National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

NCS Technologies, Inc.

Models:
NCS Stratus CM 4110, Version: F103540-1
NCS Stratus CM 4120, Version: F103786-1

Report Number: [To be completed by CCEVS]
Dated: **April 30, 2013**
Version: **1.0**

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 Panel

Paul Bicknell
Jean Petty
Franklin Haskell
The MITRE Corporation, McLean, VA

Common Criteria Testing Laboratory

Victor Mendoza
Marvin Byrd
InfoGard Laboratories, Inc.
San Luis Obispo, CA

Table of Contents

List of Tables and Figures

1. Executive Summary

This report is intended to assist the end-user of this product with determining the suitability of this IT product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the NCS Technologies Stratus CM 4110 and Stratus CM 4120, the target of evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation of the NCS Technologies Stratus CM 4110 and Stratus CM 4120 products were performed by InfoGard Laboratories, Inc., in San Luis Obispo, CA in the United States and was completed in April, 2013. The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and the functional testing report. The ST was written by InfoGard Laboratories. The evaluation was conducted in accordance with the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1r.3 July 2009, Evaluation Assurance Level 2 (EAL 2) and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1 r.3, July 2009.

The TOE may be packaged with two to three (2-3) independent NCS Technologies computers and may be used to control an additional customer-supplied computer that is not in the same physical package. The computers packaged with the TOE are termed “internal” computers; the computer not in the same package is termed “external.” The only requirement on the external computer is it must use USB v2.0 compatible keyboard and mouse and be compatible with version 1.1a of the DisplayPort specification; however, NCS Technologies recommends the Stratus ST 9196 or Stratus LT 9196, so the TOE can control the power state of the external computer.

The NCS Technologies Stratus CM 4110 and Stratus CM 4120 allow the sharing of a single set of peripheral components among multiple computers through a standard USB interface. The shared peripheral components include a monitor (through Display Port), keyboard, and mouse/pointer devices. The TOE offers isolation among the switchable channels to ensure that computers are thoroughly isolated within the TOE and ensures that only a single computer can access the shared peripheral resource set at one time. Dedicated push buttons with LED “switched state” indicators for each channel assure that the channel selection is unambiguously indicated. The LED indicators can individually be programmed to one of four colors to further assist in disambiguating the switched computer. The NCS Technologies Stratus CM 4110 and Stratus CM 4120 filter USB devices and only allow a basic USB mouse or keyboard to connect to any switched computer.

Each TOE consists of a Control Module and a remote control. The Control Module contains the secure KVM and the power circuitry for the TOE. The remote control has a pairing feature that can be activated with a KVM to ensure that the paired KVM can only work with that paired remote control. The remote control also consists of an LCD display which informs the user of any potential warnings, such as an invalid USB connection or a mismatched remote and KVM.

The NCS Technologies Stratus CM 4110 and Stratus CM 4120 conform to the Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile Version 2.1 dated 7 September 2010.

The NCS Technologies Stratus CM 4110 and Stratus CM 4120 product consists of the following components:

Model	**Version**
NCS Stratus CM 4110	F103540-1
NCS Stratus CM 4120	F103786-1

2. Identification of the TOE

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) for EAL 1 through EAL 4 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 NIAP 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 organizations and individuals participating in the evaluation.

Table 1: Product Identification

Evaluation Scheme	United States Common Criteria Evaluation Validation Scheme
Evaluated Target of Evaluation	NCS Stratus CM 4110, Version: F103540-1; NCS Stratus CM 4120, Version: F103786-1
Protection Profile	Peripheral Sharing Switch (PSS) for Human Interface Devices Protection Profile

	Version 2.1, 7 September 2010
Security Target	NCS Technologies Model Stratus CM 4110 and Stratus CM 4120 Security Target, Version 1.778, Date: 4-26-2013
Dates of Evaluation	October 2012 – April 2013
Conformance Result	EAL 2 augmented ALC_FLR.2
Common Criteria Version	Common Criteria for Information Technology Security Evaluation Version 3.1, August 2007
Common Evaluation Methodology (CEM) Version	CEM Version 3.1, September 2007
Evaluation Technical Report (ETR)	13-2476-R-0017 Version 1.1
Sponsor/Developer	NCS Technologies, Inc.
Common Criteria Testing Lab (CCTL)	InfoGard Laboratories, Inc.
CCTL Evaluators	Victor Mendoza, Marvin Byrd
CCEVS Validators	Jean Petty, Franklin Haskell, Paul Bicknell

3. Interpretations

The Evaluation Team performed and found that there were no applicable interpretation of the CC or CEM.

4. Security Policy

The NCS Technologies Stratus CM 4110 and Stratus CM 4120 supports the following Security Function Policy to ensure that the only the correct remote control can be used to control the KVM:

Data Separation Security Function Policy (SFP):

The TOE shall allow PERIPHERAL DATA and STATE INFORMATION to be transferred only between PERIPHERAL PORT GROUPS with the same ID.

Any User who has access to the TOE is considered an Authorized User as stated in the secure usage assumption section of the Security Target.

5. TOE Security Environment

5.1. Secure Usage Assumptions

The following assumptions are made about the usage of the TOE:

A.ACCESS An AUTHORIZED USER possesses the necessary privileges to access the information transferred by the TOE. USERS are AUTHORIZED USERS.

A.MANAGE The TOE is installed and managed in accordance with the manufacturer’s directions.

A.NOEVIL The AUTHORIZED USER is non-hostile and follows all usage guidance.

A.PHYSICAL The TOE is physically secure.

5.2. Threats Countered

The TOE is designed to fully or partially counter the following threats:

T.INVALIDUSB The AUTHORIZED USER will connect unauthorized USB devices to the peripheral switch.

T.RESIDUAL RESIDUAL DATA may be transferred between PERIPHERAL PORT GROUPS with different IDs.

T.ROM_PROG The TSF may be modified by an attacker such that code embedded in reprogrammable ROMs is overwritten, thus leading to a compromise of the separation-enforcing components of the code and subsequent compromise of the data flowing through the TOE.

T.SPOOF Via intentional or unintentional actions, a USER may think the set of SHARED PERIPHERALS are CONNECTED to one COMPUTER when in fact they are connected to a different one.

T.TRANSFER A CONNECTION, via the TOE, between COMPUTERS may allow information transfer.

5.3. Organizational Security Policies

P.RC_PAIRING_PROTECTION:
The KVM portion of the TOE shall establish a unique logical pairing with a given remote control; if a different pairing is attempted, the KVM portion of the TOE will ignore commands from the remote control, and instruct the remote control to display an error message.

5.4. Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. The following are some of the more important limitations and clarifications that should be noted for this evaluation:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL 2 augmented with ALC_FLR.2).
- This evaluation only covers the specific platforms and software version identified in this document, and not any earlier or later versions released or in process.
- The following features are not included in the evaluated configuration:

- TOE Tamper Detection/Tamper Response mechanisms, and
- CAC Reader, which must be disabled in the evaluated configuration.

6. Architectural Description of the TOE

The TOE is comprised of the Control Module and the Remote Control. The TOE hardware components are made up of the following Architectural Subsystems:

- KVM Subsystem
- Remote Control Subsystem
- Power Subsystem

The Control Module contains the KVM and Power Subsystems.

6.1. KVM Subsystem

The KVM Subsystem is responsible for the switching functionality of the TOE. The data of each computer that is connected to the TOE is kept separate by the KVM Subsystem, which allows a user to access multiple computers using one keyboard, one mouse, and dual monitors. The KVM component includes a general-purpose processor, included in the Control Module shown in Figure 1, that executes internal TOE software as well as volatile and non-volatile storage components for logical IDs.

6.2. Remote Control Subsystem

The Remote Control Subsystem provides the user interface for the TOE, which allows the user to select which computer to switch to. There are multiple buttons.

6.3. Power Subsystem

The Power Subsystem provides the power for the KVM and the internal computers that are connected to the TOE. Different power options are included with each of the different TOEs.

