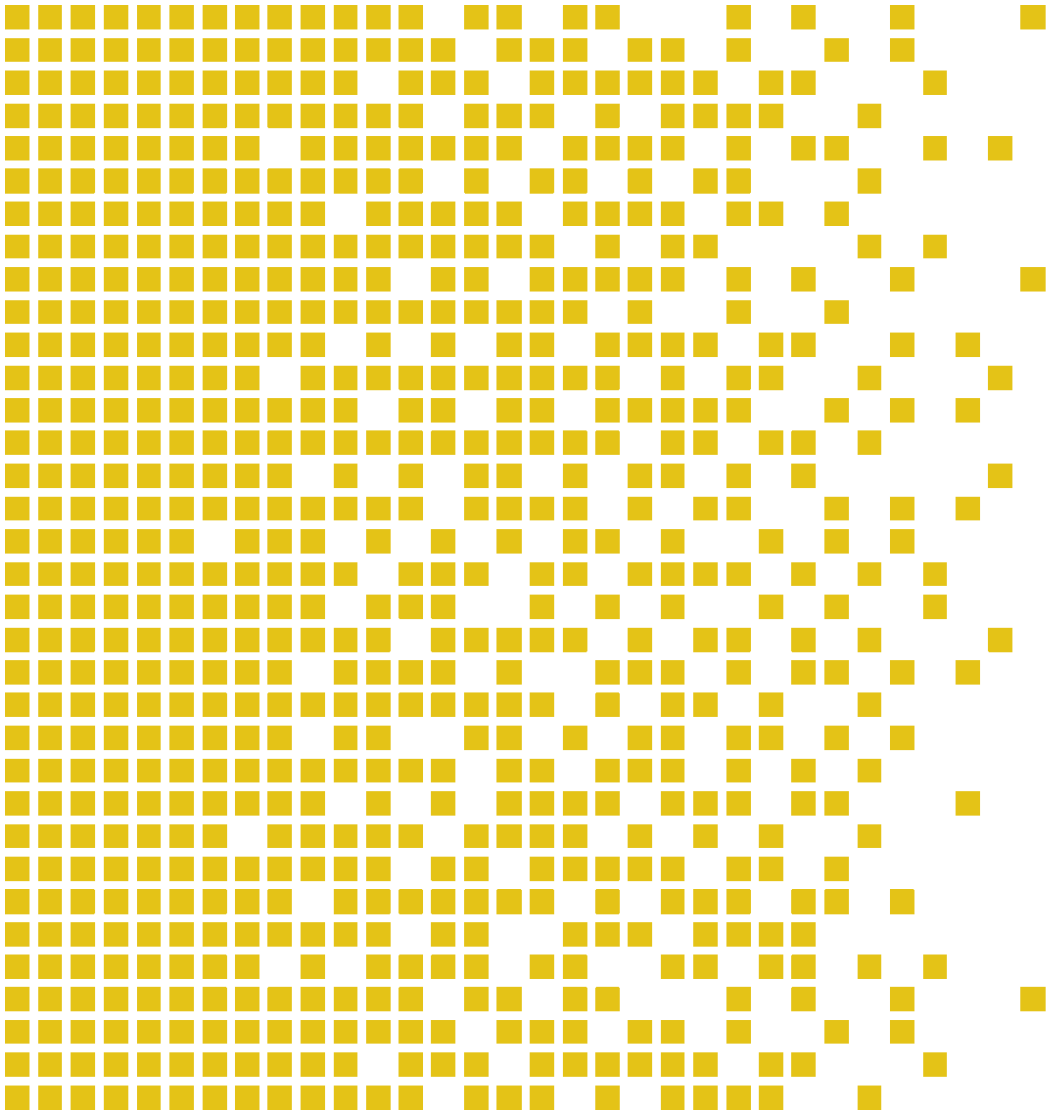
SERTIT-016 CR Certification Report

Issue 1.0 18th April 2011

Thinklogical VX 40 Router KVM Matrix Switch (VXR-000040 Rev B)



SERTIT, P.O. Box 14, N-1306 Bærum postterminal, 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 Norwegian 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 the CC recognition arrangement applies to EAL 4.]

