Document Number 21537

Version 2.1

25 pages

DD1G Gen2

Security Target

Table of contents

1 Document information

1.1 Version history

Version	Date	Author / changed by	Reviewed by	Approved by
1.0	2024-10-02	Christian Nord	Magnus Ahlbin	-
2.0	2026-02-24	Tove Bergdahl	Jens Bogarve	Tove Bergdahl
2.1	2026-02-25	Tove Bergdahl	Jens Bogarve	Tove Bergdahl

1.2 Changes since previous version

Chapter	Change Description
1.5	Updated references to user guidance documents.

1.3 Purpose of the document

This is the Security Target description for the TOE DD1G Gen 2.

1.4 Terms and abbreviations

Term	Explanation
TOE	Target of Evaluation, the scope for the Common Criteria evaluation and certification
PoE	Power over Ethernet
PSU	Power Supply Unit
ST	Security Target
Upstream	Refers to the data source side or the side of the diode where the data flows in to the device
Downstream	Refers to the data destination side or the side of the diode where the data flows out of the device
TSF	Target Security Function
OSP	Organisational Security Policy

1.5 References

[1] 21350, (21350v1.0)QuickGuide_DD1G_Gen_2

[2] 17113, (17113v1.3)Recommended_Security_Management_SecuriCDS_DD1000A_DD1G

1.6 List of appendices

None.

2 Introduction

2.1 Security Target Reference

Title:	DD1G Gen2, Security Target
Document number	21537
Version:	2.1
Date:	2026-02-25

2.2 TOE Reference

Target of Evaluation (TOE):	DD1G Gen 2 with Product ID BSF-DD18605C01
Developer:	Advenica AB

2.3 TOE Overview

A data diode is used for sending data from one independent network to another while ensuring the networks remain physically isolated. The data diode guarantees that data can only flow in the allowed direction.

The TOE in this ST is an Ethernet-based data diode with 1 Gigabit performance.

The TOE is determined by the physical borders of the box. See Figure 1: DD1G Gen2, Target of Evaluation.

Figure 1: DD1G Gen2, Target of Evaluation

2.4 TOE Description

2.4.1 TOE System overview

The TOE is used for two main scenarios.

Ensuring that information originating from devices connected to the downstream network remains confidential and is not accessible or visible to the upstream network.

Guaranteeing that data originating from the upstream network is protected from unauthorized modifications or tampering when transmitted to devices connected to the downstream network. This ensures the integrity of the upstream network data and prevents any unauthorized alterations during its transmission.

Figure 2: TOE Overview

The one-way data flow is ensured by the Target Security Function that is implemented by the Unidirectional Optical Link separating the Upstream and Downstream side in the TOE using an optical fibre. See Figure 2: TOE Overview.

