Waterfall Security Solutions Ltd.

waterfall

# WF-600 Waterfall-Security Unidirectional Security Gateway

# Security Target

Version 1.5

Updated: 25 Sep 2024

# Legal Notice and Disclaimer

All intellectual property rights in this publication (including, without limitation all of Waterfall Security Solutions Ltd.'s (Waterfall) trademarks, logo types, trade names, and insignia) are owned by Waterfall, constitute valuable intellectual property of Waterfall, protected by applicable patent, copyright and trade secret laws and international treaty provisions. Please see https://waterfall-security.com/company/legal for further information. Waterfall retains all rights not expressly granted.

No part of this publication may be reproduced in any form whatsoever or used to make any derivative work without prior written approval by Waterfall.

Waterfall reserves the right to revise this publication, and/or make improvements or changes in the product(s) and/or the program(s) described in this publication at any time without prior notice.

Any software on removable media described in this publication is furnished to you under a license agreement included with the product as a separate document. If you are unable to locate a copy, please contact Waterfall and a copy will be forwarded to you.

No representation of or warranties for fitness for any purpose other than what is specifically stated in this guide is made either by Waterfall or by its agents.

The information in this publication is provided in good faith and under the explicit understanding, that Waterfall shall have no liability whatsoever arising from any errors and/or omissions and/or inaccuracies which may be contained unintentionally in this publication. Furthermore, no rights, implied or assumed, shall be furnished or derived through this publication and no rights, implied or assumed are furnished under any patent or pending patent with the sale or delivery of any Waterfall product.

Other third party intangible and/or proprietary and/or intellectual property rights mentioned in this publication are the property of their respective owners. It is forbidden to copy, modify or sell products derived from, or in any other way exploit or use such third parties' rights without the express authorization of their respective owners. Waterfall does not guarantee nor make any representations with regard to any and all third party intellectual property mentioned herein.

Publication Date: July 2024

# Document Version Control Log

| Document Version | Date | Author | Description |
|---|---|---|---|
| 0.1 | 5/6/2023 | Yinnon Sharon | Template for WF-600 |
| 0.2 | 10/09/2023 | Gabriel Dekel | WF-600 updated documents |
| 0.3 | 19/09/2023 | Gabriel Dekel | Update the TOE schema and yellow marking |
| 0.4 | 27/03/2024 | Gabriel Dekel | Update the ST to the last updates of WF-600 |
| 0.5 | 15/04/2024 | Gabriel Dekel | Updates comments |
| 0.6 | 29/05/2024 | Gabriel Dekel | Updates product part numbers and product versions. |
| 1.0 | 30/05/2024 | Gabriel Dekel | Final draft |
| 1.1 | 06/06/2024 | Gabriel Dekel | Update the evaluated hardware configurations. |
| 1.2 | 29/07/2024 | Gabriel Dekel | Fixing the document according to "Action Item List V1.0 and fixed on V1.1" |
| 1.3 | 11/08/2024 | Gabriel Dekel | Fixing the document according to "Action_item_List_ALC_WF-600_v1.1.docx" |
| 1.4 | 17/09/2024 | Gabriel Dekel | Fixing the document according to "Action_item_List_ASE_AGD_ADV_WF-600_v2.0.docx" |
| 1.5 | 25/09/2024 | Gabriel Dekel | Fixing the document according to "Action_item_List_ASE_AGD_ADV_WF-600_v3.0.docx" |

# Table of Contents

## List of Tables

## List of Figures

# 1 ST Introduction

## 1.1 ST Reference

| | |
|---|---|
| Title: | WF-600 Waterfall-Security Unidirectional Security Gateway Security Target |
| ST Version: | 1.5 |
| ST Date: | 25 Sep 2024 |
| Author: | Gabriel Dekel |
| CC Version: | Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017 |

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: WF-600 Waterfall-Security Unidirectional Security Gateway

The TOE, WF-600-TC, component, is separated into two parts, one is the TX Traffic Controller, and the other part is the RX Traffic Controller. The only connection between the TX Traffic Controller and the RX Traffic Controller is the fiber optic that transmits data only from the TX Traffic Controller to the RX Traffic Controller, there is no option to transmit data from the RX Traffic Controller to the TX Traffic Controller.

The TOE, WF-600-TC component identifier is made by a unique part number and unique revision, the TOE, WF-600-TC is built as a parent product and a child product, the parent product includes two children, the TX Traffic Controller and the RX Traffic Controller. Every change in each child part, TX Traffic Controller, or the RX Traffic Controller, will cause a change in the TOE WF-600-TC, parents part number or TOE, WF-600-TC revision.

