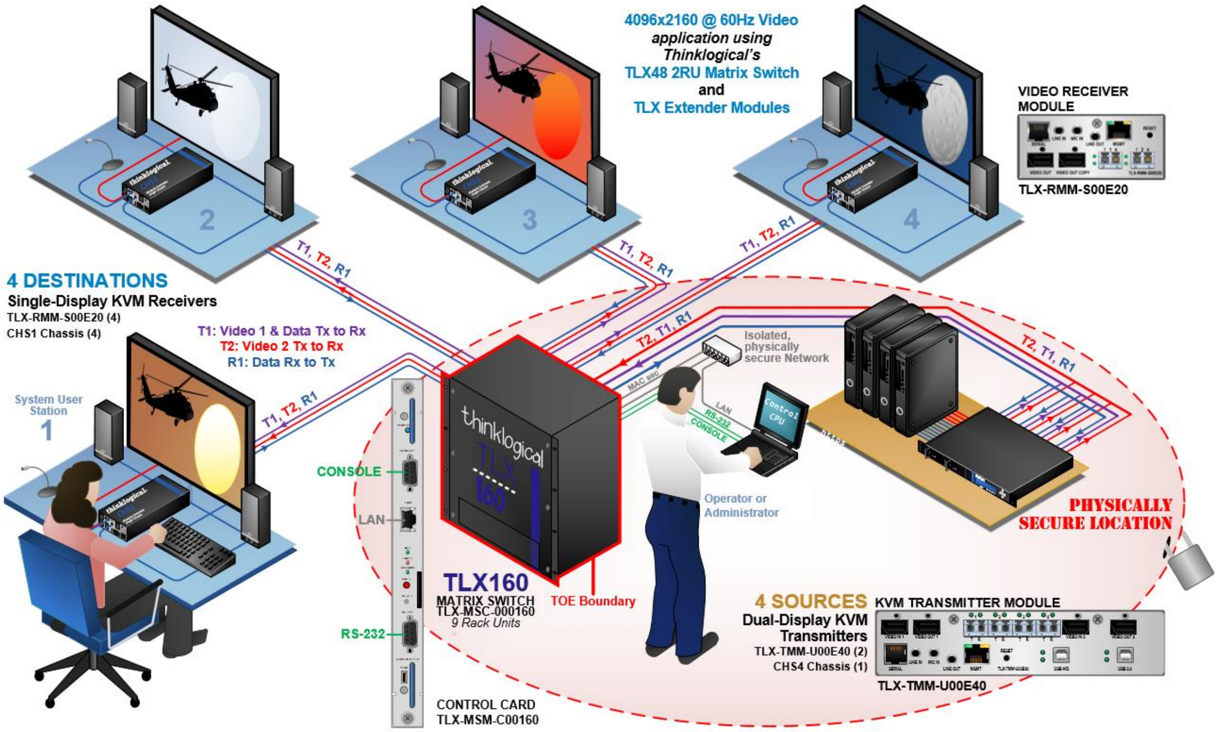

Figure 2b. Typical TOE TL160 Matrix Switch Installation

2.2 TOE Physical Boundaries

TOE Physical scope is as follows.

1) The TLX160 Matrix Switch is a hardware device. TOE Physical Boundaries then correspond to the physical boundaries of the device.

The TOE consists of the following hardware devices:

1. Thinklogical KVM Matrix Switch (TLX160 Matrix Switch Rev B)

   NOTE: Base Chassis “Thinklogical KVM Matrix Switch (TLX160 Matrix Switch Rev B)” consists of
   TLX160 Matrix Switch Module Controller Card, (TLX-MSM-C00160 Rev B) – qty 1
   iMX6 Processor Board, (DCSA000081 Rev C) - qty 1
   TLX160 Matrix Switch Module Fan Tray, (TLX-MSM-F00160 Rev B) – qty 1
   TLX160 Matrix Switch Module Power Supply, (TLX-MSM-P00160 OEM / No Rev) – qty 2
   TLX160 Backplane Board, (XGXA000019 Rev B) – qty 1

2. 16 Data Input/Output Cards in any combination of the following:

   TLX160 Matrix Switch Data Input and Output Card, 10 Ports, SFP+, 10G Multi-Mode (TLX-MSD-M00010 Rev A)

   TLX160 Matrix Switch Data Input and Output Card, 10 Ports, SFP+, 10G Single Mode (TLX-MSD-S00010 Rev A)

   TLX160 Matrix Switch Data Input and Output Card, 10 Ports, SFP+, 10G unpopulated (TLX-MSD-000010 Rev A)

   TLX160 Matrix Switch Data Input and Output Card, 10 Ports, SFP+, 6G Multi-Mode (TLX-MSD-MV0010 Rev A)

   TLX160 Matrix Switch Data Input and Output Card, 10 Ports, SFP+, 6G Single Mode (TLX-MSD-SV0010 Rev A)

The TOE is shipped out of the Thinklogical shipping department following our “Packaging and Shipping” requirements document which requires tamper evident packaging.

Thinklogical uses preferred carriers unless specified by our customers. In those cases, we are required by Purchase Order Flow Down Requirements to use the customers designated carriers.

Carriers that Thinklogical uses are industry leaders in ground, air, and rail and well-equipped to handle Thinklogical needs and customer delivery expectations. All these carriers provide tracking, customer support, and delivery confirmation.