2.4.2 TOE Physical Scope

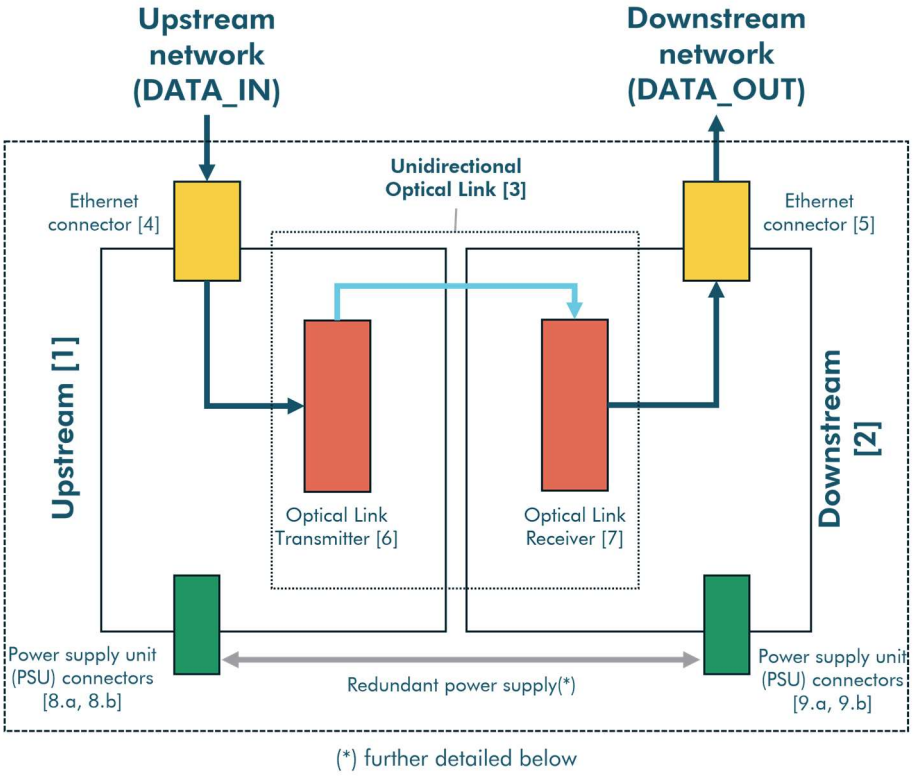

Figure 3: TOE block diagram

2.4.2.1 TOE Components

The TOE consists of a single device with three subsystems, denoted Upstream [1], Downstream [2], and Unidirectional Optical Link [3]. See Figure 3: TOE block diagram.

The TOE is physically connected to networks using the Upstream [4] and Downstream Ethernet connector [5] respectively. These are the only network connectors and the only offered communication ports on the TOE.

The Unidirectional Optical Link [3] is implemented using an optical fibre mounted to a transmitter [6] and receiver [7]. It provides the physical separation between the Upstream [1] and the Downstream [2] subsystems. This removes any risk of data being transferred in the reverse direction when installed correctly.

The upstream network (DATA_IN) should be configured to send all relevant network traffic through the TOE and physically ensure that all connections between the upstream and downstream (DATA_OUT) networks pass through the TOE.

Full operability of the TOE is achieved by powering the device and connecting the network interfaces.

There are several options for powering the device. By connecting to external power supply unit(s) [8,9] or via Power over Ethernet (PoE) [4,5].

The device also supports redundant power supply. This is further detailed in section 2.4.2.5.

2.4.2.2 States

The TOE has two operational states, on and off, with no intermediate or initial states where the one-way functionality is inactive.

2.4.2.3 Communication interfaces

The only interface of communication to and from the TOE are the Ethernet interfaces [4,5] dedicated for traffic over the device from the upstream network to the downstream network.

- Ethernet
    - IF.ETH-US: Data interface towards the upstream network [4]
    - IF.ETH-DS: Data interface towards the downstream network [5]

2.4.2.4 Power Interfaces

The external power supply unit(s) (PSU) can be connected with either a barrel or Phoenix connector. See Figure 4: TOE power interfaces.

Figure 4: TOE power interfaces

As an alternative way of providing power to the TOE, the TOE Ethernet connectors also has a Power over Ethernet (PoE) capability.

See Table 1 below for an overview of all power interfaces.

Table 1: Power interfaces

Reference name	Type	Description
IF.BAR_US	Barrel connector	DC power supply interface to the Upstream subsystem [8a].
IF.BAR_DS	Barrel connector	DC power supply interface to the Downstream subsystem [9.a].
IF.POE_US	Power over Ethernet	Power over Ethernet to the Upstream subsystem [4].
IF.POE_DS	Power over Ethernet	Power over Ethernet to the Downstream subsystem [5].
IF.PHX_US	Phoenix connector	DC power supply interface to the Upstream subsystem [8.b].
IF.PHX_DS	Phoenix connector	DC power supply interface to the Downstream subsystem [9.b].

2.4.2.5 Power redundancy

The TOE supports redundant power supply. This means that the power supply connected to the Upstream subsystem [1] can also power the Downstream subsystem [2], and vice versa. This is true for either choice of power supply, external power supply unit (PSU) or via Power over Ethernet (PoE).

The purpose of this feature is to make sure the device remains operational in the case of a power supply failure on either side of the TOE.

The power redundancy feature is typically used as a safety precaution in installation environments for one of the main target customer groups for this product, where availability is of highest priority.

The TOE power supply is designed as shown in the block diagram in Figure 5: TOE power supply block diagram.

