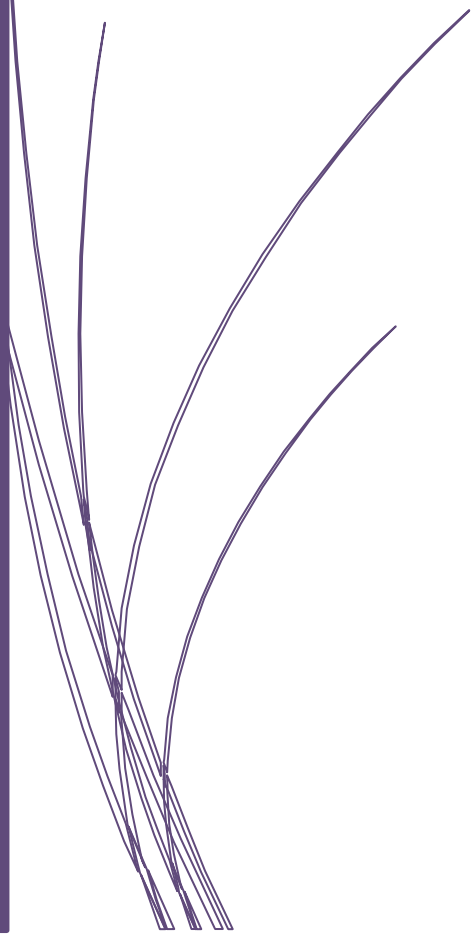
2024-09-29

Security Target LITE

A.R.I.C. NDS Optical Industry Data Diode

Version 1.0



DYNACON SP. Z O.O.

Table of content

List of schemas

List of tables

1. Introduction

1.1.Security Target Identification

Title	Security Target A.R.I.C. NDS Optical Industry Data Diode - LITE
ST Revision ID	LITE_1.0
ST Revision Date	29.09.2024
ST Status	Final
ST Publication Date	29.09.2024
Sponsor	Dynacon Sp. z o.o.
Authors	Barbara Szymańska, Andrzej Cieślak
Key words	OT, Data Diode, Security, One-way communication, Industry Communication

Table 1. Security Target Identification

1.2.TOE Identification

A.R.I.C. NDS Optical Industry Data Diode – Artificial Reaction Intelligent Conscious Network Distributed System Optical Industry Data Diode, to be referred to as A.R.I.C NDS DD

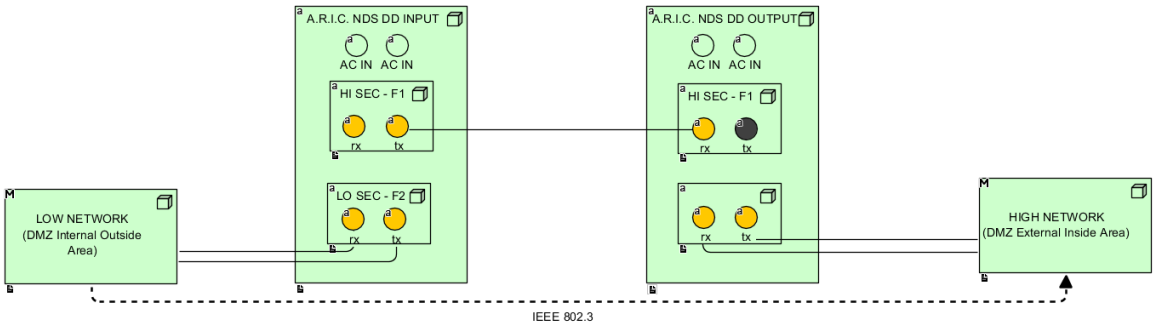
Data Diode for OT communication.