Please see list below for the approved logistics services Thinklogical uses:

- Federal Express
- United Parcel Service
- TForce Freight
- BTX Global Logistics

2) Software/Firmware within the hardware device configures the data separation security policy.
The Software/Firmware revision is SFT-TLX160-15 [TLX160 FIRMWARE VERSION V 5.10.0~~2~~3]

The system software, which resides on the SD card, is always shipped installed on the system controller card which is part of the Thinklogical KVM Matrix Switch (TLX160 Matrix Switch Rev B) chassis.

The Administrator, Operator, or System user cannot download the system software. The Administrator can request to get a software upgrade which is provided as a shipped with SD card. The entire operating system is on the SD card. The SD card is formatted with the EXT4 journaling file system. The operating system is Ubuntu [v.20.04.6 LTS (Focal Fossa)] and is setup with the standard Ubuntu Linux based directory structure. Within that directory structure are binary, shell script, and python files.

For security, the SD card is placed into a tamper evident Security Bag for shipment. The Security Bag has a self-sealing closure, a unique alphanumeric serial number with barcode, and a receipt to allow for tracking purposes. When shipping the SD Card, the serial number receipt from the bag is sent to the customer as a separate shipment. When the customer receives the SD card shipment, they can verify that the Security bag serial number matches the receipt number indicating that the shipment has not been tampered with.

3) FPGA Firmware within the hardware device controls the control plane of system.
The FPGA Firmware revision is FLX-C00160-002 [TLX160 FIRMWARE VERSION 0x100F]

4) Guidance documentation for TLX160 Matrix Switch is as follows:
TLX160 Product Manual [Revision I, June 2025]
TLX160 Quick Start Guide - QSG_TLX160_Rev_B.pdf [Revision B, Jan 2024]

Additional general Matrix Switch documentation is as follows:
Manual_Configuring_the_TLX_ASCII_Interface_Rev_F.pdf
Manual_TLX_Matrix_Switch_ASCII_API_V5_Rev_N.pdf
Manual_How_To_Change_A_TLX_Matrix_Switch's_IP_Address_Rev_E.pdf
Manual_TLX_Matrix_Switch_Interfaces_Rev_I.pdf
Manual_TLX_Matrix_Switch_SNMP_Traps_Rev_K.pdf
Manual_TLX_Matrix_Switch_ADM_Rev_C.pdf

Documentation is not shipped with the hardware but can be downloaded from the Thinklogical support download section of the website as a pdf file (https://www.thinklogical.com/downloads). Documentation for the matrix switches would include Product Manual and Quick Start Guide.

2.3 TOE Logical Boundaries

TOE logical boundaries include all software and firmware components inside the TLX160 Matrix Switch as well as functions within the physical boundary.

The following Security Functions are provided by the TOE

- User Data Protection (enforces Data Separation SFP)
- Security Management (enforces security attributes that can only be modified by authorized users)
- Protection of the TSF (enforces passive detection of physical attack and self-testing)

This Security Target includes all product security features. There are no security features outside the scope of the evaluation.

3 Security Problem Definition

This section describes the assumptions, threats, and policies that are relevant to both the TOE and the Operational Environment.

Note: there is currently no Protection Profile directly applicable to the type of technology provided by the TOE. Protection Profile for Peripheral Sharing Device [Version: 4.0 2019-07-19] PSDPP is applicable to the situation, where there is a single user and multiple set of peripherals locally managing multiple computers. In the case of the TOE there are *multiple users managing multiple* sets of peripherals which *remotely are* managing multiple computers. The aim of this Security Target is to stay close to the requirements of the PSDPP generalizing them for the case of multiple user with multiple sets of peripherals and remote connectivity.

3.1 Secure Usage Assumptions

The TOE is physically protected and managed as required for the highest level of security classified data handled or transferred by the TOE.
The following Table defines the Secure Usage Assumptions.

Table 2: Secure Usage Assumptions

Assumption	Definition
A.PHYSICAL	The switch, the control computer, the transmitters, the receivers, the optical connections from the Switch to the transmitters and receivers and the wired network connections from the Switch to the administrators are physically secure. Essentially the operational environment will provide physical security, commensurate with the value of the TOE and the data that transits it. Note: The TOE does not encrypt optical or wired network connections. Therefore, such connections need to be physically secured. **Note: This assumption exists in PSDPP**. In the case of PSDPP connections from the TOE to the set of peripherals and to the managed computers are short-distance local connections. Therefore, PSDPP does not raise questions regarding physical security of physical connections. In present case due to the long-distance nature of the connections, separate care must be given to physically securing optical and network connections. As an example, an outdoor optical connection may be subject to eavesdropping.
A.EMISSION	The TOE meets the appropriate national requirements (in the country where used) for conducted/radiated electromagnetic emissions. [In the United States, Part 15 of the FCC Rules for Class B digital devices.
A.MANAGE	The TOE is installed and managed in accordance with the manufacturer’s directions.
A.NOEVIL	The TOE Administrators, Operators, and System users are non-hostile and follow all usage guidance. A hostile user could easily circumvent the security restrictions, by, e.g. switching to a classified Computer1, copying a file from Computer1 to a USB drive, then switching to an unclassified Computer2 and copying the file from the USB drive to Computer2. The Data Separation SFP may only be effective if the users do not intentionally violate the SFP.