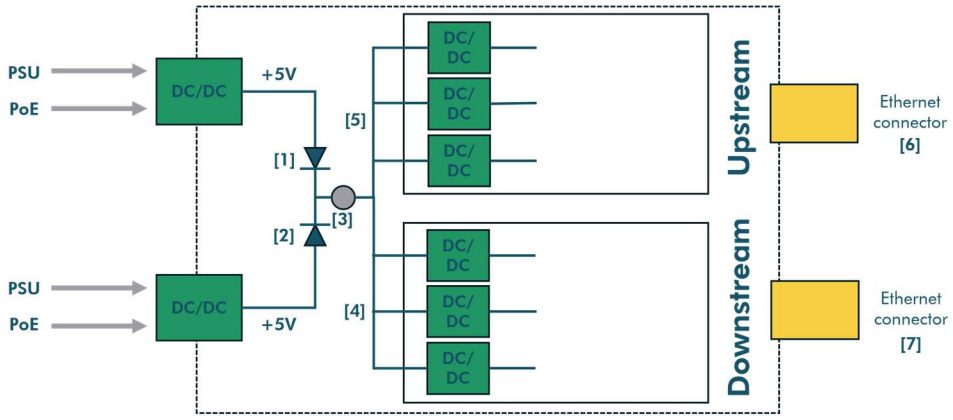

Figure 5: TOE power supply block diagram

Electrical voltage input, whether via PSU or PoE, is converted to +5V in the DC/DC converters. Each side is separated by electrical diodes, [1,2] before reaching the only place where the current from both sides are joined [3].

The electrical voltage is then converted from +5V using 3 DC/DC converters on each side, [4] and [5], to voltage levels needed for supplying the other internal components with power.

It can be concluded that:

- Power is the only shared resource between the two sides, upstream and downstream.
- Power supply is kept completely separate from the data flow.
- When powering the device using PoE, power supply is separated from the data input or output in the Ethernet (RJ45) connectors, [6] and [7].
- Electrical current from the two sides is divided into separate parts using 3 DC/DC converters on each side, [4] and [5], making it impossible to determine which part of the current will be sent to the upstream or downstream respectively from the common point at [3].
- The redundant power supply functionality does not introduce any possibility of data flow from the downstream side to the upstream side.

- There is no risk of affecting the upstream side from the downstream side through the PSU or PoE power supply from the downstream side as there is no way of controlling how the electrical current flow is separated at the DC/DC converters by manipulating with the input power supply.

2.4.2.6 TOE Configuration

Since the TOE is a hardware-only device, it has no communication interface for administration or configuration.

2.4.2.7 TOE Guidance

Guidance on TOE installation is available in [1] and [2].

2.4.2.8 TOE Delivery

The TOE is delivered to customers through a secure and validated delivery process. The customer will receive customer order specific information, including the ID number of the sealed security bag. This ensures that the customer can verify that the product has not been manipulated or tampered with upon receiving the product.

Shipment to customers is handled by Advenica AB.

2.4.2.9 Installation and tamper protection

The TOE should be installed with visible tamper detection marking for ocular inspection to determine whether tampering has occurred. This tamper seal is already attached on delivery, but a proper visual examination of the TOE before installation is recommended.

All personnel doing installation and administration of the TOE should be authorized to do so, have the necessary training required to do this according to the requirements, and follow the recommended steps when doing so.

The environment in which the TOE is installed should not be accessible by unauthorized personnel to prevent the device from being tampered with, or even disconnected, since it can then no longer fulfill its security function.

2.4.3 TOE Environment

The TOE is a hardware only data diode that ensures unidirectional Ethernet data traffic through the TOE. It is intended for installation in a network environment.

There are no dependencies to other hardware, firmware or software to use the functionality of the TOE.

2.4.4 TOE Logical Scope

The TOE allows data to flow from the Upstream side to the Downstream side but physically prevents data to flow in the reverse direction.

The only physical access to the light transmitter in the Unidirectional Optical Link is through the Upstream subsystem Ethernet connector. Rendering it impossible to reverse any data flow through the TOE without tampering of the device.

The logical sequence of data flow is as follows, see also Figure 6: TOE logical scope:

1. Data is received through the Upstream Ethernet connector.
2. The Upstream subsystem converts the electrical signal to light using the Optical Link Transmitter.
3. The data is transmitted over the optical fibre link and received by the Optical Link Receiver.
4. The light is converted to electrical signals and passed on to the Downstream Ethernet connector.

