blackline systems

BSC-CDS Unidirectional Subsystem

Security Target

Version 0.9

August 2021

Document prepared by

Lightship Security

www.lightshipsec.com

Document History

Version	Date	Author	Description
0.1	Mar 26, 2020	L Turner	Draft for review.
0.2	July 16, 2020	L Turner	EAL4 updates.
0.3	Sep 22, 2020	L Turner	EAL4+ updates.
0.4	Oct 2, 2020	L Turner	Address lab observations.
0.5	Oct 23, 2020	L Turner	Address observations.
0.6	Nov 2, 2020	L Turner	Address observations.
0.7	Aug 6, 2021	R Yeomans	Addressed observation in OR 10
0.8	Aug 20, 2021	M Heffer	Updated TOE P/N in Table 1
0.9	Aug 23, 2021	M Heffer	Updated 2.4.1

Table of Contents

List of Tables

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the Blackline Systems Corporation BSC-CDS Unidirectional Subsystem Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 The BSC-CDS Unidirectional Subsystem is a part of a cross-domain solution (data diode) that provides 1Gbps of reliable unidirectional throughput while preventing the possibility of any reverse communication channel being established.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	Blackline Systems Corporation BSC-CDS Unidirectional Subsystem Part Number: 710-0185-00
Security Target	Blackline Systems Corporation BSC-CDS Unidirectional Subsystem Security Target, v0.9

1.3 Conformance Claims

3 This ST supports the following conformance claims:

a) CC version 3.1 Release 5

b) CC Part 2 conformant

c) CC Part 3 conformant

d) EAL4 augmented with ADV_INT.2, ALC_CMC.5, ALC_CMS.5, ALC_DVS.2, ALC_FLR.3, ATE_DPT.2 and AVA_VAN.4

1.4 Terminology

Table 2: Terminology

Term	Definition
CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile
TOE	Target of Evaluation
TSF	TOE Security Functionality

2 TOE Description

2.1 Type

4 The TOE is a data diode subsystem.

2.2 Usage

5 The TOE is part of the BSC-CDS, which is deployed as a cross domain solution between two networks (see Figure 1). Deployment primarily consists of correctly connecting the source and destination network equipment. No configuration of the TOE is required for enforcement of unidirectional data transfer.

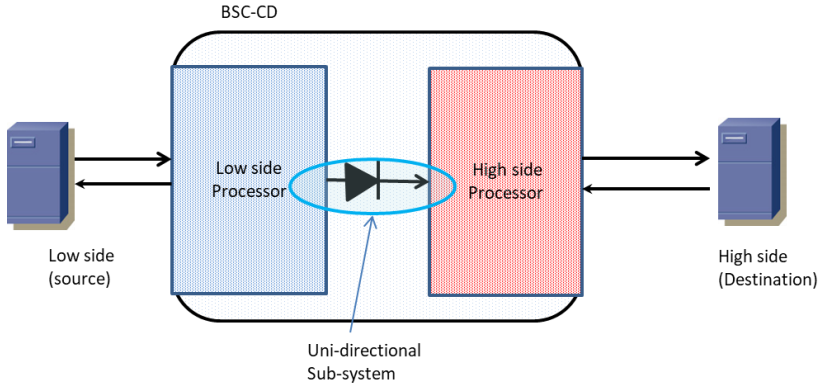

Figure 1: Example TOE Deployment

6 The BSC-CDS is intended for deployment in a secured, access restricted space. Once installed, the possibility of a threat through physical access to the device is significantly limited. The BSC-CDS enclosure is tamper protected and tamper evident labels prevent access to components inside the enclosure.

2.3 Logical Scope

7 The logical scope of the TOE is comprised of the following security functions:

a) **Unidirectional Data Transfer.** The TOE ensures that data can only be transmitted in one direction and that no data can be passed, either explicitly or covertly, in the reverse direction.

b) **Failure with Preservation of Secure State.** The TOE will not allow data to be transmitted from high side to low side in the event power or hardware failures.