Table 1: Secure Usage Assumptions *(continued)*

Assumption	Definition
A.SCENARIO	Vulnerabilities associated with attached devices are a concern of the application scenario and not of the TOE. The TOE is not intended to mitigate or protect against security vulnerabilities in the attached devices.
A.PERSON	TOE users will follow TOE guidance and the security procedures of the operational environment in which the TOE is installed.
A.TRUSTED_CONFIG	Personnel configuring the TOE and its operational environment follow the applicable security configuration guidance. **Note: This assumption exists in PSDPP**.
A. TRUSTED_USER	TOE users are trusted to follow and apply all guidance and security procedures in a reliable manner.

3.2 Threats

The asset under attack is the information transiting the TOE. The threat agent is most likely people with TOE access that possess average expertise, with few resources, and moderate motivation. The following Table defines the Threats to Security.

Table 3: Threats

Threat	Definition
T.INSTALL	The TOE may be delivered and installed in a manner which violates the security policy as a result of an attacker, malicious user or human agent, attempting to perform actions that the individual is not instructed to do as per the guidance.
T.ATTACK	An attack on the TOE may violate the security policy as a result of an attacker, malicious user or human agent, attempting to perform actions that the individual is not authorized to perform.
T.RESIDUAL	Residual data may be transferred between different port groups in violation of data separation security policy as a result of an attacker, malicious user or human agent, attempting to compromise the security policy.
T.PHYSICAL_TAMPER	A malicious user or human agent could physically modify the TOE to allow unauthorized information flows. **Note: This threat exists in the PSDPP**

Threat	Definition
T.DATA_LEAK	A connection via the TOE between one or more computers may allow unauthorized data flow through the TOE or its connected peripherals as a result of an attacker, malicious user or human agent, attempting to compromise the security policy.. **Note: This threat exists in the PSDPP**
T.UNAUTH	A malicious user could tamper with the security attributes that determine allowed data flows, resulting in unauthorized data flows between connected devices, and an attack on the connected computers.
T.FAILED	A failure may cause an unauthorized information flow or weakening of TOE security functions.

3.3 Organizational Security Policies

There are no Organizational Security Policies claimed in this ST.

4 Security Objectives

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

4.1 Security Objectives for the TOE

The following are the TOE Security Objectives.

Table 4: Security Objectives for the TOE

O.CONF	The TOE is not data content aware and therefore shall not violate the confidentiality of information which it processes. Information generated within any peripheral set/computer connection shall not be accessible by any other peripheral set/computer connection.
O.CONNECT	No information shall be shared between switched computers and peripheral sets via the TOE in violation of Data Separation SFP. This ST adds the requirement that information shall not be shared between peripheral sets.
O.CHANNEL_ISOLATION	User data must be routed by the TOE only to the appropriate computer interface. The TOE must provide electrical isolation of the data flowing from the peripheral device to the connected computer.
O.STATIC_ATTRIBUTES	The TOE will protect all security attributes from being altered by the TOE unauthorized users.
O.SELF_TEST	The TOE shall perform self-tests following power up or powered reset. **Note: This objective exists in PSDPP**

4.2 Security Objectives for the Environment

All of the Secure Usage Assumptions are considered to be Security Objectives for the Environment. These Objectives are to be satisfied without imposing technical requirements on the TOE; they will not require the implementation of functions in the TOE hardware and/or software, but will be satisfied largely through application of procedural or administrative measures.

Table 5: Security Objectives for the Environment

Security Objective for the Environment	
OE.EMISSION	The customer shall verify that the TOE meets the appropriate national/regional requirements if those requirements for conducted/radiated electromagnetic emissions fall outside the scope of testing currently performed on the TOE. In the United States, Part 15 of the FCC Rules for Class B digital devices.
OE.MANAGE	The TOE shall be installed and managed in accordance with the manufacturer's directions.
OE.NOEVIL	The authorized Administrators, Operators, and System user shall be non-hostile and follow all usage guidance.
OE.PHYSICAL	The Switch, the control computer, the transmitters, the receivers, the optical connections from the Switch to the transmitters and receivers and the wired network connections from the TOE to the administrators shall be physically secure. Essentially the operational environment will provide physical security, commensurate with the value of the TOE and the data that transits it. Note: The TOE does not encrypt optical or wired network connections. Therefore, such connections need to be physically secured. **Note: A similar objective exists in PSDPP**. In the case of PSDPP connections from the TOE to the peripheral sets and to the managed computers are short-distance local connections. Therefore, PSDPP does not raise questions regarding physical security of such connections. In the case of the TOE separate care must be given to physically securing optical and network connections.
OE.SCENARIO	Vulnerabilities associated with attached devices or their connections to the TOE, shall be a concern of the application scenario and not of the TOE. The TOE does not mitigate vulnerabilities in attached devices.
OE.PERSON	TOE users will follow TOE guidance and the security procedures of the operational environment in which the TOE is installed.
OE.TRUSTED_CONFIG	The operational environment will ensure that administrators configuring the TOE and its operational environment follow the applicable security configuration guidance. **Note: This objective exists in PSDPP**
OE.TRUSTED_USER	TOE users are trusted and shall follow and apply all guidance and security procedures in a reliable manner.

5 Security Requirements

This section defines the functional requirements for the TOE that are relevant to supporting the secure operation of the TOE, as well as the assurance requirements for the TOE.

