Certification Report

Basic Network Pump with Data Diodes (BANPUMP)

Author: Eugenia Ana CAPOTA

Table of Contents

[1 Certification Statement 3](#_Toc167633746)

[2 Executive Summary 3](#_Toc167633747)

[2.1 Introduction 3](#_Toc167633748)

[2.2 Evaluated product 3](#_Toc167633749)

[2.3 TOE scope 3](#_Toc167633750)

[2.4 Protection Profile Conformance 4](#_Toc167633751)

[2.5 Assurance Level 4](#_Toc167633752)

[2.6 Security Policy 4](#_Toc167633753)

[2.7 Security Claims 4](#_Toc167633754)

[2.8 Threats Countered 4](#_Toc167633755)

[2.9 Threat Countered by the TOE’s environment 4](#_Toc167633756)

[2.10 Threats and Attacks not Countered 4](#_Toc167633757)

[2.11 Environmental Assumptions and Dependencies 4](#_Toc167633758)

[2.12 Security Objectives for the TOE 5](#_Toc167633759)

[2.13 Security Objectives for the TOE’s Environment 5](#_Toc167633760)

[2.14 Evaluation Objectives 5](#_Toc167633761)

[2.15 General Points 5](#_Toc167633762)

[3 Evaluation Findings 5](#_Toc167633763)

[3.1 Introduction 6](#_Toc167633764)

[3.2 Misuse 6](#_Toc167633765)

[3.3 Vulnerability Analysis 6](#_Toc167633766)

[3.4 Evaluator’s Tests 7](#_Toc167633767)

[4 Evaluation Outcome 7](#_Toc167633768)

[4.1 Certification Result 7](#_Toc167633769)

[4.2 Recommendations 7](#_Toc167633770)

[5 References 7](#_Toc167633771)

[Annex A: Evaluated Configuration 8](#_Toc167633772)

[TOE Documentation 10](#_Toc167633773)

# Certification Statement

The Basic Network Pump with Data Diodes (BANPUMP) is a new network pump architecture which guarantees the Bell-LaPadula confidentiality properties and, implicitly, the BIBA integrity rules, between the connected networks, even when software components of the pump are under total adversary control.

The Basic Network Pump with Data Diodes (BANPUMP) may be evaluated to check if it meets the security assurance requirements of the Evaluation Assurance Level 7 (EAL 7 – Formally verified design and tested), augmented with the classes ASE\_TSS.2 – TOE summary specification with architectural design summary and ALC\_FLR.3 – Systematic flaw remediation.

# Executive Summary

## Introduction

This Certification Report proposes a model for evaluating the Basic Network Pump with Data Diodes (BANPUMP), and is intended to assist prospective users when judging the IT security of the product.

Prospective users are advised to read this report and the Security Target [1], which specifies the assurance evaluation requirements.

## Evaluated product

The product to be evaluated is the Basic Network Pump with Data Diodes (BANPUMP), which is also described in this report as the Target of Evaluation (TOE). The purpose of the TOE is to transfer data from the Low security network (Network Level A) to the High security network (Network Level B), while guaranteeing the Bell-LaPadula Confidentiality and, implicitly, the BIBA Integrity properties between the connected networks, even when software components of the pump are under total adversary control.

According to the Bell-LaPadula Confidentiality Model (BLP) [4]:

* The Simple Security property: A subject in the Low network may not read an object from the High network (no read-up).
* The Star security property: A subject in the High network may not write to object in the Low network (no write-down).
* The Strong Star property: A subject in the Low network may not write to object in the High network (no write-up).

According to the BIBA Integrity Model [5]:

* The Simple Integrity property: A subject in the High network may not read an object from the Low network (no read-down).
* The Star Integrity property: A subject in the Low network may not write to object in the High network (no write-up).

Annex A contains details of the proposed configuration to be evaluated and any additional TOE documentation.

## TOE scope

The scope of the TOE is described in the Security Target [1], chapter 1.4.

## Protection Profile Conformance

The Security Target [1] did not claim conformance to any protection profile.

## Assurance Level

The Security Target [1] specifies the assurance requirements for the proposed evaluation. The assurance incorporates predefined evaluation assurance level EAL7 (EAL 7 – Formally verified design and tested), augmented with the classes ASE\_TSS.2 – TOE summary specification with architectural design summary and ALC\_FLR.3 – Systematic flaw remediation. The assurance given by levels EAL1 to EAL2 is described in Part 3 of the Common Criteria Part 3 [2]. An overview of Common Criteria is given in Part 1 of the Common Criteria [3].

## Security Policy

There are no Security Policies or rules with which the TOE must comply.

## Security Claims

The TOE threats, assumptions, security objectives, security requirements and security assurance requirements are fully specified in the Security Target [1].

## Threats Countered

An unauthorized party that deliberately attempts to reverse the information flow between network levels by using:

1. Temperature measurements.
2. Time measurements.
3. Consumption measurements.
4. Acoustics (e.g. using a hard disk as a microphone).

An unauthorized party that deliberately attempts to overwrite files from Network Level A (Low) to Network Level B (High).

## Threat Countered by the TOE’s environment

An unauthorized party that deliberately attempts to access the equipment within a Single Board Computer.

## Threats and Attacks not Countered

This certification report does not describe any threats or attacks which are not countered.

## Environmental Assumptions and Dependencies

The following assumptions exist in the TOE environment:

* The intended operation environment must store and operate the TOE in accordance with the highest of each of the requirements below. The internal and external connections of the TOE are implemented correctly. No unauthorized party has direct physical access to the TOE or any of the TOE components.
* Two unauthorized parties cannot communicate in any other way (e.g. through light signals), unless they attempt to reverse the direction of communication inside the TOE.
* The TOE shall be powered such that an unauthorized party or process on the transmitter and/or receiver side cannot evaluate the power fluctuation and consumption. This prevents an unauthorized party from using the power input as a covert channel.
* The only method of interconnecting Network Level A (Low) and Network Level B (High) is by using the TOE, where all of the units are operating in the same data flow direction. This prevents an unauthorized party from circumventing the security provided by the TOE through an untrustworthy product or by reversing the data flow direction of the TOE.
* Files cannot be overwritten from Network Level A (Low) to Network Level B (High).

## Security Objectives for the TOE

* The information on Network Level A (Low) is kept confidential from Network Level B (High).
* The information flow of the TOE is kept accurate and consistent so that it cannot be reversed by an unauthorized party.

## Security Objectives for the TOE’s Environment

* The intended operational environment shall be capable of storing and operating the TOE. The TOE components are only accessible to authorized parties.
* The intended operational environment shall provide power to the TOE such that the TOE power cannot be evaluated or interfered with through Network Level A (Low) and/or Network Level B (High).
* All the TOE components shall operate in the same data flow direction, from Network Level A (Low) to Network Level B (High).
* The TOE network shall respect the BIBA Integrity Model.

## Evaluation Objectives

The purpose of this report is to propose an evaluation model that can provide assurance about the effectiveness of the TOE in meeting it’s Security Target [1].

## General Points

The proposed evaluation addresses the security functionality claimed in the Security Target [1], with reference to the assumed operating environment. The proposed configuration is specified in Annex A.

This Certification Report offers an evaluation model which can be verified by potential users of the TOE.

# Evaluation Findings

The security assurance requirements for the TOE are those of the Evaluation Assurance Level 7 (EAL 7 – Formally verified design and tested), augmented with the classes ASE\_TSS.2 – TOE summary specification with architectural design summary and ALC\_FLR.3 – Systematic flaw remediation. These components are explained in Part 3 of the Common Criteria [2].

|  |  |
| --- | --- |
| **Assurance Class** | **Assurance Component** |
| ADV: Development | ADV\_ARC.1 – Security architecture description |
| ADV\_FSP.6 – Complete semi-formal functional specification with additional formal specification |
| ADV\_IMP.2 – Complete mapping of the implementation representation of the TSF |
| ADV\_INT.3 – Minimally complex internals |
| ADV\_SPM.1 – Formal TOE security policy model |
| ADV\_TDS.6 – Complete semiformal modular design with formal high level design presentation |
| AGD: Guidance documents | AGD\_OPE.1 – Operational user guidance |
| AGD\_PRE.1 – Preparative procedures |
| 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.2 – Measurable life-cycle model |
| ALC\_TAT.3 – Compliance with implementation standards – all parts |
| 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.2 – TOE summary specification with architectural design summary |
| ATE: Tests | ATE\_COV.3 – Rigorous analysis of coverage |
| ATE\_DPT.4 – Testing: implementation representation |
| ATE\_FUN.2 – Ordered functional testing |
| ATE\_IND.3 – Independent testing - complete |
| AVA: Vulnerability assessment | AVA\_VAN.5 – Advanced methodical vulnerability analysis |

## Introduction

The requirements specified in the Security Target [1] are addressed in this evaluation. The following sections contain considerations relevant to either users or those involved in subsequent assurance maintenance and re-evaluation of the TOE.

## Misuse

A risk of intentional and unintentional misconfigurations that could compromise confidential information always exists. In order to ensure that the TOE operates in a secure manner, users should follow the adequate guidance documents [1].

The guidance documents outline how to operate the TOE, the assumptions about the intended environment and all the requirements for external security. There is sufficient guidance for the user to effectively administer and use the TOE.

## Vulnerability Analysis

The TOE, in its intended environment, should be resistant to attackers. This Certification Report addresses all the potential exploitable vulnerabilities of the TOE.

The TOE is resistant against known attacks at the time of this proposed evaluation, but this could change in the future, as attack methods become more sophisticated.

## Evaluator’s Tests

The expected results of the evaluation are the following:

* No unauthorized party has direct physical access to the TOE or any of the TOE components.
* The components of the TOE operate in the same data flow direction, from Network Level A (Low) to Network Level B (High).
* The TOE cannot be bypassed through other communication channels such as:
  + Temperature readings.
  + Time measurements.
  + Power fluctuation or consumption.
  + Acoustics (using a hard disk as a microphone).
  + Light signals.
* The information on Network Level A is kept confidential from Network Level B.
* Files cannot be overwritten from Network Level A (Low) to Network Level B (High).
* The TOE Network follows the BIBA Integrity Model.

# Evaluation Outcome

## Certification Result

According to the expected results, the Basic Network Pump with Data Diodes (BANPUMP) should meet the security assurance requirements of the Evaluation Assurance Level 7 (EAL 7 – Formally verified design and tested), augmented with the classes ASE\_TSS.2 – TOE summary specification with architectural design summary and ALC\_FLR.3 – Systematic flaw remediation. These security assurance requirements are explained in Part 3 of the Common Criteria [2].

## Recommendations

Prospective users of the Basic Network Pump with Data Diodes (BANPUMP) should understand the specific scope of the certification by reading this report and the Security Target [1]. The TOE should be used according to the environmental considerations specified in the Security Target [1].

# References

1. Security Target - BANPUMP. Internal document.
2. Common Criteria for Information Technology Security Evaluation. *Part 3: Security Assurance Components, Version 3.1, Revision 5,* April 2017. <http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf>
3. Common Criteria for Information Technology Security Evaluation. *Part 1: Introduction and General Model, Version 3.1, Revision 5,* April 2017. <http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf>
4. Bell, D. E., & La Padula, L. J. (1976). Secure computer system: Unified exposition and multics interpretation.
5. Biba, K. J. (1977). Integrity considerations for secure computer systems.

# Annex A: Evaluated Configuration

This certification report is a proposed model. Figure 1 shows the proposed evaluation configuration of the TOE when Network Level A (Low) needs to communicate (send files) to Network Level B (High):

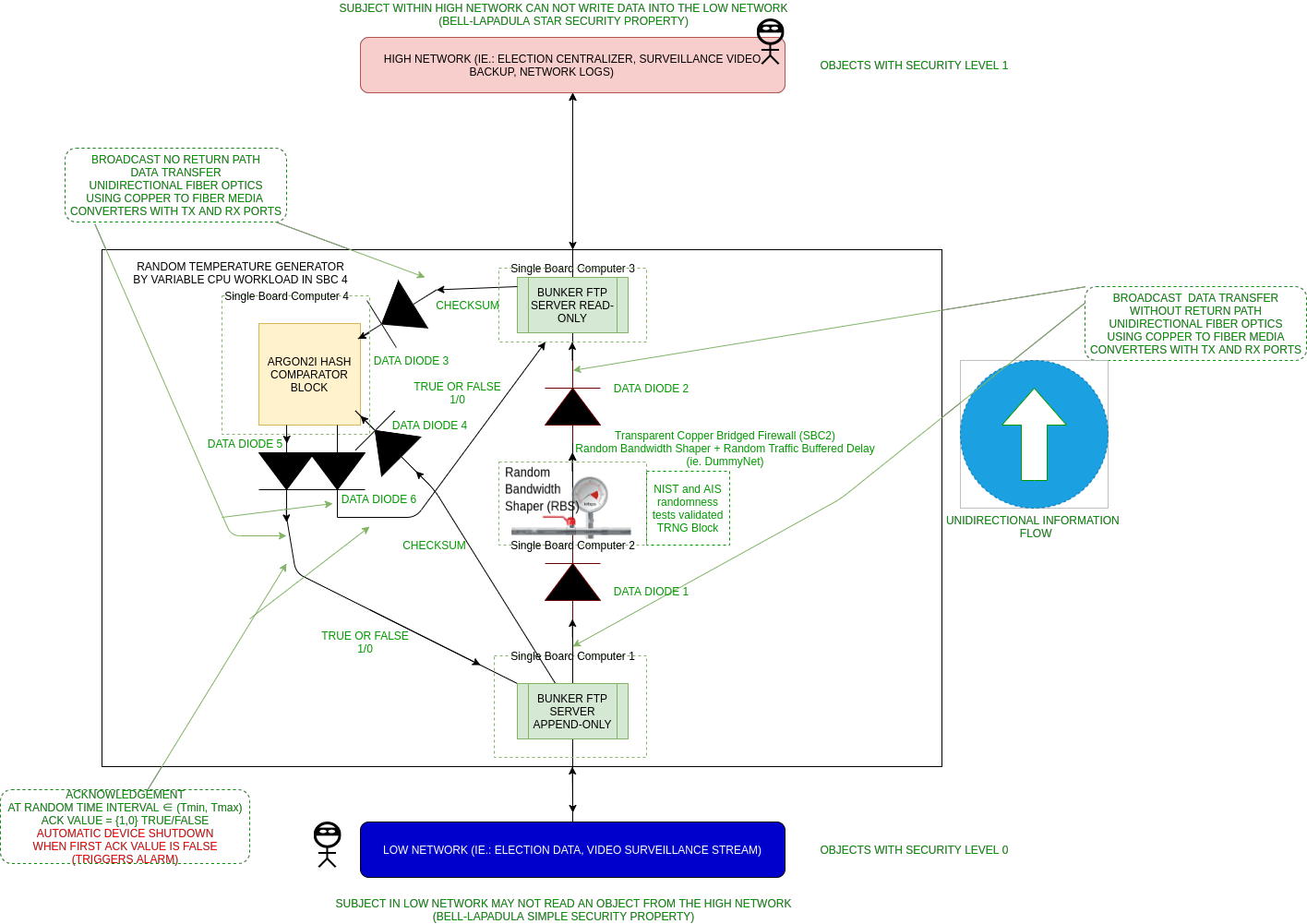


Figure 1. Proposed evaluation configuration of the TOE when Network Level A (Low) needs to communicate with Network Level B (High).

The reversed scenario of the proposed evaluation configuration is when Network Level B (High) needs to communicate with Network Level A (Low), in Figure 2:

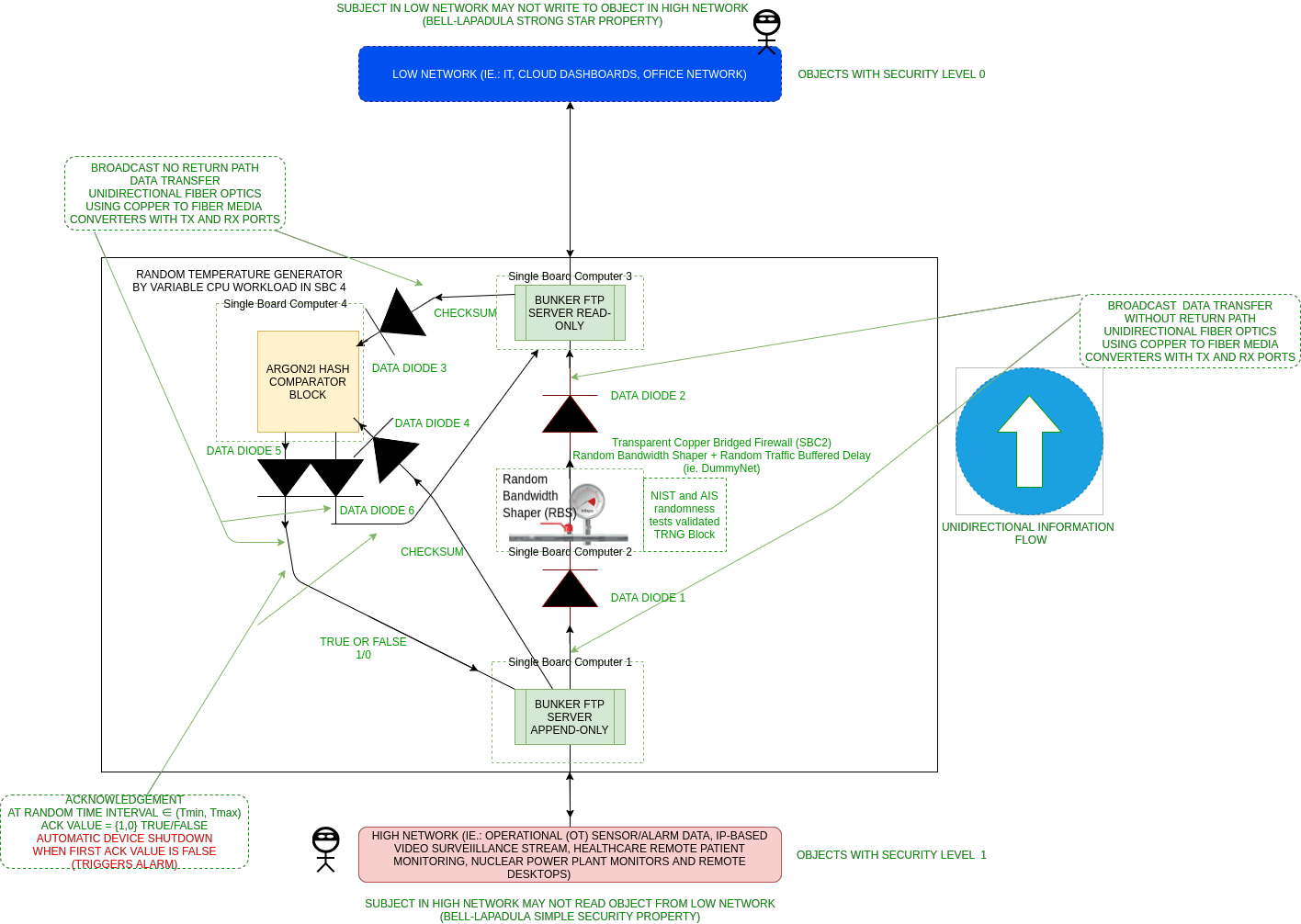


Figure 2. Proposed evaluation configuration of the TOE when Network Level B (High) needs to communicate with Network Level A (Low).

All the Single Board Computers (SBCs) are isolated from each other using 6 hardware commodity off-the-shelf data diodes. The data diodes are made from ordinary copper-to-fiber-optics mediaconverters, so a total of 18 mediaconverters are used.

The testing methods used to evaluate the TOE should focus on:

* Verifying that no unauthorized party can reverse the information flow of the TOE by:
  + Ensuring the TOE operates in a secure environment, so that unauthorized parties do not have access to the TOE.
  + Ensuring the information flow of the TOE is kept accurate and consistent so that it cannot be reversed by an unauthorized party through: temperature, time, and power consumption readings or acoustics.
* Verifying that no unauthorized party can overwrite files from Network Level A (Low) to Network Level B (High) by:
  + Ensuring the TOE operates in a secure environment, so that unauthorized parties do not have access to the TOE.
  + Ensuring the information on Network Level A (Low) is kept confidential from Network Level B (High), so unauthorized parties can not overwrite files from Network Level A (Low) to Network Level B (High).
  + Ensuring the TOE Network follows the BIBA Integrity Model. This prevents data modification by unauthorized parties, and it also prevents unauthorized data modification by authorized parties.

# TOE Documentation

The supporting document evaluated was the Security Target for the Basic Network Pump with Data Diodes (BANPUMP).