Security Target

for

ADPICS Data Diode

Date: 10 August 2021

Revision History: 4

ATTILA CYBERTECH PTE LTD
39 Ubi Road 1, #05-01, World Publications Building, Singapore 408695
Tel: +65 6747 6116 | Fax: +65 6858 2884 | www.attilatech.com

Contents

ATTILA CYBERTECH PTE LTD
39 Ubi Road 1, #05-01, World Publications Building, Singapore 408695
Tel: +65 6747 6116 | Fax: +65 6858 2884 | www.attilatech.com

1. Security Target Introduction (ASE_INT.1)

1.1. Security Target Reference

ST Title	ADPICS® Data Diode Security Target
ST Version	4.0
ST Classification	Public
Evaluation Assurance Level	EAL 1
Number of pages	9
Common Criteria Version	3.1, Revision 5, April 2017

1.2. TOE Reference

Developer Name	Attila Cybertech Pte Ltd
TOE Name	ADPICS Data Diode (ADPICS-DD)
TOE Version Number	ADPICS-DD v1.0

1.3. TOE Overview

The Target of Evaluation (TOE) is a network gateway that ensures **physical layer** one-way data transmission through the TOE.

The Target of Evaluation (TOE) is the ADPICS Data Diode (ADPICS-DD) developed by Attila Cybertech Pte Ltd, and will hereafter be referred to as the TOE throughout this document.

The TOE is a unidirectional network, as shown in figure 1, allowing data to travel only in one direction.

The one-way physical connection of the TOE allows information to be transferred optically from a Source Zone (eg: PLCs, Field devices) to a Destination Zone (eg: Corporate network) without compromising the availability of the information on the Source Zone.

To ensure signals can only pass in one direction, but not vice versa, the TOE deploys a light source and corresponding photocell.

Fibre-optic cables are used to minimize the electromagnetic radiation when the TOE input is connected to Source Zone's Proxy the and the TOE output is connected to the Destination Zone's Proxy.

Once manufactured, there is no way to alter the function of the TOE.

When the Source Zone's Proxy is connected to Destination Zone's Proxy as is indicated in figure 1 the TOE and can be deployed in the following scenarios:

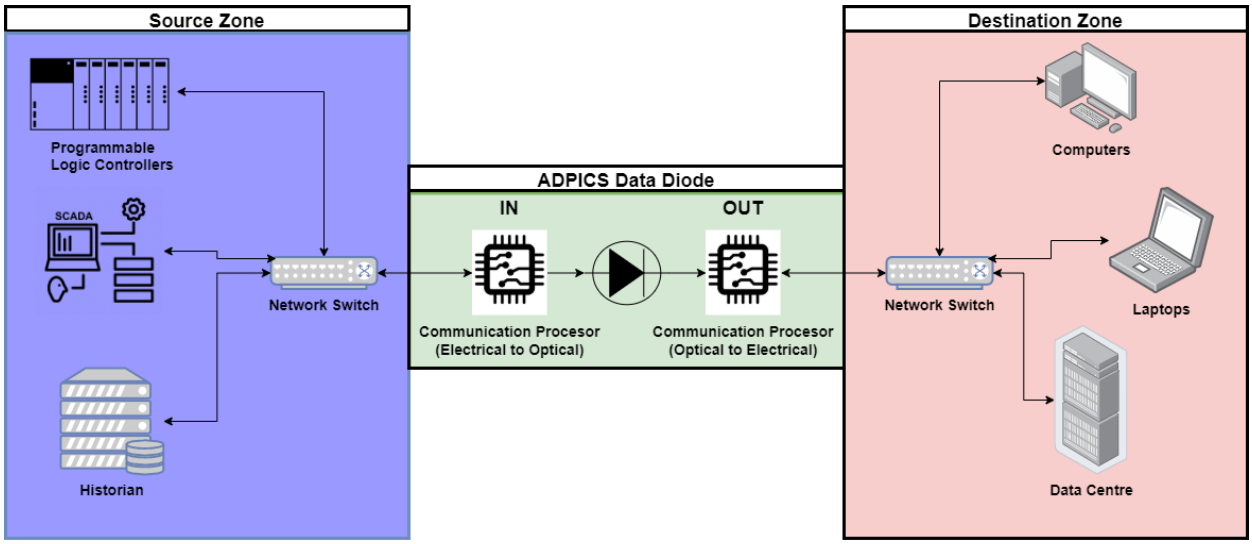

Figure 1 – Possible Deployment Scenario

1.4. TOE Description

1.4.1. Physical Scope

No.	Item	Version	Type	Part of TOE?
1	Attila ADPICS Data Diode	1.0	Hardware	YES
2	Attila ADPICS Data Diode User Guidance	1.0	Soft Copy Documentations (.pdf)	YES

Delivery Method

The delivery of the ADPICS Data Diode would be done by a trusted courier. Both data diode hardware, User guidance will be included in the package. The ADPICS Data Diode, should be free from any tempering by checking the security seal and the serial number should coincide with the packaging box or the delivery order.