2.4 Physical Scope

8 The physical boundary of the TOE is limited to the hardware elements within the BSC-CDS that implement the unidirectional link between the internal low side (or source) and high side (or destination) BSC-CDS processor cards. As shown in purple in Figure 2, this consists of:

a) The low side transmitter

b) The interconnecting fiber

c) The high side receiver

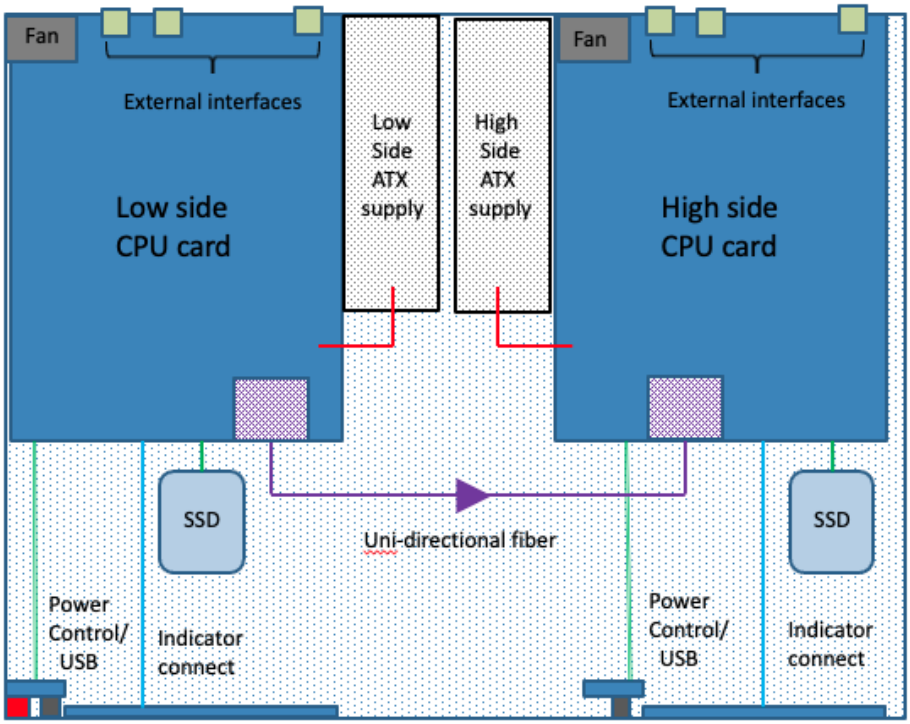

Figure 2: Physical Scope

9 The TOE is a component of the BSC-CDS device which is delivered to customers via commercial carrier.

2.4.1 Guidance Documents

10 The TOE includes the following guidance documents:

a) Blackline CD User Guide V2.0 (PDF delivered on CD-ROM with the BSC-CDS)

b) BSC-CDS TOE User Guidance V1.3 (CC specific document, PDF delivered on CD-ROM with the BSC-CDS)

2.4.2 Non-TOE Components

11 The TOE operates with the following components in the environment:

a) **Connecting equipment.** The low side and high side connected network equipment.

b) **BSC-CDS device.** The TOE is subsystem of the BSC-CDS device.

3 Security Problem Definition

3.1 Threats

Table 3: Threats

Identifier	Description
T.TRANSFER	A user or process on the destination network accidentally or deliberately transmits data through the TOE to the source network resulting in the unauthorized disclosure of information from the high side to the low side.
T.TAMPER	An adversary tampers with the contents of the TOE during delivery, and/or after installation resulting in the unauthorized disclosure of information from the high side to the low side.
T.FAILURE	The TOE fails in some manner resulting in the unauthorized disclosure of information from the high side to the low side.

3.2 Assumptions

Table 4: Assumptions

Identifier	Description
A.PHYSICAL	The TOE will be stored and deployed in accordance with the physical security requirements of the high side.
A.CONNECT	The TOE is the only method of interconnecting the high side and low side networks.
A.NO_EVIL	Authorised users of the TOE are non-hostile and follow all usage guidance to ensure that the TOE is configured and operated in a secure manner.
A.ENCLOSURE	The TOE enclosure is constructed to resist tampering efforts and employs mechanisms to detect and respond to tamper attempts.