TOE name	A.R.I.C. NDS Optical Industry Data Diode (to be referred to as A.R.I.C NDS DD)
TOE Version	2.0.0
TOE Status	Release
Release Date	04.2020
Sponsor	Dynacon Sp. z o.o.
Developer	Dynacon Sp. z o.o.
Key words	OT, Data Diode, Security, One-way communication, Industry Communication

Table 2. Target of Evaluation Identification

1.3.TOE Overview

The data diode A.R.I.C. NDS DD provides security features for OT communication – it enables one-way communication for data flow over Ethernet protocol and it ensures that the flow initialized in opposite direction is completely blocked. The diode main aim is to secure OT system against injection of malicious data from another autonomous system. The diode is targeted for OT communication allowing secure data flow between defined objects in OT network. The secure data flow is defined as one-way communication, which allows sending data from critical infrastructure/critical technology process components to another autonomous system, while assuring no data to be sent backwards.



Schema 1.The A.R.I.C. NDS DD general overview

The A.R.I.C. NDS DD architecture is based on two hardware units:

- A.R.I.C NDS DD INPUT,
- A.R.I.C NDS DD OUTPUT.

The TOE provides one-way communication replicating data from the inside trusted (LOW NETWORK in Schema 1) system to the outside system (HIGH NETWORK in Schema 1) which is located in a separate security zone. The data received on A.R.I.C. NDS DD INPUT on the HI-SEC interface is pushed through a single fiber-optic cable to the A.R.I.C. NDS DD OUTPUT. Blocking of the flow in opposite direction is ensured by using only single fiber-optic cable in the direction indicated earlier. The fiber-optic cable is not connected in the direction from A.R.I.C. NDS DD OUTPUT to the A.R.I.C. NDS DD INPUT, which ensures that the data is not sent back or data generated on A.R.I.C. NDS DD OUTPUT site would not be sent to A.R.I.C. NDS DD INPUT. The A.R.I.C. NDS DD OUTPUT receives data on the HIGH NETWORK side. The only data flow allowed is from A.R.I.C. NDS DD INPUT to A.R.I.C. NDS DD OUTPUT, which is controlled on physical layer. Physical connectivity is based on standard duplex SFP modules and duplex fiber-optic patch cord, of which only single fiber is used for transferring the data.

The LOW NETWORK can be any system, which is supposed to send data to HIGH NETWORK over IEEE 802.3 standard based protocols (Ethernet).

1.3.1. TOE Type

One-way data gateway (a data diode) for OT communication.

1.3.2. Usage

The increasing need to improve production effectiveness comes with more common need to connect OT network and system to other autonomous systems, which further brings threat from various actors to gain access to process technology data or cause interruption or modifications to the data processed in OT infrastructure, has forced many companies to control, secure and adjust separation of their production network from less trusted areas such as the external autonomous system.

While it is necessary to get information from the OT system or exchange data between OT systems, in many cases it is crucial that the data flow is unidirectional, in order to assure that the external autonomous system will not affect technological process and will not affect business goals of production. On one hand there is a need of data exchange, on the second hand no data can be sent from untrusted external system to OT, trusted system.

In many cases, in order to secure OT system from other system, there are firewalls and IDS/IPS used with appropriate flow policies, however since this solution allows data to flow back, it is not fully secure, and the level of security provided for crucial OT system is not sufficient. The hidden data can be sent in allowed traffic, the traffic could be modified so it fits the polices, etc. In order to truly separate connected segments, only one-way communication can be allowed.

The data diode (the TOE) is the connection point between two separate autonomous systems. The actual transmission is handled by defined objects, with the data diode implemented in-line. The sender is an OT system (LOW NETWORK), and the receiver (HIGH NETWORK) is external autonomous system. The data diode ensures that information can only flow from the OT system to the external autonomous system, but not the other way. This allows for automated information transfer from the LOW NETWORK to the HIGH NETWORK without manual intervention, while preventing the opposite flow direction. The security goal is to allow the export of information from a protected network to a more open environment, 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 power plant, to an external log analyser. The data diode will allow the export, while preventing any influence back into the SCADA system.

Consequently, two user roles are considered for TOE operation, the *internal_user* located in the LOW NETWORK and *external_user* located in the HIGH NETWORK. The *internal_user* role covers the all entities authorized to initiate the information flow originating from the LOW NETWORK towards the HIGH NETWORK that is allowed (forwarded) by the TOE. The *external_user* role covers the all entities residing in HIGH NETWORK that are able to receive information flow originating from the LOW NETWORK (through the TOE) and that are able to initiate the information flow originating from the HIGH NETWORK towards the A.R.I.C NDS DD that is explicitly denied (blocked) by the TOE.

1.3.3. Major Security Features

The major security feature of the A.R.I.C. NDS DD is to ensure one-way communication from trusted OT system (LOW NETWORK) through the data diode towards the system located in the different security zone (HIGH NETWORK) while blocking the communication in the opposite direction. The goal is to protect trusted OT system against injection of network communications from the system located in different security zone while enabling communication in the opposite direction (from LOW NETWORK towards HIGH NETWORK). Access from outside to the trusted OT system is forbidden to increase security of data and not to allow the access to data and the system itself.

1.4.TOE Description

1.4.1. Physical Scope of the TOE

The A.R.I.C NDS DD product, delivered to the Customer, consists of:

- 2 pcs of A.R.I.C hardware appliance
    - A.R.I.C NDS DD INPUT
    - A.R.I.C NDS DD OUTPUT
- 2 pcs of Gigabit SFP modules according to Table 3 (for HI-SEC port of each appliance)
    - 2 pcs of DSFP-DX-SM-1G, or

- 2 pcs of DSFP-DX-MM-1G

- 1 pcs of fiber-optic cable, with specification according to Table 3
- 2 pcs of user guidance: preparative guidance and operational user guidance.

The physical connection between the hardware appliances A.R.I.C NDS DD INPUT and A.R.I.C NDS DD OUTPUT is provided by two SFP modules and the fiber-optic cable. The following options regarding the technological standards of SFP modules and fiber-optic cable are used:

- Single-mode
  - SFP module
    - Single-mode, duplex, 1310/1550 nm, LC for 1Gbps, P/N:DSFP-DX-SM-1G

Schema 2. SFP Single mode Fiber Optical module for A.R.I.C NDS DD

  - Fiber-optic patch cable:
    - Single-mode fiber, duplex, OS1 cable, LC-LC, to be referred as FO-SM-Duplex-OS1
    - Single-mode fiber, duplex, OS2 cable, LC-LC to be referred as FO-SM-Duplex-OS2
- Multi-mode
  - SFP module
    - Multi-mode, duplex, 850/1310 nm, LC for 1Gbps, P/N:DSFP-DX-MM-1G

Schema 3. SFP Multi mode Fiber Optical module for A.R.I.C NDS DD

  - Fiber-optic patch cable:
    - Multi-mode fiber, duplex, OM1 cable, LC-LC, to be referred as FO-MM-Duplex-OM1
    - Multi-mode fiber, duplex, OM2 cable, LC-LC, to be referred as FO-MM-Duplex-OM2
    - Multi-mode fiber, duplex, OM3 cable, LC-LC, to be referred as FO-MM-Duplex-OM3
    - Multi-mode fiber, duplex, OM4 cable, LC-LC, to be referred as FO-MM-Duplex-OM4
    - Multi-mode fiber, duplex, OM5 cable, LC-LC, to be referred as FO-MM-Duplex-OM5

FO mode	A.R.I.C NDS DD INPUT	Int.	A.R.I.C NDS DD OUTPUT	Int.	Fiber-optic cable
Single-mode	DSFP-DX-SM-1G	F1	DSFP-DX-SM-1G	F1	FO-SM-Duplex-OS1
Single-mode	DSFP-DX-SM-1G	F1	DSFP-DX-SM-1G	F1	FO-SM-Duplex-OS2

Multi-mode	DSFP-DX-MM-1G	F1	DSFP-DX-MM-1G	F1	FO-MM-Duplex-OM1
Multi-mode	DSFP-DX-MM-1G	F1	DSFP-DX-MM-1G	F1	FO-MM-Duplex-OM2
Multi-mode	DSFP-DX-MM-1G	F1	DSFP-DX-MM-1G	F1	FO-MM-Duplex-OM3
Multi-mode	DSFP-DX-MM-1G	F1	DSFP-DX-MM-1G	F1	FO-MM-Duplex-OM4
Multi-mode	DSFP-DX-MM-1G	F1	DSFP-DX-MM-1G	F1	FO-MM-Duplex-OM5

Table 3. Matrix of SFP and FO cable combination to be installed in A.R.I.C. NDS DD.
Abbreviations: FO – Fiber-Optic; Int. – Interface; F1 – HI-SEC interface (see schema 2).

