Waterfall Unidirectional Security Gateway WF-500
Version 1

Security Target

Version 1.2

December 01, 2016

Waterfall Security Solutions Ltd.
21 Hamelacha St., Afek Industrial Park
Rosh Ha'ayin, Israel 48091

Document Version Control Log

Ver-sion	Date	Author	Description
0.1	October 09, 2015	Waterfall	This ST derives from "Waterfall Unidirectional Security Gateway WF-40 Security Target", v1.4, April 5 2013.
1.1	December 15, 2015	Waterfall	New figures 1-4 and 1-5 New guidance version v1.0.6
1.2	December 01, 2016	Waterfall	New guidance version v1.0.9

Table of Contents

List of Tables

List of Figures

1. ST Introduction

1.1. ST Reference

Title:	Waterfall Unidirectional Security Gateway WF-500 Security Target
ST Version:	1.2
ST Date:	December 01, 2016
Author:	Waterfall
CC Version:	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012
Evaluation Assurance Level (EAL):	EAL 4, augmented with AVA_VAN.5 (Advanced methodical vulnerability analysis), ALC_DVS.2 (Sufficiency of security measures), and ALC_FLR.2 (Flaw reporting procedures).

1.2. TOE Reference

TOE Name:	Waterfall Unidirectional Security Gateway
TOE identifier:	WF-500, Version 1.

The evaluated hardware configurations of the TOE are:

- WF-500-Compact (CC)
- WF-500-Standard (CC)
- WF-500-Standard-Split (CC)
- WF-500-Standard-Host (CC)

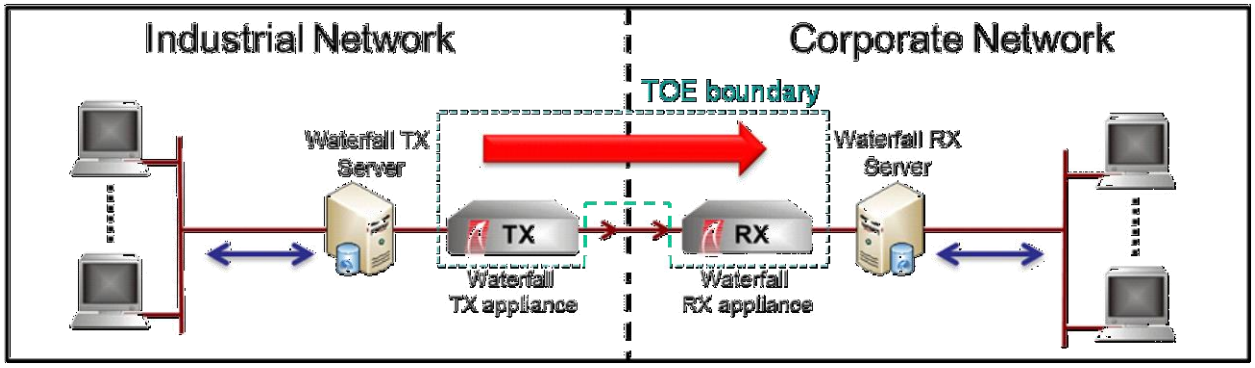
1.3. TOE Overview

The Target of Evaluation (TOE) is a network gateway that enforces a unidirectional information flow control policy on network traffic flowing through the gateway. The TX Module reads network frames from the sending network, and transmits them to the RX Module for writing to the receiving network. The TOE hardware ensures that no information can flow from the receiving network to the sending network. The TOE includes the hardware configurations as defined in section 1.2.

The TOE does not require nor provide any management capabilities. The unidirectional traffic flow is operational once the TX Module is connected to the sending network, the RX Module to the receiving network, the two Modules connected by a single fiber-optic cable, and the two Modules are each powered up.

A typical usage scenario consists of a sending network that represents a utility's industrial network, and a receiving network that represents the corporate or monitoring environment. For example, a power plant or other SCADA network is required to transmit status information in real-time, while preventing an attack from the external network that might impact its integrity or result in a denial of service.