3.3 Organizational Security Policies

Table 5: Organizational Security Policies

Identifier	Description
OSP.PERSONNEL	The TOE shall be administered by authorized personnel who possess the necessary privileges to access high side network equipment.

4 Security Objectives

4.1 Objectives for the Operational Environment

Table 6: Security Objectives for the Operational Environment

Identifier	Description
OE.PHYSICAL	The TOE will be stored and deployed in accordance with the physical security requirements of the high side.
OE.CONNECT	The TOE shall be the only method of interconnecting the high side and low side networks.
OE.NO_EVIL	Authorised users of the TOE shall be non-hostile and follow all usage guidance to ensure that the TOE is configured and operated in a secure manner.
OE.ENCLOSURE	The TOE enclosure shall resist, detect and respond to tamper attempts.
OE.PERSONNEL	The TOE shall be administered by authorized personnel who possess the necessary privileges to access high side network equipment.

4.2 Objectives for the TOE

Table 7: Security Objectives

Identifier	Description
O.ONE_WAY	The TOE shall ensure that data can only be transmitted from the low side to the high side.
O.FAIL_SECURE	The TOE shall maintain a secure state in the event of a power or hardware failure ensuring that no data can be transferred from the high side to the low side, even in the event of such failures.

5 Security Requirements

5.1 Conventions

12 This document uses the following font conventions to identify SFR operations:

a) **Assignment.** Indicated with italicized text.

b) **Refinement.** Indicated with bold text and strikethroughs.

c) **Selection.** Indicated with underlined text.

d) **Assignment within a Selection:** Indicated with italicized and underlined text.

e) **Iteration.** Indicated by adding a string starting with "/" (e.g. "FCS_COP.1/Hash").

5.2 Extended Components Definition

13 None defined.

5.3 Functional Requirements

Table 8: Summary of SFRs

Requirement	Title
FDP_IFC.2	Complete information flow control
FDP_IFF.1	Simple security attributes
FDP_IFF.5	No illicit information flows
FPT_FLS.1	Failure with preservation of secure state

5.3.1 User Data Protection (FDP)

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 [*Unidirectional Flow Policy*] on [

- *Subjects: Source Port, Destination Port*
- *Information: All Data Transiting the TOE*]

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.

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 [*Unidirectional Flow Policy*] based on the following types of subject and information security attributes: [

- *Subjects: Source Port, Destination Port*
- *Information: All Data Transiting the TOE*
- *Attributes: Inherent attributes*].

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: [*data may flow from the Source Port to the Destination Port*].

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

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [*none*].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [*none*].

FDP_IFF.5 No illicit information flows

Hierarchical to: FDP_IFF.4 Partial elimination of illicit information flows

Dependencies: FDP_IFC.1 Subset information flow control

FDP_IFF.5.1 The TSF shall ensure that no illicit information flows exist to circumvent [*Unidirectional Flow Policy*].

5.3.2 Protection of the TSF (FPT)

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [

- *Power failure*
- *Hardware failure*]

5.4 Assurance Requirements

14 The TOE security assurance requirements (EAL4+) are summarized in Table 9. Augmented components are shown in bold text.

Table 9: Assurance Requirements

Assurance Class	Components	Description
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_INT.2	**Well-structured internals**
	ADV_TDS.3	Basic modular design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative User Guidance
ALC: Life-cycle Support	**ALC_CMC.5**	**Advanced support**
	ALC_CMS.5	**Development tools CM coverage**
	ALC_DEL.1	Delivery Procedures
	ALC_DVS.2	**Sufficiency of security measures**
	ALC_FLR.3	**Systematic flaw remediation**
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
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

Assurance Class	Components	Description
	ATE_DPT.2	**Testing: security enforcing modules**
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
AVA: Vulnerability Assessment	**AVA_VAN.4**	**Methodical vulnerability analysis**

6 TOE Summary Specification

6.1 Unidirectional Data Transfer

15 The TOE implements multiple redundant unidirectional enforcing mechanisms in hardware, as shown in Figure 3 (transceiver modules and fiber cable).