The TOE evaluated configuration cover both single and multi-mode options for connecting A.R.I.C NDS DD INPUT HI-SEC port and A.R.I.C NDS DD OUTPUT HI-SEC port. Please note that the used mode for internal connection between A.R.I.C NDS DD appliances, described in Table 3, does not determines the TOE functionality and its security features.

Each set of above listed SFP modules and fiber-optic cables (Single-mode communication or Multi-mode communication – Table 3) provides physical connectivity for the communication at physical layer of ISO/OSI model. The elements are required to provide data transfer between A.R.I.C devices. The security functionality of the TOE is assured by using only A.R.I.C NDS DD INPUT TX interface and A.R.I.C NDS DD OUTPUT RX interface, without connection for opposite direction, i.e. without connection between A.R.I.C NDS DD INPUT RX interface and A.R.I.C NDS DD OUTPUT TX interface. Regardless of the used SPF modules and fiber-optic cables, all of the above presented sets of SFP modules and patch cords will fulfil the requirement.

1.4.1.1. *TOE delivery method*

The A.R.I.C NDS DD data diode solution is delivered to the Customer premises as two hardware appliances A.R.I.C with two SFP modules and related fiber-optic cable as presented below:

No.	Delivered Equipment description	Quantity	Identified by	Role
1.	A.R.I.C hardware appliance	1	Device Serial Number	A.R.I.C NDS DD INPUT
2.	A.R.I.C hardware appliance	1	Device Serial Number	A.R.I.C NDS DD OUTPUT
3.	DSFP-DX-SM-1G SFP module	2	Device Serial Number	Interface Extension for transmission medium
4.	Fiber-optic Cable, duplex, LC-LC	1	No ID	Transmission medium

Table 4. BOM Delivery for Single Mode

No.	Delivered Equipment description	Quantity	Identified by	Role
1.	A.R.I.C hardware appliance	1	Device Serial Number	A.R.I.C NDS DD INPUT
2.	A.R.I.C hardware appliance	1	Device Serial Number	A.R.I.C NDS DD OUTPUT
3.	DSFP-DX-MM-1G SFP module	2	Device Serial Number	Interface Extension for transmission medium
4.	Fiber-optic Cable, duplex, LC-LC	1	No ID	Transmission medium

Table 5. BOM Delivery for Multi Mode

The TOE is installed by an engineer certified by TOE manufacturer.

Customer obtains a copy of user guidance (preparative guidance and operational user guidance) before TOE installation. The operational user guidance provides instructions for operating the product in its evaluated configuration and deployed environment. The preparative guidance shows the implementation and deployment of the product in customer's environment. The user guidance is

delivered in electronic version (PDF format), through the dedicated storage resource. The Customer receives link to dedicated documentation storage, from where the customer can download the guidance.

Customer receives the hardware with uniquely identified S/N of the A.R.I.C NDS DD and SFP module. The S/N is shown on the permanent label on each component.

1.4.2. Logical Scope of the TOE

TOE ensures that the data is always allowed to flow only from trusted area (LOW NETWORK) to untrusted area (HIGH NETWORK), and the data flow in the opposite direction is denied at all times. The data transfer bases on Ethernet protocol (IEEE. 802.3) implemented on the single fiber-optic cable to guarantee unidirectionality.

The LOW NETWORK data received by A.R.I.C. NDS DD INPUT is sent to A.R.I.C. NDS DD OUTPUT. The TOE has two internal interfaces, one on each A.R.I.C NDS DD hardware appliances – HI-SEC ports. The A.R.I.C NDS DD INPUT HI-SEC TX interface is connected by single fiber-optic cable with A.R.I.C NDS DD OUTPUT HI-SEC RX interface, what ensures that communication originating at LOW NETWORK is transferred through the TOE. Since the connection is ensured only by the fiber-optic cable attached to the TX and RX interfaces of the INPUT and OUTPUT devices respectively, there is no back channel which can be used to send data or provide communication from HIGH NETWORK to LOW NETWORK (i.e. from OUTPUT to INPUT device).

