Arbit Data Diode
Security Target

Eurotempest AB
Teknikringen 10
SE-583 30 Linköping
Sweden

eurotempest.net
e-mail: info@eurotempest.net
tel: +46 142 525 10
fax: +46 142 507 90

Document history

Version	Change Date	Author	Changes
3.0	7/5/16	Robert Hoffmann	First release
4.0	5/9/16	Tommy Pedersen	Second release

Table of Contents

1 Introduction

1.1 Security Target Identification

Title:	Arbit Data Diode Security Target
Version:	4.0
Status:	Release
Date:	2016-09-05
Sponsor:	Eurotempest AB
Developer:	Eurotempest AB
Keywords:	Data Diode, One-Way Gateway

1.2 TOE Identification

Arbit Data Diode v2.0

1.3 TOE Overview

1.3.1 TOE Type

One-way data diode for optical information.

1.3.2 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 high security and low security network. The actual transmission is handled by two dedicated servers, with the data diode in between them. The sending server is called a pitcher, and the receiving server is called a catcher. The data diode ensures that information can only flow from the pitcher to the catcher, but not the other way. This allows for automated information transfer from the low security network to the high security network without manual intervention, while preventing the opposite flow direction.

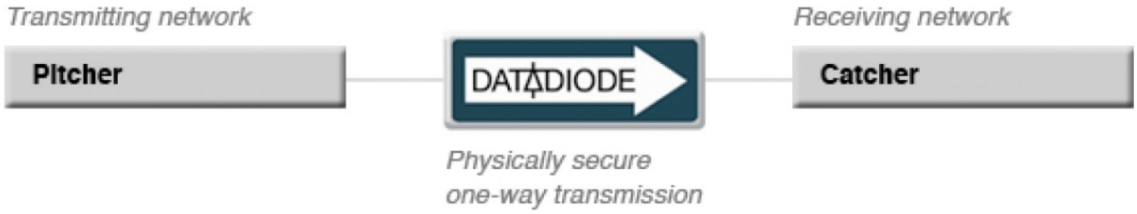

Figure 1: Overview of the concept of the one-way data diode

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.

1.3.3 Major Security Features

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

1.3.4 Required non-TOE Hardware/Software/Firmware

The TOE requires a single fiber optic cable from the pitcher and a single fiber optic cable to the catcher.

No further non-TOE software or firmware is required.

1.3.5 Optional non-TOE Software

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

1.4 TOE Description

Figure 2: TOE placement and interfaces

The TOE implements the one-way data diode by repeating the signal emitted by the pitcher (part of the LOW network) to the catcher (part of the HIGH network). The optical fiber from the pitcher connects to the LOW port of the TOE. The optical fiber to the catcher connects to the HIGH port of the TOE. The only allowed information flow is therefore from the LOW to the HIGH side.

The HIGH port has a physical light emitter.

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

All signal processing in the TOE is performed in hardware at the Physical Medium Dependent sublayer in Ethernet [IEEE 802.3]. The TOE does not perform any higher layer signal parsing such as Ethernet frames or TCP/IP processing.

The TOE supports a range of light signals up to 10.3125 Gbps. The specific supported light range of each TOE is determined during production based on customer requirements.

1.4.1 Physical Scope of the TOE

The TOE is hardware-only, and consists of a printed circuit board.

The TOE is provided in a variant with a receiver and a transmitter suitable for a wavelength of 850nm.The TOE guidance is also within the physical scope, and consist of the “Arbit Data Diode Integrator Guide v2.0”.

1.4.2 Logical Scope of the TOE

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

- Ensuring that the information flow from the LOW port to the HIGH port is one-way only.

2 Conformance Claim

Common Criteria [CC] version 3.1 revision 4 is the basis for this conformance claim.

This Security Target is CC Part 2 conformant and CC Part 3 conformant, with a claimed Evaluation Assurance Level of EAL5, augmented by AVA_VAN.5 and ALC_FLR.1.

This Security Target does not claim conformance to any Protection Profile.

3 Security Problem Definition

3.1 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
HIGHINFO	Any information entering the HIGH port of the TOE from the HIGH network.

Table 1: Assets

Threat Agent	Definition
TA-LOW	Any LOW system connected to TOE on the LOW network or attackers having access to the LOW system. The LOW 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-HIGH	Any HIGH system connected to TOE on the HIGH network or attackers having access to the HIGH system. The HIGH 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

3.1.1 Threats

Threat	Definition
T.DATA_LEAK	TA-LOW and/or TA-HIGH threat agents may be able to cause HIGHINFO to exit the TOE through the LOW port.

Table 3: Threats

3.2 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.

Table 4: Assumptions

3.3 Organizational Security Policies

P.ONE_WAY_FLOW	The TOE shall allow information to enter through the LOW port and then leave through the HIGH port.

Table 5: Organizational Security Policies

4 Security Objectives

4.1 Security Objectives for the TOE

Objective	Definition
O.NO_HIGH_INFO	The TOE must ensure that no information that may have entered through the HIGH port is able to leave through the LOW port.
O.ONE_WAY_FLOW	The TOE shall allow information to enter through the LOW port and then leave through the HIGH port.

Table 6: Security Objectives for the TOE

4.2 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 and mechanical, electrical, optical, radiation or any other form of physical influence.

Table 7: Security Objectives for the Operational Environment

4.3 Security Objectives Rationale

4.3.1 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_HIGH_INFO	T.DATA_LEAK
O.ONE_WAY_FLOW	P.ONE_WAY_FLOW

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

Table 9: Operational Environment Security Objectives Coverage

4.3.2 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-LOW and/or TA-HIGH threat agents may be able to cause HIGHINFO to exit the TOE through the LOW port.* This threat is diminished by: • O.NO_HIGH_INFO, which ensures that no information is able to spill over inside the TOE from the HIGH port to the LOW 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 and mechanical, electrical, optical, radiation or any other form of physical influence.