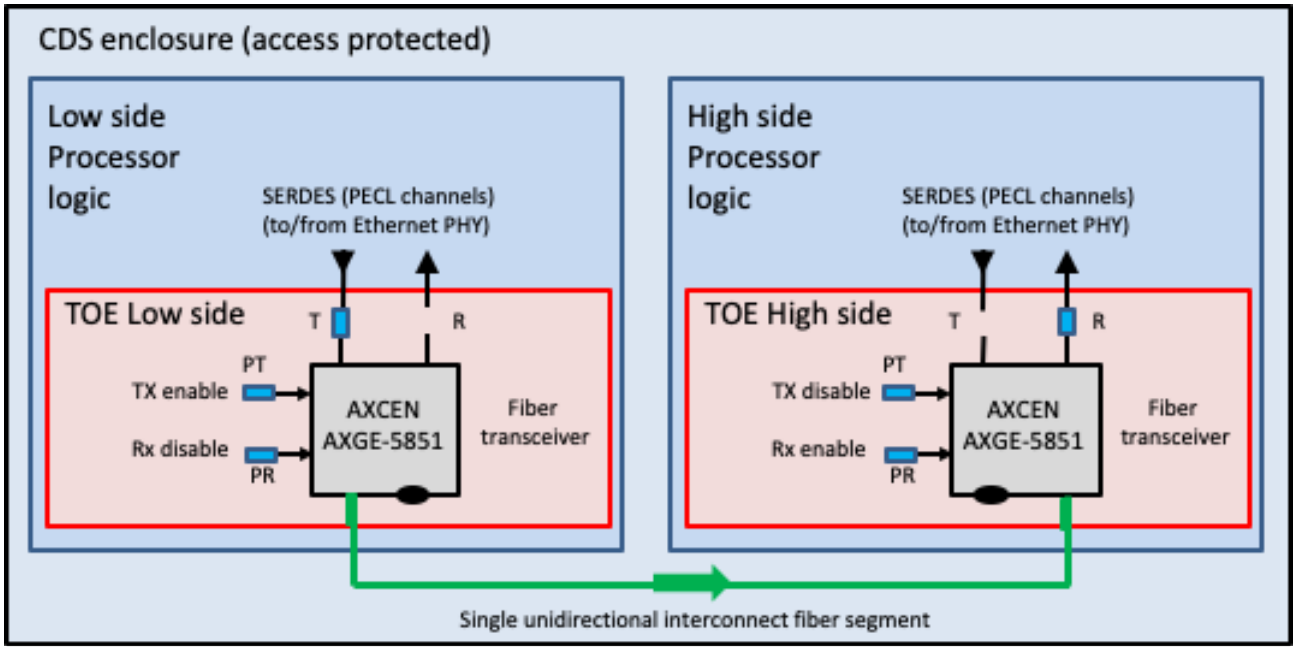

Figure 3: TOE Security Enforcing Mechanisms

16 The security enforcing mechanisms are described in the following sections. A failure in any of these mechanisms will not result in a violation of unidirectional data transfer.

6.1.1 Interconnect Fiber Cable

17 The BSC-CDS incorporates two fully independent processor cards, each purpose-configured to the low or high side. A single patch cable connects the low side transmit port to the high side receive port, thus providing a point of unidirectional data transfer enforcement.

18 Cable end points (fiber connectors) are fixed in place with epoxy to prevent removal and/or in-stream insertion of any device.

19 Unused fiber ports on the transceiver are flooded with epoxy to prevent insertion of a fiber connector.

6.1.2 Transceiver Configuration

20 The transceivers are configured to enforce unidirectional data transfer:

a) Two separate fibre optic cables are required for duplex operation - only one is installed

b) There is no receive logic on the low side transmission path

c) There is no transmission logic on the high side reception path

d) The transmitter and receiver logic are powered from separate sources

e) The low side transceiver receive circuit is un-powered (grounded)

f) The high side transceiver transmit circuit is un-powered (grounded)

21 Driving any form of signal in the reverse direction to the flow of traffic, specifically into the transmitter is not possible.

6.2 Fail Secure

22 The absence of a reverse signal path ensures that no data can be transferred from high side to low side regardless of hardware or power failure. Security policy enforcement does not rely on power or active components.

