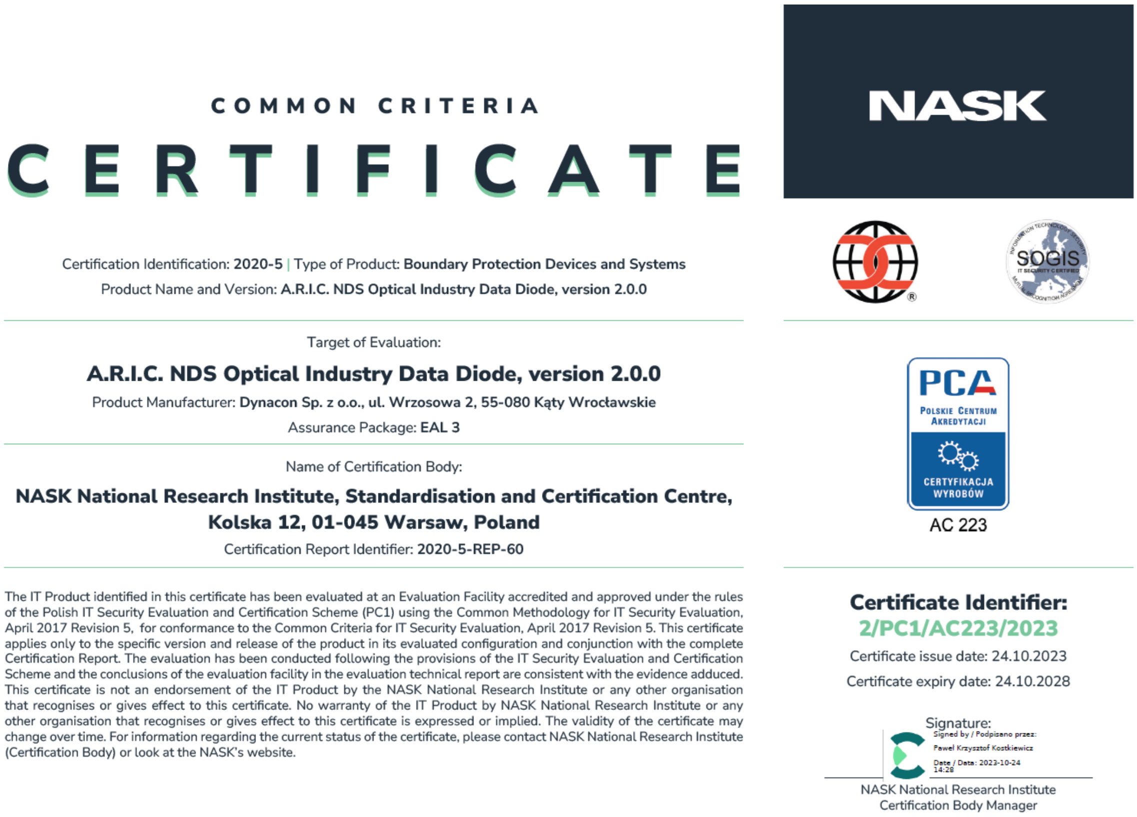
Certification Dossier Code:	2020-5
Certification Report Creation Date:	20th June 2023
Certification Report Code:	2020-5-REP-60 (internal) 2020-5-REP-86 (public)
NASK RWA code:	OSiC.8711.5.2021

Certification Report

[2020-5] Certification Report on A.R.I.C. NDS Optical Industry Data Diode EAL3



COMMON CRITERIA

CERTIFICATE

Certification Identification: **2020-5** | Type of Product: **Boundary Protection Devices and Systems**
Product Name and Version: **A.R.I.C. NDS Optical Industry Data Diode, version 2.0.0**

Target of Evaluation:

A.R.I.C. NDS Optical Industry Data Diode, version 2.0.0

Product Manufacturer: **Dynacon Sp. z o.o., ul. Wrzosowa 2, 55-080 Kąty Wrocławskie**

Assurance Package: **EAL 3**

Name of Certification Body:

NASK National Research Institute, Standardisation and Certification Centre, Kolska 12, 01-045 Warsaw, Poland

