Arbit Data Diode 10GbE
Security Target Lite

Arne Stig Peters, Confiware ApS
Rasmus Borch, Arbit Cyber Defence Systems ApS

10.12.2020

Contents

1 Introduction

1.1 Security Target Identification

Title:	**Arbit Data Diode 10 GbE Security Target Lite**
Version:	1.01
Date:	10.12.2020
Sponsor:	Arbit Cyber Defence Systems ApS
Developer:	Arbit Cyber Defence Systems ApS

1.2 TOE Identification

Identification:	**Arbit Data Diode 10 GbE**
Version:	1.00

1.3 Certification ID

The BSI Certification ID is BSI-DSZ-CC-1096.

2 TOE

2.1 TOE Overview

2.1.1 TOE Type

One-way data diode for optical information.

2.1.2 Usage

The increasing threat from various actors to gain access to confidential company data or cause unauthorized modifications to the IT infrastructure has forced many companies to separate their production network from less trusted networks such as the Internet.

While this eliminates the immediate threat, it also has a negative impact on productivity. Networks may need access to up-to-date data only available on the less secure one. It could be a need for information available on the Internet or on less secure internal networks. While a physical separation and manual media transfer is possible it is not a convenient way to allow unidirectional information flow only.

Other companies choose a middle way and enforce flow policies through routers and firewalls between networks. While this provides a certain level of protection, it does not prevent unwanted information flows that are able to hide within allowed traffic nor does it prevent interactive access to the closed network either by approved or covert channels in the product.

A data diode combines the advantages of both solutions. It is the connection point between a receiving security and sending security network. The actual transmission

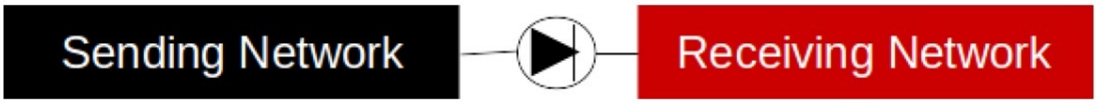

Figure 1: Overview of the concept of the one-way data diode.

is handled by two dedicated servers, with the data diode in between them. The data diode ensures that information can only flow from the Sending Network to the Receiving Network, but not the other way. This allows for automated information transfer from the sending security network to the receiving security network without manual intervention, while preventing the opposite flow direction.

Another usage scenario is the export of information from a protected network to a more open environment. The security goal is in this case to allow the export, while preventing any potential attacks from reaching the protected network. One example is the export of log data from a sensitive SCADA system such as a nuclear plant, to an external log analyzer. The data diode will allow the export, while preventing any influence back into the SCADA system.

Major Security Features:

Ensuring that the information flow through the data diode is one-way only.

2.1.3 Required non-TOE Hardware/Software/Firmware

The TOE requires a single fiber optic cable from the sender and SPF+ cage and its electrical interface connector to TOE. The formfactor and electrical interface shall be respectively in accordance with [2] and [1].

No further non-TOE software or firmware is required.

2.1.4 Optional non-TOE Software

As an option not required by the TOE, Arbit ApS has developed a highly reliable implementation of the communication software that can utilize the TOE.

2.2 TOE Description

The TOE implements the one-way data diode by sending the signal emitted by the sender (part of the Sending network) to the Receiver (part of the Receiving network). The optical fiber from the Sender connects to the INPUT port of the TOE. The electrical connection to the receiver connects to the OUTPUT and POWER port of the TOE. The only allowed information flow is therefore from the Sending to the Receiving Network.

The OUTPUT and POWER port is two logical interfaces which are located in one physical connector. TOE is physical separate circuit board, which can be attached to

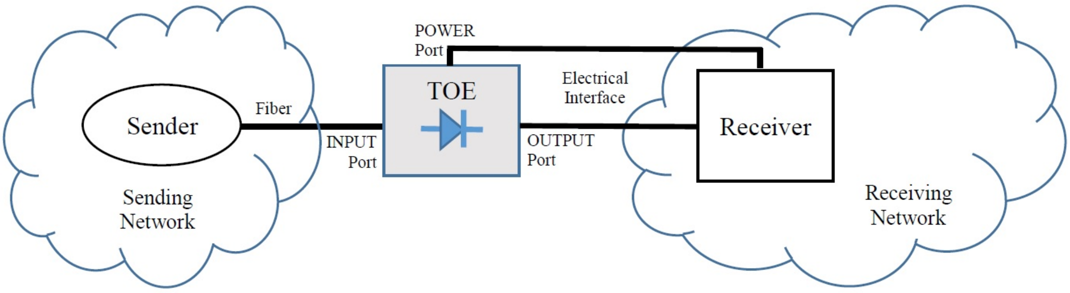

Figure 2: TOE placement and interfaces.

a Receiver. The INPUT port has a physical light receiver and has no light emitting capability. The TOE implementation is only utilizing the physical property of the TOE and is not dependent on any software or firmware.