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.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.ONE_WAY_FLOW

Table 12: Sufficiency of objectives holding OSPs

5 Extended Component Definition

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

6 Security Requirements

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

Subjects:

- LOW port
  The input interface of the data diode.
- HIGH port
  The output interface of the data diode.

Information:

- Please see “Information” in 8.2 “Terminology“.

Policy:

- Information is allowed to enter the TOE through the LOW port and may leave through the HIGH port.
- Information is not allowed to leave the TOE through the LOW port.

6.1 TOE Security Functional Requirements

The following table shows the SFRs for the TOE, and the operations performed on the components according to CC part 2: iteration (Iter.), refinement (Ref.), assignment (Ass.) and selection (Sel.).

Security functional group	Security functional requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
FDP - User data protection	FDP_IFC.2 Complete information flow control	CC Part 2	N	N	Y	N
	FDP_IFF.1 Simple security attributes	CC Part 2	N	N	Y	N

Table 13: SFR operations

6.1.1 User data protection (FDP)

6.1.1.1 Complete information flow control (FDP_IFC.2)

FDP_IFC.2.1 The TSF shall enforce the **One-Way SFP** on **the subjects LOW port and HIGH port and the information “any optical signal that can traverse the HIGH or LOW 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.

6.1.1.2 Simple security attributes (FDP_IFF.1)

FDP_IFF.1.1 The TSF shall enforce the **One-Way SFP** based on the following types of subject and information security attributes: **subjects LOW port and HIGH port and information “any optical signal that can traverse the HIGH or LOW 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: **None**.

FDP_IFF.1.3 The TSF shall enforce the **rules in FDP_IFF.1.4 and FDP_IFF.1.5 only**.

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: **Any information received on the LOW port and originating from the LOW network may exit through the HIGH port into the HIGH network.**

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: **Any information attempting to leave through the LOW port.**

6.2 Security Requirements Rationale

6.2.1 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_HIGH_INFO O.ONE_WAY_FLOW
FDP_IFF.1	O.NO_HIGH_INFO O.ONE_WAY_FLOW

Table 14: Mapping of security functional requirements to security objectives

6.2.2 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_HIGH_INFO	*The TOE must ensure that no information that may have entered through the HIGH port is able to leave through the LOW 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 to leave through the LOW port.
O.ONE_WAY_FLOW	*The TOE shall allow information to enter through the LOW port and then leave through the HIGH 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 allows any internal flow of information incoming from the LOW port and sent out on the HIGH port.

Table 15: Security objectives for the TOE rationale

6.2.3 Security Requirements Dependency Analysis

Dependencies within the EAL5 package selected for the security assurance requirements have been considered by the authors of CC Part 3 and are not analyzed here again.

The included component on flaw remediation (ALC_FLR.1) has no dependencies on other requirements.

The included component on vulnerability analysis (AVA_VAN.5) has dependencies on the following components:

Dependent Component	Resolution
ADV_ARC.1	Included in EAL5.
ADV_FSP.4	Included in EAL5 through ADV_FSP.5.
ADV_TDS.3	Included in EAL5 through ADV_TDS.4.
ADV_IMP.1	Included in EAL5.
AGD_OPE.1	Included in EAL5.
AGD_PRE.1	Included in EAL5.
ATE_DPT.1	Included in EAL5 through ATE_DPT.3.

Table 16: AVA_VAN.5 Dependency Analysis

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 modeled 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	FDP_IFC.2
	FMT_MSA.3	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

6.3 Security Assurance Requirements Description

The security assurance requirements (SARs) for the TOE are the Evaluation Assurance Level 5 components as specified in [CC] part 3, augmented by AVA_VAN.5 and ALC_FLR.1.

No operations have been performed on the SARs.

6.4 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 TOE Summary Specification

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

7.1 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 LOW port and a fiber optic network cable is connected to the HIGH port.

Information can only be received from the LOW network connected on the LOW port, and no light can spill over to the LOW port from the HIGH port.

Information received on the LOW port is allowed to exit through the HIGH port, without further processing.

This TSF is mapped to the following SFRs: FDP_IFC.2, FDP_IFF.1

8 Abbreviations, Terminology and References

8.1 Abbreviations

ID	Description
CC	Common Criteria
EAL	Evaluation Assurance Level
OSP	Organizational Security Policy
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

Table 18: Abbreviations

8.2 Terminology

Catcher
The entity receiving information from the data diode. It resides on the HIGH network.

Data diode
A device that allows information to flow from the input to the output, but not the other way.

HIGH network
The network which is to receive information from the LOW network, through the TOE.

HIGH port
The output interface of the data diode. HIGH devices and networks are connected to this interface.

HIGH system
Any system residing on the HIGH network, excluding the TOE.

Information
An optical signal that can traverse the HIGH or LOW port.

LOW network
The network from which information is to be sent to the HIGH network, through the TOE.

LOW port
The input interface of the data diode. LOW devices and networks are connected to this interface.

LOW system
Any system residing on the LOW network, excluding the TOE.

Pitcher
The entity sending information to the data diode. It resides on the LOW network.

Port
The physical interface by which the optical cables are connected to the TOE.

8.3 References

ID	Description
[CC]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model September 2012, Version 3.1, Revision 4 CCMB-2012-09-001 Part 2: Security functional components September 2012, Version 3.1, Revision 4 CCMB-2012-09-002 Part 3: Security assurance components September 2012, Version 3.1, Revision 4 CCMB-2012-09-003
[IEEE 802.3]	IEEE Standard for Ethernet http://standards.ieee.org/about/get/802/802.3.html

Table 19: References