Certification Report Identifier: **2020-5-REP-60**

The IT Product identified in this certificate has been evaluated at an Evaluation Facility accredited and approved under the rules of the Polish IT Security Evaluation and Certification Scheme (PC1) using the Common Methodology for IT Security Evaluation, April 2017 Revision 5, for conformance to the Common Criteria for IT Security Evaluation, April 2017 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and conjunction with the complete Certification Report. The evaluation has been conducted following the provisions of the IT Security Evaluation and Certification Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT Product by the NASK National Research Institute or any other organisation that recognises or gives effect to this certificate. No warranty of the IT Product by NASK National Research Institute or any other organisation that recognises or gives effect to this certificate is expressed or implied. The validity of the certificate may change over time. For information regarding the current status of the certificate, please contact NASK National Research Institute (Certification Body) or look at the NASK's website.

NASK

PCA
POLSKIE CENTRUM AKREDYTACJI
CERTYFIKACJA WYROBÓW
AC 223

Certificate Identifier:
2/PC1/AC223/2023
Certificate issue date: 24.10.2023
Certificate expiry date: 24.10.2028

Signature:
Signed by / Podpisano przez:
Paweł Krzysztof Kostkiewicz
Date / Data: 2023-10-24
14:28

NASK National Research Institute
Certification Body Manager

Podpisany elektronicznie przez
NASK - PIB
11.06.2025
10:12:33 +02'00'

Table of content

1. Introduction

The Information Technology (IT) and Operational Technology (OT) product identified in this certification report and its associated certificate, has been tested at an approved Laboratory (IT Security Evaluation Facility) – on the basis of the IT Security Evaluation and Certification Scheme – using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5. This certification report and its associated certificate applies only to the identified version and release of the product in its tested and evaluated configuration. The evaluation has been conducted in accordance with the provisions of the PC1 Scheme and the conclusions of the Laboratory in the technical evaluation report are consistent with the evidence. This report and its associated certificate, are not an endorsement of the IT product by the NASK National Research Institute, or any other organization that recognizes or gives effect to this report and its associated certificate and no warranty for the IT product by the NASK National Research Institute, or any other organization that recognizes or gives effect to this report and its associated certificate, is either expressed or implied. This certification report and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration.

2. Certification overview

The NASK's "IT Security Evaluation and Certification Scheme" (Accreditation AC-223 by Polish Centre of Accreditation) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by an approved Laboratory under the oversight of the Certification Body, which is managed by the NASK National Research Institute. Laboratory is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025:2018- The General Requirements for the Competence of Testing and Calibration Laboratories. By awarding a Common Criteria certificate, the Certification Body asserts that the product complies with the security requirements specified in the associated Security Target. A security target is a requirements specification document that defines the scope of the evaluation activities. **The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality and the testing and analysis conducted by the Laboratory**. The Certification Report, Product Certificate and Security Target are posted to the Certified Products List for the IT Security Evaluation and Certification Scheme published by NASK National Research Institute.

Recognition of the certificate

European Recognition of CC Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3) became effective in April 2010. It defines the recognition of certificates for IT-Products up to EAL4. A higher recognition levels are provided for IT-Products related to certain SOGIS Technical Domains only.

The current list of signatory nations and approved certification schemes can be found on https://www.sogis.eu/.

The SOGIS-MRA logo printed on the certificate indicates that it is recognized under the terms of this agreement by signatory nations. This certificate is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the Common Criteria (Common Criteria Recognition Arrangement, CCRA) became effective in September 2014. It covers Common Criteria certificates based on: collaborative Protection Profiles, assurance components up to EAL2 augmented by ALC_FLR and certificates for PP and cPP.

The current list of signatory nations and of collaborative Protection Profiles can be found on https://www.commoncriteriaportal.org.

The CCRA logo printed on the certificate indicates that it is recognized under the terms of this agreement by signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition. This certificate is recognized under CCRA up to EAL2.