Figure 1-1 – Typical Usage Scenario



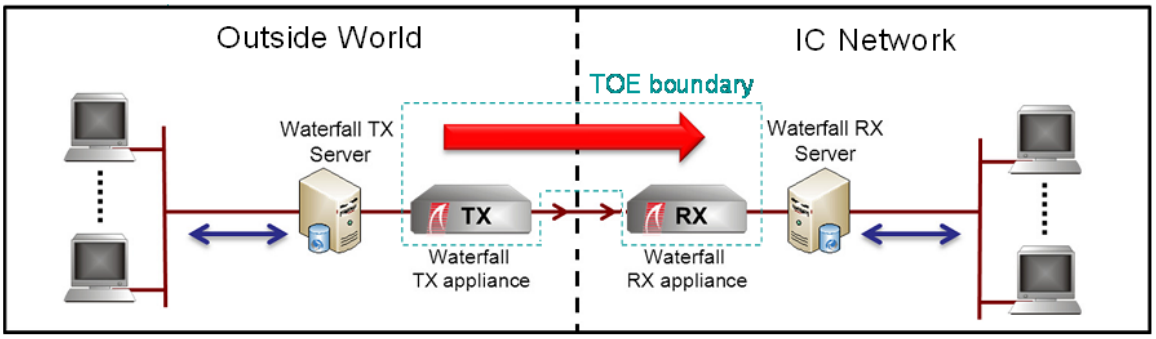
A secondary objective is to protect against threat Agents that might gain access to the industrial network in an attempt to attack the corporate network. For example, the sending network might be a network of distributed video security cameras that is transmitting live video feeds to the receiving network for storage, analysis and review. Whereas the primary objective is to prevent an attacker from hacking into the receiving network and controlling the cameras, the physical accessibility of the cameras requires that the receiving network also be protected from attacks from the sending network.

The TOE allows information to flow from the industrial network to the corporate network, while preventing any information flows through the gateway to the industrial network. This serves to prevent a wide range of online attacks:

- The sending network is fully protected against any online cyber attacks initiated at the receiving network, since no information can be transmitted from the receiving network to the sending network.
- Most network-based attacks require feedback from the network-connected entity under attack[1]. Since no information can be transmitted back from the receiving network to the sending network, network-connected Hosts on the receiving network are thus protected against many forms of online cyber attacks initiated at the sending network. Where this protection is applied in conjunction with a traffic filtering capability (outside the TOE), a high degree of protection is provided for the receiving network.
- The receiving network is fully protected against information leaks into the sending network, since no information can be transmitted from the receiving network to the sending network.

An alternative usage scenario might involve a classified Intelligence Community (IC) network that must receive information from the outside world (e.g. from sensors or from other operational networks), while preventing leakage of classified information. In this scenario, the TOE is configured such that the IC network is the receiving network.

Figure 1-2 – An Intelligence Community Usage Scenario



The Waterfall Unidirectional Security gateway is used as the security-enforcing core for a set of Waterfall products that include, in addition to the gateway, TX and RX Agent software running on servers in the sending and receiving networks, respectively. The Agents provide product management and monitoring capabilities and support for standard network protocols, including: FTP (file transfer), SMTP (email), SNMP traps, Syslog, Remote Screen View (RSV), OSIsoft PI, System 1, Modbus, ASDE-X, WMQ, eDNA, ICCP, OPC-DA, and others.

[1] For example, an attacker in the industrial network cannot easily complete a TCP handshake with the corporate network if she is prevented from receiving the acknowledgement from the targeted server.

As depicted in Figure 1-1 above, the servers, Agent software and fiber-optic cable are outside the TOE; they cannot affect the enforcement of unidirectional information flow by the TOE.

1.4. TOE Description

1.4.1. Physical Scope and Boundaries of the TOE

1.4.1.1. TOE Hardware, Firmware, and Software

The Waterfall Unidirectional Security gateway WF-500 (Figure 1 - 3) is a modular hardware system architecture with embedded computing capabilities that provides flexibility and scalability for unidirectional security gateway deployments.

The WF-500 series architecture consists of one or more half-depth or full-depth 1u rack-mount
Waterfall WF-500 Cabinets (Figure 1-4 and Figure 1-5), each populated with Waterfall Modules (Figure 1-6). The Compact full-depth cabinet holds up to four Modules, and the Standard half- depth cabinet holds up to two Modules. Cabinets are Completely enclosed by an aluminum casing.

A physical divider separates the left from right sides of each cabinet, to make it clear that no electrical & cabling connections exist between TX and RX sides of the cabinet. All connections between Modules are via the front panel.

Waterfall Modules include:

- TX Modules (WF-500TX)
- RX Modules (WF-500RX)
- Linux/Windows Agent Host Modules

Each of the above Modules performs a specific function:

- Gateway (TOE)
  - Waterfall TX Module WF-500TX: is the transmitting appliance with Dual power supply input. It receives data from a server equipped with Waterfall software and transmits packets via a fiber optic cable to the RX Module.
  - Waterfall RX Module WF-500RX with Dual power supply input: is the receiving appliance. It receives packets from the TX via a single fiber optic cable and relays the data to a server equipped with Waterfall software.

- Agent Host (out of scope of the TOE)
  - TX & RX Agent Host Modules: is a normal PC, it can transmit data to the TX for transfer, or from the RX post transfer. The Agent Host function is to organize, encode, and filter data per customer specifications. All Waterfall software configurations are performed on Agent Host Modules.