7 Rationale

7.1 Security Objectives Rationale

23 Table 10 provides a coverage mapping between security objectives, threats, OSPs and assumptions.

Table 10: Security Objectives Mapping

	T.TRANSFER	T.TAMPER	T.FAILURE	A.PHYSICAL	A.CONNECT	A.NO_EVIL	A.ENCLOSURE	OSP.PERSONNEL
O.ONE_WAY	X							
O.FAIL_SECURE			X					
OE.PHYSICAL		X		X				
OE.CONNECT	X				X			
OE.NO_EVIL						X		
OE.ENCLOSURE		X					X	
OE.PERSONNEL						X		X

24 Table 11 provides the justification to show that the security objectives are suitable to address the security problem.

Table 11: Suitability of Security Objectives

Element	Justification
T.TRANSFER	**O.ONE_WAY.** Enforcing one-way data transmission prevents the disclosure of information from high side to low side. **OE.CONNECT.** The operational environment ensures that the TOE is the only interconnection point between the high side and the low side.
T.TAMPER	**OE.PHYSICAL.** The operational environment ensure that delivery, storage and operation occur in a secure manner, commensurate with the security requirements of the high side – thereby reducing the risk of tampering to acceptable levels.

Element	Justification
	OE.ENCLOSURE. The 1U enclosure surrounding the TOE is resistant to tampering due to its construction and incorporates tamper detection and response mechanisms.
T.FAILURE	**O.FAIL_SECURE.** Ensures that a failure of the TOE does not result in a violation of one-way data transmission.
A.PHYSICAL	**OE.PHYSICAL.** Upholds the assumption by restating it as an objective for the operational environment.
A.CONNECT	**OE.CONNECT.** Upholds the assumption by restating it as an objective for the operational environment.
A.NO_EVIL	**OE.NO_EVIL.** Upholds the assumption by restating it as an objective for the operational environment. **OE.PERSONNEL.** Also contributes to upholding this assumption as high side security requirements will likely include personnel vetting measures commensurate with the information being protected.
A.ENCLOSURE	**OE.ENCLOSURE.** Upholds the assumption by restating it as an objective for the operational environment.
OSP.PERSONNEL	**OE.PERSONNEL.** Upholds the policy by restating it as an objective for the operational environment.

7.2 Security Requirements Rationale

7.2.1 SAR Rationale

25 EAL4+ has been selected at the direction of the evaluation sponsor.

7.2.2 SFR Rationale

Table 12: Security Requirements Mapping

	O.ONE_WAY	O.FAIL_SECURE
FDP_IFC.2	X	
FDP_IFF.1	X	

	O.ONE_WAY	O.FAIL_SECURE
FDP_IFF.5	X	
FPT_FLS.1		X

Table 13: Suitability of SFRs

Objectives	SFRs
O.ONE_WAY	**FDP_IFC.2.** Defines the scope of the Unidirectional Flow Policy (i.e. source, destination, data). **FDP_IFF.1.** Defines the Unidirectional Flow Policy requiring that data only flow from source to destination. **FDP_IFF.5.** Requires that there be no illicit information flows from destination to source.
O.FAIL_SECURE	**FPT_FLS.1.** Requires the TOE to maintain a secure state in the event of a failure covering power and hardware components.

Table 14: Dependency Analysis

SFR	Dependencies	Rationale
FDP_IFC.2	FDP_IFF.1	Met
FDP_IFF.1	FDP_IFC.1	Met
	FMT_MSA.3	Not met – the security attributes used to define the Unidirectional Flow SFP are inherent (i.e. they are not data objects) and therefore do not need to be initialized per.
FDP_IFF.5	FDP_IFC.1	Met
FPT_FLS.1	None	n/a

7.3 TOE Summary Specification Rationale

26 Table 15 provides a coverage mapping showing that all SFRs are mapped to the security functions described in the TSS.

Table 15: Map of SFRs to TSS Security Functions

	Unidirectional Data Transfer	Fail Secure
FDP_IFC.2	X	
FDP_IFF.1	X	
FDP_IFF.5	X	
FPT_FLS.1		X

--END OF DOCUMENT--