The TOE parent part number is WF-600-TC, and its revision is F, the part number and revision identification in the WF-600 product are written on the product sticker, see Figure 2: TOE Part Number and Revision.

The TOE component product tree is described in Figure 1: TOE product tree structure.

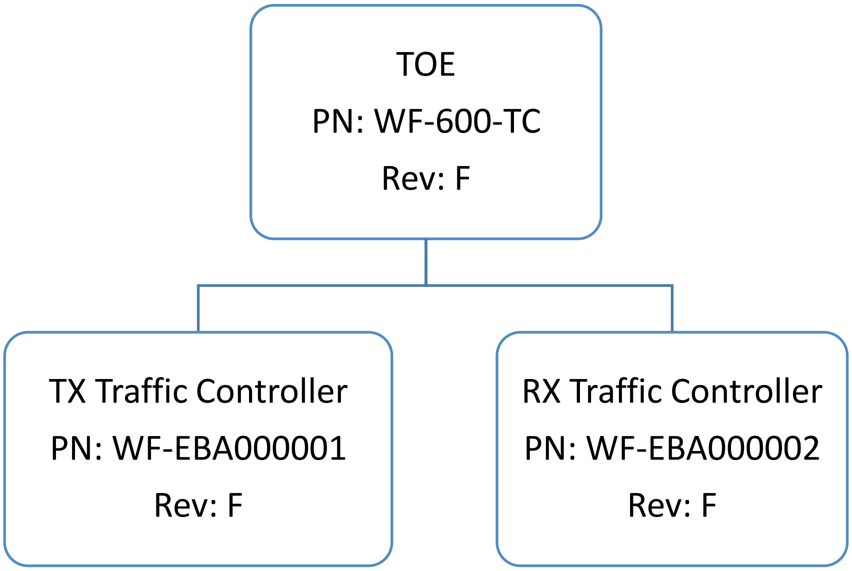


Figure 1: TOE product tree structure

### 1.2.1 TOE components:

- **TOE – (Parent component)**
  - **PN:** WF-600-TC
  - **Revision:** F
  - **Description:** WF600 Traffic Controller.

- **TX Traffic Controller: (Child Component)**
  - **PN**: WF-EBA000001
  - **Revision**: F
  - **Description**: WF600 Tx Board Assembly
- **RX Traffic Controller: (Child Component)**
  - **PN**: WF-EBA000002
  - **Revision**: F
  - **Description**: WF600 Rx Board Assembly

The TOE, WF-600-TC, the TX Traffic Controller, and RX Traffic Controller are implemented in several Waterfall-Security systems configurations. The TOE, WF-600-TC implemented in the Waterfall-Security system configuration is the same TOE, WF-600-TC component, without any change, and the identifier is as described above.

Any change in the TOE component will impact the Waterfall-Security systems configuration revision. A change in the Waterfall-Security systems configuration doesn't impact or influence the TOE, WF-600-TC component.

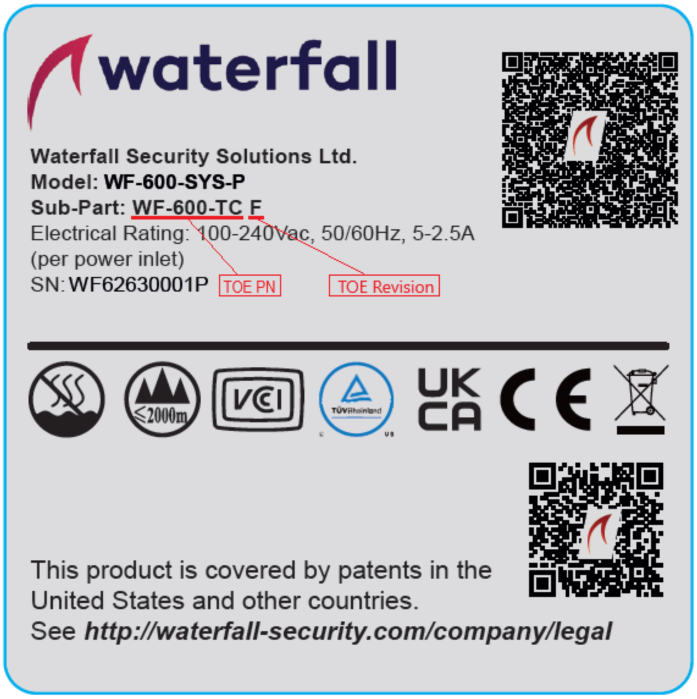
The TOE, WF-600-TC component is implemented in the following Waterfall-Security systems configuration and revision. The TOE component, part number, and revision are implemented in the following Waterfall-Security systems configuration.