1.4.2. Logical Scope

The TOE only allows data to flow from the Source Zone to the Destination Zone. Due the physical customisation of the cable and the interface, data does not flow in the reverse direction. Reverse data flow interfaces are physically disconnected hence it's physically not possible to transmit data.

2. Conformance Claim (ASE_CCL.1)

2.1. CC Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 5, dated: April 2017. The TOE and ST are CC Part 2 conformant and CC Part 3 conformant.

2.2. Protection Profile Claim, Package Claim

Claim conformance to EAL 1.

2.3. Conformance Rationale

None

3. Security Objectives (ASE_OBJ.1)

3.1. Security Objectives for the Operational Environment

The following security objectives are required in correctly providing its one-way data transmission security function of Source Zone, in accordance with the following objectives:

OE.PHYSICAL	The intended operation environment shall be capable of storing and operating the TOE in accordance with the requirements of the Source Zone.
OE.NETWORK	The TOE is the only method of interconnecting Source Zone to the Destination Zone.
OE.USER	The users are trusted; the users shall not maliciously compromise the security functionality of the TOE.

4. Security Requirements (ASE_REQ.1)

4.1. Security Functional Requirements (SFRs)

The TOE uses two subjects: Input and Output. These represent the input and output of the TOE. These subjects have no attributes.

This statement of SFRs does not define other subjects, objects, operations, security attributes or external entities.

There are four font conventions used :-

1) Assignment : Indicated with **bold** text
2) Selection : Indicated with *italicized* text
3) Iteration : Indicated by appending the iteration symbol (FCS_COP.1/AES, FCS_COP.1/RSA)
4) Refinement : Indicated with ***bold italicized*** text

4.1.1. Complete Information Flow Control (FDP_IFC.2)

Hierarchical to FDP_IFC.1 Subset information flow control

Dependencies FDP_IFF.1 Simple security attributes

FDP_IFC.2.1 The TSF shall enforce the **one-way data transmission in the physical layer** on **all information from Source Zone to Destination Zone through the TOE** and all operations that cause that information to flow to and from subjects covered by the TOE.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered.

4.1.2. Simple Security Attributes (FDP_IFF.1)

Hierarchical to No other components

Dependencies FDP_IFC.1 Subset information flow control
FMT_MSA.3[1] Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the **one-way data transmission in the physical layer** based on the following types of subject and information security attributes:
Subject: Source Zone, Destination Zone
Information security attribute: Subject Identity[2]

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:

a) **The TSF shall allow the data from Source Zone to flow to the Destination Zone.**

FDP_IFF.1.3 The TSF shall enforce the **None**.

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: **None**.

[1] FMT_MSA.3 is not applicable as there is no security attributes to initalise
[2] The subject identity is defined as the Source Zone and Destination Zone

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: **None**.

4.2. Security Assurance Requirements (SARs)

The security assurance requirements for the TOE are the Evaluation Assurance Level 1.

Assurance Class	Assurance Component
ADV: Development	ADV_FSP.1 – Basic functional specification
AGD: Guidance documents	AGD_OPE.1 – Operational user guidance
	AGD_PRE.1 – Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 – Labelling of the TOE
	ALC_CMS.1 – TOE CM coverage
ASE: Security Target evaluation	ASE_CCL.1 – Conformance claims
	ASE_ECD.1 – Extended components definition
	ASE_INT.1 – ST introduction
	ASE_OBJ.1 – Security objectivates for the operational environment
	ASE_RFQ.1 – Stated security requirements
	ASE_TSS.1 – TOE summary specification
ATE: Tests	ATE_IND.1 – Independent testing – conformance
AVA: Vulnerability assessment	AVA_VAN.1 – Vulnerability survey

4.3. Extended Component Definition (ASE_ECD.1)

All security requirements in this ST are based on components from CC Part 2 [2] and CC Part 3 [3], therefore there are no Extended Component Definitions.

4.4. Security Requirements Rationale

The table below shows the rationale on the satisfaction of all security requirement dependencies.

SFR	Dependency	Justification
FDP_IFC.2	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC1	FDP_IF.2
	FMT_MSA.3	FMT_MSA.3 is not applicable because there is no security attributes to initialize

5. TOE Summary Specification (ASE_TSS.1)

The TOE focuses on two security functional requirements: FDP_IFC.2 and FDP_IFF.1. Both works together to comply to the security objective of the TOE.

FDP_IFC.2: The TOE consists of two independent network interfaces where one is connected to the Source Zone and the other to the Destination Zone.

FDP_IFF.1: The IN network interface converts incoming electrical signals from the source zone into optical signals and sends it to the optical receiver and converts to electrical signal and sends it through the OUT network interface to the Destination Zone, hence enforcing a one way communication.

References

1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, April 2017, Version 3.1 Revision 5

2. Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, April 2017, Version 3.1 Revision 5

3. Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, April 2017, Version 3.1 Revision 5

4. Common Criteria for Information Technology Security Evaluation, Evaluation methodology, April 2017, Version 3.1 Revision 5.