The TX Module contains a laser LED that converts electronic signals to light. The RX Module contains a photoelectric cell that can sense light and convert it to electronic signals. The Waterfall TX Module and Waterfall RX Module are connected via a single standard fiber-optic cable, allowing light to be transmitted from the TX LED to the RX photoelectric cell. The cable is not included in the TOE.

The TOE Security Functionality is implemented entirely in hardware. The TOE also contains firmware that implements functionality such as control of the front-panel display LEDs.

The following gateway Modules are only included in the TOE:

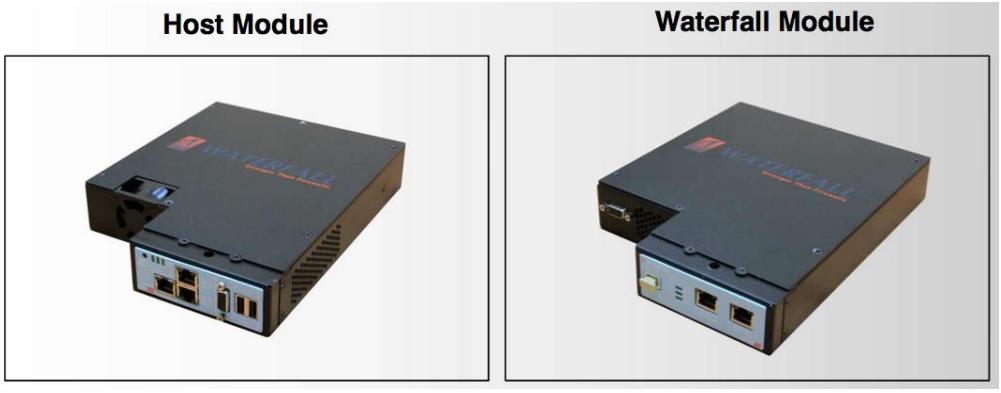
- WF-500TX
- WF-500RX

Figure 1-3 – Outside view of the WF-500 system

Figure 1-4 - WF-500 Modular Architecture (Standard Cabinet)

Figure 1-5 – WF-500 Modular Architecture (Compact Cabinet)

Figure 1-6 – Separated Modules for Gateway (TX and RX) and Host



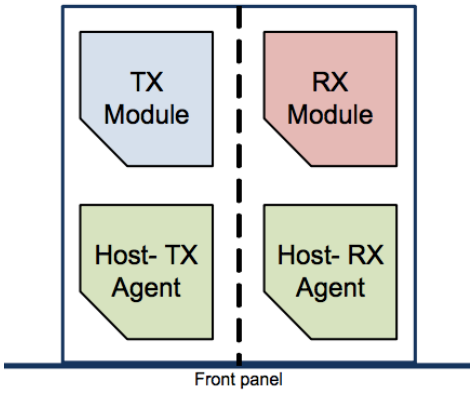
Modules are individual units that can be arranged together in a variety of hardware configurations within a single WF-500 cabinet.

The TOE can operate in the following four evaluated configurations. These differing hardware configurations don't affect the functionality and the security of WF-500 version 1.

1. WF-500-Compact (CC)

   The full-depth cabinet holds one Waterfall TX Module and one Waterfall RX Module connected by a single fiber optic cable, and two TX & RX Agent Host Modules with the Waterfall software agents- one connected to the Waterfall TX Module and one connected to the Waterfall RX Module.

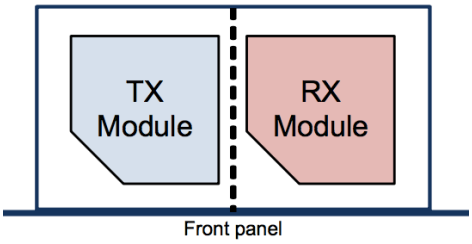
Figure 1-7 – WF-500 Compact configuration



2. WF-500-Standard (CC)

   The half- depth cabinet holds Waterfall TX and RX Modules only. Waterfall agent software is installed on customer-supplied servers.

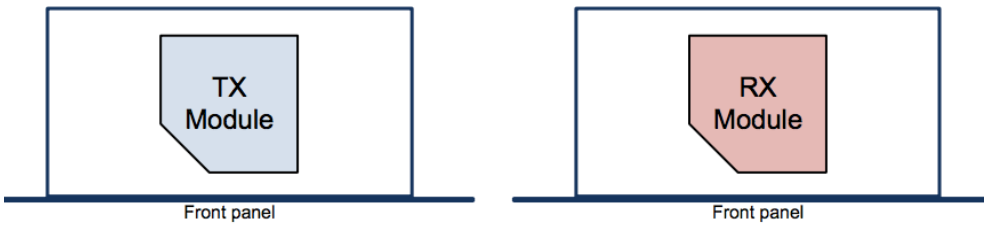
Figure 1-8 – WF-500 Standard configuration



3. WF-500-Standard-Split (CC)

   Waterfall TX and RX Modules are split across two half-depth cabinets to support deployment in different racks, different rooms, or even different buildings.