All signal processing in the TOE is performed in hardware at the Physical Medium Dependent sublayer in Ethernet. The TOE does not perform any higher layer signal parsing such as Ethernet frames or TCP/IP processing.

2.2.1 Physical Scope of the TOE

The TOE is hardware-only, and consists of a SFP+ formfactor module. Installation of TOE shall be performed in accordance with the integration guidance, [5].

The delivery of TOE and its Integration Guide shall be performed as trusted personal handover in accordance with the delivery procedure. The delivery consist of the following items:

1. SFP+ module.
2. Integration Guide on paper format.

2.2.2 Logical Scope of the TOE

The security feature within the logical scope of the TOE is:

- Ensuring that the information flow from the INPUT port only can be received and it is not possible to send any information from the OUTPUT port via the INPUT port to sending network.

3 Conformance Claim

Common Criteria version 3.1 revision 5 is the basis for this conformance claim. This Security Target is CC Part 2 [3] conformant and CC Part 3 [4] conformant, with a claimed Evaluation Assurance Level of EAL7, augmented by ALC_FLR.1. This Security Target does not claim conformance to any Protection Profile.

4 Security Problem Definition

4.1 Threat Environment

A threat consists of an adverse action performed by a threat agent on an asset. Adverse actions are actions performed by a threat agent on an asset. These actions influence one or more properties of an asset from which that asset derives its value. Threat agents are described as types of entities or groups of entities.

Asset	Definition
RECEIVING_INFO	Any information entering the OUTPUT port of the TOE.

Table 1: Assets.

Threat Agent	Definition
TA-SENDING	Any SENDING system connected to TOE on the INPUT port or attackers having access to the SENDING network. The SENDING system might consist of a diversity of products and equipment with very high capabilities for subverting the security policy. Attackers have high motivation and capabilities.
TA-RECEIVING	Any RECEIVING system connected to TOE on the OUTPUT port or attackers having access to the RECEIVING network. The RECEIVING system might consist of a diversity of products and equipment with very high capabilities for subverting the security policy. Attackers have high motivation and capabilities.

Table 2: Threat Agents.

4.1.1 Threats

Threat	Definition
T.DATA_LEAK	TA-SENDING and/or TA-RECEIVING threat agents may be able to manipulating the INPUT and/or OUTPUT port such that RECEIVING-INFO to exit the TOE through the INPUT port.

Table 3: Threats.

4.2 Assumptions

Assumption	**Definition**
A.INTEGRATOR	The integrator who is performing the installation of the TOE is well-trained and competent in the prevention of signal leakage, and will properly adhere to the TOE guidance.
A.PHYSICAL	The TOE and its interfaces will be physically protected from unauthorized access and mechanical, electrical, optical, radiation or any other form of physical influence.
A.POWER	Power supply to TOE shall be 3.3 V +/-5%. The minimum current capacity, both continuous and peak, shall be 500 mA.

Table 4: Assumptions.

4.3 Organizational Security Policies

Organizational Security Policy	**Definition**
P.ONE_WAY_FLOW	The TOE shall allow information to enter through the INPUT port and then leave through the OUTPUT port and deny information flow from the OUTPUT to the INPUT.

Table 5: Organizational Security Policies.

Application Note:

The policy is only concerning the allowed information flow which may flow. It is not a policy concerning availability, e.g. the guarantee that information received on INPUT port actually will be transmitted on the OUTPUT port.

5 Security Objectives

5.1 Security Objectives for the TOE

Objective	**Definition**
O.NO_RECEIVING_INFO	The TOE must ensure that no information that may have entered through the OUTPUT port is able to leave through the INPUT port.

Table 6: Security Objectives for the TOE.

5.2 Security Objectives for the Operational Environment

Objective	Definition
OE.INTEGRATOR	The integrator who is performing the installation of the TOE shall be well-trained and competent in the prevention of signal leakage, and shall properly adhere to the TOE guidance.
OE.PHYSICAL	The TOE and its interfaces shall be physically protected from unauthorized access.
OE.POWER	Power supply to TOE shall be 3.3 V +/-5%. The minimum current capacity, both continuous and peak, shall be 500 mA.

Table 7: Security Objectives for the Operational Environment.

5.3 Security Objectives Rationale

5.3.1 Coverage

The following table provides a mapping of TOE objectives to threats and policies, showing that each objective counters or enforces at least one threat or policy, respectively.

Objective	Threat / OSP
O.NO_RECEIVING_INFO	T.DATA_LEAK

Table 8: TOE Security Objectives Coverage.