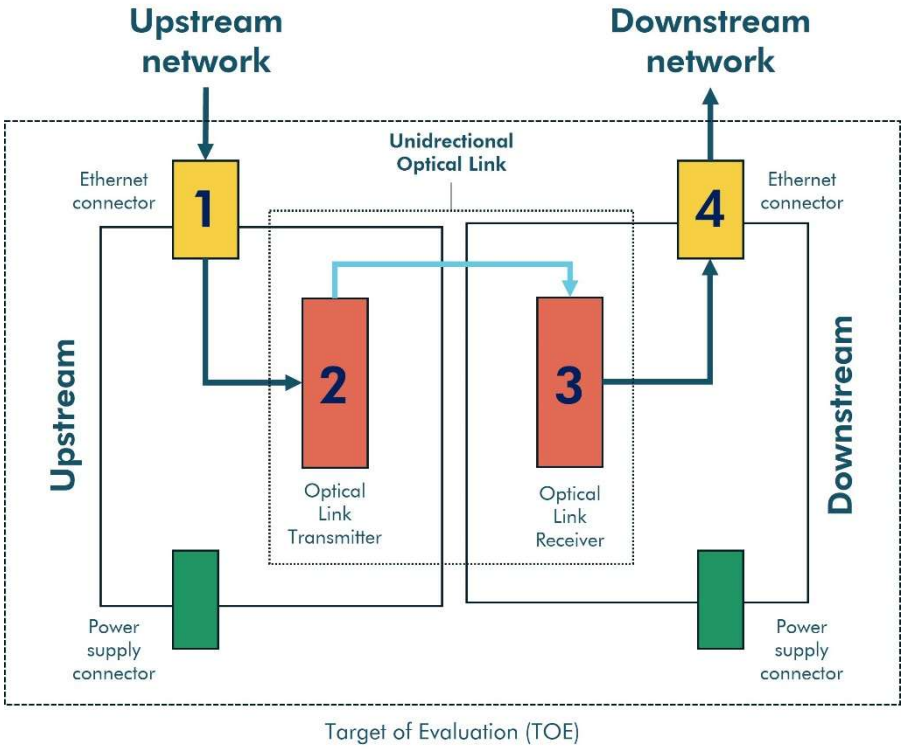

Figure 6: TOE logical scope

2.4.5 TOE Roles

The following user roles are applicable for the TOE.

Table 2: TOE Roles

Role	Description
USERS	Users sending information to be transferred from the upstream network to the downstream network via the TOE.
ADMINS	People that are responsible to install and operate the device.

3 Conformance Claims

3.1 CC Conformance Claim

This Security Target is conformant to:

- Common Criteria: ISO/IEC 15408:2022, Fourth edition, 2022-08 and CC:2022, Revision 1, CCMB-2022-11-001—005
    - Part 2 conformant
    - Part 3 conformant

The Common Methodology for Information Technology Security Evaluation ISO/IEC 18045:2022, Third edition, 2022-08 and CEM:2022, Revision 1, CCMB-2022-11-006 has been taken into account.

The Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version: 1.1, 2024-07-22 has been taken into account.

3.2 PP Conformance Claims

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

3.3 Package Conformance Claims

The ST and TOE claim the package: EAL4 and “package-augmented”. Additional Component is AVA_VAN.4.

3.4 Conformance Rationale

This Security Target does not claim conformance of the TOE with any Protection Profile; therefore, a conformance rationale is not applicable.

4 Security Problem Definition

4.1 Introduction

The security problem definition described below includes threats, organisational security policies and security usage assumptions.

4.1.1 Security policy

To facilitate controlled, one-way data transfer while maintaining a strong separation between networks of different security levels, the TOE implements the following security policy [POL-1]:

1. Information is allowed to flow from the upstream network to the downstream network.
2. Information is not allowed to flow in the opposite direction.

4.2 Threats

Threats are described by an adverse action performed by defined threat agents on the assets that the TOE has to protect. The assets and their protection needed, the threat agents and their attack potential, and the threat adverse actions are described below.

4.2.1 Assets

Table 3: Assets that the TOE protects

Asset	Description
USER_DATA_IN_TRANSIT	Any data sent in the allowed direction by a user, i.e. upstream to downstream.
USER_RESOURCES_US	Any other data or resources available in the network to which the TOE Upstream port is connected.

4.2.2 Threat Agents

Table 4: Threat agents

Threat agents	Description

ATTACKER	A malicious entity that either wants to violate the directional aspect of the TOE, i.e. to send information or perform an attack against the allowed traffic direction of the TOE.

4.2.3 Threats

Table 5: Threats against the TOE

Name	Threat
T.LEAKAGE_VIA_DIODE	A USER on the downstream network accidentally transmitting data through TOE to the upstream network.
T.ATTACK_VIA_DIODE	An ATTACKER tries to send data from downstream to upstream via the TOE with the purpose to violate resources or access data at USER_RESOURCES_US.