Executive Summary

This document constitutes the Certification Report for the certification file of the product: **A.R.I.C. NDS Optical Industry Data Diode**

TOE Version:	2.0.0
Developer:	Dynacon Sp. z o.o.
Sponsor:	Project co-financed from the NCBiR national programme „Cybersecurity and e-Identity” as part of the KSO3C project
Security Target:	Security Target LITE A.R.I.C. NDS Optical Industry Data Diode, Version1.0, issue date 29.09.2024
Protection Profile:	None
Laboratory/ITSEF:	Instytut Łączności Państwowy Instytut Badawczy (AB 1787)
Evaluation Level:	Common Criteria version 3.1 Revision 5, Evaluation Assurance Level EAL3
Evaluation end date:	16/05/2023 (Final ETR ver.2.0.0, issue date 16.05.2023)
Expiration Date:	24.10.2028

Documentation available for users

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version:

[EXT-975] [EVD-ST-V1.6]	**Security Target v. 1.6, Issue date 21.04.2023 (confidential document – LITE version available)**
[EXT-984] [EVD-AGD_PRE-V1.4]	**Preparative guidance, v. 1.4, issue date 21.04.2023 (confidential document)**
[EXT-985] [EVD-AGD_OPE-V1.4]	**Operational user guidance, v. 1.4, issue date 21.04.2023 (confidential document)**

Security Target

Along with this certification report, the complete Security Target of the evaluation is stored and protected in the Certification Body premises. This document is identified as:

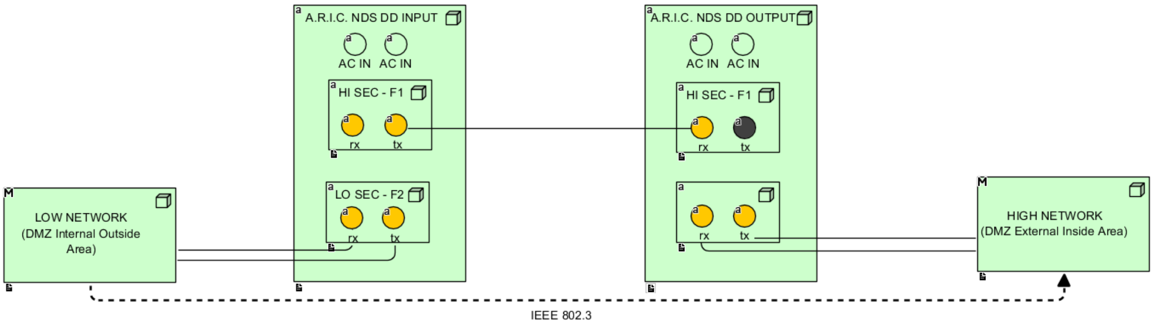
Security Target A.R.I.C. NDS Optical Industry Data Diode, Version1.6, issue date 21.04.2023

The public version of this document is published along with this Certification Report on the Certification Body website.

3. TOE Summary

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.

TOE 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.

Security Assurance Requirements

The product was evaluated with all the evidence required to fulfil the evaluation level EAL3, according to Common Criteria v3.1 Revision 5.

Assurance Class	Assurance Component
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

Security Policy

TOE provides following security policies:

- User Data Protection

User Data Protection

The TOE provides information protection by implementation of the One-Way information flow control policy which ensures data flow in on one direction:

- 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.
- 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 is not allowed to do so.

Security Functional Requirements

Functional requirement	Description
FDP: User Data Protection	FDP_IFC.2 Complete information flow control
	FDP_IFF.1 Simple security attributes

4. Assumptions and Clarification of Scope

The assumptions are constraints to the conditions used to assure the security properties and functionalities introduced by the Security Target. All assumptions are to be taken into consideration, when the attack potential is calculated and the impact of the vulnerability on the product is presented (mostly in terms of reduction). In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its usage and operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE. These assumptions have been applied during the evaluation in order to determine, if the identified vulnerabilities can be exploited.

Usage Assumptions

The Security Target [EVD-ST-V1.6] contains two assumptions related to the usage of the TOE.

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.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.

Environmental Assumptions

The Security Target [EVD-ST-V1.6] makes three assumption on the operational environment of the TOE:

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.

Clarification of Scope

Threats

The Security Target [EVD-ST-V1.6] defines two threats which have been taken into consideration during the evaluation process.

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.

OSPs

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

5. Architectural Information

Physical scope

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 (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
- 2 pcs of user guidance: preparative guidance and operational user guidance.

Logical scope

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.