5.1 TOE Security Functional Requirements

Many of the TOE Security Functional Requirements are the same or similar to those of PSDPP.

5.1.1 User Data Protection (FDP)

Table 6: TOE FDP Security Functional Requirements

TOE Security Functional Requirements	
FDP_ETC.1	Export of User Data Without Security Attributes
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FDP_ITC.1	Import of User Data Without Security Attributes

5.1.1.1 FDP_ETC.1 Export of user data without security attributes

FDP_ETC.1.1 The TSF shall enforce the [Data Separation SFP] when exporting user data, controlled under the SFP, from outside of the TOE.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

5.1.1.2 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [Data Separation SFP] on [the set of Transmitter and Receiver Port Groups, and the bi-directional flow of data and state information between the shared peripherals and the switched computers].

5.1.1.3 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the [Data Separation SFP] based on the following types of subject and information security attributes: [Transmitter and Receiver Port Groups (subjects), peripheral data and state information (objects), port group IDs, logical connections of Transmitter and Receiver Groups (attributes)].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [peripheral data and state information can only flow between Transmitter and Receiver port groups that have been previously logically connected by the administrator using the TOE management interface].

FDP_IFF.1.3 The TSF shall enforce a [Transmitter Port Group may be logically connected to multiple Receiver Port Groups, out of which bi-directional information flow will be established only with a single Primary Receiver Port Group selected by the administrator. The remaining Non-Primary Receiver port groups will only receive unidirectional multicast audio and video signals. Any Receiver Port Group may only be logically connected to a single Transmitter Port Group].

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

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [No data or state information flow shall be allowed between logically unconnected port groups. No data or state information flow shall be allowed between any two Receiver Port Groups. No data or state information flow shall be allowed between any two Transmitter Port Groups. No data or state information flow shall be allowed between any Receiver or Transmitter Port Group and any other non-optical physical port on the Switch].

5.1.1.4 FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1.1 The TSF shall enforce the [Data Separation SFP] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [no additional rules].

5.1.2 Security Management (FMT)

Table 7: TOE FMT Security Functional Requirements

TOE Security Functional Requirements	
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles

5.1.2.1 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [*Data Separation SFP*] to restrict the ability to [*modify*] the security attributes [*logical secure connections via Restrict, Partition, and P2P tables*] to [*administrator*].

5.1.2.2 FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the [*Data Separation SFP*] to provide [*permissive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*administrator*] to specify alternative initial values to override the default values when an object or information is created.

5.1.2.3 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [*changing of logical secure connections via Restrict, Partition, and P2P tables*].

5.1.2.4 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [*operator, administrator*].

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

5.1.3 Protection of the TSF (FPT)

Table 8: TOE FPT Security Functional Requirements

TOE Security Functional Requirements	
FPT_TST.1	TSF testing

5.1.3.1 FPT_TST.1 TSF Testing

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

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

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

5.1.4 Identification and Authentication (FIA)

Table 9: TOE FIA Security Functional Requirements

TOE Security Functional Requirements	
FIA_UID.1	Timing of identification
FIA_UAU.1	Timing of authentication

5.1.4.1 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [API interface, access to system management command line via SSH requesting user to identify themselves by entering name] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.4.2 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow [API interface, access to system management command line via SSH requesting user to authenticate themselves by entering password] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.2 TOE Security Assurance Requirements

This section defines the assurance requirements for the TOE as EAL4 requirements augmented with ALC_FLR.2.

5.2.1 Assurance Components

The table below summarizes the components for EAL4 + ALC_FLR.2.

Table 10: TOE Security Assurance Requirements

Assurance Class	Assurance Component	
Life Cycle Support	ALC_CMC.4	Product support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
	ALC_FLR.2	Flaw remediation Procedures
Development	ADV_ARC.1	Security Architectural Description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation of the TSF
	ADV_TDS.3	Basic modular design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_VAN.3	Focused vulnerability analysis

6 TOE Summary Specification

This section addresses IT security functions and the corresponding assurance measures.

6.1 TOE Security Functions

The TOE includes the following Security Functions:

- User Data Protection
- Security Management
- Protection of the TSF
- Identification and Authentication

6.1.1 User Data Protection

The TOE logically connects Transmitter and Receiver Port Groups according to the current switching configuration. The data flows between a particular Transmitter Port Group and a set of Receiver Port Groups if and only if there is an active logical connection connecting these. If there are multiple Receiver Port Groups connected to a Transmitter Port Group, bi-directional information flow will be then established between the Primary Receiver Port Group and the Transmitter Port Group. The remaining Non-Primary Receiver Port Groups will receive unidirectional multi-cast video and audio signals from the Transmitter Port Group.

The TOE security functions (TSF) shall enforce the Data Separation SFP when exporting user data, controlled under the SFP(s), outside of the TOE and the TSF shall export the user data without the user data's associated security attributes.

Also, the TSF shall enforce the Data Separation SFP when importing user data, controlled under the SFP, from outside the TOE and ignore any security attributes associated with the user data when imported from outside the TOE.

TOE Security Functional Requirements addressing Data Separation SFP: FDP_IFF.1, FDP_IFC.1, FDP_ITC.1, FDP_ETC.1.

6.1.2 Security Management

6.1.2.1 Security Attributes

The TSF shall enforce security attributes through identification and authentication of administrators and operators before giving any administrative access to the TOE (i.e., giving any access to TSF management functions (Restrict, Partition, and P2P Tables).