1. **Waterfall-Security system configuration #1:** WF-600-SYS-P, Revision: G
2. **Waterfall-Security system configuration #2:** WF-600-SYS-P-Split, Revision: C.
3. **Waterfall-Security system configuration #3:** WF-600-SYS-L, Revision: C
4. **Waterfall-Security system configuration #4:** WF-600-SYS-L-Split, Revision: B.

### 1.2.2 TOE Identification.

The WF-600 product is identified by a unique part number (PN) displayed on a label that sticks on the system top cover, which the customer uses to verify the product PN, against the label. Similarly, the TOE, WF-600-TC, identification follows the same procedure, each product has its TOE, WF-600-TC parent PN, and revision marked on the WF-600 system, and the customer verifies the TOE, WF-600-TC part number and revision that is declared in the HW user manual against the label on the product.

The TOE part number, WF-600-TC, Rev F, includes the TX Traffic Controller and the RX Traffic Controller. The TOE identification detailed in Figure 2: TOE Part Number and Revision.



waterfall

**Waterfall Security Solutions Ltd.**
**Model: WF-600-SYS-P**
**Sub-Part: WF-600-TC F**
Electrical Rating: 100-240Vac, 50/60Hz, 5-2.5A
(per power inlet)
SN: WF62630001P

This product is covered by patents in the
United States and other countries.
See ***http://waterfall-security.com/company/legal***

Figure 2: TOE Part Number and Revision

## 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 Host Agent reads network frames from the sending network and transmits them to the RX Traffic Controller 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 the section 1.2.

The unidirectional traffic flow is operational once the TX Traffic Controller is connected to the Tx Host Agent, the RX Traffic Controller is connected to the Rx Host Agent, and the two Modules are connected by a single unidirectional fiber-optic cable, Both Traffic Controllers are powered up individually and independently.

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.

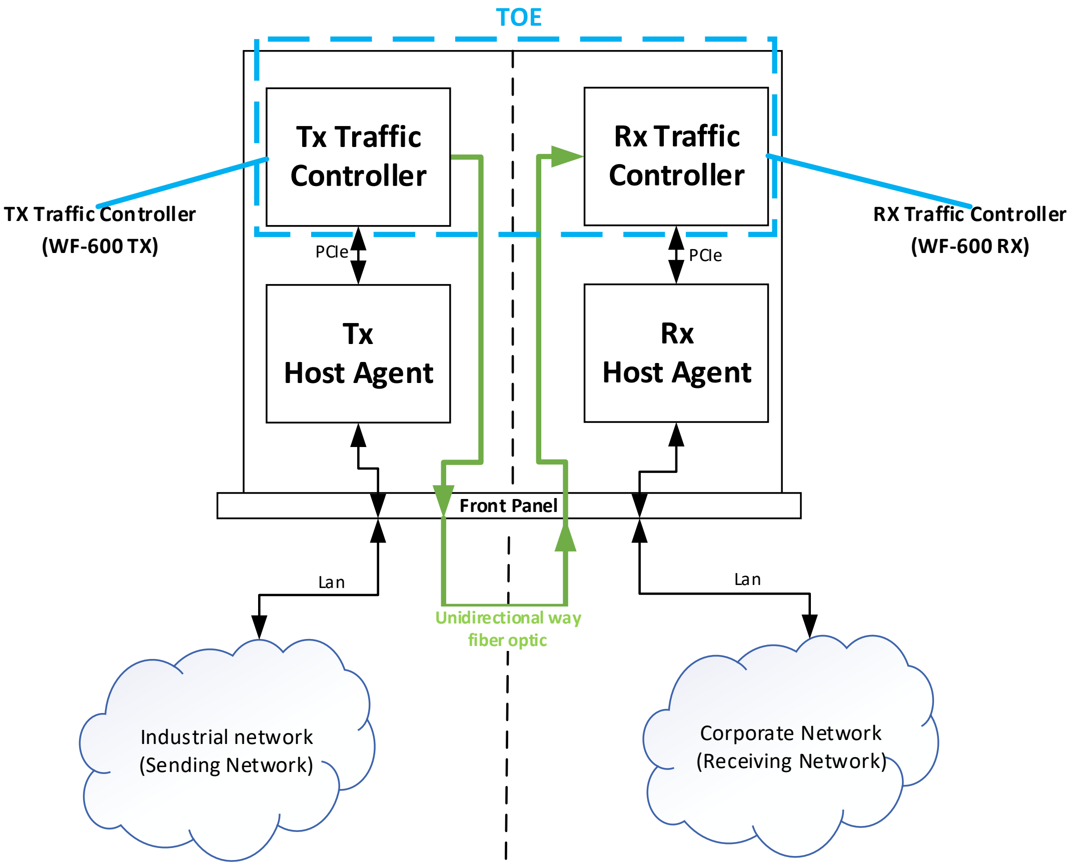

TOE
Tx Traffic Controller
Rx Traffic Controller
TX Traffic Controller (WF-600 TX)
RX Traffic Controller (WF-600 RX)
PCIe
PCIe
Tx Host Agent
Rx Host Agent
Front Panel
Lan
Lan
Unidirectional way fiber optic
Industrial network (Sending Network)
Corporate Network (Receiving Network)

Figure 1-3 :Typical usage scenario.