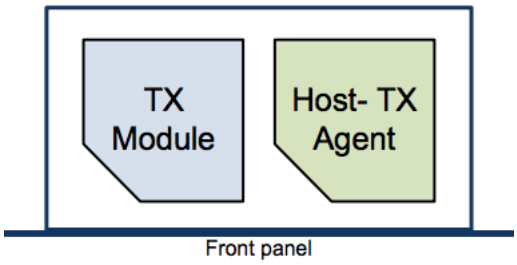
Figure 1-9 – WF-500 Standard Split configuration



4. WF-500-Standard-Host (CC)

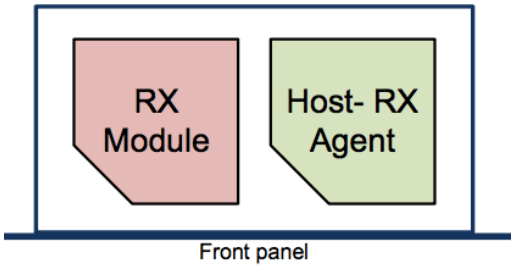
   The Standard Host TX configuration contains the TX unit and a server with the Waterfall Agent, with no RX module. It is intended to be used in conjunction with the Standard Host RX configuration.

Figure 1-10 – WF-500 Standard Host TX configuration



The Standard Host RX configuration contains the RX unit and a server with the Waterfall Agent, with no TX module. It is intended to be used in conjunction with the Standard Host TX configuration.

Figure 1-4 – WF-500 Standard Host RX configuration



1.4.1.2. TOE Guidance

The following Waterfall guidance is considered part of the TOE:

Title	Date
Waterfall Unidirectional Security Gateway WF-500 Common Criteria Evaluated Configuration Guide, version 1.0.9	November, 2016

Waterfall customers may contact Waterfall support to request a copy of the guidance, which provides instructions and cautions for operating the product in its evaluated configuration.

1.4.2. Logical Scope of the TOE

1.4.2.1. Summary of TOE Security Functionality

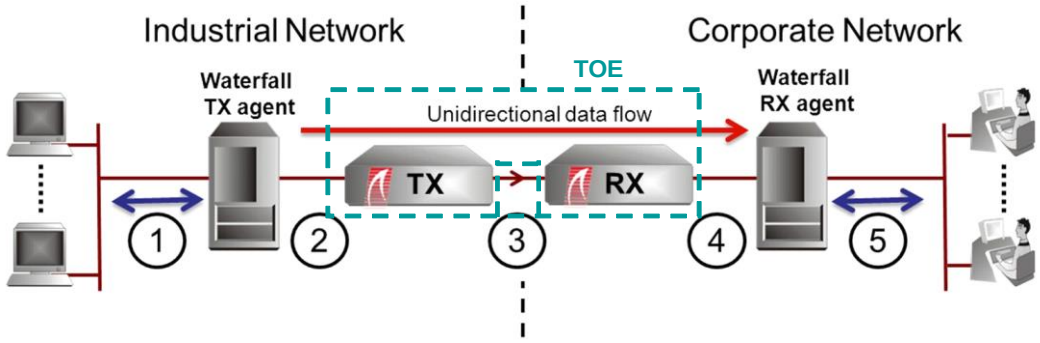
The TOE enables online transmission of data (e.g. information, alerts, files, video streams, etc.) from a designated sending network to a designated receiving network in a unidirectional mode only. No information can be transmitted in the reverse direction through the TOE.

The TOE does not provide any management or auditing functionality.

1.4.2.2. Information Flow through the TOE

The Waterfall Unidirectional Security Gateway can be provided both as a stand-alone solution and as an integrated component in large scale IT security projects, enabling secure one-way data transfer from a critical industrial network to the corporate network.

Figure 1-5 – Information Flow through the TOE



The following sequence describes the information flow through the TOE (steps 3 and 4 below describe processing that is within the TOE):

1. The Waterfall TX Agent Host Module (outside the TOE) on TX side receives a protocol-specific data stream from the industrial network servers or stations.
2. The Waterfall TX Agent Host Module handles the translation of the data into Waterfall's proprietary protocol and sends the information to the Waterfall TX Module through electrical Ethernet.
3. The Waterfall TX Module reads the information from its network interface and transmits the information to the Waterfall RX over a single fiber-optic cable (the cable is outside the TOE but maintained within a physically secure environment).
4. The Waterfall RX Module receives the information and sends it to the Waterfall RX Agent Host Module on the RX server (outside the TOE) by writing it to the RX network interface (Ethernet). The Waterfall RX Agent Host Module handles the

retrieval of the information from the Waterfall RX Module and the translation of the data from Waterfall's proprietary protocol.

