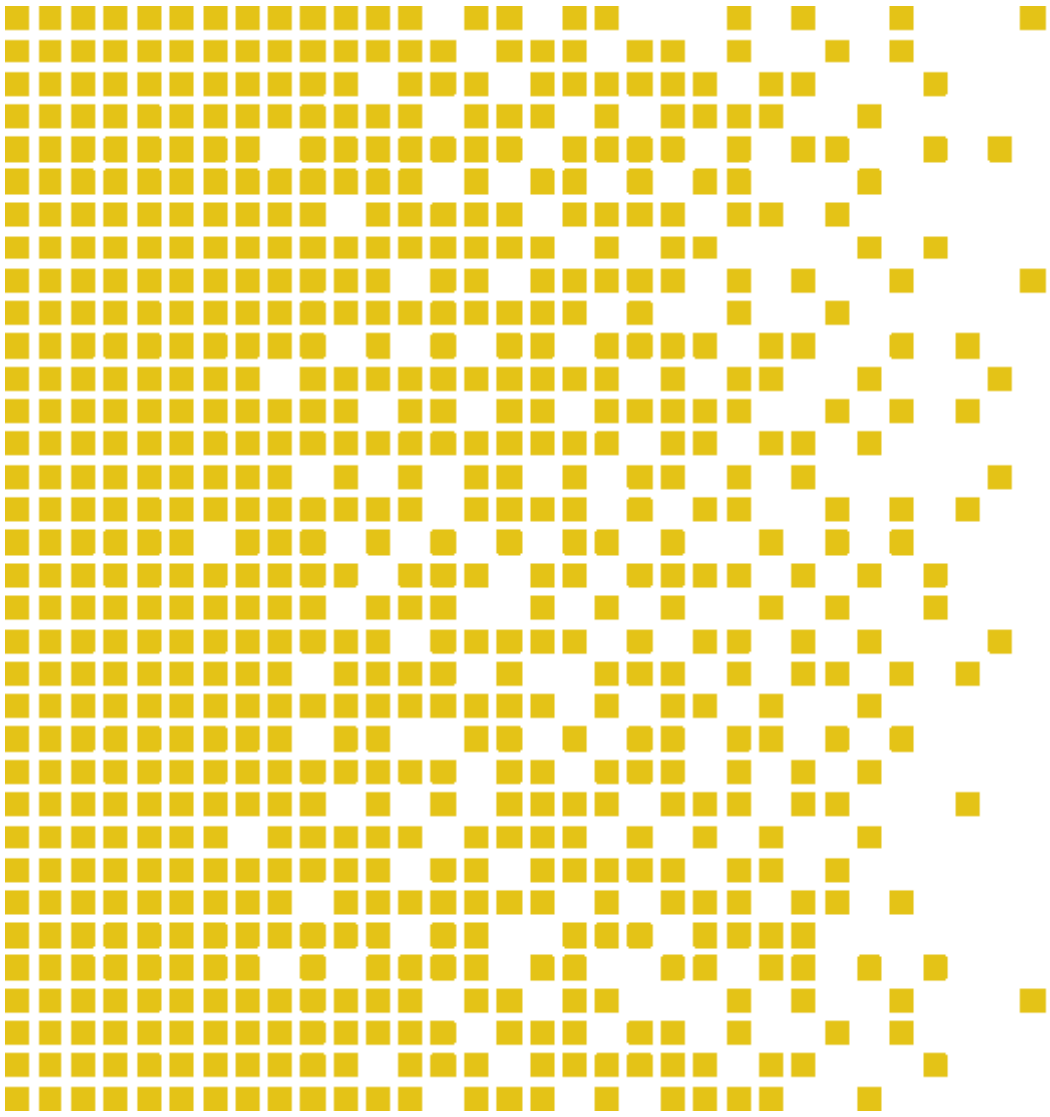
SERTIT-076 CR Certification Report

Issue 1.0 22 September 2016

Thinklogical TLX320 Matrix Switch



SERTIT, P.O. Box 814, N-1306 Sandvika, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognized under the terms of the CCRA July 2nd 2014. The recognition under CCRA is limited to cPP related assurance packages or EAL 2 and ALC_FLR CC part 3 components.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES (SOGIS MRA)

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Agreement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Agreement and is the Party's claim that the certificate has been issued in accordance with the terms of this Agreement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

Mutual recognition under SOGIS MRA applies to components up to EAL 4.

Contents

1 Certification Statement

Thinklogical TLX 320 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.