The TOE allows information to flow from the industrial network to the corporate network while preventing any information flowing through the receiving network 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 control capability, 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.

The Waterfall Unidirectional Security gateway is used as the security-enforcing core for a set of Waterfall-Security products that include, in addition to the gateway, TX, and RX Host Agent software running on the Host Agent in the sending and receiving networks, respectively. The Host Agents provide product management and monitoring capabilities and support for standard network protocols, including FTP (file transfer), SMTP (email), SNMP traps, Syslog, PI, Modbus, WMQ, ICCP, OPC-DA, and others, The Host Agent is not included in the TOE.

[1] For example, an attacker in the corporate network cannot make any connection or make a TCP handshake with the industrial network because of the Unidirectional information can flow from the TX Traffic Controller to the RX Traffic Controller only.

### 1.3.1 Non-TOE components required by the TOE

The TOE has a peripheral component, but they aren’t included in the TOE and don’t have any influence on the unidirectional information flow or any security issues.

The following Table 1-1: Non-TOE components required table contains the peripheral components not included in the TOE.

Table 1-1: Non-TOE components required table

| Non-TOE components required | | | | | |
|---|---|---|---|---|---|
| **WF-600 system Sub-part** | **Main Component** | **Description** | **RX quantity** | **TX quantity** | **Relation between TX and RX** |
| **HW** | Host Agent | PC Motherboard | 1 | 1 | Non |
| | LCD | Display a WF-600 system status | 1 | 1 | Non |
| | Power Supply redundant | Powered the system power | 1 | 1 | Non |
| | Fans | Fans | 2 | 2 | Non |
| **Mechanical** | Chassis | WF-600 CHASSIS ASSY | 1 | 1 | Separation metal wall between TX and RX side |
| | | WF-600 MAIN COVER ASSY | 1 | 1 | Same cover |
| **SW** | Host Agent SW | Waterfall-Security proprietary SW | 1 | 1 | Different SW for the TX and the RX Host Agent |
| **FW** | Aria 10 | Main Traffic Controller Waterfall-security application | 1 | 1 | There is no relation between TX and RX in this FW |
| | Max 10 | Power sequencer for the traffic controller | 1 | 1 | There is no relation between TX and RX in this FW. |

## 1.4 TOE Description

### 1.4.1 Physical Scope and Boundaries of the TOE

**TOE Hardware, Firmware, and Software**

The WF-600 Waterfall Unidirectional Security Gateway system (Figure 1-4: Front view of the WF-600 system.) is a hardware system with embedded computing capabilities that provide flexibility and scalability for unidirectional security gateway deployments.

The WF-600 system series architecture consists of 1U rack-mount Waterfall WF-600's each populated with Waterfall Traffic Controllers (TOE). The WF-600 system is completely enclosed by a metal chassis.

A physical metal divider separates the two sides of the TOE, the TX side from the RX side of each cabinet, to make it clear that no electrical & cabling connections exist between the TX side and RX sides of the cabinet. All connections between the TX and RX sides apply via the front panel.

WF-600 Waterfall-Security TOE consists of these components:

- TX Traffic Controller
- RX Traffic Controller
- TOE Guidance – see Table 1-2: TOE Guidance.

Each of the Traffic Controllers performs a specific function:

- The Waterfall TX Traffic Controller receives information from a Host Agent software and transmits information via a unidirectional fiber optic cable to the RX Traffic Controller.
- The Waterfall RX Traffic Controller receives information from the TX Traffic Controller via a single unidirectional fiber optic cable and sends the information to an RX Host Agent.
- The TX & RX Host Agents are normal Personal Computer (PC), and are not included in the TOE. The TX Host Agent transmits information from the TX network to the TX Traffic Controller, and the TX Traffic Controller sends the data to the RX Traffic Controller. The RX Traffic Controller received information from the TX Traffic Controller. The received information is sent to the RX Host Agent, and the RX Host Agent sends the information to the corporate network. The Host Agent's function is to organize, encode, and filter information per customer specifications. All Waterfall-Security software configurations are performed on the Host Agent. The Host Agent, on the TX side and on the RX, side is not included in the TOE.
- The TX Traffic Controller uses an SFP that contains a laser diode that only transmits the light, that converts electronic signals to light. The RX Traffic Controller contains a photoelectric cell that can sense light and convert it to electronic signals. The TX and RX Traffic Controllers are connected via a single standard unidirectional fiber-optic cable, allowing light to be transmitted from the TX laser diode to the RX photoelectric cell.