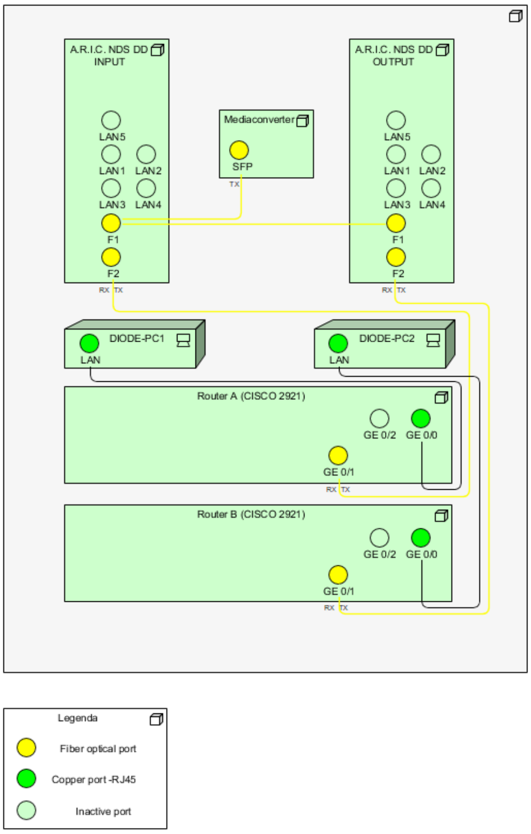
The LOW NETWORK data received by A.R.I.C. NDS DD INPUT is sent to A.R.I.C. NDS DD OUTPUT. The TOE has two internal interfaces, one on each A.R.I.C NDS DD hardware appliances – HI-SEC ports. The A.R.I.C NDS DD INPUT HI-SEC TX interface is connected by single fiber-optic cable with A.R.I.C NDS DD OUTPUT 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.

6. IT security evaluation

Evaluated Configuration

Physical network topology required to perform tests is shown below on Figure 1. Physical testing environment. Additionally, the following console connections are available to enable access to A.R.I.C. NDS DD INPUT and A.R.I.C. NDS DD OUTPUT devices (from the DIODE-PC1 and DIODE-PC2 accordingly).



- The USB port of DIODE-PC1 is connected to the serial port of A.R.I.C. NDS DD INPUT devi (with USB to serial console cable),
- The USB port of DIODE-PC2 is connected to the serial port of A.R.I.C. NDS DD OUTPUT device (with USB to serial console cable).

The PCs (PC1 and PC2) shall satisfy the minimum requirements for the Debian 10 OS (minimum RAM: 512MB, minimum Hard Drive Space: 10 GB, minimum 1GHz Pentium processor) and shall be equipped with minimum one ethernet port (1 Gbps) and one USB port.

The detailed configuration of A.R.I.C. NDS Optical Industry Data Diode could be found in the paragraph 1.4 of the Security Target v. 1.6.

Figure 1. Physical testing environment

The configuration items of the test bed for A.R.I.C. NDS DD consist of the following elements shown in Table 1.

Element description	ID	Type	Network
Operator PC Linux OS with monitor, keyboard.	PC-1	Host	LOW
Intermediate device	Router A (Cisco 2921)	Router	LOW
A.R.I.C. NDS DD INPUT device	A.R.I.C. NDS DD INPUT	Data Diode	LOW
Mediaconverter		Light Source	NONE
A.R.I.C. NDS DD OUTPUT device	A.R.I.C. NDS DD OUTPUT	Data Diode	LOW
Intermediate device	Router B (Cisco 2921)	Router	HIGH
Server PC Linux OS with monitor, keyboard.	PC-2	Host	HIGH

Table 1. Test bed elements description

Functional testing

The Evaluation Assurance Level EAL3 requires the Developer to devise and conduct the complete set of tests covering all TSFIs and interactions between subsystems of the TOE. The Evaluator's task is divided into two activities. The Evaluators shall confirm the Developer's tests results using the sampling strategy described in details by the Common Criteria methodology. Additionally, the Evaluators are expected to devise and perform their own subset of tests which are intended to be the supplementary for the tests prepared by the Developer.

Developer testing

The Developer has tested covers all TSFIs and their security functional behaviour. As the TOE consists of two subsystems, the tests covered both the behaviour of the TOE subsystems and the interaction between them.

The Developer prepared and performed 10 tests.

All the test cases have obtained a PASS verdict.