Contents

1 Certification Statement

Forsvarets Logistikkorganisasjon / Investeringsavdelingen/ NBF Thinklogical VX 40 Router KVM 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 VX 40 Router KVM Matrix Switch (VXR-000040 Rev B) has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 4 for the specified Common Criteria Part 2 conformant functionality in the specified environment when running on the platforms specified in Annex A.

Author	Kjartan Jæger Kvassnes Certifier
Quality Assurance	Lars Borgos Quality Assurance
Approved	Kjell W. Bergan Head of SERTIT
Date approved	18th April 2011

2 Abbreviations

CC	Common Criteria for Information Technology Security Evaluation
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
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
SERTIT	Norwegian Certification Authority for IT Security
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

3 References

[1] Thinklogical VX 40 Router KVM Matrix Switch Security Target, version 3.6, January 2011.

[2] Common Criteria Part 1, CCMB-2009-07-001, Version 3.1 R3, July 2009.

[3] Common Criteria Part 2, CCMB-2009-07-002, Version 3.1 R3, July 2009.

[4] Common Criteria Part 3, CCMB-2009-07-003, Version 3.1 R3, July 2009.

[5] The Norwegian Certification Scheme, SD001E, Version 8.0, 20 August 2010.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2009-07-004, Version 3.1 R3, July 2009.

[7] Evaluation Technical Report Common Criteria EAL4 Evaluation of Thinklogical Router KVM Matrix Switches, v 1.1, 2011-02-17.

[8] Configuration Management_1_3.doc

[9] VX40_160_320_Manual_Rev_I.pdf

[10] VX40 Assembly Procedure_Rev A.pdf

[11] VX40 Configuration List_1_2.doc

[12] VxRouter-ASCII-API_4_1.pdf

[13] VX Routers Switch Tables

[14] VX40_VEL-4_VEL-24_Quick_Start_Rev_B.pdf.

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Thinklogical VX 40 Router KVM Matrix Switch (VXR-000040 Rev B) to the Sponsor, Forsvarets Logistikkorganisasjon / Investeringsavdelingen/ NBF, 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 requirements.

4.2 Evaluated Product

The version of the product evaluated was Thinklogical VX 40 Router KVM Matrix Switch (VXR-000040 Rev B).

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

Thinklogical VX 40 Router KVM Matrix Switch 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 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 extender. The resulting signal is used by the shared peripherals.

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

4.3 TOE scope

4.3.1 System Type and Overview

The TOE is a Bi-directional routing system, which provides connection of 40 optical inputs located on the Upstream ports to any or all of the 40 optical outputs located on the Downstream ports and connection of 40 optical inputs located on the Downstream ports to any or all of the 40 optical outputs located on the Upstream ports. The TOE consists of 8 Data Upstream Cards having 5 optical input and Output ports and 8 Data Downstream Cards having 5 optical input and Output ports. 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:

- Thinklogical KVM Matrix Switch (VX40 Router)
- 8 Data Upstream Cards
- 8 Data Downstream Cards

Velocity Transmitter Extenders are connected to Transmitter Port Groups on the Data Upstream Cards of the Switch using optical fibers connections. Transmitter Port Groups are marked green on the VX40 Switch.

Velocity Receiver Extenders are connected to receiver port groups on the Data Downstream Cards of the Switch using optical fiber connections. Receiver Port Groups are marked blue on the VX40 Switch.

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 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 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 TOE can be administered over a wired 10/100BASE-TX LAN connection or the Serial (RS232) connection using an external management computer. This computer was not part of the evaluation, but assumed to be physically secure.