Thinklogical TLX 320 Matrix Switch (for version see chapter 4.2) has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met Common Criteria Part 3 (ISO/IEC 15408) conformant components of Evaluation Assurance Level EAL 4 for the specified Common Criteria Part 2 (ISO/IEC 15408) conformant functionality when running on the platforms specified in Annex A.

Author	Arne Høye Rage Certifier
Quality Assurance	Kjartan Jæger Kvassnes Quality Assurance
Approved	Kristian Bae Head of SERTIT
Date approved	22 September 2016

2 Abbreviations

CC	Common Criteria for Information Technology Security Evaluation(ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
ISO/IEC 15408	Information technology –- Security techniques –- Evaluation criteria for IT security
SERTIT	Norwegian Certification Authority for IT Security
SOGIS MRA	SOGIS Mutual Recognition Agreement
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

3 References

[1] Thinklogical TLX320 Matrix Switch Security Target Document Version 1.3, January 2016.

[2] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CCMB-2012-09-001, Version 3.1 R4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, CCMB-2012-09-002, Version 3.1 R4, September 2012.

[4] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, CCMB-2012-09-003, Version 3.1 R4, September 2012.

[5] The Norwegian Certification Scheme, SD001E, Version 9.0, 02 April 2013.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1 R4, September 2012.

[7] NO-5152147_ Evaluation Technical Report_v1.1 20 September 2016.

[8] TLX320 10G Matrix Switch Product Manual Rev. A

[9] TLX320 10G Matrix Switch QUICK-START GUIDE As used with Thinklogical's Q-Series & TLX Video Extension Systems

[10] TLX 320 Matrix Router Design Specification 1.2

[11] Changing a Routers' IP Address Rev. A

[12] Thinklogical System Management Portfolio Configurator Hot Key Manager -On-Screen Display System Management Interface Drag & Drop Product Manual Rev. A

[13] VxRouter ASCII Interface 4.1

[14] Using the VxRouter ASCII Interface 4.0

[15] ALC.DEL_1_0.doc v1.0 Thinklogicals delivery procedure 06/01/10

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Thinklogical TLX 320 Matrix Switch (for version see chapter 4.2), and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target[1] which specifies the functional, environmental and assurance evaluation components.

4.2 Evaluated Product

The version of the product evaluated Thinklogical TLX 320 Matrix Switch in the following configurations:

- **TLX320 Matrix Switch Chassis (TLX-MSC-000320 Rev A)**
- TLX48 / TLX320 Matrix Switch Data Input and Output Card, 16 Ports, SFP+, Multi-Mode (TLX-MSD-M00016 Rev A), Single Mode (TLX-MSD-S00016 Rev A)
- Velocity Matrix Switch 320 Data Input Retimer Card, 16 Ports, SFP+, Multi-Mode (VXM-D00T16 Rev A), Single Mode (VXM-D0ST16 Rev A)

This product is also described in this report as the Target of Evaluation (TOE). The developer was Thinklogical

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

4.3 TOE scope

The TOE scope is described in the Security Target [1] chapter 2.

4.4 Protection Profile Conformance

The Security Target[1] did not claim conformance to any protection profile.

4.5 Assurance Level

The Security Target[1] specified the assurance components for the evaluation. Predefined evaluation assurance level EAL 4 was used. Common Criteria Part 3[4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

4.6 Security Policy

The TOE security policies are detailed in the Security Target[1].

There are no Organizational Security Policies or rules with which the TOE must comply.

4.7 Security Claims

The Security Target[1] fully specifies the TOE's security objectives, the threats which these objectives counter and security functional components and security functions to elaborate the objectives. All of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

4.8 Threats Countered

- T.INSTALL The TOE may be delivered and installed in a manner which violates the security policy.
- T.ATTACK An attack on the TOE may violate the security policy.
- T.RESIDUAL Residual data may be transferred between different port groups in violation of data separation security policy.
- T.STATE State information may be transferred to a port group other than the intended one.

4.9 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.10 Environmental Assumptions and Dependencies

- A.PHYSICAL The switch, 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.
- 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 users and administrators are non-hostile and follow all usage guidance.
- A.SCENARIO Vulnerabilities associated with attached devices are a concern of the application scenario and not of the TOE.

4.11 Security Objectives for the TOE

- O.CONF The TOE 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.

4.12 Security Objects for the environment

- OE.EMISSION The TOE shall meet 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.MANAGE The TOE shall be installed and managed in accordance with the manufacturer's directions.
- OE.NOEVIL The authorized user shall be non-hostile and follow all usage guidance.
- OE.PHYSICAL The Switch, 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.
- 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.