The following table provides a mapping of the objectives for the Operational Environment to assumptions, threats and policies, showing that each objective holds, counters or enforces at least one assumption, threat or policy, respectively.

Objective	Assumption / Threat / OSP
OE.INTEGRATOR	A.INTEGRATOR T.DATA_LEAK
OE.PHYSICAL	A.PHYSICAL T.DATA_LEAK
OE.POWER	A.POWER T.DATA_LEAK

Table 9: Operational Environment Security Objectives Coverage.

5.3.2 Sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat.

Threat	Rationale for Security Objectives
T.DATA_LEAK	TA-SENDING and/or TA-RECIEVING threat agents may be able to cause RECEIVING_INFO to exit the TOE through the SENDING port. This threat is diminished by: • O.NO_RECEIVING_INFO, which ensures that no information is able to spill over inside the TOE from the OUTOPUT port to the INPUT port. • OE.INTEGRATOR, which ensures that the integrator who is performing the installation of the TOE is well-trained and competent in the prevention of signal leakage, and is properly adhering to the TOE guidance. • OE.PHYSICAL, which ensures that the TOE and its interfaces are physically protected from unauthorized access. • OE.POWER, which ensures that components are operating within power supply specification.

Table 10: Sufficiency of objectives countering threats.

The rationale for the assumptions is done by a direct mapping of each assumption to a security objective for the environment with corresponding name and description. Each security objective is a restatement of the assumption, it is therefore self-explanatory.

Assumption	Rationale for Security Objectives
A.PHYSICAL	OE.PHYSICAL
A.POWER	OE.POWER
A.INTEGRATOR	OE.INTEGRATOR

Table 11: Sufficiency of objectives holding assumptions.

The rationale for the organizational security policy is done by a direct mapping of the OSP to the security objective for the TOE with corresponding name and description. The TOE security objective is a restatement of the OSP, it is therefore self-explanatory.

OSP	Rationale for Security Objectives
P.ONE_WAY_FLOW	O.NO_RECEIVING_INFO

Table 12: Sufficiency of objectives holding OSPs.

6 Extended Component Definition

No additional extended components are needed and therefore none are defined.

7 Security Requirements

The TOE implements the One-Way information flow control policy (One-Way SFP), which is defined as:

Subjects:

- INPUT port
  The input interface of the data diode.
- OUTPUT port
  The output interface of the data diode.

Object:

- The Information received or send on the INPUT port and/or OUTPUT port. Information is on the INPUT port an optical signal and on the OUTPUT port is Information an electrical signal.

Policy:

- Information is allowed to enter the TOE through the INPUT port and may leave through the OUTPUT port.
- Information from the OUTPUT port is not allowed to leave the TOE through the INPUT port.

Object Information on INPUT port and OUTPUT port is not exact the same Information representation, but a transformed representation.

7.1 TOE Security Functional Requirements

7.1.1 User data protection (FDP)

Complete information flow control (FDP_IFC.2)

FDP_IFC.2.1 The TSF shall enforce the [assignment: One-Way SFP] on [assignment: the subjects INPUT port and OUTPUT port] and all operations that cause that information to flow to and from subjects covered by the SFP.

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 by an information flow control SFP.

Simple security attributes (FDP_IFF.1)

FDP_IFF.1.1 The TSF shall enforce the [assignment: One-Way SFP] based on the following types of subject and information security attributes: [assignment: subjects INPUT port and OUTPUT port].

Application Note: No security attributes are stated. Any instance of defined information type, independent of its further properties, is covered by this SFR.

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: [assigment:

- Object Information read from subject INPUT port shall allow the transformation operation f write to subject OUTPUT port, where f is a transformation function from an optical signal to an electrical signal.
- Object Information read from subject OUTPUT port shall deny the transformation operation g write to subject INPUT port, where g is a transformation function from electrical signal to an optical signal.
- Object Information read from subject OUTPUT port shall allow the transformation operation h_1 write to subject OUTPUT port, where h_1 is a transformation function from an electrical signal to an electrical signal.
- Object Information read from subject INPUT port shall allow the transformation operation h_2 write to subject INPUT port, where h_2 is a transformation function from an optical signal to an optical signal.].

FDP_IFF.1.3 The TSF shall enforce the [assignment: rule in FDP_IFF.1.2 only].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: No further rules].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [assignment: No further rules].

7.2 Security Requirements Rationale

7.2.1 SFR Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

Security functional requirement	Objectives
FDP_IFC.2	O.NO_RECEIVING_INFO
FDP_IFF.1	O.NO_RECEIVING_INFO

Table 15: Mapping of security functional requirements to security objectives.