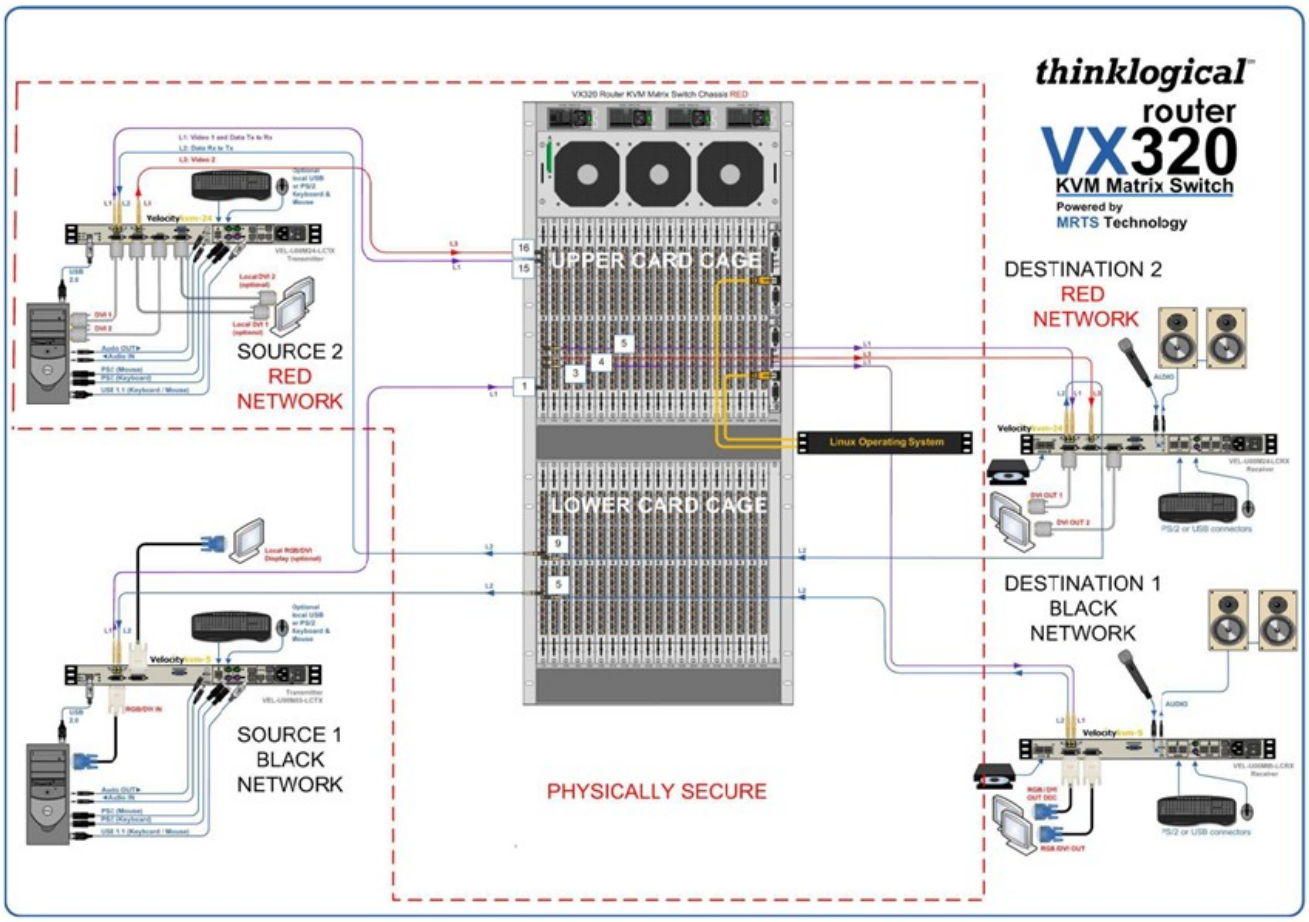


Figure 1 shows the VX320 Router in an evaluated configuration. An equivalent layout is the evaluated configuration for the VX40 and VX160 Routers.

4.3.2 TOE Physical Boundaries

VX 40 Router KVM Matrix Switch is a hardware device. TOE Physical Boundaries then correspond to the physical boundaries of the device enclosure.

4.3.3 TOE Logical Boundaries

TOE logical boundaries include all software and firmware components inside the VX40 Router KVM Matrix Switch.