4.13 Security Functional Components

- 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

4.14 Security Function Policy

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.

Data Separation Security Function Policy 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.

4.15 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001E[5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target[1], which prospective consumers are advised to read. To ensure that the Security Target[1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[4] and the Common Evaluation Methodology (CEM)[6].

SERTIT monitored the evaluation which was carried out by the Norconsult AS Commercial Evaluation Facility (EVIT). The evaluation was completed when the EVIT submitted the Evaluation Technical Report (ETR)[7] to SERTIT in 20 September 2016. SERTIT then produced this Certification Report.

4.16 General Points

The evaluation addressed the security functionality claimed in the Security Target[1] with reference to the assumed operating environment specified by the Security Target[1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

5 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC Part 3[4]. These classes comprise the EAL 4 assurance package.

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_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

All assurance classes were found to be satisfactory and were awarded an overall “pass” verdict.

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target[1]. The results of this work were reported in the ETR[7] under the CC Part 3[4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

The procedure for physical distribution of the TOE is described in Thinklogicals delivery procedure[15].

This procedure describes how the TOE is shipped from Thinklogicals warehouse via Federal Express, UPS or DHL to the customer.

The procedure explains that all tracking and shipment information are logged, and upon delivery of the TOE a signature is required

Each shipment is noted with dimension and weight, and hard copies of each shipment are held in Thinklogicals Sales Order folder.

5.3 Installation and Guidance Documentation

A description of the secure installation of the TOE and the secure preparation of the operational environment in accordance with the security objectives in the ST[1] can be found in the guidance documents.

The guidance documentation also describes the security functionality and interfaces provided by the TOE. It provides instructions and guidelines for the secure use of the TOE, it addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states.

A list of all guidance documents evaluated can be found in Annex A.

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. The user should always follow the guidance for the TOE in order to ensure that the TOE operates in a secure manner.

The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements

for external security. Sufficient guidance is provided for the consumer to effectively use the TOE's security functions.

5.5 Vulnerability Analysis

The evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process and evaluation process of previous versions of the TOE.

The evaluators have devised a set of tests to test potential vulnerabilities to the TOE. The tests were performed at the developer's site in Milford, Connecticut in October 2015.

The result of the vulnerability analysis is that the TOE in its evaluated configuration and in its intended environment has no exploitable vulnerabilities.

5.6 Developer's Tests

The evaluators' assessment of the developer´s tests shows that the developer´s tests cover all the TSFIs and all SFRs.

The evaluators have confirmed the developer have correctly performed and documented the tests according to the test documentation.

5.7 Evaluators' Tests

The evaluators have independently tested a sample of the developer´s tests and verified that the TOE behaves as specified. Confidence in the developer's test results is gained by performing a sample of the developer's tests.

The evaluators tests were conducted at the developer's site in Milford, Connecticut in October 2015.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[7], produced by the evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that Thinklogical TLX 320 Matrix Switch (version see chapter 4.2) meets the Common Criteria Part 3 conformant components of Evaluation Assurance Level EAL 4 for the specified Common Criteria Part 2 conformant functionality, in the specified environment, when running on platforms specified in Annex A.

6.2 Recommendations

Prospective consumers of Thinklogical TLX 320 Matrix Switch (version see chapter 4.2) should understand the specific scope of the certification by reading this report in conjunction with the Security Target[1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above in Section 4.3 “TOE Scope” and Section 5 “Evaluation Findings”.

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

The above “Evaluation Findings” include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

- **TLX320 Matrix Switch Chassis (TLX-MSC-000320 Rev A)**
- TLX48 / TLX320 Matrix Switch Data Input and Output Card, 16 Ports, SFP+, Multi-Mode (TLX-MSD-M00016 Rev A), Single Mode (TLX-MSD-S00016 Rev A)
- Velocity Matrix Switch 320 Data Input Retimer Card, 16 Ports, SFP+, Multi-Mode (VXM-D00T16 Rev A), Single Mode (VXM-D0ST16 Rev A)