4.3 Organisational Security Policies

There are no organisational security policies, OSPs, for the TOE.

4.4 Assumptions

Assumptions on the TOE operational environment are made according to Table 6.

Table 6: Assumptions TOE operational environment

Name	Assumptions on the TOE operational environment
A.NO_MALICIOUS_ADMINS	Personnel doing the installation of TOE are assumed to be authorized, trusted, and have the necessary training.
A.PHYSICAL_PROTECTION	TOE is installed such that only authorized personnel has access.
A.NO_BYPASS	TOE is installed such that it forms a separation between upstream and downstream networks. The network is configured such that all traffic from upstream to downstream network must go through the TOE.

5 Security Objectives

5.1 Introduction

The statement of security objectives defines the security objectives for the TOE and its environment. The security objectives intend to address all security environment aspects identified. The security objectives reflect the stated intent and are suitable to counter all identified threats and cover all identified organisational security policies and assumptions. The following categories of objectives are identified:

- The security objectives for the TOE.
- The security objectives for the environment.

5.2 Security Objectives for the TOE

The following security objectives for the TOE are defined.

Table 7: Security Objectives for the TOE

Security Objective	Description
O.ONEWAY	The TOE will only allow data to flow from Upstream side to the Downstream side and never in the reverse direction.
O.NO_DATA_LEAK	The TOE must ensure that data never is leaked between the Downstream side and the Upstream side.

5.3 Security Objectives for the Operational Environment

The following security objectives for the TOE environment are defined.

Table 8: Security Objectives for the TOE environment

Security Objective	Description
OE.ADMINS	Personnel doing the installation of the TOE shall be authorized, trusted, and have the necessary training.
OE.PHYSICAL_PROTECTION	TOE shall be installed such that only authorized personnel has access.
OE.NO_BYPASS	TOE is installed such that it forms a separation between upstream and downstream networks.

Security Objective	Description
	The network is configured such that all traffic from upstream to downstream network must go through the TOE.

5.4 Security Objectives Rationale

5.4.1 Security Objectives Coverage

This section provides tracings of the security objectives for the TOE to threats, OSPs, and assumptions.

Table 9: Security Objectives Coverage

	T.LEAKAGE_VIA_DIODE	T.ATTACK_VIA_DIODE	A.NO_MALICIOUS_ADMINS	A.PHYSICAL_PROTECTION	A.NO_BYPASS
O.ONEWAY	x	x			
O.NO_DATA_LEAK	x	x			
OE.ADMINS			x		
OE.PHYSICAL_PROTECTION				x	
OE.NO_BYPASS					x

5.4.2 Security Objectives Sufficiency

The following rationale provides justification that the security objectives for the TOE and the security objectives for the environment are suitable to cover each individual threat. The rationale also provides justification that the security objectives for the environment are suitable to cover each individual assumption.

Table 10: Security Objectives Sufficiency

Threat/Assumption	Objective	Rationale
T.LEAKAGE_VIA_DIODE	O.ONEWAY, O.NO_DATA_LEAK	The threat summarized: A USER accidentally transmitting data through TOE to the upstream network. This is covered by O.ONEWAY: The TOE will only allow data to flow from Upstream side to the Downstream side and never in the reverse direction. O.NO_DATA_LEAK: The TOE must ensure that data never is leaked between the Downstream side and the Upstream side
T.ATTACK_VIA_DIODE	O.ONEWAY, O.NO_DATA_LEAK	The threat: An ATTACKER tries to send data from downstream to upstream via the TOE with the purpose to violate resources or access data at USER_RESOURCES_US. This is covered by O.ONEWAY: The TOE will only allow data to flow from Upstream side to the Downstream side and never in the reverse direction. O.NO_DATA_LEAK: The TOE must ensure that data never is leaked between the Downstream side and the Upstream side
A.NO_MALICIOUS_ADMINS	OE.ADMINS	The security objectives for the environment directly reflect the assumption
A.PHYSICAL_PROTECTION	OE.PHYSICAL_-PROTECTION	The security objectives for the environment directly reflect the assumption
A.NO_BYPASS	OE.NO_BYPASS	The security objectives for the environment directly reflect the assumption

6 Extended Components Definition

No extended components are defined.

7 Security Requirements

7.1 Security Functional Requirements

The following conventions have been applied in this document.