The default security attributes are permissive in that the Restrict, Partition, and P2P tables allow for any connection to any. No user is able to change those default values as only the administrator can modify attributes of the default tables to manage the security policy that is required. Switching may be done by the user with hot keys however the allowed hot key switching attributes can only be provisioned by the administrator.

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

6.1.2.2 Security Management and Roles

The TSF provides security management functions to configure the administrator and operator authentication. Users cannot use these functions and are not required to authenticate. The TSF management functions allow for the changes of logical TOE connection via the Restrict, Partition, and P2P Tables. Note: prior to authentication, only the API can be used on the TOE.

The TSF provides for security roles. The TOE maintains a single administrator role and operator roles. All others are users (non-administrative or non-operators). Refer to Table 21. A properly authenticated administrator has the ability to view audit records/log files, reset to factory defaults, change passwords, remove operators, and modify Restrict, Partition, and P2P tables.

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

6.1.3 Protection of the TSF

6.1.3.1 TSF Testing

The TOE runs a suite of self-tests during initial startup and or after activating the reset button. The self-test includes a test of the basic TOE hardware and firmware integrity. The self-test provides the administrator with the capability to verify the integrity of the TSF and the TSF functionality by producing a log file (bist.log) which can be inspected for pass or fail conditions.

TOE Security Functional Requirements addressed: FPT_TST.1

6.1.4 Identification and Authentication

6.1.4.1 Timing of identification

The TOE does allow for an API interface prior to user name entry. The TOE does not provide any security services or allow any TOE management actions by the operator or administrator unless identified by the TOE TSF:

The TOE maintains a single administrator role and operator role with the “Timing of identification” SFR which insures that only an operator or administrator can identify themselves to the TOE.

TOE Security Functional Requirements addressed FIA_UID.1:

This SFR requires that an operator or administrator provides their "username" to the TOE as a preliminary step before being able to authenticate with the TOE.

During “Timing of identification” the operator or administrator cannot perform any functions on the TOE other than providing the TOE with the username.

After “Timing of identification” the operator or administrator cannot perform any functions on the TOE other than providing the TOE with the password.

6.1.4.2 Timing of authentication

The TOE does allow for an API interface prior to password entry. The TOE does not provide any security services or allow any TOE management actions by the operator or administrator unless authenticated by the TOE TSF:

The TOE maintains a single administrator role and operator role with the “Timing of authentication” SFR which insures that the operator and administrator are credentialed into the TOE preventing a threat attempting to manage the TOE despite access to it.

TOE Security Functional Requirements addressed FIA_UAU.1:
Dependencies: FIA_UID.1 Timing of identification.

During “Timing of authentication” the operator or administrator cannot perform any functions on the TOE other than providing the TOE with the password.

After “Timing of identification” the operator or administrator can perform any functions on the TOE as specified in Table 21: User Role Access.

6.2 Assurance Measures

The assurance measures addressed in this section apply to the EAL4+ requirements augmented with ALC_FLR.2 and are presented in the following table.

Table 11: Assurance Measures

Assurance Requirement	Name	Assurance Measure
ALC_CMC.4	Product support, acceptance procedures and automation	Thinklogical Product Support Plan and Procedures Thinklogical Acceptance Plan and Procedures
ALC_CMS.4	Problem tracking CM coverage	Thinklogical Configuration Management Plan and Procedures
ALC_DEL.1	Delivery procedures	Thinklogical Delivery Plan and Procedures
ALC_DVS.1	Identification of security measures	Thinklogical Security Measures Plan and Procedures
ALC_LCD.1	Developer defined life-cycle model	Thinklogical Life-Cycle Model Plan and Procedures
ALC_TAT.1	Well-defined development tools	Thinklogical Development Tools Plan and Procedures
ALC_FLR.2	Flaw remediation	Thinklogical Remediation Plan and Procedures Document
ADV_ARC.1	Security Architectural Description	Thinklogical Security Architectural Description Document
ADV_FSP.4	Complete functional specification	Thinklogical Functional Specification Document
ADV_IMP.1	Implementation of the TSF	Thinklogical TSF implementation
ADV_TDS.3	Basic modular design	Thinklogical High-Level Design Document
AGD_OPE.1	Operational user guidance	Thinklogical Operational User Guidance
AGD_PRE.1	Preparative User guidance	Thinklogical Preparative User Guidance
ATE_COV.2	Analysis of coverage	Thinklogical Analysis of Coverage Document
ATE_DPT.1	Testing: basic design	Thinklogical Testing Setup Document Thinklogical Security Enforcing Modules Testing Plan and Procedures Thinklogical Security Enforcing Modules Testing Report
ATE_FUN.1	Functional testing	Thinklogical Testing Setup Document Thinklogical Functional Testing Plan and Procedures Thinklogical Functional Testing Report
ATE_IND.2	Independent testing – sample	Thinklogical Testing Setup Document Lab Independent Testing Report
AVA_VAN.3	Focused vulnerability analysis	Thinklogical Testing Setup Document Lab Vulnerability Analysis Report

7 Rationale

This section provides the rationale for the selection of the IT security requirements, objectives, assumptions, and threats. In particular, it shows that the IT security requirements are suitable to meet the security objectives, which in turn are shown to be suitable to cover all aspects of the TOE security environment.

7.1 Rationale for Security Objectives

The following table provides mapping of threats to objectives and the corresponding rationale describing how the threat is addressed by the SFR.

Table 12: Security Objectives Rationale

Threat	**Objective**	**Rationale**
T.INSTALL The TOE may be delivered and installed in a manner which violates the security policy	OE.MANAGE	The TOE shall be installed and managed in accordance with the manufacturer's directions.
T.ATTACK An attack on the TOE may violate the security policy.	O.CONF	Information generated within any peripheral set/computer connection shall not be accessible by any other peripheral group/computer connection. Otherwise, the security policy is violated.
T.RESIDUAL Residual data may be transferred between different port groups in violation of data separation security policy	O.CONF O.CONNECT	The requirement that information generated within any peripheral group/computer connection shall not be accessible by any other peripheral group/computer connection includes the residual information. No information shall be shared between switched computers and sets of peripherals via the TOE in violation of data separation security policy. This includes the residual information.
T.DATA_LEAK A connection via the TOE between one or more computers may allow unauthorized data flow through the TOE or its connected peripherals. .	O.CHANNEL_ISOLATION O.STATIC_ATTRIBUTES	It is ensured that data flows only to the appropriate interfaces of the connected computer, and is therefore unavailable to an unauthorized user. All security attributes that determine data flows cannot be altered to allow an unauthorized data transfer.
T.PHYSICAL_TAMPER A malicious user or human agent could physically modify the TOE to allow unauthorized information flows.	OE.PHYSICAL OE.PERSON	The operational environment will provide physical security, commensurate with the value of the PSD and the data that transits it. (PSDPP) TOE users will follow the security procedures of the operational environment in which the TOE is installed. (PSDPP)

T.UNAUTH A malicious user could tamper with the security attributes that determine allowed switch connections and allowed data flows, resulting in the use of unauthorized peripheral devices that may allow unauthorized data flows between connected devices, or an attack on the TOE or its connected computers.	O.STATIC _ATTRIBUTES	TOE threat is ensured in that the security attributes that determine allowed peripheral devices and allowed data flows may not be altered by unauthorized users.
T.FAILED A failure may cause an unauthorized information flow or weakening of TOE security functions.	O.SELF_TEST OE.MANAGE	The TOE mitigates the threat of failures leading to compromise of security functions through self-tests of its own functionality. The TOE shall be installed and managed in accordance with the manufacturer's directions.

Table 13: Mapping of Threats to Security Objectives

Objective	T.INSTALL	T.ATTACK	T.RESIDUAL	T.DATA_LEAK	T.UNAUTH	T.PHYSICAL _TAMPER	T.FAILED
O.CONF		X	X				
O.CONNECT			X				
OE.MANAGE	X						X
O.CHANNEL_ISOLATION				X			
OE.PHYSICAL						X	
OE.PERSON						X	
O.STATIC _ATTRIBUTES				X	X		
O.SELF_TEST							X

7.2 Rationale for Security Objectives for the Environment

All of the Security Objectives for the Environment are considered to be Secure Usage Assumptions. These objectives on the environment do not contain any IT security requirements because they are non-IT related objectives. Thus, the CC does not mandate it map to any requirements.

Mapping of Assumptions to the Security Objectives for the Environment including the corresponding rationale is provided below.

Table 14: Security Objectives for the Environment Rationale

Assumption	Objective	Rationale
A.PHYSICAL The TOE, the optical connections from the TOE to the transmitters and receivers and the wired network connections from the TOE to the users are physically secure.	OE.PHYSICAL The TOE shall be physically secure.	The TOE is assumed to be protected from physical attack (i.e. theft, modification, reconfiguration, or eavesdropping). Physical attack could include unauthorized intruders into the TOE environment, but it does not include physical destructive actions that could be taken by an individual that is authorized to access the TOE environment.
A.EMISSION The TOE meets the appropriate national requirements (in the country where used) for conducted/radiated electromagnetic emissions. [In the United States, Part 15 of the FCC Rules for Class B digital devices.]	OE.EMISSION The TOE shall pass testing for conducted/radiated electromagnetic emissions, Part 15 of the FCC Rules for Class B digital devices.	TOE chassis construction is such that emissions will be below that of the appropriate national requirements (in the country where used) for conducted/radiated electromagnetic emissions. [In the United States, Part 15 of the FCC Rules for Class B digital devices.]

Table 15: Security Objectives for the Environment Rationale *(continued)*

Assumption	Objective	Rationale
A.MANAGE The TOE is installed and managed in accordance with the manufacturer’s directions.	OE.MANAGE The TOE shall be installed and managed in accordance with the manufacturer’s directions.	Complying with Manufacturers documentation for installation and operation assures that the TOE is operating properly.
A.NOEVIL The TOE users are non-hostile and follow all usage guidance.	OE.NOEVIL The TOE users shall be non-hostile and follow all usage guidance.	Correct usage of the TOE assures operation as expected.
A.SCENARIO Vulnerabilities associated with attached devices are a concern of the application scenario and not of the TOE.	OE.SCENARIO Vulnerabilities associated with attached devices shall be a concern of the application scenario and not of the TOE.	Vulnerabilities associated with attached devices due to an application scenario are a concern of the application scenario and not that of the TOE.
A.PERSON	OE.PERSON	Complying with Manufacturers documentation for secure