Evaluator testing

The Evaluator decided to repeat all functional tests delivered by the Developer. The positive results of the Developer's tests were confirmed.

Additionally the Evaluator devised a test subset supplementing the Developer's test approach by usage of different tools, using other types of protocols and simultaneously tracing on all available TSFIs.

The independent tests plan covered the whole TOE functionality: all the SFRs have been tested through their TSFIs as well as the interactions between the subsystems.

The total number 23 cases were performed and obtained a PASS verdict.

Penetration testing

The attack potential used for this evaluation is consistent with AVA_VAN.2: Basic attack potential. The Evaluators analysis is based on vulnerability survey of the evaluation evidence as well as the information available in the public to ascertain potential vulnerabilities that may be easily found by an attacker.

The intention of the vulnerability analysis is to determinate if there are faults or weaknesses of the TOE that can be exploited in the operational environment.

The evaluation of documentation analysis and tests resulted in the 10 vulnerability notes, which represented a potential vulnerability. Additionally 13 publicly available vulnerabilities (acquired from databases and scientific publications) have been taken into consideration during the analysis.

Analysis of the assumptions for the operational environment presented in the final Security Target version 1.6 showed that **NONE** of the potential vulnerabilities could be exploited due to the strong restrictions regarding the TOE accessibility.

As the result NO vulnerability testing was performed by the Evaluators.

Evaluation verdicts

The Evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation and concluded that the TOE meets the security objectives stated in the Security Target for an attack potential Enhanced-Basic.

The Certifier reviewed the work of the Evaluator and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The verdicts for the assurance classes and components are summarised in the following table:

Assurance Class	Assurance Component	Laboratory Verdict	Certification Body Validation
ADV: Development	ADV_ARC.1 Security architecture description	PASS	CONFORMANT
	ADV_FSP.3 Functional specification with complete summary	PASS	CONFORMANT
	ADV_TDS.2 Architectural Design	PASS	CONFORMANT
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	PASS	CONFORMANT
	AGD_PRE.1 Preparative procedures	PASS	CONFORMANT

Assurance Class	Assurance Component	Laboratory Verdict	Certification Body Validation
ALC: Life-cycle support	ALC_CMC.3 Authorisation controls	PASS	CONFORMANT
	ALC_CMS.3 Implementation representation CM coverage	PASS	CONFORMANT
	ALC_DEL.1 Delivery procedures	PASS	CONFORMANT
	ALC_DVS.1 Identification of security measures	PASS	CONFORMANT
	ALC_LCD.1 Developer defined life-cycle model	PASS	CONFORMANT
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims	PASS	CONFORMANT
	ASE_ECD.1 Extended components definition	PASS	CONFORMANT
	ASE_INT.1 ST introduction	PASS	CONFORMANT
	ASE_OBJ.2 Security objectives	PASS	CONFORMANT
	ASE_REQ.2 Derived security requirements	PASS	CONFORMANT
	ASE_SPD.1 Security problem definition	PASS	CONFORMANT
	ASE_TSS.1 TOE summary specification	PASS	CONFORMANT
ATE: Tests	ATE_COV.2 Analysis of coverage	PASS	CONFORMANT
	ATE_DPT.1 Testing: basic design	PASS	CONFORMANT
	ATE_FUN.1 Functional testing	PASS	CONFORMANT
	ATE_IND.2 Independent testing - sample	PASS	CONFORMANT
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis	PASS	CONFORMANT

Certifier's Comments

Recommendations regarding the secure usage of the TOE are provided in the documentation. These have been collected along the evaluation process and shall to be considered when using the product.

The use of the TOE is recommended due to the lack of vulnerabilities that could be exploited in the operational environment which is achieved due to the fact that the attack potential is reduced to zero by restrictive objectives for the operational environment. The potential for attack is radically limited because the TOE is physically protected from any access in a way that can be considered the most significant factor in protecting the TOE and its security functionality.

Nonetheless, the following usage recommendations are given:

- It is mandatory to strictly follow the steps indicated in the installation documentation in order to install the correct version of the TOE in a proper manner.
- The user guidance must be read and understood in order to operate the TOE in an adequate manner according to the Security Target.