The following Security Functions are provided by the TOE

- User Data Protection (enforces Data Separation SFP),

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

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 requirements 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 ST[1].

4.7 Security Claims

The Security Target[1] fully specifies the TOE's security objectives, the threats, Organisational Security Policies which these objectives meet and security functional requirements 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

- Residual data may be transferred between different port groups in violation of data separation security policy
- State information may be transferred to a port group other than the intended one

4.9 Threats Countered by the TOE's environment

- The TOE may be delivered and installed in a manner which violates the security policy.
- An attack on the TOE may violate the security policy.

4.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.11 Environmental Assumptions and Dependencies

- 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.
- The TOE meets the appropriate national requirements (in the country where used) for conducted/radiated electromagnetic emissions.
- The TOE is installed and managed in accordance with the manufacturer's directions.
- The TOE users and administrators are non-hostile and follow all usage guidance.

- Vulnerabilities associated with attached devices are a concern of the application scenario and not of the TOE.

4.12 IT Security Objectives

- 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.
- No information shall be shared between switched computers and peripheral sets via the TOE in violation of Data Separation SFP.

4.13 Non-IT Security Objectives

- The TOE shall meet the appropriate national requirements (in the country where used) for conducted/radiated electromagnetic emissions.
- The TOE shall be installed and managed in accordance with the manufacturer's directions.
- The authorized user shall be non-hostile and follow all usage guidance.
- 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.
- Vulnerabilities associated with attached devices or their connections to the TOE, shall be a concern of the application scenario and not of the TOE.

4.14 Functional Security Requirements

- Enforce the Data Separation Policy when exporting user data, controlled under the SFP, from outside of the TOE.
- Export the user data without the user data's associated security attributes.
- Enforce the Data Separation Policy 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.
- Enforce the Data Separation Policy 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)
- 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
- Enforce that 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.

- 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

4.15 Security Function Policy

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 uni-directional multi-cast video and audio signals from the Transmitter Port Group.

4.16 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 SD001[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 EVIT Commercial Evaluation Facility (CLEF/EVIT). The evaluation was completed when the EVIT submitted the final Evaluation Technical Report (ETR)[7] to SERTIT in 17.02.2011. SERTIT then produced this Certification Report.

4.17 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.

The EAL 4 evaluation of the Thinklogical VX 40 Router KVM Matrix Switch has shown that the TOE is methodically designed, tested and reviewed. The evaluation has further shown that the TOE is developed in a secure environment, uses well-defined development tools, has a properly defined life-cycle model and has procedures for standard commercial delivery services. The TOE is under proper configuration management, and follows strict procedures on how for instance changes to the TOE are reviewed and accepted. The guidance documentation helps install, administer and use the TOE in a secure manner. The TOE has been tested and reviewed for exploitable vulnerabilities using an Enhanced-Basic attack potential, by both the developer and evaluators.

If the TOE is not physically protected and managed as required for the highest level of security classified data handled or transferred by the TOE, the KVM switch can be tampered with leading to the compromise of sensitive data or a denial of service caused by the disruption of the systems the KVM switch is connected. In an evaluated configuration, the KVM switch is physically protected in accordance with the requirements of the highest classification connected to the KVM switch.

Without a backup of the KVM switch's configuration, a denial of service may occur if the configuration cannot be restored quickly in the advent that it is lost or a faulty switch needs to be replaced. Tests performed by the evaluator verify that configurations are not lost in case of fail-over between primary and secondary controller card, upstream/downstream cards or SFP+ modules.

If a network attached KVM switch is attached to a dedicated network there is less opportunity for a malicious user to compromise the interface and create a denial of service by issuing disruptive commands to a server. The guidance documentation states that the Network Hub is a dedicated network that is only used to connect the VX Router to the computer server. This dedicated network does not connect to any other components and does not extend beyond the physically secure environment. The dedicated network connection could be replaced by a direct serial connection (RS-232) between the VX Router and the computer server. It also states that the VX Router and the computer server used to manage the Router must be protected according to the highest security classification of any component in the entire network application.