- Iteration: Allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a number in parenthesis placed at the end of the component. For example FCS_COP.1 (1) and FCS_COP.1(2) indicate that the ST includes two iterations of the FCS_COP.1 requirement, "1" and "2".
- Assignment: Allows the specification of an identified parameter. Assignments performed in this ST are indicated using **bold italics** and are surrounded by brackets (e.g., [**assignment**]).
- Selection: Allows the specification of one or more elements from a list. Selections performed in this ST are indicated using **bold** and are surrounded by brackets (e.g., [**selection**]).
- Refinements performed in this ST are identified with "**Refinement**:" right after the short name.

Table 11: Security Functional Requirements

Requirements		Component
User Data Protection (FDP)	Complete information flow control	FDP_IFC.2
	Simple Security attributes	FDP_IFF.1

7.1.1 User Data Protection (FDP)

7.1.1.1 FDP_IFC.2 Complete information flow control

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 [**POL-1**] on [
Subjects: the Upstream side and the Downstream side
Information: USER_DATA_IN_TRANSIT]
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.

7.1.1.2 FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

Dependencies:

FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the [**POL-1**] based on the following types of subject and information security attributes:
[**Subjects: the Upstream side and the Downstream side**
Subject attributes: the Upstream side and the Downstream side
Information: USER_DATA_IN_TRANSIT
Information attributes: none].

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: [**no security attribute-based rules**].

FDP_IFF.1.3 The TSF shall enforce the [**no additional rules**].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [**no additional rules**].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [**any data from the Downstream side**].

7.2 Security Assurance Requirements

The TOE assurance requirements for this ST consist of the requirements corresponding to the assurance level EAL4 augmented with AVA_VAN.4.

7.3 Security Requirements Rationale

7.3.1 Security Functional Requirements Dependencies

Table 12: Security Functional Requirements Dependencies

Requirement	Dependencies	Analysis
FDP_IFC.2	FDP_IFF.1	Fulfilled

Requirement	Dependencies	Analysis
FDP_IFF.1	FDP_IFC.1 and FMT_MSA.3	FDP_IFC.1 is fulfilled by FDP_IFC.2. FMT_MSA.3 is not applicable, because it is no security attributes to be initialized.

7.3.2 Security Assurance Dependencies Analysis

The chosen evaluation assurance level EAL4 augmented by AVA_VAN.4. Since all dependencies are met internally by the EAL4 package only the dependencies for the augmented assurance component are analysed.

Table 13: Security Assurance Requirements Dependencies

Assurance Component	Dependencies	Met
AVA_VAN.4	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, AGD_OPE.1, AGD_PRE.1 and ATE_DPT.1	Yes, all these components are included in the EAL4 package

All dependencies are met.

7.3.3 Security Functional Requirements Coverage

The following Table provides a mapping between the Security Functional Requirements (SFRs) and Security Objectives.

Table 14: Security Functional Requirements Coverage

	O.ONEWAY	O.NO_DATA_LEAK
FDP_IFC.2	x	x
FDP_IFF.1	x	x

7.3.4 Security Functional Requirements Sufficiency

Table 15: Security Functional Requirements Sufficiency

Objective	SFR	Rationale
O.ONEWAY	FDP_IFC.2, FDP_IFF.1	The TOE will only allow data to flow from Upstream side to the Downstream side and never in the reverse direction by implementing the policy POL-1.
O.NO_DATA_LEAKAGE	FDP_IFC.2, FDP_IFF.1	The TOE will not allow any data to flow from the Downstream side to the Upstream side by implementing the policy POL-1.

7.3.5 Justification of the Chosen Evaluation Assurance Level

The TOE assurance requirements for this ST consist of the requirements corresponding to the assurance level EAL4 augmented with AVA_VAN.4.

EAL 4 ensures that the product has been designed, tested, and reviewed with high assurance. EAL4+ was chosen for competitive reasons.

8 TOE Summary Specification

This section presents information to how the TOE meets the functional requirements described in previous sections of this ST.

8.1 TOE Security Functions

The TOE consists of a single device with three subsystems, denoted Upstream, Downstream, and Unidirectional Optical Link. The TOE is physically connected to networks using the Upstream and Downstream Ethernet connector respectively.

The TOE TSF (Unidirectional Optical Link) is implemented using an optical fibre mounted to a transmitter and receiver. It provides the physical separation between the Upstream and the Downstream subsystems. It is physically impossible by the design that any data can be transferred in the reverse direction.

TOE Security Functional Requirements addressed: FDP_IFC.2 and FDP_IFF.1.