Any network protocol, after adjustment performed by the *Sender Software* and *Receiver Software*, could be used to implement the communication, if it is compatible with IEEE 802.3 standard (Ethernet) used by TOE at the link layer. The TOE itself is independent from the higher layer protocols carried in the IEEE 802.3 frames. The TOE scope constitutes only a part of A.R.I.C NDS DD solution. All the necessary adjustments of the bidirectional TCP protocol in order to be transferred over the one-way connection provided by TOE are performed by the Sender Software and Receiver Software. The TOE itself does not modify the data by any means.

2. Conformance Claim

Common Criteria [CC] version 3.1 revision 5 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 EAL3. This Security Target does not claim conformance to any Protection Profile.

3. Security Problem Definition

3.1.Threat Environment

Asset	Definition
LOWINTEGRITY	The network communication originating from HIGH NETWORK directed towards LOW NETWORK is always denied (blocked by the TOE). The denial of communication (from HIGH to LOW NETWORK) protects the LOW NETWORK (OT System) integrity, reliability, and correctness of operation from being compromised by the injection of data from the HIGH NETWORK. The integrity, reliability and correctness of the OT system processes are protected from any interference coming from external systems by denying any communication flow towards the LOW NETWORK.
OUTCOMMUNICATION	The network communication originating from LOW NETWORK directed towards HIGH NETWORK is allowed (forwarded by the TOE).

Table 6. Assets

Threat Agent	Definition
TA-HIGH	Any entity connected to TOE on the HIGH NETWORK or attackers having access to the HIGH NETWORK resources. TA-HIGH entities and attackers are characterized with an attack potential of Basic.
TA-LOW	Any LOW entities connected to TOE on the LOW NETWORK.

Table 7.Threat Agents

3.1.1. Threats

Threat	Definition
T.DATA_INJECTION	TA-HIGH threat agent is able to inject data to TOE causing any of the following: - data to flow from HIGH NETWORK to LOW NETWORK (OT system) through TOE (what may compromise integrity, reliability or correctness of operation of the OT system), - interruption or distortion of communication forwarded by TOE from LOW NETWORK towards HIGH NETWORK (what may compromise integrity, reliability or correctness of communication of the OT system).
T.GET_DATA_FROM_HIGH	TA-LOW threat agent authorised to access the OT system from the LOW NETWORK trying to inject data from HIGH NETWORK to LOW NETWORK by any mean.

Table 8.Threats

3.2.Assumptions

Assumption	Definition
A.INTEGRATOR	It is assumed that the integrator who is performing the installation and maintenance of the TOE is well-trained and competent in the prevention of data injection, and the integrator competence is confirmed by the TOE manufacturer's certificate.
A.PHYSICAL	It is assumed that all TOE and non-TOE hardware will be physically protected from unauthorized access and mechanical, electrical, optical, radiation or any other form of physical influence. The A.R.I.C NDS DD INPUT, the A.R.I.C NDS DD OUTPUT, the fiber-optic cable and the media converter are located in controlled secure facility with access control.
A.NETWORK	Apart from network path through the TOE, it is assumed that there are no other channels for the information to flow between HIGH NETWORK and LOW NETWORK.
A.MEDIACONVERTER	The media converter is only connected to A.R.I.C. NDS DD INPUT HI-SEC RX interface as the light (signal) source, and it is not connected to any other devices.
A.TRUSTED_OPERATOR	It is assumed that the operator who is authorized to access any information process in LOW NETWORK and HIGH NETWORK, is always trusted and will never inject information from HIGH NETWORK to LOW NETWORK by any mean.

Table 9. Assumptions

3.3.Organizational Security Policies

There are no Organizational Security Policies that the TOE must comply to.