Without a written description of the KVM switch, the management devices (CSCS) attached to the KVM switch, and the classification level of each information system attached to the KVM switch, tampering with the KVM switch by adding or moving

connections cannot be verified and the physical configuration cannot be reproduced if needed. This can lead to a denial of service if a connection is removed or moved or a compromise of sensitive data if a connection is added or moved. When the TOE is implemented in its operational environment, a written description of the KVM switch, the information systems attached to the KVM switch, and the classification level of each information system attached to the KVM switch should be created.

As the guidance documentation describes, it is recommended that the messages file are reviewed and any errors in the Restrictive Switching Table be corrected before implementing multiple levels of security classification domains on the same VX Router. It is also recommended that Restrictive Switching be fully tested before implementing multiple levels of security classification domains on the same VX Router.

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 Thinklogical Configuration Management process [8] assures that all products shipped from the warehouse are fully documented and that they follow the CM procedures. Products are shipped via Federal Express, UPS or DHL to the consumer. A signature is required at the receiving end for all shipments.

Dimensions and weight are noted for each shipment. The CM process assures that all tracking information and shipment information within Intuitive software are logged as well as hard copies in the Sales Order folder.

In the product manual [9], Part 1, Installation, there are provided acceptance procedures describing what the consumers should check for in the delivered product. These procedures should ensure that the consumers inspects the delivered product and finds it in good condition so that the installation process can begin.

5.3 Installation and Guidance Documentation

In the product manual [9] "Part 1: Hardware" there is included a text describing that user has to check that all parts of the TOE as indicated in the ST have been delivered in the correct version. If you have ordered an EAL4 certified unit, please verify that you have received the proper materials. The label described is in accordance with the ST [1].

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. Administrators should follow the guidance [9] for the TOE in order to ensure that the TOE operates in a secure manner.

The guidance documents adequately 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 administer and use the TOE's security functions.

5.5 Vulnerability Analysis

The evaluators' assessment of potential exploitable vulnerabilities in the TOE has been addressed and shows that the vulnerability analysis is complete, and that the TOE in its intended environment is resistant to attackers with an Enhanced-Basic attack potential.

5.6 Developer's Tests

The evaluators' assessments of the developers' tests shows that the developer testing requirements is extensive and that the TSF satisfies the TOE security functional requirements. The testing performed on the TOE by both the developer and evaluator showed that the EAL 4 assurance components requirements are fulfilled.

5.7 Evaluators' Tests

The evaluator have independently tested the TSFs and verified that the TOE behaves as specified in the design documentation and confidence in the developer's test results is gained by performing a sample of the developer's tests.

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 VX 40 Router KVM Matrix Switch (VXR-000040 Rev B) meet the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 4 for the specified Common Criteria Part 2 conformant functionality in the specified environment.

6.2 Recommendations

Prospective consumers of Thinklogical VX 40 Router KVM Matrix Switch (VXR-000040 Rev B) 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 under 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.

6.2.1 Restrictive Switching

Restrictive Switching is used to provide for multiple levels of security classification domains on the same VX Router. Each destination needs to ensure that no unauthorized content is displayed or accessed. Therefore, each input and output needs to be prioritized. Priorities can range from 1 to the total number of ports that can be connected in a switch matrix. An output can connect to an input with a priority greater than or equal to its priority.

The Restricted Switching function is performed according to a table defining the Input and Output port number and its priority value. The restricted output is determined before enabling the output.

VX40_160_320_320V_Manual_Rev_H.pdf, Appendix D: Secure Applications shows an explanation of how to provide a table defining priorities for each input and output of the switch matrix. This document describes how to create a csv file that will enable restrictive switching.
One very important point from this document is the exact description of the characters that **must** be used in the table, these are quoted below. Failing to use the characters exactly as described this will cause the Restrictive Switching to fail. Using advanced text editors (e.g. MS Word) to build the table can cause problems as many advanced text editors use auto-correct functions that will replace some ASCII characters with others.