5. The Waterfall RX Agent Host Module communicates the data stream to the corporate network servers or stations.

1.5. Document Organization

Section 1 provides the introductory material for the security target, including ST and TOE references, TOE Overview, and TOE Description.

Section 2 identifies the Common Criteria conformance claims in this security target.

Section 3 describes the security problem solved by the TOE, in terms of the expected operational environment and the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE or through additional environmental controls identified in the TOE documentation.

Section 4 defines the security objectives for both the TOE and the TOE environment.

Section 5 gives the functional and assurance requirements derived from the Common Criteria, Parts 2 and 3, respectively that must be satisfied by the TOE.

Section 6 explains how the TOE meets the security requirements defined in section 6, and how it protects itself against bypass, interference and logical tampering.

Section 7 provides external references used in this security target document

2. Conformance Claims

2.1. CC Conformance Claim

The TOE is conformant with the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012, CCMB-2012-09-002, conformant (CC Part 2 Conformant)
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003, conformant (CC Part 3 Conformant)

2.2. Protection Profile and Package Conformance Claims

This Security Target claims conformance to assurance package EAL4 augmented with AVA_VAN.5, ALC_DVS.2, and ALC_FLR.2.

The TOE does not claim conformance with any Protection Profile.

2.3. Conformance Rationale

None.

3. Security Problem Definition

3.1. Threats

This section describes the threats that are addressed by the TOE:

T.LEAKAGE	A user with access to the receiving network accidentally or maliciously transmits information to the sending network.
T.HACK_HIGH	A user with access to the receiving network compromises the integrity of a host or process on the sending network.
T.HACK_LOW	A user with access to the sending network compromises the integrity of a host or process on the receiving network.

3.2. Organizational Security Policies

This Security Target does not identify any rules or guidelines that must be followed by the TOE and/or its operational environment, phrased as Organizational Security Policies.

All defined security objectives are derived from assumptions and threats only.

3.3. Assumptions

The assumptions made about the TOE's intended environment are:

A.PHYSICAL	The TOE and the fiber-optic cable connecting its separate parts will be located within controlled access facilities, which will prevent unauthorized physical access.
A.ADMIN	Personnel with authorized physical access to the TOE will not attempt to circumvent the TOE's security functionality.
A.NETWORK	There will be no channel for information to flow between the sending and receiving networks unless it passes through the TOE.

4. Security Objectives

4.1. Security Objectives for the TOE

O.UNIDIRECTIONAL The TOE shall allow information to flow only from the sending network to the receiving network and not vice versa.

4.2. Security Objectives for the Operational Environment

4.2.1. Traffic Filtering Objectives for the IT Environment

As explained in section 1.3 above, the TOE provides mitigation against online cyber attacks initiated at the sending network, given that most online attacks require feedback from the entity under attack. The following security objective for the IT environment complements this by requiring the environment to filter or transform the traffic from the sending network in order to prevent attacks from the sending network.

OE.FILTER_LOW The IT environment shall filter or transform the information transmitted through the TOE to the receiving network such that it cannot result in compromise of the integrity of hosts or processes on the receiving network.

Note: The Waterfall TX and RX Agent Host Modules (considered to be in the IT environment) proxy the information transmitted through the TOE to the receiving network, thereby implementing a restrictive traffic filter that allows only a specific unidirectional protocol stream into the receiving network. This filtering functionality is not being evaluated in the context of this Security Target.

4.2.2. Security Objectives for the Environment Upholding Assumptions

The assumptions made in this ST about the TOE's operational environment must be upheld by corresponding security objectives for the environment.

The following security objectives are intended to be satisfied without imposing technical requirements on the TOE. These objectives are intended to be satisfied through the application of procedural or administrative measures.

NOE.PHYSICAL The intended operation environment shall prevent unauthorized physical access to the TOE and to the fiber-optic cable connecting its separate parts.

NOE.ADMIN Physical access to the TOE shall be authorized only to personnel that will not attempt to circumvent the TOE's security functionality.

NOE.NETWORK The TOE is the only interconnection between the sending and receiving networks.

Application Note: It is recommended to use separate power and network infrastructure for the sending and receiving networks, connected to the TX and RX, respectively.

4.3. Security Objectives Rationale

Table 4-1 maps security objectives to threats and assumptions described in chapter 3. The table clearly demonstrates that each threat is countered by at least one security objective, that each assumption is upheld by at least one security objective, and that each objective counters at least one threat or upholds at least one assumption.