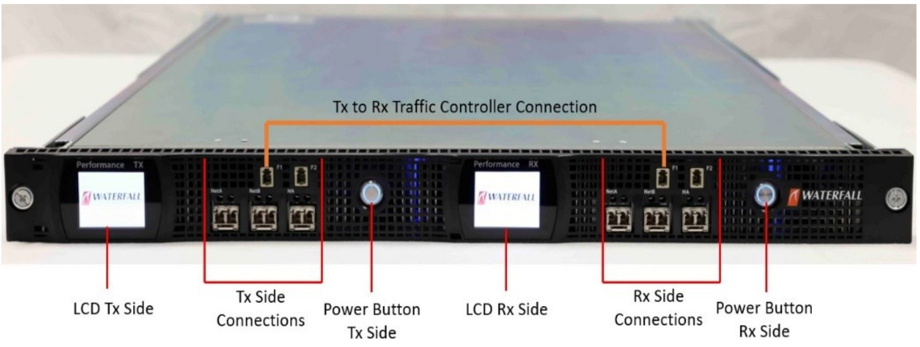


Figure 1-4: Front view of the WF-600 system.

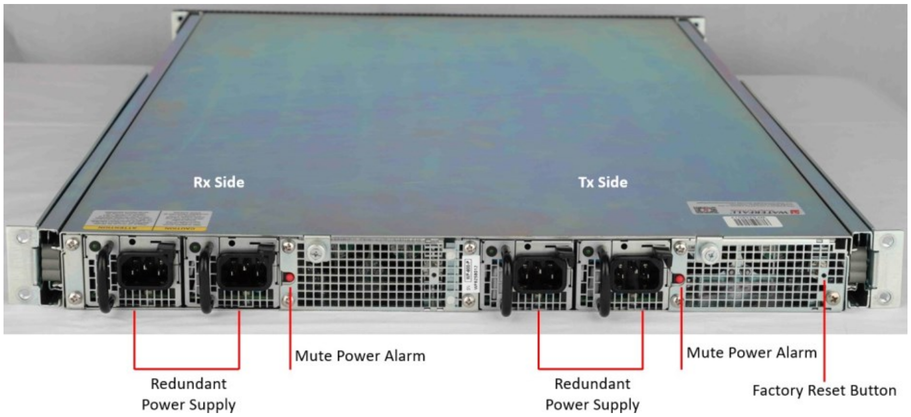


Figure 1-5: Rear view of the WF-600 system.

The TOE can operate in the following evaluated configurations. These differing hardware configurations don’t affect the functionality and security of WF-600.

1. WF-600 systems.

   The TX Traffic Controller and RX Traffic Controller are connected by a single unidirectional fiber optic cable, and two TX & RX Host Agent with the Waterfall software, one connected to the Waterfall-Security TX Traffic Controller, and the other one connected to the Waterfall RX Traffic Controller.

   The WF-600 has two main system versions, WF-600-SYS-P, and WF-600-SYS-L. The difference between them is the Host Agent CPU, the WF-600-SYS-P Host Agent has a different CPU than the WF-600-SYS-L Host Agent CPU. The Host Agent isn’t included in the TOE, and it’s irrelevant to this TOE. The TOE that are assembled in those systems are identical.