7.2.2 SFR Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives.

Security objectives	Rationale
O.NO_RECEIVING_INFO	The TOE must ensure that no information that may have entered through the OUTPUT port is able to leave through the INPUT port. This objective is satisfied by: • FDP_IFC.2, which ensures that any information flow in the TOE is covered by the "One-Way" SFP. • FDP_IFF.1, which denies any information from OUTPUT port to leave through the INPUT port.

Table 16: Security objectives for the TOE rationale.

7.2.3 Security Requirements Dependency Analysis

Dependencies within the EAL7 package selected for the security assurance requirements have been considered by the authors of CC Part 3 and are not analysed here again. The included component on flaw remediation (ALC_FLR.1) has no dependencies on other requirements.

The security functional requirements in this Security Target do not introduce dependencies on any security assurance requirement; neither do the security assurance requirements in this Security Target introduce dependencies on any security functional requirement.

The following table demonstrates the dependencies of SFRs modelled in CC Part 2 and how the SFRs for the TOE resolve those dependencies.

Security functional requirement	Dependencies	Resolution
FDP_IFC.2	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	FDP_IFC.2 Not resolved. The TOE configuration is static and has therefore no concept of manageable security attributes. This dependency SFR is therefore not applicable.

Table 17: TOE SFR dependency analysis.

7.3 Security Assurance Requirements Description

The security assurance requirements (SARs) for the TOE are the Evaluation Assurance Level 7 components as specified in [4], augmented by ALC_FLR.1.

The following assignment operations have been perform for the SAR:

Security policy modelling (ADV_SPM.1)

ADV_SPM.1.1D The devloper shall provide a formal security policy model for the [assignment: One-Way SPF defined by FDP_IFC.2 and FDP_IFF.1].

7.4 Security Assurance Requirements Rationale

The evaluation assurance requirements were selected from an EAL to provide a balanced level assurance and to be appropriate with this assurance level for this type of product and consistent with the security objectives of the TOE, the TOE should withstand an attacker with an attack potential of High.

7.5 TOE Summary Specification

The TOE provides one security functionality, which represents the overall TOE Security Function (TSF).

7.6 One-Way Information Flow

The TOE implements the one-way data diode through a repeater, where a fiber optic network cable is connected to the INPUT port and a Receiver connection on the OUTPUT port. Information can only be received from the Sending network connected on the INPUT port, and no information can spill over to the INPUT port from the OUTPUT port. Information received on the INPUT port is allowed to exit through the OUTPUT port, without further processing. This TSF is mapped to the following SFRs: FDP_IFC.2, FDP_IFF.1

A Revisions, Abbreviations and Terminology

Revision	Date	Author	Description
1.00	08-12-2020	RB	First version compiled from ST authored by ASP.
1.01	10-12-2020	RB	Prepared for BSI web publication.

Table 18: Revision history.

Abbreviation	Description
BSI	Bundesamt für Sicherheit in der Informationstechnik. In English: Federal Office for Information Security.
CC	Common Criteria
EAL	Evaluation Assurance Level
ID	Identity document
nm	Nano meter
OSP	Organizational Security Policy
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFP+	Enhanced Small form-Factor Pluggable according to [2].
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

Table 19: Abbreviation.

Terminilogy	**Description**
Receiver	The entity receiving information from the data diode. It resides on the Receiving network.
Data diode	A device that allows information to flow from the input to the output, but not the other way.
Receiving network	The network which is to receive information from the Sending network, through the TOE.
OUTPUT port	The output interface of the data diode. Receiving devices and networks are connected to this interface.
Receiving system	Any system residing on the Receiving network, excluding the TOE.
Information	A signal that can traverse the OUTPUT or INPUT port.
Sending network	The network which is to send information through the TOE.
INPUT port	The input interface of the data diode. Sending devices and networks are connected to this interface.
Sending system	Any system residing on the Sending network, excluding the TOE.
Sending	The entity sending information to the data diode. It resides on the Sending network.
Port	The physical interface by which the cables are connected to the TOE.

Table 20: Terminology.

References

[1] SFF Committee. *SFF-8431 Specifications for Enhanced Small Form Factor Pluggable Module SFP+*. https://www.snia.org, Rev 4.1, 6th of July 2009.

[2] SFF Committee. *SFF-8432 Specification for SFP+ Module and Cage*. https://www.snia.org, Rev 5.2a November 30, 2018.

[3] Common Criteria. *Common Criteria for Information Technology Security Evaluation. Part 2: Security functional components*. Number CCMB-2017-04-002. Common Criteria, April 2017 Version 3.1, Revision 5.

[4] Common Criteria. *Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance components*. Number CCMB-2017-04-003. Common Criteria, April 2017 Version 3.1, Revision 5.

[5] Arne Stig Peters. *Arbit Data Diode 10GbE – Integration Guide*. Number ARBIT0006. Arbit Cyber Defence Systems ApS, 2020, version 1.08.