This is then followed by explanatory text providing justification for each defined threat that if all security objectives that trace back to the threat are achieved, the threat is removed, sufficiently diminished, or that the effects of the threat are sufficiently mitigated. In addition, each defined assumption is shown to be upheld if all security objectives for the operational environment that trace back to the assumption are achieved.

Table 4-1- Tracing of security objectives to threats

	T.LEAKAGE	T.HACK_HIGH	T.HACK_LOW	A.PHYSICAL	A.ADMIN	A.NETWORK
O.UNIDIRECTIONAL	✓	✓	✓			
OE.FILTER_LOW			✓			
NOE.PHYSICAL				✓		
NOE.ADMIN					✓	
NOE.NETWORK						✓

T. LEAKAGE *A user with access to the receiving network accidentally or maliciously transmits information to the sending network.*

O.UNIDIRECTIONAL ensures that information flows through the TOE will be allowed only from the sending network to the receiving network and not vice versa.

T. HACK_HIGH *A user with access to the receiving network compromises the integrity of a host or process on the sending network.*

O.UNIDIRECTIONAL ensures that information flows through the TOE will be allowed only from the sending network to the receiving network and not vice versa. A user with access to the receiving network cannot transmit any information to any host or process on the sending network, and therefore the threat of compromising the integrity of such hosts or processes is removed.

T. HACK_LOW *A user with access to the sending network compromises the integrity of a host or process on the receiving network.*

O.UNIDIRECTIONAL ensures that information flows through the TOE will be allowed only from the sending network to the receiving network and not vice versa. This provides mitigation for the majority of online attacks, as most attacks require feedback from the entity under attack.

OE.FILTER_LOW requires the IT environment to ensure that the unidirectional information flows through the TOE to the receiving network are filtered or transformed such that they cannot result in compromise of the integrity of hosts or processes on the receiving network.

Together, O.UNIDIRECTIONAL and OE.FILTER_LOW counter T.HACK_LOW.

A.PHYSICAL *The TOE* and the fiber-optic cable connecting its separate parts *will be located within controlled access facilities, which will prevent unauthorized physical access.*

NOE.PHYSICAL directly upholds A.PHYSICAL.

A.ADMIN *Personnel with authorized physical access to the TOE will not attempt to circumvent the TOE's security functionality.*

NOE.ADMIN directly upholds A.ADMIN. Together with NOE.PHYSICAL, this ensures that the TOE will not be subject to physical tampering, such as short-circuiting the TX and RX Modules and thereby bypassing the unidirectional optical transmission channel.

A.NETWORK *There will be no channels for information to flow between the sending and receiving networks unless it passes through the TOE.*

NOE.NETWORK directly upholds A.NETWORK.

5. Security Requirements

5.1. Security Functional Requirements

The security functional requirements (SFRs) for this ST consist of the following components from CC Part 2, summarized in Table 5-1.

Table 5-1 –Security functional requirement components

Functional Component		CC Operations Applied
FDP_IFC.2	**Complete Information Flow Control**	**Assignment**
FDP_IFF.1	**Simple Security Attributes**	**Assignment**

The terminology used in the SFRs is as defined in Common Criteria Part 2.

5.1.1. User data protection (FDP)

5.1.1.1. Complete Information Flow Control (FDP_IFC.2)

FDP_IFC.2.1 The TSF shall enforce the **Unidirectional SFP** on **the TX, the RX, and all information flowing through 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.

5.1.1.2. Simple security attributes (FDP_IFF.1)

FDP_IFF.1.1 The TSF shall enforce the **Unidirectional SFP** based on the following types of subject and information security 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 **following additional information flow control SFP rules**:

- **a) The TSF shall permit the TX to read information from the sending network;**
- **b) The TSF shall permit the TX to transmit information to the RX;**
- **c) The TSF shall permit the RX to receive information from the TX; and**
- **d) The TSF shall permit the RX to write information to the receiving network**.

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: **no rules that explicitly authorise information flows**.

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules:

- **a) The TSF shall deny the RX to transmit information to the TX; and**
- **b) The TSF shall deny the TX to receive information from the RX**.

Application Note: The Unidirectional SFP permits information flow from the sending network to the receiving network via TOE TX and RX subjects, and denies information flow in the inverse direction. Enforcement of this SFR does not involve any guarantees for delivery of information between sending and receiving networks. Such guarantees if required must be allocated to the IT and non-IT environment of the TOE.

For example, the Waterfall TX Agent Host Module (in the IT environment) queues information received for transmission from the sending network, and sequentially labels the information as transmitted to the receiving network through the TOE such that the Waterfall RX Agent Host Module (in the IT environment) can automatically identify and report any information loss. The TX Agent Host Module also provides the capability for manually retransmitting the missing information, on command.

