National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Sierra Nevada Corporation

11551 East Arapahoe Road

Centennial, CO 80112, USA

Sierra Nevada Corporation Binary Armor SCADA Network Guard

Report Number:	**CCEVS-VR-10879-2018**
Dated:	**08/07/2018**
Version:	**0.3**

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Marybeth Panock,
Kenneth Stutterheim
The Aerospace Corporation

Common Criteria Testing Laboratory

Katie Sykes
Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Sierra Nevada Corporation Binary Armor SCADA Network Guard solution provided by Sierra Nevada Corporation. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Catonsville, MD, United States of America, and was completed in August 2018. The information in this report is largely derived from the proprietary Evaluation Technical Report (ETR) and associated test reports, as summarized in the publicly available Assurance Activity Report for this evaluation, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the collaborative Protection Profile for Network Devices Version 2.0 + Errata 20180314, Version 2.0, 14 March 2018.

The Target of Evaluation (TOE) is the Sierra Nevada Corporation Binary Armor SCADA Network Guard (hardware version 7000-SNC-01) running software version 1.6.19.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report 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 and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the validation team concludes that the testing laboratory’s findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Sierra Nevada Corporation Binary Armor SCADA Network Guard (NDcPP20E) Security Target, version 0.7, 07/31/2018 and analysis performed by the Validation Team.

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, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) 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 information technology 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 Validated Products List.

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

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile 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	Sierra Nevada Corporation Binary Armor SCADA Network Guard (hardware version 7000-SNC-01) running software version 1.6.19
Protection Profile	collaborative Protection Profile for Network Devices Version 2.0 + Errata 20180314, Version 2.0, 14 March 2018
ST	Sierra Nevada Corporation Binary Armor SCADA Network Guard Security Target (NDcPP20E), version 0.7, 07/31/2018
Evaluation Technical Report	Evaluation Technical Report for Sierra Nevada Corporation Binary Armor SCADA Network Guard, version 0.3, 08/03/2018
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Sierra Nevada Corporation
Developer	Sierra Nevada Corporation
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Marybeth Panock, Kenneth Stutterheim

3 Architectural Information

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

Binary Armor (BA) is designed 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. Binary Armor supports TLS encryption. The TOE provides two, separate, physical interfaces: a “high” NIC (typically connected to SCADA/ICS equipment) and a “low” NIC- (typically connected to external systems such as Human Machine Interface, HMI). The TOE supports remote administration over the network as well as local administration (through a directly networked workstation).

The TOE works by processing every byte of every message with a dynamic state-based rule-set that processes messages based on system control logic. This process ensures only safe message traffic reaches critical SCADA systems.

For the purpose of this evaluation, BA will be treated 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 transmit audit records).

3.1 TOE Evaluated Platforms

The evaluated configuration consists of the following model:

- Sierra Nevada Corporation Binary Armor SCADA Network Guard hardware version 7000-SNC-01
- Binary Armor firmware version 1.6.19
- Binary Armor software suite version 1.6.19 consisting of:
    - Binary Armor Forge (management client that provides administrative access to the TOE)
    - (optional) Binary Armor Monitor (status and monitoring client for a single TOE)
    - (optional) Binary Armor Armory Client & Server (the Armory Server gathers status and monitoring from multiple TOEs and then makes that information available to Armory Clients (which connect to the Armory Server)).

3.2 TOE Architecture

BA is provided as a hardware network appliance. The product provides an administrative interface over TLS.

3.3 Physical Boundaries

The TOE boundary includes the BA itself; the management workstation and software resides in the TOE's Operational Environment.

The TOE has a ruggedized enclosure that protects it from modification and contains a single embedded board containing an Intel Atom E3845 processor, memory, and flash storage. The TOE's firmware consists of a hardened operating system (RHEL 7.4) that does not permit operators (even an authorized administrator) access to the OS with the SNC developed firmware running atop it. The TOE provides a TLS-protected management interface which is accessed via SNC's Forge, Armory, and Monitor applications running on a Windows 7, 8 or 10 PC/workstation in the operational environment. 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.

The administrator gains local access by physically pressing and holding the TOE's configuration (CFG) button and then accessing the TOE's TLS management interface from a directly networked workstation. In this context, "directly networked" means connected via a "crossover" cable or through a network switch to which the TOE and the workstation are the only devices 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 limits on the evaluated appliance.