4. Security Objectives

4.1.Security Objectives for the TOE

Objective	Definition
O.ONE_WAY_FLOW	The TOE shall physically ensure data to flow only from LOW NETWORK to HIGH NETWORK. Specifically: - the data flow from HIGH NETWORK to LOW NETWORK shall by always denied; - the data flow from LOW NETWORK to HIGH NETWORK shall be always allowed.

Table 10. Security Objectives for the TOE

4.2.Security Objectives for the Operational Environment

Objective	Definition
OE.INTEGRATOR	The integrator who is performing the installation and maintenance of the TOE shall be well-trained and competent in the prevention of data injection, and the integrator competence is confirmed by the TOE manufacturer's certificate.
OE.PHYSICAL	All TOE and NON-TOE hardware and their interfaces shall be physically protected from unauthorized access and mechanical, electrical, optical, radiation or any other form of physical influence. The A.R.I.C NDS DD INPUT, the A.R.I.C NDS DD OUTPUT, the fiber-optic cable and the media converter are located in controlled secure facility with access control.
OE.NETWORK	The architecture of the infrastructure shall be implemented according to OT communication and architecture networking standards (IEC 62443 series of standards, CPwE - Converged Plantwide Ethernet). The network architecture of the LOW NETWORK and the HIGH NETWORK must be properly protected against unauthorized access. These standards indicate, among others, that the OT network is protected against influence from external untrusted systems and the environment the TOE operates in, is separated from any unauthorised actions. The only physical connection between the LOW

	NETWORK and the HIGH NETWORK is through the A.R.I.C. NDS DD.
OE.MEDIACONVERTER	The media converter is connected only to A.R.I.C. NDS DD INPUT HI-SEC RX interface.
OE.TRUSTED_OPERATOR	The operator who is authorized to access any information process in LOW NETWORK and HIGH NETWORK, is always trusted and will never inject information from HIGH NETWORK to LOW NETWORK by any mean.

Table 11. 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.ONE_WAY_FLOW	T.DATA_INJECTION

Table 12. 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 hold, counters or enforces at least one assumption, threat or policy, respectively.

Objective	Assumption / Threat / OSP
OE.INTEGRATOR	A.INTEGRATOR T.DATA_INJECTION
OE.PHYSICAL	A.PHYSICAL T.DATA_INJECTION
OE.NETWORK	A.NETWORK T.DATA_INJECTION T.GET_DATA_FROM_HIGH
OE.MEDIACONVERTER	A.MEDIACONVERTER
OE.TRUSTED_OPERATOR	A.TRUSTED_OPERATOR T.GET_DATA_FROM_HIGH

Table 13. 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_INJECTION	The treat is countered by:
	• O.ONE.WAY_FLOW
	  ○ which on physical level allows only data to flow from the A.R.I.C NDS DD INPUT through its TX interface to the A.R.I.C NDS DD OUTPUT through its RX interface, no physical connection between A.R.I.C NDS DD INPUT RX and A.R.I.C NDS DD OUTPUT TX interfaces ensures that no data generated in the A.R.I.C NDS DD OUTPUT and in HIGH NETWORK reaches the A.R.I.C NDS DD INPUT and LOW NETWORK.
	  ○ which ensures that communication from LOW NETWORK towards HIGH NETWORK is forwarded.
	• OE.INTEGRATOR, which ensures that the integrator who is performing the installation and maintenance of the TOE is well-trained and competent in the prevention of data injection, 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.
	• OE.NETWORK, which ensures that the TOE is the only one communication path between LOW NETWORK and HIGH NETWORK, and both LOW NETWORK and HIGH NETWORK are protected from any unauthorized actions.

T.GET_DATA_FROM_HIGH	The treats are countered by: • OE.TRUSTED_OPERATOR, which ensures that the operator who is authorized to access any information from both LOW NETOWRK and HIGH NETWORK, will never inject data from HIGH NETWORK to LOW NETWORK by any mean, and therefore the threat is countered. • OE.NETWORK, which ensures that both LOW NETWORK and HIGH NETWORK are protected from any unauthorised actions, according to industrial standards.