5.2. Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level (EAL) 4 components defined in Part 3 of the Common Criteria, augmented with the CC Part 3 components ALC_FLR.2, ALC_DVS.2, and AVA_VAN.5.

No operations are applied to any assurance component.

Table 5-2- TOE Security Assurance Requirements

Assurance Class	Assurance Components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	Sufficiency of security measures
	ALC_FLR.2	Flaw reporting procedures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools

Assurance Class	Assurance Components	
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
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_VAN.5	Advanced methodical vulnerability analysis

5.3. Extended Components Definition

There are no extended components defined in this Security Target. All security requirements have been drawn from the [CC] Parts 2 and 3.

5.4. Security Requirements Rationale

5.4.1. Security Functional Requirements Rationale

Table 5-3 provides a mapping between the security requirements and the security objective for the TOE that has been defined in section 4. This is followed by a detailed rationale of this mapping.

Table 5-3- Tracing of SFRs to security objectives for the TOE

SFRs	O.UNIDIRECTIONAL
FDP_IFC.2	X
FDP_IFF.1	X

O.UNIDIRECTIONAL *The TOE shall allow information to flow only from the sending network to the receiving network and not vice versa.*

FDP_IFC.2 requires that all information flowing through the TOE be covered by the information flow control SFP. This ensures that no information flows, whether explicit or covert, are exempt from the Unidirectional SFP.

FDP_IFF.1 allows information to flow from the sending network to the receiving network as follows: the TX reads the information from the sending network; the TX transmits the information to the RX; the RX receives the information from the TX and writes it to the receiving network.

The inverse information flow (from the receiving network to the sending network) is explicitly denied by FDP_IFF.1, as the TX cannot read information from the receiving network, and no information can flow from the RX (which is connected to the receiving network) to the TX (which is connected to the sending network).

FDP_IFC.2 and FDP_IFF.1 together enforce the Unidirectional SFP on all information flows through the TOE.

5.4.2. Security Assurance Requirements Rationale

The level of assurance chosen for this ST is that of Evaluation Assurance Level (EAL) 4, as defined in CC Part 3, augmented with the CC Part 3 components AVA_VAN.5, ALC_DVS.2, and ALC_FLR.2.

EAL 4 ensures that the product has been methodically designed, tested, and reviewed with maximum assurance from positive security engineering based on good commercial development practices. It is applicable in those circumstances where developers or users require a moderate to high level of independently assured security.

AVA_VAN.5 Advanced Methodical Vulnerability Analysis augments EAL4 by ensuring that the product has undergone advanced methodical vulnerability analysis to confirm that the product is resistant to attacks with up to High attack potential.

EAL 4 augmented by AVA_VAN.5 is appropriate for a TOE designed to protect industrial networks from cyber attacks and to prevent leakage of information from classified networks. These use cases may attract attackers with high motivation and therefore High attack potential.

The ALC_DVS.2 Sufficiency of Security Measures augmentation was included to provide justification that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE in its development environment.

In addition, the assurance requirements have been augmented with ALC_FLR.2 (Flaw reporting procedures) to provide assurance that the TOE will be maintained and supported in the future, requiring the TOE developer to track and correct flaws in the TOE, and providing guidance to TOE users for how to submit security flaw reports to the developer.

5.4.3. Dependency Rationale

Table 5-4 depicts the satisfaction of all security requirement dependencies. For each security requirement included in the ST, the CC dependencies are identified in the column "CC dependency", and the satisfied dependencies are identified in the "ST dependency" column.

Dependencies that are satisfied by hierarchically higher or alternative components are given in **boldface**, and explained in the "Justification" column.

Table 5-4- Security Requirements Dependency Mapping

SFR/SAR	CC dependency	ST component	Justification (where needed)
FDP_IFC.2	FDP_IFF.1	FDP_IFF.1	
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	**FDP_IFC.2**	The dependency on FMT_MSA.3 is not applicable as there are no security attributes to initialize.
ADV_ARC.1	ADV_FSP.1, ADV_TDS.1	**ADV_FSP.4, ADV_TDS.3**	Consistent with EAL4

