Analysis: TLX1280 Matrix Switch Security Target

1. **Basics of Device Certified** The TOE is a 1280 x 1280 routing system, which provides connection of 1280 optical inputs located on the upper and lower card cage ports to any or all of the 1280 optical outputs located on the same upper and lower card cage ports. The TOE consists of 40 Data Input and Output Cards having 32 optical input and output ports. The 40 data Input and Output Cards installed in the upper and lower card cages can be used to connect any of the 1280 inputs, in one direction, to any output or multiple outputs.
2. **Assumed Attacker's model** No assumption about the attacker's model are explained in the Certificate Report. However as per threat model, the major threats are
   - The TOE may be delivered & installed in a manner that violates security policy.
   - An attack on TOE may violate security policy.
   - Residual data may be transferred between different port groups in violation of data separation security policy.
   - State information may be transferred to unintended port group.

3. **Testing mechanism**

   The evaluator vulnerability analysis was based on both public domain sources and the visibility of the TOE given by evaluation process. The vulnerability analysis took into consideration the Enhanced –Basic attack potential.

   Evaluators have devised set of tests to test potential vulnerabilities to TOE. The results of vulnerability analysis are that the TOE in its evaluated configuration and in its intended environment has no exploitable vulnerabilities.

   Developer's test and Evaluator's test have been carried out to ensure the TOE has desired behaviour. **No details about the type of test and mechanism are explained in the Certificate Report**.

4. **Referenced relevant Security Functional Components (SARs)**

   There is currently no Protection Profile directly applicable to the type of technology provided by the TOE. Peripheral Sharing Switch (PSS) For Human Interface Devices Protection Profile Version 1.2 (PSSPP) is applicable to the situation, where there is a single set of peripherals locally managing multiple computers.

5. Security Functional Components (SFRs)

- The TOE shall not violate the confidentiality of the information which it processes. Information gathered within the peripheral shall not be accessible by any other connection.
- No information shall be shared between switches computers and peripheral set via the TOE in violation of data separation SFP.
- The TOE shall meet the appropriate national requirements for electromagnetic emission.
- TOE doesn’t encrypt optical, wired network connections. The switch, the transmitter, the receiver and the optical connections from the Switch to the transmitter and receiver and the wired network connection has to be physically secured.
- Most of the TOE Security functional requirements are similar to the PSSPP.
    - 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 attributes

6. Out of scope of certification

- Vulnerabilities associated with attached devices or connections to TOE shall be concern of the application scenario not the TOE.
- The TOE users shall be non-hostile and follow all usage guidance.
- TOE shall be managed and installed as per manufacturer’s diections.

7. Evaluation and conclusions

As per my opinion, there are various shortcomings in the Certificate Report. The details about the attacker model are missing. There are no details about evaluation procedure described.

As per the Certificate Report the evaluators just independently tested a sample of developers test and verified that the TOE behaves as specified. However, it should have conducted more detailed tests. The tests are just carried out to check Functional testing and Independent testing.