7. Certifier’s Recommendations

All the assurance components required by the evaluation level EAL3 of Common Criteria standard have been assigned a “PASS” verdict. Consequently, the laboratory assigned the “PASS” VERDICT to the whole evaluation due all the evaluation requirements are satisfied for the EAL3, as defined by the Common Criteria v3.1 Revision 5 and the CEM v3.1 Revision 5.

Considering the obtained and validated evidence and gained the Certification Team experience of the Certification Team during the certification process of the product A.R.I.C. NDS Optical Industry Data Diode v. 2.0.0 evaluation, a positive resolution is proposed.

8. Acronyms

EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ITSEF	Information Technology Security Evaluation Facility
CB	Certification Body
TOE	Target Of Evaluation

9. Bibliography

The following standards and documents have been used for the evaluation of the product:

1. [CC31p1] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model, Version 3.1, Revision 5

2. [CC31p2] Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components, Version 3.1, Revision 5

3. [CC31p3] Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components, Version 3.1, Revision 5

4. [CEM31] Common Criteria for Information Technology Security Evaluation. Evaluation Methodology, Version 3.1 Revision 5

References

List of normative documents

SOG-IS MRA Mutual Recognition Agreement of Information Technology Security Evaluation Certificates

CCRA Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security

ISO/IEC 15408 Information technology - Security techniques - Evaluation criteria for IT security

ISO/IEC 17025 General requirements for competence of calibration and testing laboratories

ISO/IEC 17065 Conformity assessment - Requirements for bodies certifying products, processes and services

ISO/IEC 18045 Information technology — Security techniques — Methodology for IT security evaluation

PC1 IT Security Evaluation and Certification Scheme

List of related documents:

[EXT-999] [FIN-ETR-V2.0.0]	**Final Evaluation Technical Report, v. 2.0.0, issue date 16.05.2023 (ITSEF confidential document)**
[EXT-975] [EVD-ST-V1.6]	**Security Target v. 1.6, issue date 21.04.2023 (confidential document)**
[EXT-1260] [EVD-ST-V1.0 LITE]	**Security Target LITE A.R.I.C. NDS Optical Industry Data Diode, v. 1.0, issue date 29.09.2024**
[EXT-984] [EVD-AGD_PRE-V1.4]	**Preparative guidance, v. 1.4, issue date 21.04.2023 (confidential document)**
[EXT-985] [EVD-AGD_OPE-V1.4]	**Operational user guidance, v. 1.4, issue date 21.04.2023 (confidential document)**
[EXT-986] [EVD-ADV-ARC-V1.4]	**Security Architecture, v. 1.4, issue date 21.04.2023 (confidential document)**
[EXT-987] [EVD-ADV-FSP-V1.4]	**Functional Specification, v. 1.4, issue date 21.04.2023 (confidential document)**
[EXT-988] [EVD-ADV-TDS-V1.4]	**TOE Design, v. 1.4, issue date 21.04.2023 (confidential document)**
[EXT-785] [EVD-ALC_CMC-V1.5]	**Configuration Management Plan, v. 1.5, issue date 12.07.2022 (confidential document)**
[EXT-786] [EVD-ALC_CMS-V1.1]	**Configuration Items List, v. 1.1, issue date 12.07.2022 (confidential document)**
[EXT-787] [EVD-ALC_DEL-V1.3]	**TOE Delivery Procedure, v. 1.3, issue date 12.07.2022 (confidential document)**
[EXT-788] [EVD-ALC_DVS-V1.3]	**Development security measures description, v. 1.3, issue date 12.07.2022 (confidential document)**
[EXT-789] [EVD-ALC_LCD-V1.1]	**Development life cycle model definition, v. 1.1, issue date 12.07.2022 (confidential document)**
[EXT-784] [EVD-SVCL-EAL3]	**Site visit checklist EAL3, v. 1.4, issue date 18.06.2022 (confidential document)**
[EXT-983] [EVD-ATE-ALL-V1.3]	**ATE Vendor test plan supporting document, v. 1.3, issue date 21.04.2023 (confidential document)**
[EXT-780] [EVD-ATE-DTR-V1.2]	**ATE Vendor test plan, v. 1.2, issue date 18.08.2022 (confidential document)**
[EXT-808] [EVD-ATE-DTS-V1.2]	**ATE Test Scripts, v. 1.2, no issue date (confidential document)**