Optionally, an administrator can configure the TOE to solicit time from an NTP server, if present in the environment (the administrator can manually set the TOE's time if no such NTP server exists). NTP communications are not across a trusted channel.

The TOE's Operating Environment includes the following

- A Windows workstation - The Binary Armor suite of tools operates on Microsoft Windows 7, 8 or 10.
- A security token in the form of a PKCS#11 compliant smart card or USB device present on the workstation. The security token is used by the TOE to sign and encrypt configuration files and to activate override mode.[1] The token is configured by loading private/public key pairs in the form of X509 certificates onto the TOE and then pairing them to the override and configuration operations on the device.
- A TLS-protected syslog server that receives audit events from the TOE
- Optionally, an NTP server with which the TOE can synchronize its clock. It must be noted that the BA does not provide any trusted channel capability for NTP traffic.

[1] The security token related functions are outside the scope of this evaluation.

NOTE: The suite also requires the administrator have a PKCS#11 compliant smart card[2] or USB device present on the workstation. Binary Armor uses PKCS#11 compliant smart cards or USB devices for its encryption and digital signatures. BA configuration files must be encrypted and signed by the paired security token prior to deployment.

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. Identification and authentication
4. Security management
5. Protection of the TSF
6. TOE access
7. Trusted path/channels

4.1 Security audit

The TOE generates audit events associated with identification and authentication, management, updates, and user sessions. The TOE can store the events in a local log or export them to a syslog server using a TLS protected channel.

4.2 Cryptographic support

The TOE provides CAVP certified cryptography in support of its TLS implementation and administrator authentication. Cryptographic services include key management, random bit generation, encryption/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 exceptions of reading the login banner, obtaining status, and (if configured) restarting the TOE and enabling override. It provides the ability to both assign attributes (user password) and to authenticate users against these attributes. The TOE also provides X.509 certificate checking for its TLS connections.

4.4 Security management

The TOE provides a management interface that an administrator can access via a network port. The SNC Forge, Monitor, and Armory applications utilize the TOE's API. The management interface is protected with TLS. The management interface is limited to the authorized administrator.

[2] Test configuration utilized a Yubico Yubikey as the PKCS#11 device.

4.5 Protection of the TSF

The TOE provides mechanisms for self-protection. The TOE performs self-tests that cover the correct operation of the TOE. It provides the functions necessary to securely update the TOE. It relies upon either manually provided time or optionally, an NTP server can be used in its environment to ensure reliable timestamps. It protects sensitive data such as stored passwords and cryptographic keys stored on the TOE's internal Flash so that they are not accessible, even by an authorized administrator.

4.6 TOE access

The TOE can be configured to display a logon banner before a user session is established. The TOE enforces inactivity timeouts for administrative sessions.

4.7 Trusted path/channels

The TOE provides local administration capabilities which are subject to physical protection. To access local administrator functions, an operator must directly network their workstation to the TOE, and then physically press the TOE's configuration button. This transitions the TOE into its configuration mode, whereby an administrator can configure it locally. For both local and remote access, the administrative session is protected by TLS thus ensuring protection against modification and disclosure.

The TOE also protects its audit records from modification and disclosure by using TLS to communicate with the syslog server.

5 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- collaborative Protection Profile for Network Devices Version 2.0 + Errata 20180314, Version 2.0, 14 March 2018

That information has not been reproduced here and the NDcPP20E should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP20E as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

6 Clarification of Scope

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

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the collaborative Protection Profile for Network Devices Version 2.0 + Errata 20180314, Version 2.0, 14 March 2018 and performed by the evaluation team).
- This evaluation covers only the specific device model and software as identified in this document, and not any earlier or later versions released or in process.
- 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 functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP20E and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

7 Documentation

The following documents were available with the TOE for evaluation:

Administrator Guide for Common Criteria for Binary Armor, 0318-0200-0001, Rev B, 03 Aug 18

Binary Armor User Manual, 0318-0100-0015, Version Rev B, 17 July 18

To use the product in the evaluated configuration, the product must be configured as specified in those guides. 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 device in its evaluated configuration. Consumers are encouraged to download the CC configuration guides directly from the NIAP website to ensure the device is configured as evaluated.

8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary Detailed Test Report (NDcPP20E) for Sierra Nevada Corporation Binary Armor SCADA Network Guard, Version 0.3, 08/03/2018 (DTR).

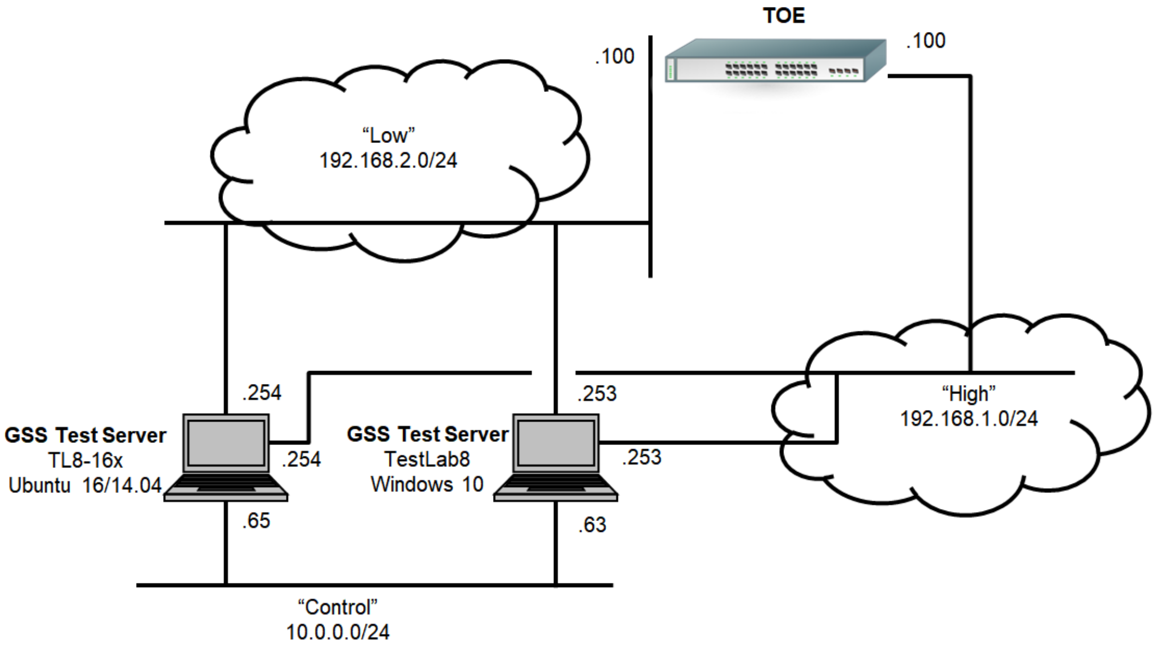
8.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according a Common Criteria Certification document and ran the tests specified in the NDcPP20E including those tests associated with optional requirements.

8.3 Test Bed Configuration



8.4 Test Tools

- Standard Windows utilities (e.g., notepad, snip tool)
- Putty version 0.70
- Wireshark Version 2.2.3 (v2.2.3-0-g57531cd)
- OpenSSL version 1.0.2g
- s_client – TLS Client
- tcpdump
- rsyslog version 8.6.0
- Ntpserver version 4.2.8p4
- Sierra Nevada Corporation Blaster 3.5
- stunnel4 version 5.30

9 Evaluated Configuration

The TOE is the Sierra Nevada Corporation Binary Armor SCADA Network Guard composed of the following hardware and software:

- Binary Armor hardware version 7000-SNC-01
- Binary Armor firmware version 1.6.19.
- Binary Armor software suite version 1.6.19 consisting of:
  - Binary Armor Forge (management client that provides administrative access to the TOE)
  - (optional) Binary Armor Monitor (status and monitoring client for a single TOE)
  - (optional) Binary Armor Armory Client & Server (the Armory Server gathers status and monitoring from multiple TOEs and then makes that information available to Armory Clients (which connect to the Armory Server)).

The TOE has a ruggedized enclosure that contains a single embedded board containing an Intel Atom E3845 processor, memory, and flash storage. The TOE's firmware consists of a hardened operating system (RHEL 7.4) that does not permit operators (even an authorized administrator) access to the SNC developed firmware running atop the OS. The TOE provides a TLS-protected management interface which is accessed via SNC's Forge, Armory, and Monitor applications running on a Windows 10 PC/workstation in the operational environment. 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.

The administrator gains local access by physically pressing and holding the TOE's configuration (CFG) button and then accessing the TOE's TLS management interface from a directly networked workstation. In this context, "directly networked" means connected via "crossover" cable or through a network switch to which only the TOE and the workstation are connected.

9.1 Operating Environment

- A Windows workstation - The Binary Armor suite of tools operates on Microsoft Windows 7, 8 or 10.
- A security token in the form of a PKCS#11 compliant smart card or USB device present on the workstation. The security token is used by the TOE to sign and encrypt configuration files and to activate override mode.[3] The token is configured by loading private/public key pairs in the form of X509 certificates onto the TOE and

[3] The security token related functions are outside the scope of this evaluation.

then pairing them to the override and configuration operations on the device. The test configuration utilized the Yubico Yubikey as the PKCS#11 device

- A TLS-protected syslog server that receives audit events from the TOE
- Optionally, an NTP server with which the TOE can synchronize its clock

10 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

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 rev 4 and CEM version 3.1 rev 4. The evaluation determined the Binary Armor SCADA Network Guard TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP20E.

10.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Sierra Nevada Corporation Binary Armor SCADA Network Guard products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target and guidance documents. Additionally, the evaluator performed the assurance activities specified in the NDcPP20E related to the examination of the information contained in the TSS.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

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

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the NDcPP20E and recorded the results in a proprietary Test Report, as summarized in the publicly available AAR for this evaluation.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the evaluation sensitive Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

On May 23, 2018 and again on August 3, 2018, the evaluator searched the following sources for vulnerabilities:

- National Vulnerability Database (https://web.nvd.nist.gov/vuln/search),
- Vulnerability Notes Database (http://www.kb.cert.org/vuls/),
- Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities),

- Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories),
- Exploit / Vulnerability Search Engine (http://www.exploitsearch.net),
- SecurITeam Exploit Search (http://www.securiteam.com),
- Offensive Security Exploit Database (https://www.exploit-db.com/)
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search),

Each site was searched using the following terms:

a. TCP
b. TLS
c. Openssl 1.0.2k
d. RHEL 7.4
e. SNC
f. Sierra Nevada
g. Binary Armor
h. SCADA Network Data Guard
i. Network device
j. P/N7000-SNC-01
k. 7000-SNC-01
l. Red Hat Enterprise Linux 7.4
m. Red Hat Enterprise Linux 7
n. RHEL 7
o. NSS

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. 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.

11 Validator Comments/Recommendations

The system administrator should be aware that if NTP is implemented, the product does not protect the communications channel with the NTP server. As well, administrators should be aware that in the event of power loss, device time will default to the firmware release date; this may impact audit continuity.

The device provides functionality, such as SCADA firewall services that was not evaluated and therefore no claims can be inferred as to their correct operation. The TOE does not support IPv6.

Binary Armor® configuration files must be encrypted and signed by the paired security token prior to deployment**.** SNC recommends using the Yubico Yubikey 4 and offers these for purchase with Binary Armor® units**.** The security token related functions (pairing, signing, encrypting and activating) have not been evaluated and are outside the scope of this evaluation.

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: *Sierra Nevada Corporation Binary Armor SCADA Network Guard (NDcPP20E) Security Target, Version 0.7, 07/31/2018*.

14 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.

- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

15 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2102.

[4] collaborative Protection Profile for Network Devices Version 2.0 + Errata 20180314, Version 2.0, 14 March 2018.

[5] Sierra Nevada Corporation Binary Armor SCADA Network Guard (NDcPP20E) Security Target, Version 0.7, 07/31/2018 (ST).

[6] Assurance Activity Report (NDcPP20E) for Sierra Nevada Corporation Binary Armor SCADA Network Guard, Version 0.4, 08/03/2018 (AAR).

[7] Detailed Test Report (NDcPP20E) for Sierra Nevada Corporation Binary Armor SCADA Network Guard, Version 0.3, 08/03/2018 (DTR).

[8] Evaluation Technical Report for Sierra Nevada Corporation Binary Armor SCADA Network Guard, Version 0.3, 08/03/2018 (ETR)

[9] Administrator Guide for Common Criteria for Binary Armor, 0318-0200-0001, Rev B, 3 Aug 18

[10] Binary Armor User Manual, 0318-0100-0015, Rev B, Prepared for Version 1.6.19, 17 July 18