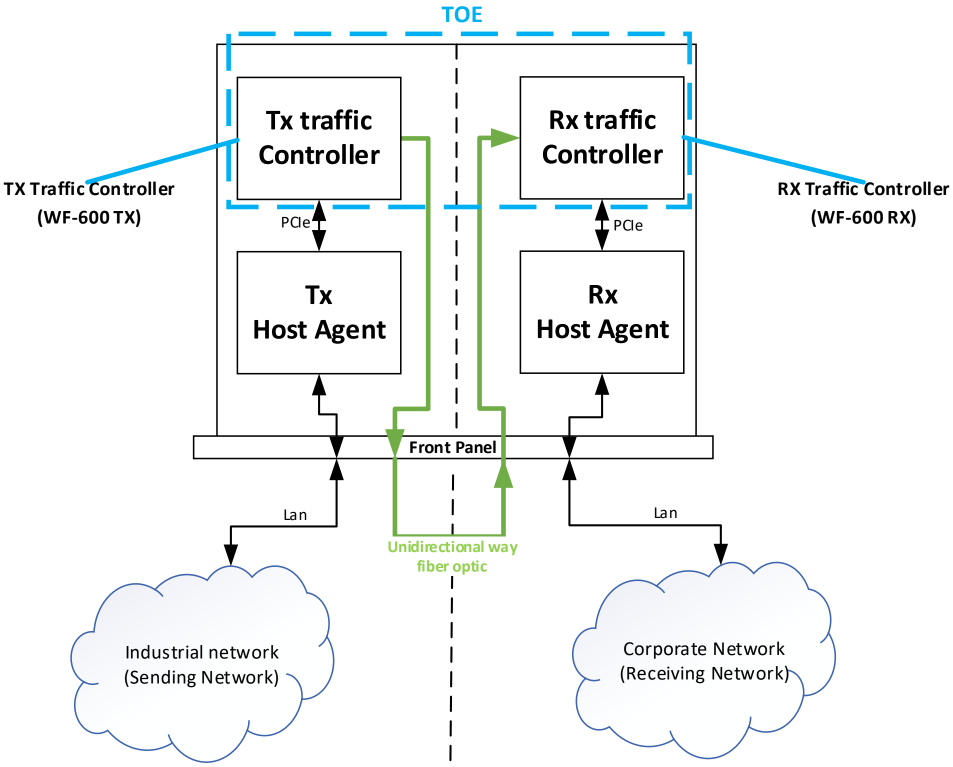

TOE
Tx traffic Controller
Rx traffic Controller
TX Traffic Controller (WF-600 TX)
RX Traffic Controller (WF-600 RX)
PCIe
PCIe
Tx Host Agent
Rx Host Agent
Front Panel
Lan
Lan
Unidirectional way fiber optic
Industrial network (Sending Network)
Corporate Network (Receiving Network)

Figure 1-6: WF-600-SYS-P/WF-600-SYS-L

2. WF-600 - Split

Waterfall TX and RX Traffic Controllers are split across two different cabinets, in one cabinet the TX system is assembled, and the RX side is omitted, and in the second cabinet the RX system is assembled the TX side is omitted, and the connections between the systems made by a unidirectional single fiber optic cable.

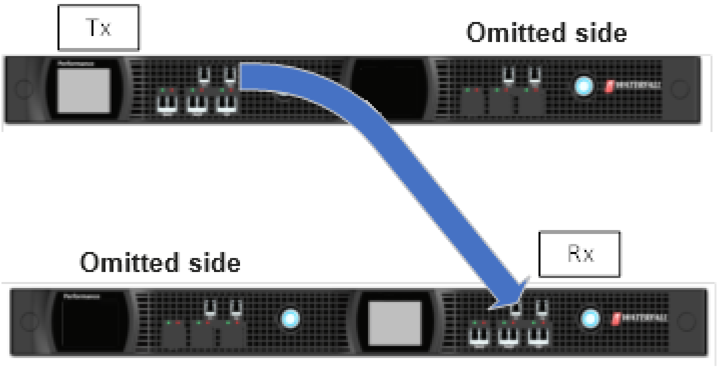


Figure 1-7: WF-600 Performance Split configuration.

**TOE Guidance**

The following Waterfall guidance is considered part of the TOE:

Table 1-2: TOE Guidance

| Title | Date |
|---|---|
| WF-600 Hardware User Guide 1.5., WF-600 Hardware User Guide 1.5.pdf | August 2024 |

Waterfall customers get the user guides as well as the software either by Secure FTP or digital Media secured shipment.

### 1.4.2 Delivery Method Overview

1. Shipping Equipment: When Waterfall-Security ships equipment to its customers, Waterfall-Security will provide a “shipment document” that acts as the attached commercial invoice for the equipment. This document will contain the following essential information:

    - Customer address.
    - Contact person’s information.
    - Purchase Order number.
    - Equipment part number, description, and serial number.
    - Shipment incoterms and HS code.
    - Weight and dimensions of the shipment.

**HS code** is short for Harmonized Commodity Description and Coding System. It's a list of numbers used by customs to classify a product.

**Incoterms**, or International Commercial Terms, are a standardized set of terms and definitions used in global trade. They clarify the responsibilities of buyers and sellers regarding the shipping and delivery of goods internationally, ensuring transparency in each party's obligations.

The shipment document will be forwarded by the Waterfall-Security contact person by mail to the customer contact person for review and approval before the creation of the Air Waybill (AWB).

2. Creation of the Air Waybill (AWB): Upon receiving approval for the shipment document, Waterfall-Security will generate the AWB using the provided

details. Waterfall-Security will be utilizing a delivery company as the carrier. The Commercial Invoice number will be referenced on the AWB.

