Certification Report

Thinklogical TLX160 Matrix Switch Chassis (TLX-MSC-000160) Rev. B

Sponsor and developer:	***Thinklogical LLC*** **100 Washington Street, Milford** **Connecticut, 06460** **USA**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-2400066-01-CR**
Report version:	**1**
Project number:	NSCIB-2400066-01
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**29 January 2026**
Number of pages:	**12**
Number of appendices:	**0**

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TrustCB B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TrustCB B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TrustCB B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

Recognition of the Certificate

Presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Thinklogical TLX160 Matrix Switch Chassis (TLX-MSC-000160) Rev. B. The developer of the Thinklogical TLX160 Matrix Switch Chassis (TLX-MSC-000160) Rev. B is Thinklogical LLC located in Milford, USA and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

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 has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 29 January 2026 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the Thinklogical TLX160 Matrix Switch Chassis (TLX-MSC-000160) Rev. B, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the Thinklogical TLX160 Matrix Switch Chassis (TLX-MSC-000160) Rev. B are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.2 (Flaw reporting procedures).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TrustCB B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Thinklogical TLX160 Matrix Switch Chassis (TLX-MSC-000160) Rev. B from Thinklogical LLC located in Milford, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier		Version
Hardware	Thinklogical TLX160 Matrix Switch Chassis TLX-MSC-00160		Rev B
	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
	TLX160 Matrix Switch Module Controller Card TLX-MSM-C00160		Rev B
	iMX6 Processor Board, DCSA000081		Rev C
	TLX160 Matrix Switch Module Fan Tray TLX-MSM-F00160		Rev B
	TLX160 Backplane Board XGXA000019		Rev B
	TLX160 Matrix Switch Module Power Supply TLX-MSM-P00160		OEM / No Rev
Software	SFT-TLX160-15		TLX160 FIRMWARE VERSION V 5.10.03
	FLX-C00160-002		TLX160 FIRMWARE VERSION 0x100F

To ensure secure usage a set of guidance documents is provided, together with the Thinklogical TLX160 Matrix Switch Chassis (TLX-MSC-000160) Rev. B. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

The TOE includes the following Security Functions:

- **User Data Protection**
  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.

- **Security Management**
  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. The TSF management functions allow for the changes of logical TOE connection via the Restrict, Partition, and P2P Tables.

- **Protection of the TSF**
  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.

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

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

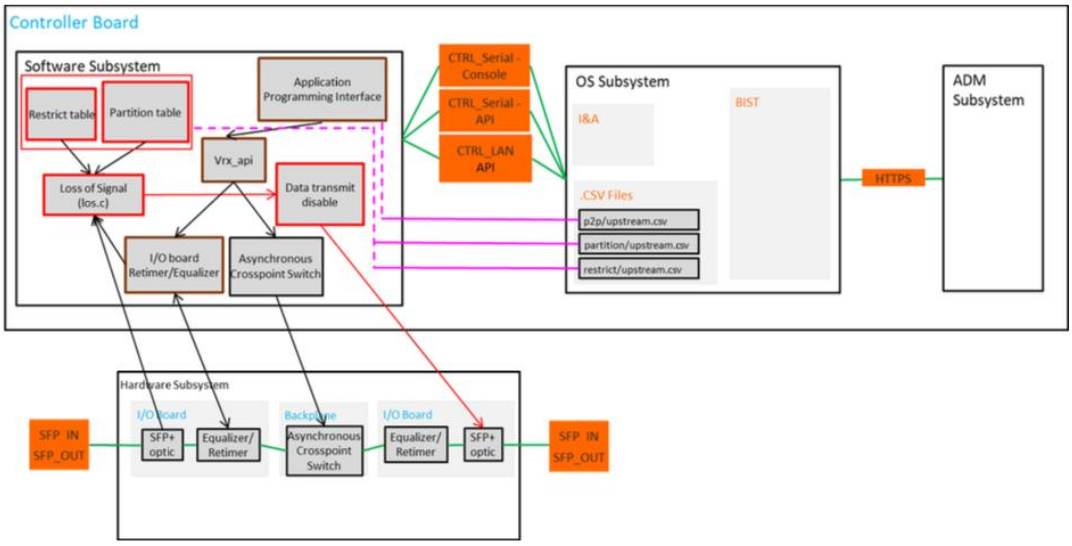
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

The TOE architecture can be depicted as follows:



2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
TLX160 Product Manual, dated June 2025	Revision I
TLX160 Quick Start Guide, dated January 2024	Revision B
Manual_Configuring_the_TLX_ASCII_Interface_Revision F March 2022 v_F, dated March 2022	Revision F
Manual_TLX_Matrix_Switch_ASCII_API_V5_Rev_N, dated October 2023	Revision N
Manual_How_To_Change_A_TLX_Matrix_Switch's_IP_Address_Rev_E, dated March 2022	Revision E
Manual_TLX_Matrix_Switch_Interfaces_Rev_I, dated March 2022	Revision I
Manual_TLX_Matrix_Switch_SNMP_Traps_Rev_K, dated March 2022	Revision K
Manual_TLX_Matrix_Switch_ADM_Rev_C, dated June 2024	Revision C

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer performed extensive testing on functional specification, subsystem and module level. All parameter choices were addressed at least once. All boundary cases identified were tested explicitly, and additionally the near-boundary conditions were covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. Test scripts were used extensively to verify that the functions return the expected values.

The evaluators reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

2.6.2 Independent penetration testing

Because the TOE is located in a physically protected environment where only trusted authorized administrator can access it and make any change (physical and logical) to it. The system user has very limited interaction with the TOE (switch the ports based on the restrictions, send hot key to make pre-defined connection, send key/mouse signal passing the TOE to the source, receive response from the source). Therefore, there is very limited attack surface and attack path to the TOE.

Due to the very limited attack path, the vulnerability analysis is performed in only three parts

- SFR Design Analysis: Based on the information obtained in the evaluation evidence, the SFR implementation details were examined. The aspects described in CEM annex B were considered. During this examination several potential vulnerabilities were identified.
- CWE Vulnerability focus: When the implementation of the SFR was understood, a coverage check were performed on the relevant aspects of all SFRs. This expanded the list of potential vulnerabilities.
- Public domain analysis: The evaluator performed public domain vulnerability search based on the TOE name, TOE type, and identified 3rd party security relevant libraries and/or services. Several additional potential vulnerabilities were identified during a search in the public domain.
- User mistakes: Considering that no external threat can reach the TOE and the internal users are trusted according to the OE, the only thing that remains are user mistakes. Potential vulnerabilities were identified during a search in this domain.

The potential vulnerabilities identified were analyzed, and some of the potential vulnerabilities were concluded not exploitable within in the Enhanced-Basic attack potential, or covered by guidance. For remaining potential vulnerabilities, penetration tests were devised.

The total test effort expended by the evaluators was 70 hours. During that test campaign, 100% of the total time was spent on logical tests.

2.6.3 Test configuration

The TOE was tested in the following configuration:

- TLX Matrix Switch Chassis TLX-MSC-000160 Rev B quantity 1
- TLX Matrix Switch Controller Card TLX-MSM-C000160 Rev B, quantity 2
- CONTROLLER CARD, PCB 000525-R REV A, ASSY XGXA-000020
- TLX Matrix Switch Data I/O Card TLX-MSD-M00010 Rev A, quantity 16
- 10 PORT FIBER I/O CARD, PCB 000527-R Rev A, ASSY XGXA-000022
- IMX6 PROCESSOR CARD, PCB 000458 –R REV C, ASSY DCSA-000081
- FAN TRAY, PCB 000529-R REV B, ASSY XGXA-000024
- BACKPLANE, PCB 000524-R REV B, ASSY XGXL-000019

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Reused Evaluation Results

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of 1 Site Technical Audit Report.

No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Thinklogical TLX160 Matrix Switch Chassis (TLX-MSC-000160) Rev. B.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the Thinklogical TLX160 Matrix Switch Chassis (TLX-MSC-000160) Rev. B, to be **CC Part 2 conformant, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC_FLR.2**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

The user of the TOE must carefully verify the correctness of the Restriction, Partition, and P2P csv tables as mentioned in the TLX160 Product Manual p.43, p47, and p49. The csv tables must be entirely correct, strictly follow the syntax defined for the restriction table, p42, partition table p45, P2P

table p48, and located in the right folder. Any error in the csv table may cause unexpected information flow or unexpected behaviour of the TOE.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

3 Security Target

The Thinklogical TLX160 Matrix Switch Security Target, Version 1.7, Dated November 2025 *[ST]* is included here by reference.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
NSCIB	Netherlands Scheme for Certification in the area of IT Security
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[ETR]	Evaluation Technical Report Thinklogical TLX160 Matrix Switch Chassis – EAL4+, 24-RPT-1218, Version 4.0, dated 8 December 2025
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[ST]	Thinklogical TLX160 Matrix Switch Security Target, Version 1.7, Dated November 2025

(This is the end of this report.)