It is a concern that TOE users will follow TOE guidance and the security procedures of the operational environment in which the TOE is installed.	TOE users will follow TOE guidance and the security procedures of the operational environment in which the TOE is installed.	operation assures that the TOE is operating securely.
A.TRUSTED_CONFIG Personnel configuring the TOE and its operational environment follow the applicable security configuration guidance.	OE.TRUSTED_CONFIG The operational environment will ensure that administrators configuring the TOE and its operational environment follow the applicable security configuration guidance.	If TOE administrators follow the provided security configuration guidance, then the assumption is satisfied.
A. TRUSTED_USER It is a concern to trust that TOE users will follow and apply all guidance and security procedures in a reliable manner.	OE.TRUSTED_USER TOE users are trusted and shall follow and apply all guidance and security procedures in a reliable manner.	Following guidance for TOE assures operation as expected

Table 16: Mapping of Assumptions to Environmental Security Objectives

Objective	A.PHYSICAL	A.EMISSION	A.MANAGE	A.NOEVIL	A.SCENARIO	A.PERSON	A.TRUSTED _CONFIG	A.TRUSTED _USER
OE.PHYSICAL	X							
OE.EMISSION		X						
OE.MANAGE			X					
OE.NOEVIL				X				
OE.SCENARIO					X			
OE.PERSON						X		
OE.TRUSTED_ CONFIG							X	
OE.TRUSTED_ USER								X

7.3 Security Requirements Rationale

This section demonstrates that the functional components selected for the TOE provide complete coverage of the defined TOE security objectives.

Table 17: Security Requirements Rationale

Objective	**Security Requirement**	**Rationale**
O.CONF The TOE shall not violate the confidentiality of information which it processes. Information generated within any peripheral group/computer connection shall not be accessible by any other peripheral group/computer connection.	FDP_ETC.1 (Export of User Data Without Security Attributes) FDP_IFC.1 (Subset Information Flow Control) FDP_IFF.1 (Simple Security Attributes) FDP_ITC.1 (Import of User Data Without Security Attributes)	The TOE enforces Data Separation SFP on user data. No security attributes are added to data going to peripheral devices. The TOE enforces Data Separation SFP which is based on establishing logical connections between Transmitter and Receiver Port Groups. Information flow is only permitted between input and Receiver Port Groups that have been logically connected. When TOE inputs user data, no security attributes are imported.
O.CONNECT No information shall be shared between switched computers and sets of peripherals via the TOE in violation of data separation security policy.	FDP_ETC.1 (Export of User Data Without Security Attributes) FDP_IFC.1 (Subset Information Flow Control) FDP_IFF.1 (Simple Security Attributes) FDP_ITC.1 (Import of User Data Without Security Attributes)	The TOE enforces Data Separation SFP on user data. No security attributes are added to data going to peripheral devices. The TOE enforces Data Separation SFP which is based on establishing logical connections between Transmitter and Receiver Port Groups. Information flow is only permitted between input and Receiver Port Groups that has been logically connected using the TOE management interface. When TOE inputs user data, no security attributes are imported.

O.CHANNEL_ISOLATION User data must be routed by the TOE only to the appropriate computer interface. The TOE must provide isolation of the data flowing from the peripheral device to the connected computer.	FDP_IFC.1 (Subset Information Flow Control)	The TOE enforces Data Separation SFP which is based on establishing logical connections between Transmitter and Receiver Port Groups.
	FDP_IFF.1 (Simple Security Attributes)	Information flow is only permitted between input and Receiver Port Groups that has been logically connected using the TOE management interface.
O.STATIC_ATTRIBUTES The TOE will protect all security attributes from being altered by the TOE unauthorized users.	FMT_MSA.1 (Management of security attributes)	Ensures that management of security attributes allows authorized users (roles) to manage the specified security attributes.
	FMT_MSA.3 (Static attribute initialization)	Static attribute initialization ensures that the default values of security attributes are appropriately either permissive or restrictive in nature.
	FMT_SMF.1 (Specification of Management Functions)	Ensures that the TSF prevents users from changing the values that determine the security configuration.
	FMT_SMR.1 (Security roles)	Provides the TOE user roles.
	FIA_UID.1 Timing of identification	Insures that authorized users are identified by username.
	FIA_UAU.1 (Timing of authentication)	Insures that authorized users are identified by password.
O.SELF_TEST The TOE shall perform self-tests following power up or powered reset.	FPT_TST.1 (TSF testing)	Provides support for the testing of the critical functions of the TSF's operation.

Table 18: Mapping of TOE Security Objectives to Security Requirements

Objective	FDP_ ETC.1	FDP_ IFC.1	FDP_ IFF.1	FDP_ ITC.1	FMT_ MSA.1	FMT_ MSA.3	FMT_ SMF.1	FMT_ SMR.1	FPT_ TST.1	FIA_ UAU.1	FIA_ UID.1
O.CONF	X	X	X	X							
O.CONNECT	X	X	X	X							
O.CHANNEL_ISOLATION		X	X								
O.STATIC_ATTRIBUTES					X	X	X	X		X	X
O.SELF_TEST									X		

7.4 Security Assurance Rationale

EAL4+ was chosen to provide moderate level of assurance that is consistent with good commercial practices. The EAL is consistent with the assurance measures claimed by competitive products as well as with the PSDPP.