3. Responsibility and Tracking: Waterfall will retain responsibility for the shipment until it arrives at the customer site location. Customers can track their equipment using the AWB number provided.
4. Receiving Equipment: Upon receipt of the equipment, Waterfall-Security advises customers to verify that the part number and serial number on the shipment document correspond with the labels affixed to the equipment to ensure accuracy and authentication for the sent equipment.

### 1.4.3 Logical Scope of the TOE

**Summary of TOE Security Functionality**

The TOE enables online transmission of information (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.

**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 information transfer from a critical industrial network to the corporate network.

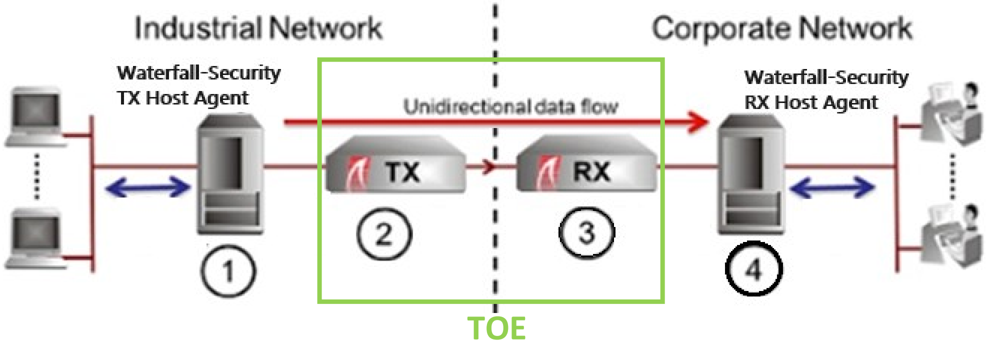


Figure 1-8: Information Flow through the TOE

The following sequence describes the information flow through the TOE.

1. The Waterfall TX Host Agent Module on the TX side receives a protocol-specific information stream from the industrial network servers or stations.

   The Waterfall TX Host Agent Module handles the translation of the information into Waterfall's proprietary protocol and sends the information to the Waterfall TX Traffic Controller.

2. The Waterfall TX Traffic Controller reads the information and transmits the information to the Waterfall RX Traffic Controller over a unidirectional single fiber-optic cable (the cable is outside the TOE but maintained within a physically secure environment).

3. The Waterfall RX Traffic Controller receives the information and sends it to the Waterfall RX Host Agent Module on the RX server. The Waterfall RX Host Agent Module handles the retrieval of the information from the Waterfall RX Traffic Controller and the translation of the information from Waterfall's proprietary protocol.

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

## 1.5 Document Organization

- Chapter 1

  Provides the introductory material for the security target, including ST and TOE references, TOE Overview, and TOE Description.

- Chapter 2

  Identifies the Common Criteria conformance claims in this security target.

- Chapter 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.

- Chapter 4

  Defines the security objectives for both the TOE and the TOE environment.

- Chapter 5

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

- Chapter 6

  Explains how the TOE meets the security requirements defined in Chapter 5, and how it protects itself against bypass, interference, and logical tampering.

- Chapter 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 5, April 2017, CCMB-2017-04-001, conformant (CC Part 2 Conformant)
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-001, 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 unidirectional fiber-optic cable connecting its separate parts will be located within controlled access facilities, which will prevents 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, 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 a compromise of the integrity of hosts or processes on the receiving network.

**Note:**

The Waterfall TX and RX Host Agent 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. The Non-

Operational Environment (OE) that is not related directly to the TOE is described below.

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

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

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

**Application Note:**

It is recommended to use a separate power grid for each power supply, 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 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 | | | ✓ | | | |
| OE.PHYSICAL | | | | ✓ | | |
| OE.ADMIN | | | | | ✓ | |
| OE.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 Agents or processes on the receiving network.

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

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

OE.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.*

OE.ADMIN directly upholds A.ADMIN. Together with OE.PHYSICAL, this ensures that the TOE will not be subject to physical tampering, such as short-circuiting the TX and RX Traffic Controllers 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.*

OE.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. All assignments are marked in boldface.

### 5.1.1 User data protection (FDP)

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.