Double quotes (or speech marks),	character code = 34	(")
Lower case i	character code = 105	(i)
Lower case o	character code = 111	(o)
Comma	character code = 44	(,)
Carriage Return	character code = 13	(CR)
Line Feed	character code = 10	(LF)

The VX Router will interpret the Restrictive Switching Table (csv file) during the boot-up. Any errors that occur during the Restrictive Switching Table interpretation process will be logged in the messages file at the following location:
var/log/messages

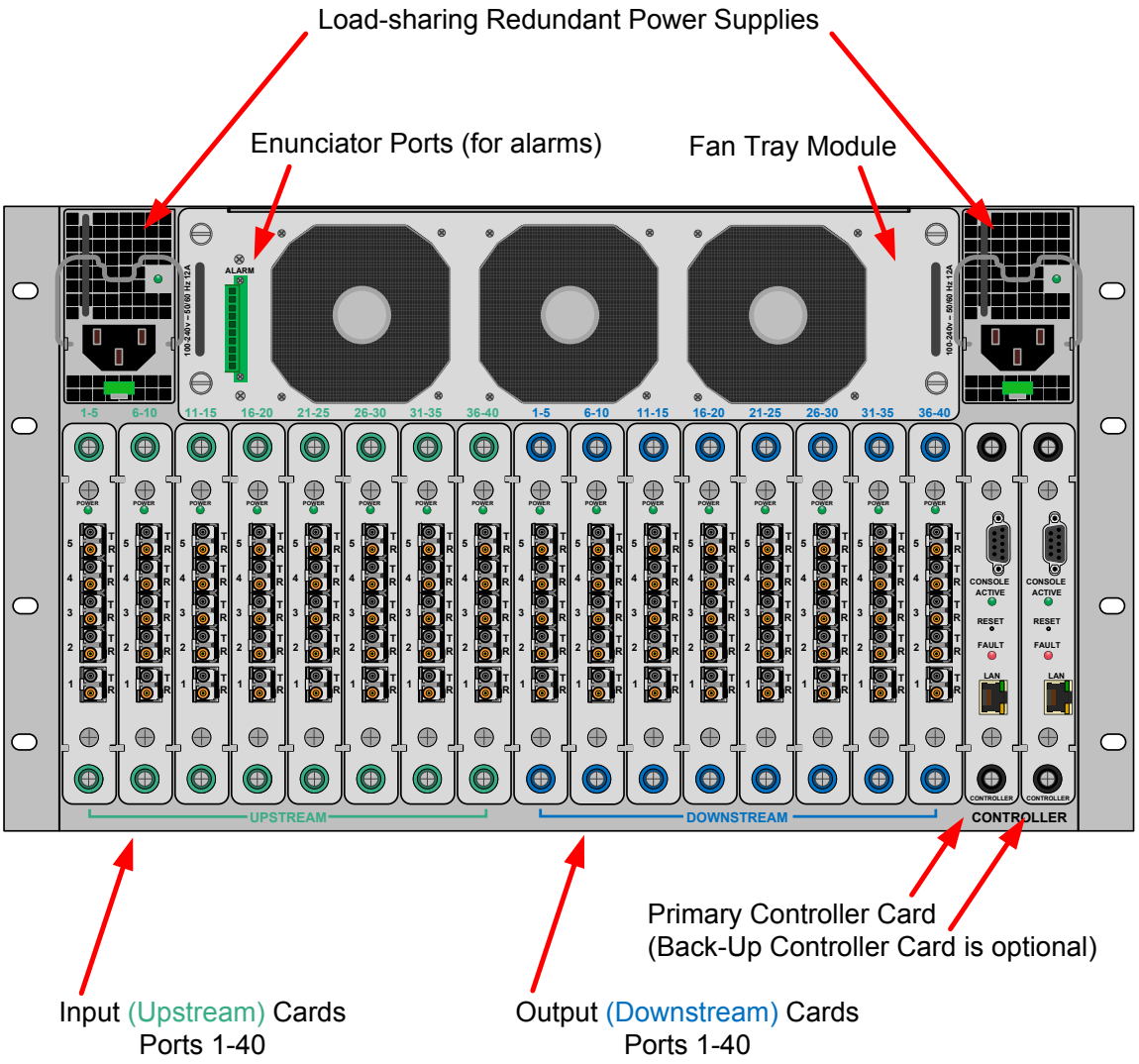
It is recommended that the messages file be reviewed and any errors in the Restrictive Switching Table be corrected before implementing multiple levels of security classification domains on the same VX Router. It is also recommended that Restrictive Switching be fully tested before implementing multiple levels of security classification domains on the same VX Router.