7.5 Rationale for Satisfying all Dependencies

Each functional requirement was analyzed to determine that all dependencies were satisfied. All requirements were then analyzed to determine that no additional dependencies were introduced as a result of completing each operation. All dependencies in this ST have been satisfied. Dependencies are illustrated in the table below.

Table 19: Dependencies

Functional Component	Dependency
FDP_ETC.1	FDP_IFC.1 or FDP_ACC.1
FDP_IFC.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 and FMT_MSA.3
FDP_ITC.1	FDP_IFC.1 or FDP_ACC.1 and FMT_MSA.3
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 and FMT_SMF.1 and FMT_SMR.1
FMT_MSA.3	FMT_MSA.1 and FMT_SMR.1
FMT_SMF.1	No dependency

FMT_SMR.1	FIA_UID.1
FPT_TST.1	No dependency
FIA_UAU.1	FIA_UID.1
FIA_UID.1	No dependency

7.6 TOE Security Functions Rationale

The following table provides a mapping between security functions and security functional requirements.

Table 20: Mapping between security functions and security functional requirements

Functional Component	User Data Protection	Security Management	Protection of TSF	Identification and Authentication
FDP_ETC.1	X			
FDP_IFC.1	X			
FDP_IFF.1	X			
FMT_MSA.1		X		
FMT_MSA.3		X		
FMT_SMF.1		X		
FMT_SMR.1		X		
FPT_TST.1			X	
FIA_UID.1		x		x
FIA_UAU.1		x		x

8 User Roles

TOE provides multiple user roles as defined in the following table. Note, FMT_SMR.1 TSF maintains the operator and the administrator roles. Users, as described below, can only use the TOE to receive a video signal from the source and send a keyboard / mouse signal to the source as prescribed by the Administrator.

Table 20: User Roles

Role	Description
Administrator	An Administrator has second level log in authentication. Therefore the Administrator cannot directly log into the system until the Operator has logged in. A user in this role has administrative rights in the operating system. Administrative rights include the ability to access .csv files and modify them, perform user access control of switch, view log data, create and break connections. Administrator cannot be deleted.
Operator	An Operator has first level log in authentication. A user in this role does not have administrative rights in the operating system. Operator rights include the ability to view .csv files but cannot modify them, cannot perform user access control of switch, cannot view log data. Operator can create and break connections. Operator cannot be deleted.
System User	A System User has no authentication required. A user in this role does not have any access to the switch operating system. A System User cannot view or modify .csv files, cannot perform user access control of switch, cannot view log data, cannot create and break connections, and has no physical access to the switch or the isolated physically secure network. The System User can only use the TOE to receive a video signal from the source and send a keyboard / mouse signal to the source.

TOE provides multiple user role access as defined in the following table.

Table 21: User Role Access

Access	Administrator	Operator	System user	Comment
Login / authentication	2nd level / un and pw	1st level / un and pw	None / none	Administrator cannot directly log into system but only after Operator login. System user has no login. Note: Username (UID) and password (UAU) will be handled solely by Ubuntu Linux operating system.
Physical access – API RS-232 Port	Yes	Yes	No	Administrator and Operator will be allowed in secure switch location System user will not be allowed in secure switch location.
Physical access – Console Port	Yes	Yes	No	Administrator and Operator will be allowed in secure switch location System user will not be allowed in secure switch location.
Physical access – Ethernet Port	Yes	Yes	No	Administrator and Operator will have access to Isolated physically secure network. System user will not have access to Isolated physically secure network.
Logical access / administrative - NTP UDP – port 123	Yes	No	No	Only Administrator can start NTP services and can create, access, and modify ntp.conf file.
Logical access / administrative - SNMP UDP – ports 161, 162	Yes	No	No	Only Administrator can start SNMP services and can create, access, and modify snmpd.conf file.
Logical access / administrative - Remote SYSLOG UDP – port 514	Yes	Limited	No	Only Administrator has access to view all log files. Operator has limited access to view log files
Logical access / administrative - SSH – port 22	Yes	No	No	Only Administrator has access to view and modify sshd.conf file.

Access	Administrator	Operator	System user	Comment
Logical access / control - UDP – port 17564	Yes	Yes	No	Just status broadcast. There is no TOE control over this interface.
Logical access / control - ICMP - ping	Yes	No	No	Only Admin can ping.
Logical access / control - TCP – port 17567	Yes	Yes	No	API access. No authentication
Logical access / WEB server control - HTTPS - port 60087	1 level authentication / un and pw	No	No	Administrative access to operating system functions, log, system, and csv files.
OS File System .csv table Access – read and write	Yes	Limited	No	Only Administrator can modify .csv table files. Operator can view .csv files. System user cannot gain access to file system.
Matrix Switch Connections	Yes	Yes	No	Only Administrator and Operator can make switch connections through the API. System user cannot make switch connections since they do not have access to physical system ports because not allowed access to secure switch location. System user cannot make switch connections since they do not have access to isolated physically secure network.

9 Acronyms

CC	Common Criteria
EAL	Evaluation Assurance Level
IT	Information Technology
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
SFP	Security Function Policy
PP	Protection Profile
PSDPP	National Information Assurance Partnership [NIAP] Peripheral Sharing Device (PSD) Protection Profile Version 4.0
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface
TSC	TSF Scope of Control
TSS	TOE Summary Specification
TSP	TOE Security Policy
CSCS	Customer Supplied Computer System