Table 14. Sufficiency

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.

Assumption	Rationale for security Objectives
A.PHYSICAL	OE.PHYSICAL

	The security objective is a restatement of the assumption, it is therefore self-explanatory.
A.INTEGRATOR	OE.INTEGRATOR The security objective is a restatement of the assumption, it is therefore self-explanatory.
A.NETWORK	OE.NETWORK The OE.NETWORK requires that the only physical connection between the LOW NETWORK and the HIGH NETWORK is through the A.R.I.C. NDS DD what implicates that there are no other channels for the information to flow between HIGH NETWORK and LOW NETWORK.
A.MEDIACONVERTER	OE.MEDIACONVERTER The security objective is a restatement of the assumption, it is therefore self-explanatory.
A.TRUSTED_OPERATOR	OE.TRUSTED_OPERATOR The security objective is a restatement of the assumption, it is therefore self-explanatory.

Table 15. Sufficiency of objectives holding assumptions.

5. Extended Component Definition

No additional extended components are required.

6. Security Requirements

The TOE uses two subjects: LOW NETWORK and HIGH NETWORK. These subjects have no attributes.

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.).

Only assignment operation applies, which is used to assign a specific value to an unspecified parameter. Assignments are denoted by **bold text**.

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 16. 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 Information Flow SFPolicy**] on [

the subjects

- **LOW NETWORK**
- **HIGH NETWORK**

the information

- **"an Ethernet frame that wants to traverse between the LOW NETWORK and HIGH NETWORK through the TOE"**]

and all operations that cause that information to flow to and from subjects covered by the SFPolicy.

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 SFPolicy.

6.1.1.2. *Simple security attributes (FDP_IFF.1)*

FDP_IFF.1.1 The TSF shall enforce the [**One-Way Information Flow SFPolicy**] based on the following types of subject and information security attributes: [

the subjects

- **LOW NETWORK**
  - **Attributes:**
    - **None**
- **HIGH NETWORK**
  - **Attributes:**
    - **None**

the information

- **"an Ethernet frame that wants to traverse between the LOW NETWORK and HIGH NETWORK through the TOE".**
    - **Attributes:**
        - **Origin of the Ethernet frame]**

Application Note: No security attributes are stated for the subjects. The attribute for the information is only the origin of it. The flow control policy acts by allowing the information to pass between subjects in only one direction (from LOW NETWORK to HIGH NETWORK).

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: [**Any information originating from the LOW NETWORK shall traverse through the TOE to the HIGH NETWORK**].

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

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [**Any information originating from the LOW NETWORK and received on the A.R.I.C. NDS DD INPUT HI-SEC port shall exit through the A.R.I.C NDS DD OUTPUT HI-SEC port into the HIGH NETWORK**]**.**

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [**Any information received on A.R.I.C NDS DD OUTPUT HI-SEC port and attempting to leave through the A.R.I.C NDS DD INPUT HI-SEC 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.ONE_WAY_FLOW
FDP_IFF.1	O.ONE_WAY_FLOW

Table 17. 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.ONE_WAY_FLOW	The TOE shall physically ensure data to flow only from LOW NETWORK to HIGH NETWORK. Specifically: - the data flow from HIGH NETWORK to LOW NETWORK shall by always denied; - the data flow from LOW NETWORK to HIGH NETWORK shall be allowed (forwarded without modification of ethernet frames content). This objective is satisfied by: • FDP_IFC.2, which ensures that any information flow in the TOE is covered by *One-Way Information Flow SFPolicy*. • FDP_IFF.1, which allows that any information incoming from the LOW NETWORK and received on the A.R.I.C. NDS DD INPUT HI-SEC port shall exit through the A.R.I.C. NDS DD OUTPUT HI-SEC port towards the HIGH NETWORK. FDP_IFF.1 also denies any information received on the A.R.I.C. NDS DD OUTPUT HI-SEC port to exit through the A.R.I.C. NDS DD INPUT HI-SEC port towards the LOW NETWORK.