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 authorize an information flow based on the following rules: **no rules that explicitly authorize 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 Host Agent 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 Host Agent Module (in the IT environment) can automatically identify and report any information loss. The TX Host Agent 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 |
| Security Target evaluation | ASE_CCL.1 | Conformance claims |
| | ASE_ECD.1 | Extended components definition |
| | ASE_INT.1 | ST introduction |
| | ASE_OBJ.2 | Security objectives |

| Assurance Class | Assurance Components | |
|---|---|---|
| | 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 chapter 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 Host Agent reads the information from the sending network; the TX Host Agent transmits the information to the TX Traffic Controller The TX Traffic Controller sends the information to the RX Traffic Controller; the RX Traffic Controller receives the information from the TX Traffic Controller and sent it to the RX Host Agent 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 Traffic Controller (which is connected to the receiving network) to the TX Traffic Controller (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,<br>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,<br>ADV_TDS.1 | **ADV_FSP.4,**<br>**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,<br>ALC_TAT.1 | ADV_TDS.3,<br>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,<br>ALC_DVS.1,<br>ALC_LCD.1 | **ALC_CMS.4,**<br>**ALC_DVS.2**,<br>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,<br>ASE_ECD.1,<br>ASE_REQ.1 | ASE_INT.1,<br>ASE_ECD.1,<br>**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,<br>ASE_ECD.1 | ASE_OBJ.2,<br>ASE_ECD.1 | |
| ASE_SPD.1 | None | | |
| ASE_TSS.1 | ASE_INT.1, | ASE_INT.1, | Consistent with EAL4 |

| SFR/SAR | CC dependency | ST component | Justification (where needed) |
|---|---|---|---|
| | ASE_REQ.1,<br>ADV_FSP.1 | **ASE_REQ.2**,<br>**ADV_FSP.4** | |
| ATE_COV.2 | ADV_FSP.2,<br>ATE_FUN.1 | **ADV_FSP.4,**<br>ATE_FUN.1 | Consistent with EAL4 |
| ATE_DPT.1 | ADV_ARC.1,<br>ADV_TDS.2,<br>ATE_FUN.1 | ADV_ARC.1,<br>**ADV_TDS.3**,<br>ATE_FUN.1 | Consistent with EAL4 |
| ATE_FUN.1 | ATE_COV.1 | **ATE_COV.2** | Consistent with EAL4 |
| ATE_IND.2 | ADV_FSP.2,<br>AGD_OPE.1,<br>AGD_PRE.1,<br>ATE_COV.1,<br>ATE_FUN.1 | **ADV_FSP.4**,<br>AGD_OPE.1,<br>AGD_PRE.1,<br>**ATE_COV.2**,<br>ATE_FUN.1 | Consistent with EAL4 |
| AVA_VAN.5 | ADV_ARC.1,<br>ADV_FSP.4,<br>ADV_TDS.3,<br>ADV_IMP.1,<br>AGD_OPE.1,<br>AGD_PRE.1,<br>ATE_DPT.1 | ADV_ARC.1,<br>ADV_FSP.4**,**<br>ADV_TDS.3,<br>ADV_IMP.1,<br>AGD_OPE.1,<br>AGD_PRE.1,<br>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 chapter 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 1.4.3 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 Traffic Controllers 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.<br>In accordance with TOE guidance, the TX Traffic Controller is connected only to the TX Host Agent which connects only to the sending network and is not connected to the receiving network in any way. Conversely, the RX Traffic Controller is connected only to the RX Host Agent which connects only to the receiving network.<br>A single unidirectional fiber-optic cable connects between the TX Traffic Controller and RX Traffic Controllers. This ensures that all the information flows through the TOE must flow through the unidirectional fiber-optic cable and is thereby covered by the Unidirectional SFP. |
| FDP_IFF.1 | The TX Traffic Controller is connected using standard PCIe communication with the TX Host Agent. The TX Host Agent cannot read information from the receiving network because its network interfaces are connected only to the sending |

| Component | Description of mechanism |
|---|---|
| | network at the RX side.<br>The TX Traffic Controller is a proprietary TX board, which converts the incoming information into a fiber-optic-based data transmission using a unidirectional single fiber-optic transmitter. The TX Traffic Controller and TX transmitter (SFP) support only data transmission, implementing galvanic isolation between the onboard circuitry and the receiving end of the transmitter, which is customized by Waterfall-Security so that it does not include a photoelectric cell for optical data reception.<br>A single unidirectional fiber-optic cable connects the TX Traffic Controller to the RX Traffic Controller and constitutes the only connection between these two components. This unidirectional fiber-optic cable connects to the RX Traffic Controller's fiber port. A proprietary RX Traffic Controller SFP converts the incoming optical data into electronic signals using a fiber-optic receiver. The RX Traffic Controller SFP and RX Traffic Controller SFP receiver support only data reception, implementing galvanic isolation between the on-board circuitry and the transmitting end of the transmitter, which is customized by Waterfall-Security so that it does not include an LED for optical data transmission.<br>The RX Traffic Controller is connected using unidirectional fiber optic cable communication with the receiving network. The RX Traffic Controller transmits the data received from the TX Traffic Controller to the receiving network. The RX Traffic Controller 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 5, April 2017, CCMB-2017-04-001, 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 |