TOE Documentation

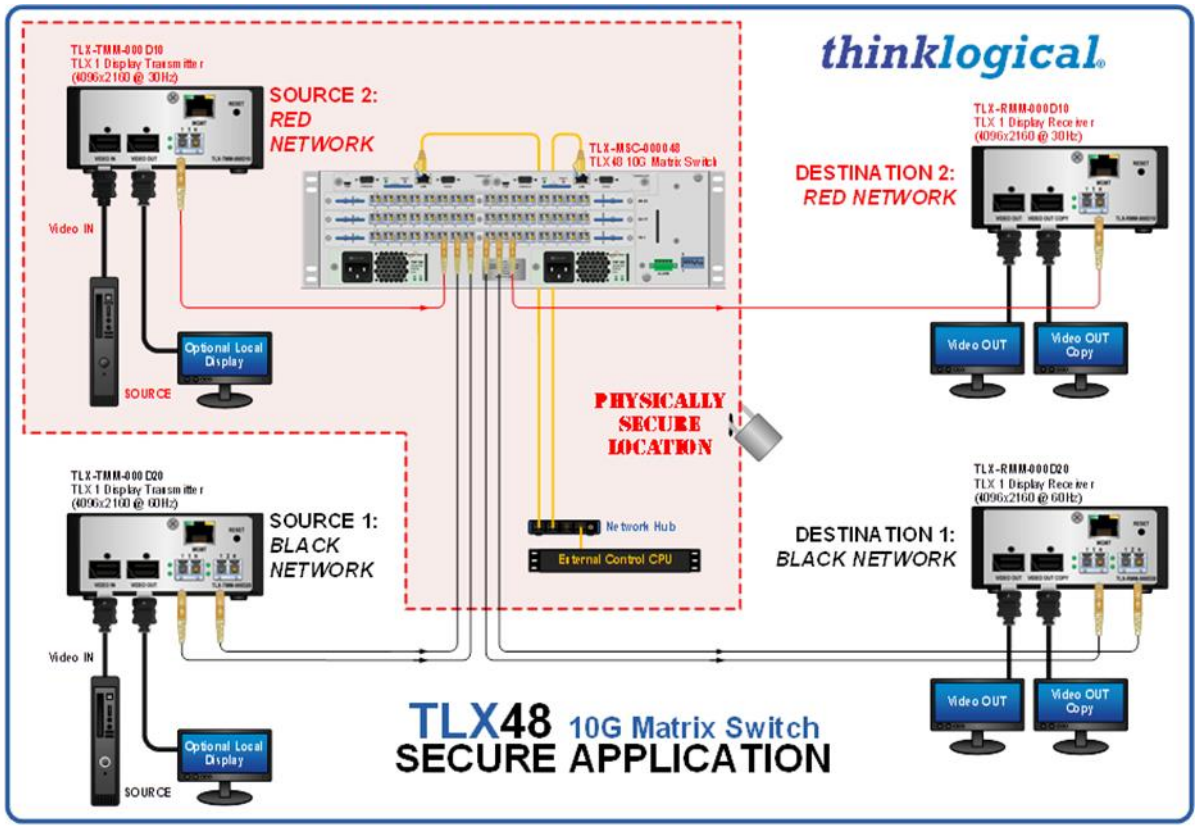
The supporting guidance documents evaluated were:

[a] TLX320 10G Matrix Switch Product Manual Rev. A
[b] TLX320 10G Matrix Switch QUICK-START GUIDE As used with Thinklogical's Q-Series & TLX Video Extension Systems
[c] TLX 320 Matrix Router Design Specification 1.2
[d] Changing a Routers' IP Address Rev. A
[e] Thinklogical System Management Portfolio Configurator Hot Key Manager -On-Screen Display System Management Interface Drag & Drop Product Manual Rev. A
[f] VxRouter ASCII Interface 4.1
[g] Using the VxRouter ASCII Interface 4.0

Further discussion of the supporting guidance material is given in Section 5.3 "Installation and Guidance Documentation".

TOE Configuration

The following configuration was used for testing:



The figure shows the TLX48 Router KVM Matrix Switch in an evaluated configuration. An equivalent layout is the evaluated configuration for the TLX320 Router KVM Matrix Switch.

Tools used during the evaluation:

- Microsoft Office 2013
- Microsoft Hyperterminal
- Oracle VM VirtualBox
- Kali Linux
- Noyes optical power meter, Model OPM 4-1D, Serialnumber 1W11NL001
- Putty Terminal Emulator
- WinSCP
- Oscilloscope Tektronic DSA72504D, asset number 1147321
- Microsoft Telnet
- TLX320 Connect Test 1 A.xls
- TLX320 Connect Test 2 A.xls
- TLX320 Connect Test 3 A.xls

Environmental Configuration

The TOE 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. 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 peripheral set to multiple computers. The TOE provides a capability to dynamically change the switching configuration.

For use in an evaluated configuration, the TOE must be located in a physically secure environment to which only authorized administrators has access. Similarly, the server used to manage the TOE must be physically protected and have suitable identification/authentication mechanism to ensure that only trusted administrators have access.