Table 18. Security objectives for the TOE rationale

6.2.3. Security Requirements Dependency Analysis

Dependencies within the EAL3 package selected for the security assurance requirements have been considered by the authors of CC Part 3 and are not analysed here again.

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	FDP_IFC.2
	FMT_MSA.3	Not resolved - excluded. This dependency SFR is not applicable because there is no security attributes to initialize. The TOE configuration is static and has therefore no concept of manageable security attributes. This dependency SFR is therefore not applicable.

Table 19. TOE SFR dependency analysis

6.3.Security Assurance Requirements Description

The security assurance requirements (SARs) for the TOE are the Evaluation Assurance Level 3 components as specified in [CC] part 3. No operations have been performed on the SARs. These requirements are listed in the table below:

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.3 Authorisation controls
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

Table 20. EAL3 Assurance Components.

6.4.Security Assurance Requirements Rationale

The evaluation assurance requirements were selected from an EAL to provide a balanced level assurance and consistent with the security objectives of the TOE.

7. TOE Summary Specification

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

7.1.One-Way Information Flow

The TOE consists A.R.I.C. NDS DD INPUT and A.R.I.C. NDS DD OUTPUT. The A.R.I.C. NDS DD INPUT is only connected to the LOW NETWORK and is not connected to the HIGH NETWORK. The A.R.I.C. NDS DD OUTPUT is only connected to the HIGN NETWORK and is not connected to the LOW NETWORK.

The TOE implements a data diode functionality (one-way gateway) through A.R.I.C. NDS DD INPUT HI-SEC port, where a fiber-optic patch cord is connected to the A.R.I.C. NDS DD OUTPUT HI-SEC port. Both A.R.I.C. NDS DD INPUT and A.R.I.C. NDS DD OUTPUT are connected with each other through HI-SEC ports using the single fibre of the optic patch cord, which is only connected to A.R.I.C. NDS DD INPUT HI-SEC TX interface and A.R.I.C. NDS DD OUTPUT HI-SEC RX interface.

Therefore, data can only flow from the A.R.I.C. NDS DD INPUT HI-SEC TX interface to A.R.I.C. NDS DD OUTPUT HI-SEC RX interface. The content of the Ethernet frames forwarded by TOE from LOW NETWORK towards HIGH NETWORK is not changed.

Data cannot flow from the A.R.I.C. NDS DD OUTPUT HI-SEC TX interface to A.R.I.C. NDS DD INPUT HI-SEC RX interface. The flow is blocked on physical layer - A.R.I.C. NDS DD OUTPUT HI-SEC TX interface is not connected to A.R.I.C. NDS DD INPUT HI-SEC RX interface, so it is not possible to transmit data to A.R.I.C. NDS DD INPUT HI-SEC port.

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

8. Abbreviations, Terminology and References

8.1.Abbreviations

BOM – Bill Of Materials

CC – Common Criteria

DZ – Demarcation Zone

EAL – Evaluation Assurance Level

FO 1J – Fibre Optic 1 (one) Join

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

IPv4 – Internet protocol version 4

OS – Operating System

OSI – Open Systems Interconnection

OSP – Organizational Security Policy

OT – Operation Technology

SAR – Security Assurance Requirement

SFP – Small Form-factor Pluggable

SFPolicy - Security Functional Policy

SFR – Security Functional Requirement

ST – Security Target

TCP – Transmission Control Protocol

TOE – Target of Evaluation

TSF – TOE Security Function

8.2.Terminology

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

DD INPUT LO-SEC port - The input interface of the data diode. LOW NETWORK devices are connected to this interface.

DD OUTPUT LO-SEC port - The output interface of the data diode. HIGH NETWORK devices and networks are connected to this interface.

HIGH NETWORK - The external autonomous system, which receives information from the LOW NETWORK, through the TOE.

LOW NETWORK - OT system from which information is to be sent to the HIGH NETWORK, through the TOE.

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 version 3.1, revision 5, April 2017 Part 2: Security functional components version 3.1, revision 5, April 2017 Part 3: Security assurance components version 3.1, revision 5, April 2017

Table 21. References