SFR/SAR	CC dependency	ST component	Justification (where needed)
ADV_FSP.4	ADV_TDS.1	**ADV_TDS.3**	Consistent with EAL4
ADV_IMP.1	ADV_TDS.3, ALC_TAT.1	ADV_TDS.3, ALC_TAT.1	
ADV_TDS.3	ADV_FSP.4	ADV_FSP.4	
AGD_OPE.1	ADV_FSP.1	**ADV_FSP.4**	Consistent with EAL4
AGD_PRE.1			
ALC_CMC.4	ALC_CMS.1, ALC_DVS.1, ALC_LCD.1	**ALC_CMS.4, ALC_DVS.2**, ALC_LCD.1	ALC_CMS.4 is consistent with EAL4; ALC_DVS.2 is hierarchical to ALC_DVS.1.
ALC_CMS.4	None		
ALC_DEL.1	None		
ALC_DVS.2	None		
ALC_FLR.2	None		
ALC_LCD.1	None		
ALC_TAT.1	ADV_IMP.1	ADV_IMP.1	
ASE_CCL.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.1	ASE_INT.1, ASE_ECD.1, **ASE_REQ.2**	Consistent with EAL4
ASE_ECD.1	None		
ASE_INT.1	None		
ASE_OBJ.2	ASE_SPD.1	ASE_SPD.1	
ASE_REQ.2	ASE_OBJ.2, ASE_ECD.1	ASE_OBJ.2, ASE_ECD.1	
ASE_SPD.1	None		
ASE_TSS.1	ASE_INT.1, ASE_REQ.1, ADV_FSP.1	ASE_INT.1, **ASE_REQ.2**, **ADV_FSP.4**	Consistent with EAL4
ATE_COV.2	ADV_FSP.2, ATE_FUN.1	**ADV_FSP.4,** ATE_FUN.1	Consistent with EAL4
ATE_DPT.1	ADV_ARC.1, ADV_TDS.2, ATE_FUN.1	ADV_ARC.1, **ADV_TDS.3**, ATE_FUN.1	Consistent with EAL4

SFR/SAR	CC dependency	ST component	Justification (where needed)
ATE_FUN.1	ATE_COV.1	**ATE_COV.2**	Consistent with EAL4
ATE_IND.2	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1	**ADV_FSP.4**, AGD_OPE.1, AGD_PRE.1, **ATE_COV.2**, ATE_FUN.1	Consistent with EAL4
AVA_VAN.5	ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1	ADV_ARC.1, ADV_FSP.4**,** ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1	

6. TOE Summary Specification

6.1. SFR Mapping

Table 6-1 provides a description of the general technical mechanisms that the TOE uses to satisfy each SFR defined in section 5. The table includes the description of security functionality given in each SFR by reference and provides a high-level view of their implementation in the TOE, referencing section 1.4.1 and 1.4.2 for descriptions of the physical and logical components of the TOE, respectively.

Table 6-1 - TOE Summary Specification SFR Mapping

Component	Description of mechanism
6.1.1. User Data Protection (FDP)	
FDP_IFC.2	The TOE is implemented in parts: the TX and RX Modules are independent, each with its own independent power and network interfaces. The cabinet enclosure does not admit electronic or light signals via any other interface than the described interfaces. In accordance with TOE guidance, the TX Module is connected only to the sending network, and is not connected to the receiving network. Conversely, the RX Module is connected only to the receiving network. A single fiber-optic cable connects TX and RX Modules. This ensures that all the information flows through the TOE must flow through the cable and are thereby covered by the Unidirectional SFP.
FDP_IFF.1	The TX Module is connected using standard RJ45 interfaces for copper-based electronic communication with the sending network. The TX Module cannot read information from the receiving network because its network interfaces are connected only to the sending network. The TX Module contains a proprietary TX board, which converts the incoming communication into a fiber-optic-based data transmission using a fiber-optic transceiver. The TX board and TX transceiver support only data transmission, implementing galvanic isolation between the on-board circuitry and the receiving end of the transceiver, which is customized by Waterfall so that it does not include a photoelectric cell for optical data reception. A single fiber-optic cable connects the TX Module to the RX Module, and constitutes the only connection between these two components. This fiber-optic cable connects to the RX Module's Fiber port. A proprietary RX board converts the incoming optical data into electronic signals using a fiber-optic transceiver. The RX board and RX transceiver support only data reception, implementing galvanic isolation between the on-board circuitry and the transmitting end of the transceiver, which is customized by Waterfall so that it does not include a LED for optical data transmission.

Component	Description of mechanism
	The RX Module is connected using standard RJ45 interfaces for copper-based electronic communication with the receiving network. The RX Module transmits the data received from the TX Module to the receiving network. The RX Module cannot transmit information to the sending network because its network interfaces are connected only to the receiving network.

7. Supplemental Information

7.1. References

The following external documents are referenced in this Security Target.

Identifier	Document
CC	Common Criteria for Information Technology Security Evaluation Parts 1-3, Version 3.1, Revision 4, September 2012, CCMB-2012-09-001, 002 and 003

7.2. Abbreviations

Abbreviation	Description
CC	Common Criteria
EAL	Evaluation Assurance Level
FTP	File Transfer Protocol
LED	Light Emitting Diode
RSV	Remote Screen View
SAR	Security Assurance Requirement
SCADA	Supervisory Control and Data Acquisition
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification