National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Sierra Nevada Corporation

Binary Armor SCADA Network Guard, with firmware version 2.1

Report Number:	**CCEVS-VR-VID11176-2021**
Dated:	**15 July 2021**
Version:	**1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

Acknowledgements

Validation Team

Paul Bicknell
Ted Farnsworth
Randy Heimann
Lisa Mitchell
Linda Morrison
The MITRE Corporation

Common Criteria Testing Laboratory

Leidos Inc.
Columbia, MD

Contents

1 Executive Summary 1
2 Identification 2
3 TOE Architecture 4
4 Security Policy 5
4.1 Security Audit 5
4.2 Cryptographic Support 5
4.3 Identification and Authentication 5
4.4 Security Management 5
4.5 Protection of the TSF 5
4.6 TOE Access 5
4.7 Trusted Path/Channels 6
5 Assumptions and Clarification of Scope 7
5.1 Assumptions 7
5.2 Clarification of Scope 7
6 Documentation 9
7 IT Product Testing 10
7.1 Test Configuration 10
8 TOE Evaluated Configuration 12
8.1 Evaluated Configuration 12
8.2 Excluded Functionality 12
9 Results of the Evaluation 13
9.1 Evaluation of the Security Target (ST) (ASE) 13
9.2 Evaluation of the Development (ADV) 13
9.3 Evaluation of the Guidance Documents (AGD) 13
9.4 Evaluation of the Life Cycle Support Activities (ALC) 13
9.5 Evaluation of the Test Documentation and the Test Activity (ATE) 14
9.6 Vulnerability Assessment Activity (AVA) 14
9.7 Summary of Evaluation Results 14
10 Validator Comments/Recommendations 15
11 Security Target 16
12 Abbreviations and Acronyms 17
13 Bibliography 18

List of Tables

Table 1: Evaluation Identifiers 2

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Binary Armor SCADA Network Guard, with firmware version 2.1 (the Target of Evaluation, or TOE) developed by Sierra Nevada Corporation. It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

This VR is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

The evaluation was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in July 2021. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report written by Leidos. The evaluation determined that the TOE is:

- Common Criteria Part 2 Extended and Common Criteria Part 3 Conformant

and demonstrates exact conformance to:

- *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 ([5])

as clarified by all applicable Technical Decisions.

The TOE is Binary Armor SCADA Network Guard, with firmware version 2.1 developed by Sierra Nevada Corporation.

The TOE identified in this VR has been evaluated at a NIAP approved CCTL using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5). The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced. Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct.

The Leidos evaluation team determined that the TOE is conformant to the claimed Protection Profile (PP) and, when installed, configured, and operated as specified in the evaluated guidance documentation, satisfies all the security functional requirements stated in the ST ([7]).

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria (CC) and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List (PCL).

Table 1 provides information needed to completely identify the product, including:

- The TOE—the fully qualified identifier of the product as evaluated
- The ST—the unique identification of the document describing the security features, claims, and assurances of the product
- The conformance result of the evaluation
- The PP/PP-Modules to which the product is conformant
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Binary Armor SCADA Network Guard, with firmware version 2.1, consisting of: • Binary Armor Hardware version 7000-SNC-01 • Binary Armor Firmware version 2.1
Security Target	Sierra Nevada Corporation Binary Armor SCADA Network Guard, with firmware version 2.1 Security Target Version 1.0, 2021-6-4
Sponsor & Developer	Sierra Nevada Corporation 11551 East Arapahoe Road Centennial, CO 80112
Completion Date	July 2021
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM Version	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
PP	collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2021
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 conformant

Item	Identifier
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Evaluation Personnel	Dawn Campbell Allen Sant Pascal Patin
Validation Personnel	Paul Bicknell Ted Farnsworth Randy Heimann Lisa Mitchell Linda Morrison

3 TOE Architecture

Note: The following architectural description is based on the description presented in the ST.

The TOE is Binary Armor SCADA Network Guard, with firmware version 2.1, consisting of Binary Armor Hardware version 7000-SNC-01 and Binary Armor Firmware version 2.1. The TOE is intended for in-line installation between Programmable Logic Controllers (PLCs), remote terminal units, intelligent electronic devices or controllers and the WAN/LAN, to provide bi-directional security across all communication layers. It provides two, separate, physical interfaces: a “high” network interface card (NIC), typically connected to SCADA/ICS equipment; and a “low” NIC, typically connected to external systems such as Human Machine Interface. The TOE supports remote administration over the network (from either the high or low networks) and local administration through a directly networked workstation. External servers are expected to be connected to the low network by default, but the TSF can be configured to interact with these servers on the high network as well if required.

The TOE is provided as a hardware network appliance. There are no virtual deployments of the TOE and the TOE is always a standalone device; its functionality is not distributed across multiple devices.

The TOE has a rugged enclosure that protects it from modification and contains a single embedded board containing an Intel Atom E3845 processor, memory, and flash storage. The TOE hardware contains a hardened operating system (RHEL 7) that does not permit operators (even an authorized administrator) access to the OS, with SNC-developed firmware running atop. The TOE provides a TLS-protected management interface that can be accessed via SNC’s Administration Tool application. This runs on a PC/workstation that is part of the operational environment of the TOE. This application is a graphical front-end for interacting with the TSF through a REST API; the REST API may also be invoked directly to interact with the TOE and its data. An administrator can configure the TOE for remote access on either its high or low network interface. The administrator always accesses the TOE through its TLS management interface, irrespective of whether the administrator configured the TOE to listen for management connections on its low or high network interface and irrespective of whether the administrator accesses the TOE remotely or locally. In this context, local access means connected via crossover cable or through a network switch to which only the TOE and the workstation are connected.

The TOE can be configured to forward its audit records to an external syslog server in the network environment. This is generally advisable given the audit log storage space on the evaluated appliance.

Additionally, the TOE can be configured to solicit time from an NTP server, and the administrator can manually set the TOE’s time.

The TOE is evaluated as a network device offering CAVP certified cryptographic functions, security auditing, secure administration, trusted updates, self-tests, and secure connections to other servers (e.g., to export audit records), protected using TLS.

4 Security Policy

The TOE enforces the following security policies as described in the ST.

Note: Much of the description of the security policy has been derived from the ST and the Final ETR.

4.1 Security Audit

The TOE generates security relevant audit records, stores them locally, and can be configured to forward them to a syslog server over TLS. The locally stored audit records are protected from unauthorized access.

4.2 Cryptographic Support

The TOE includes FIPS-approved cryptographic libraries with CAVP certificates for their cryptographic algorithms. The TOE uses its cryptographic libraries for HTTPS, TLS and certificate functionality. Cryptographic services include key management, random bit generation, symmetric encryption and decryption, digital signature, and secure hashing.

4.3 Identification and Authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, with the exception of reading the login banner, obtaining status, and requesting the TOE's public key certificate. It provides the ability to both assign credentials (user password, enrollment for PKCS#11 token) and to authenticate users against these credentials. The TOE also provides X.509 certificate checking for its TLS connections. The password-based authentication will cause a lockout in the event of an excessive number of consecutive authentication failures.

4.4 Security Management

The TOE provides a management interface that an administrator can access via a network port. To access the TOE locally, an administrator must directly network their workstation to the TOE using a crossover cable or through a network switch to which only the TOE and the workstation are connected. For remote access, the administrator uses the SNC Administration Tool application to access the TOE's REST API. This API can also be accessed directly over HTTPS. The management interface is protected with TLS and limited to the authorized administrator.

4.5 Protection of the TSF

The TOE implements features designed to protect itself to ensure the reliability and integrity of its security features, including protection of sensitive data and provision of timing mechanisms to ensure that reliable time information is available for the TOE's own use (e.g., for log accountability).

The TOE includes functions to perform self-tests so that it can detect when it is failing and transition to a secure, maintenance state. It also includes a mechanism to verify TOE updates to prevent malicious or other unexpected changes in the TOE.

4.6 TOE Access

The TOE displays a Security Administrator-specified advisory notice and consent warning message prior to establishing an administrative user session. The TOE terminates local and remote administrator interactive sessions after a Security Administrator-specified time period of inactivity. The TOE allows administrator-initiated termination of the administrator's own interactive session.

4.7 Trusted Path/Channels

The TOE provides trusted paths and channels for local and remote administration. The TOE can be configured to send audit records to external syslog server(s) using TLS in real-time.

5 Assumptions and Clarification of Scope

5.1 Assumptions

The ST references the PP to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed PP, are as follows:

- The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
- The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).
- A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
- The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.

  For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
- The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
- The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
- The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

5.2 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation shows only that the evaluated configuration meets the security claims made, with a certain level of assurance (the evaluation activities specified in *Supporting Document Mandatory Technical Document: Evaluation Activities for Network Device cPP*, Version 2.2, December 2019 ([6]) and performed by the evaluation team).
- This evaluation covers only the specific hardware, firmware distribution identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in Sierra Nevada Corporation Binary Armor SCADA Network Guard, with firmware version 2.1 Security Target Version 1.0, 2021-6-4 ([7]). Any additional security related functional capabilities included in the product were not covered by this evaluation. In particular, the functionality mentioned in Section 8.2 of this document is excluded from the scope of the evaluation.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The TOE must be installed, configured and managed as described in the documentation referenced in Section 6 of this VR.

6 Documentation

The vendor offers guidance documents describing the installation process for the TOE as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation and delivered with the TOE is as follows:

- *ADMINISTRATION GUIDE for COMMON CRITERIA for Binary Armor® SCADA Network Guard, with Firmware version 2.1, 0318-0200-0004 Document Number Rev A (Admin Guide)*
- *BINARY ARMOR® USER MANUAL 0318-0100-0015 Document Number Rev G (User Manual)*
- *Binary Armor SCADA Network Guard, with Firmware version 2.1, Binary Armor Alloy API, version 0.3 (API)*.

To use the product in the evaluated configuration, the product must be configured as specified in this documentation.

Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the TOE as evaluated. Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website.

7 IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following proprietary document:

- *Sierra Nevada Binary Armor SCADA Network Guard Common Criteria Test Report and Procedures For Network Device collaborative PP Version 2.2e, Version 1.0, June 11, 2021* ([13])

A non-proprietary description of the tests performed and their results is provided in the following document:

- *Assurance Activities Report for Sierra Nevada Corporation Binary Armor SCADA Network Guard, with firmware version 2.1, Version 1.0, 11 June 2021* ([12])

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 ([5]).

The evaluation team devised a Test Plan based on the Test Activities specified in *Supporting Document Mandatory Technical Document: Evaluation Activities for Network Device cPP*, Version 2.2, December 2019 ([6]). The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at Leidos CCTL facilities in Columbia, Maryland, from July 15, 2020 to February 12, 2021, with additional evidence collected on June 6, 2021.

The evaluators received the TOE in the form that customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for *collaborative Protection Profile for Network Devices* were fulfilled.

7.1 Test Configuration

The evaluation team established a test configuration comprising one instance of the TOE as follows:

- Binary Armor Hardware version 7000-SNC-01
- Binary Armor firmware version 2.1

The test configuration included the following devices in the operational environment of the TOE:

- Three NTP servers
- TLS Test Server for TLS client and Server testing (packet capture server). It included the following software:
  - Ubuntu 18.04
  - Wireshark 2.6.10
  - Python
  - Leidos Proprietary TLS tools
- Generic syslog server for logging

  - IP: 172.16.0.30
  - Ubuntu 18.04
  - Rsyslogd 8.32.0
- Win10 Client with administration tool installed
- Red Hat Enterprise Linux 7.9 Client with administration tool installed
- Kali Linux Test machine - Purpose: Network test tools for AVA_VAN Type 4 with the following software
- OS: Kali Linux 2019.

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The TOE is Binary Armor SCADA Network Guard, with firmware version 2.1, consisting of Binary Armor Hardware version 7000-SNC-01 and Binary Armor Firmware version 2.1. The TOE is evaluated as a single standalone network device and there are no virtual instances.

The TOE in its evaluated configuration requires the following components in its operational environment:

- A Microsoft Windows 10 or Redhat Linux version 7.7+ workstation—with the Binary Armor software suite of tools installed.
- A security token in the form of a PKCS#11-compliant smart card or USB device present on the administrative workstation. The security token is used by the TOE for administrator authentication. The token is configured by loading public key(s) onto the TOE.[1]
- A TLS-protected syslog server that receives audit events from the TOE
- An NTP server with which the TOE can synchronize its clock.

8.2 Excluded Functionality

The following features and capabilities of the Binary Armor product are not covered by the evaluation:

- SCADA interfaces
- RS-232 serial interface used to access SCADA devices
- ‘override’ mode used to define SCADA rulesets
- management of what are referred to as ‘configuration files’
- Enterprise Client Management Tool
- Physical chassis buttons.

The TOE boundary excludes SCADA interfaces and the Enterprise Client Management Tool. These interfaces are present on the product but are non-interfering with respect to security as their presence does not prevent any of the TOE’s SFR claims from being satisfied when operated in its evaluated configuration. The TOE boundary also excludes the physical chassis buttons used for resetting the device, ‘override’ mode used to define SCADA rulesets, and management of what are referred to as ‘configuration files’. The physical chassis buttons and override mode do not relate to any claimed security functionality, and the configuration files do not affect any security-relevant data with respect to the PP claims. Use of these interfaces is prevented through the achievement of the OE.PHYSICAL environmental objective. Finally, the TOE boundary excludes the RS-232 serial interface. It is physically part of the product but only used for a local interface to certain SCADA devices; all communications over this interface are therefore physically protected and its use is not security-relevant.

[1] The security token related functions (pairing, signing, encrypting and activating) have not been evaluated and are outside the scope of this evaluation. Password-based authentication is also supported.

9 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary Evaluation Technical Report for Sierra Nevada Corporation Binary Armor SCADA Network Guard v2.1, Part 2 ([11]). The reader of this VR can assume that all assurance activities and work units received passing verdicts.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1, revision 5 ([1], [2], [3]) and CEM version 3.1, revision 5 ([4]), and the specific evaluation activities specified in *Supporting Document Mandatory Technical Document: Evaluation Activities for Network Device cPP*, Version 2.2, December 2019 ([6]). The evaluation determined the TOE satisfies the conformance claims made in the Sierra Nevada Corporation Binary Armor SCADA Network Guard, with firmware version 2.1 Security Target Version 1.0, 2021-6-4, of Part 2 extended and Part 3 conformant. The TOE satisfies the requirements specified in:

- *collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020* ([5]).

The Validators reviewed all the work of the evaluation team and agreed with their practices and findings.

9.1 Evaluation of the Security Target (ST) (ASE)

The evaluation team performed each TSS assurance activity and ASE CEM work unit. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description, security problem definition in terms of threats, policies and assumptions, description of security objectives for the operational environment, a statement of security requirements claimed to be met by the product that are consistent with the claimed Protection Profile, and security function descriptions that satisfy the requirements.

9.2 Evaluation of the Development (ADV)

The evaluation team performed each ADV assurance activity and applied each ADV_FSP.1 CEM work unit. The evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed Protection Profile for design evidence. The ADV evidence consists of the TSS descriptions provided in the ST and product guidance documentation providing descriptions of the TOE external interfaces.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team performed each guidance assurance activity and applied each AGD work unit. The evaluation team determined the adequacy of the operational user guidance in describing how to operate the TOE in accordance with the descriptions in the ST. The evaluation team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in the evaluated configuration. The guidance documentation was assessed during the design and testing phases of the evaluation to ensure it was complete.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team performed each ALC assurance activity and applied each ALC_CMC.1 and ALC_CMS.1 CEM work unit, to the extent possible given the evaluation evidence required by the claimed Protection Profile. The evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence, and that the ST describes how timely security updates are made to the TOE.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team performed each test activity and applied each ATE_FUN.1 CEM work unit. The evaluation team ran the set of tests specified by the claimed PP and recorded the results in the Test Report, summarized in the AAR.

9.6 Vulnerability Assessment Activity (AVA)

The evaluation team performed each AVA assurance activity and applied each AVA_VAN.1 CEM work unit. The evaluation team performed a vulnerability analysis following the processes described in the claimed PP. This comprised a search of the public vulnerability database: National Vulnerability Database (https://nvd.nist.gov/) on 2/10/2021 and updated on 6/4/2021 as well as 7/8/2021, using the following search terms.

- Red Hat Enterprise Linux 7 / 7.9
- OpenAPI
- Boost C++ libraries
- Qt framework
- Roboto font family
- OpenSSL 1.0.2k
- OpenSC PKCS#11 wrapper library
- Xerces XML library
- Lua
- Intel Atom E3845
- 7000-SNC-01
- Sierra Nevada
- Binary Armor
- SCADA Network Guard.

The results of these searches did not identify any vulnerabilities that are applicable to the TOE. The conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met, sufficient to satisfy the assurance activities specified in the claimed Protection Profile. Additionally, the evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the document “ADMINISTRATION GUIDE for COMMON CRITERIA for Binary Armor SCADA Network Guard, with Firmware version 2.1”, dated 10 June 2021. No versions of the TOE and software, either earlier or later were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the SCADA interfaces and Enterprise Management Tool need to be assessed separately and no further conclusions can be drawn about their effectiveness.

The evaluation and testing of security functional requirements are scoped by the guidance included by the Assurance Activity associated with the Protection Profile claimed by the TOE. There is an inherent risk that elements of the TOE security functionality were not fully evaluated. It is recommended that the TOE be subject to integration testing within its intended environment to ensure proper configuration, compliance, and operation.

11 Security Target

The ST for this product's evaluation is *Sierra Nevada Corporation Binary Armor SCADA Network Guard, with firmware version 2.1 Security Target Version 1.0, 2021-6-4* ([7]).

12 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

Abbreviation	Definition
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
HMAC	Hash-based Message Authentication Code
ICS	Industrial Control System
MAC	Message Authentication Code
NSS	Network Security Services
NTP	Network Time Protocol
SCADA	Supervisory Control and Data Acquisition
SHA	Secure Hash Algorithm
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
USB	Universal Serial Bus

13 Bibliography

The validation team used the following documents to produce this VR:

[1] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017.

[2] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security assurance requirements, Version 3.1, Revision 5, April 2017.

[4] Common Criteria Project Sponsoring Organisations. Common Evaluation Methodology for Information Technology Security, Version 3.1, Revision 5, April 2017.

[5] collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020.

[6] Supporting Document Mandatory Technical Document: Evaluation Activities for Network Device cPP, Version 2.2, December 2019

[7] Sierra Nevada Corporation Binary Armor SCADA Network Guard, with firmware version 2.1 Security Target Version 1.0, 2021-6-4

[8] ADMINISTRATION GUIDE for COMMON CRITERIA for Binary Armor® SCADA Network Guard, with Firmware version 2.1, 0318-0200-0004 Document Number Rev A

[9] Binary Armor SCADA Network Guard, with Firmware version 2.1, Binary Armor Alloy API, version 0.3

[10] BINARY ARMOR® USER MANUAL 0318-0100-0015 Document Number Rev G

[11] Evaluation Technical Report for Sierra Nevada Corporation Binary Armor SCADA Network Guard v2.1, v1.0, June 11, 2020.

[12] Assurance Activities Report for Sierra Nevada Corporation Binary Armor SCADA Network Guard, with firmware version 2.1, Version 1.0, 11 June 2021.

[13] Sierra Nevada Binary Armor SCADA Network Guard Common Criteria Test Report and Procedures For Network Device collaborative PP Version 2.2e, Version 1.0, June 11, 2021.