Annex A: Evaluated Configuration

TOE Identification

Thinklogical VX 40 Router KVM Matrix Switch is a fiber optic switch using 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 particular computer to a particular peripheral set. The TOE provides a capability to dynamically change the switching configuration.

NOTE: *All modules may be replaced without interruption to other module functions.*



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.

TOE Documentation

The supporting guidance documents evaluated were:

[a] ThinklogicalSecurityTarget_3_6_VX40.doc

[b] Configuration Management_1_3.doc

[c] Quality Manual Appendix_Rev_A.pdf

[d] Quality Manual Issue_Rev_New.pdf

[e] VX40_160_320_Manual_Rev_I.pdf

[f] VX40 Assembly Procedure_Rev A.pdf

[g] ALC.TAT.1_Intuitive_1_0.pdf

[h] ECR FORM_1_0.doc

[i] VX40 Configuration List_1_2.doc

[j] ALC.DEL_1_0.doc

[k] ALC_1_1.doc

[l] FlowChart_1_1.pdf

[m] Software ALC_TAT_1_1.pdf

[n] AutoCAD TAT_1.0.pdf

[o] ALC.TAT.1_Intuitive_1_0.pdf

[p] PADS POWERPCB.pdf

[q] Guide for PADS Projects Rev2.pdf

[r] ECRs_1_0.pdf

[s] ADV_ARC_1_1.pdf

[t] VX40_FunctionalSpec_1_1.pdf

[u] VX40_DesignSpec_1_2.pdf

[v] VxRouter-ASCII-API_4_1.pdf

[w] VX Routers Switch Tables

[x] MatrixSwitchContFlow_1_1.pdf

[y] VX40_VEL-4_VEL-24_Quick_Start_Rev_B.pdf

[z] VX40_VEL-3AV+_VEL-24_Quick_Start_Rev_B.pdf

[aa] VX Common Criteria Test-VX40_1_3.pdf

[bb] VX Common Criteria Test-VX40_1_3_with_test_results.pdf

[cc] ATE_COV_VX_1_3.doc

[dd] ATE_DPT_VX_1_2.pdf

[ee] VX40 Checklist_1_0.xls

[ff] VX40_test_1_0.doc

[gg] ALC_DVS_1_0.doc

[hh] Employee Manual_Rev A.pdf

[ii] Organization Chart_1_0.docx

[jj] Part Codes_1_0.xls

[kk] ADV_IMP_VX40_1_0.pdf

[ll] Using-the-ASCII-Interface_4_0.pdf

TOE Configuration

The following configuration was used for testing:

Velocity Matrix Router 40 (VXR-000040 Rev B)

Velocity Matrix Router 40 Data Upstream Card, 5 Ports, SFP+, Multi-Mode (VXM-DI0005 Rev A)

Velocity Matrix Router 40 Data Downstream Card, 5 Ports, SFP+, Multi-Mode (VXM-DO0005 Rev A)

Item	Identifier	Version
Hardware	Velocity Matrix Router 40	VXR-000040 Rev B
Hardware	Velocity Matrix Router 40 Data Upstream Card, 5 Ports, SFP+, Multi-Mode	VXM-DI0005 Rev A
Hardware	Velocity Matrix Router 40 Data Downstream Card, 5 Ports, SFP+, Multi-Mode	VXM-DO0005 Rev A
Manuals	VX40_160_320_Manual	Rev_I