7. *TOE Boundaries*

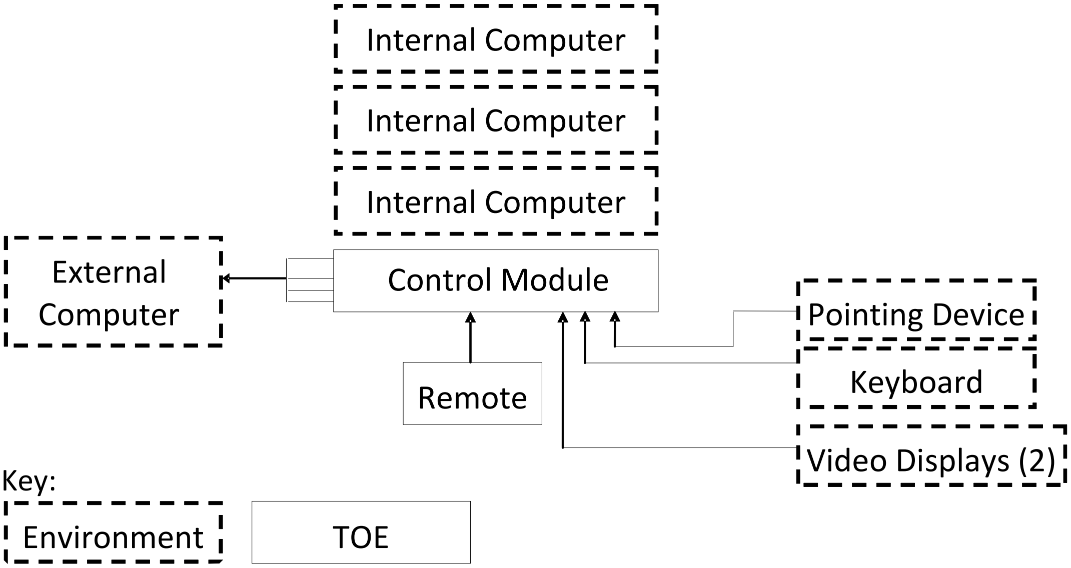

Figure 1: TOE Boundary

7.1. User Data Protection

The TOE protects user data by enforcing the information flow control policy, which assures that the TOE connects the Peripheral Port Group to only a single computer at one time. The Peripheral Port Group is the supported set of USB device interfaces that allow access to a keyboard, mouse, and video displays. Switches on the Remote Control allow the operator to select which computer is connected to the shared Peripheral Port Group at any given time. Each connected computer has a discrete switch and hub on the TOE assigned to its USB port and each connected computer has its own logical ID within the TOE through this switch arrangement. Through this dedicated switching mechanism, the connection between the shared Peripheral port group and the selected computer is activated. The design of these switches and associated circuitry assure that only a single computer can be engaged by the keyboard, mouse and video monitor resources. Through this information flow security function, the TOE precludes the sharing or transfer of data between computers by the TOE.

7.2. Security Management

The TOE supports management of the data flows using a user actuated manual switching mechanism; data can flow to or from the Shared Peripheral Group only if it was received from the same connected computer. This switching mechanism precludes activating two switched computers at once or partial activation of more than a single computer to the Shared Peripheral Group.

When power is applied to the TOE, the Shared Peripheral Group is connected to computer 1 by default.

7.3. Protection of the TSF

The TOE requires that the remote control portion of the TOE be paired with the KVM portion of the TOE to prevent other users from using a different remote control to access a KVM to which they are not authorized. The pairing of the remote control and the KVM is performed during initial setup.

7.4. Indication

The TOE provides a LED indicator light above the push button switch that indicates to the user which computer is connected to the Shared Peripheral Group; the LED remains on as long as the indicated computer is connected to the Shared Peripheral Group. The selected computer is also displayed on the small LCD screen, for example, “COMPUTER 1 SELECTED”.

The TOE ensures the USB devices connected to the Shared Peripheral Group are a valid pointing device, and/or keyboard and video displays. If an invalid device is detected, the TOE will cease communication with the device.

The TOE protects the firmware through the usage of a one-time programmable device so that the device becomes read only; after which, no modifications can be made. Additionally, all programmable devices in the TOE are permanently attached (soldered) to the PCB board.

8. Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the NCS Technologies Stratus CM 4110 and Stratus CM 4120. Note that not all evidence is available to customers. In these tables, the following conventions are used:

- Documentation that is delivered to the customer is shown with bold titles.
- Documentation that was used as evidence but is not delivered is shown in a normal typeface.
- Documentation that is delivered as part of the product but was not used in the evaluation is shown with a bold title, but a hashed background.

The TOE is physically delivered to the End-User. The guidance is part of the TOE components and is delivered with the TOE as a supplement.

8.1. Design Documentation

Document	Revision	Date
Stratus Backplane Specification Document Number V001835	0.16	4/17/2013
Stratus SKVM (Secure KVM) Firmware Specification Document Number V001837	0.5	3/26/2013
Stratus ECKVM Switch(Ethernet, Control and KVM)Specification Document Number V001833	0.15	4/17/2013

Stratus SRC (Secure Remote Control) Firmware Specification Document Number V001836	0.5	3/26/2013
Stratus SRC and Stratus CRC Hardware Specification Document Number: V001834	0.17	4/17/2013
Stratus System Specification Document Number V001832	0.15	4/17/2013
Flash Protection for Stellaris® Microcontrollers Application Note	AN01257-03	6/24/2009
Stellaris® LM3S3748 Microcontroller DATA SHEET	DS-LM3S3748-9102	1/10/2011
Stellaris® LM3S5P31 Microcontroller DATA SHEET	DS-LM3S5P31-8832	12/1/2010

8.2. Guidance Documentation

Document	Revision	Date
STRATUS CM 4110 and 4120 User Guide	**UG-STRATUS CM-3.4**	**3/26/2013**
Download Instructions for Stratus CM 4110 and 4120 User Guide	**1026489**	**N/A**
STRATUS MCS Multiple Client Station with Secure KVM Quick Start Guide	**1025278**	**N/A**

8.3. Configuration Management and Lifecycle

Document	Revision	Date
Stratus Control Module 4120 and 4110 Configuration Control Plan	2.16	3/20/2013

8.4. Test Documentation

Document	Revision	Date
Stratus CM 4110 and Stratus CM 4120 Security Feature Test Document	0.9	4/16/2013
NCS Independent and Penetration Test Plan Document ID: 13-2476-R-0019	1.0	4/18/2013

8.5. Vulnerability Assessment Documentation

Document	Revision	Date
NCS Technologies Model Stratus CM 4110 and Stratus CM 4120 Common Criteria Vulnerability Analysis AVA_VAN.2 EAL2	1.0	3/26/2013

8.6. Security Target

Document	Revision	Date
NCS Technologies Model Stratus CM 4110 **and Stratus CM 4120 Security Target**	1.778	4/26/2013

9. IT Product Testing

This section describes the testing efforts of the Developer and the evaluation team.

9.1. Developer Testing

The test procedures were written by the Developer and designed to be conducted using manual interaction with the TOE interfaces.

The Developer tested the TOE consistent with the Common Criteria evaluated configuration identified in the ST. The Developer tested all of the interfaces to the TOE and in doing so tested all TSFs.

The evaluation team analyzed the Developer's testing to ensure adequate coverage for EAL 2. The evaluation team determined that the Developer's actual test results matched the Developer's expected test results.

9.2. Evaluation Team Independent Testing

The evaluation team conducted independent testing at the CCTL. The evaluation team installed the TOE according to vendor installation instructions and the evaluated configuration as identified in the Security Target.

The evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE while performing work unit ATE_IND.2-2. The evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The evaluation team used the Developer's Test Plan as a basis for creating the Independent Test Plan. The evaluation team analyzed the Developer's test procedures to determine their relevance and adequacy to test the security function under test. The following items represent a subset of the factors considered in selecting the functional tests to be conducted:

- Security functions that implement critical security features
- Security functions critical to the TOE's security objectives
- Security functions that gave rise to suspicion regarding the behavior of the security features during the documentation evidence evaluation
- Security functions not tested adequately in the vendor's test plan and procedures

The evaluation team selected a sampling of the vendor tests based on major functionality described in the Security Target as security related functionality provided by the TOE. If a given test (or a portion of a test) covered a major functionality of the TSF, then that test (or the relevant portion) was included as a sampled test case and included in the Independent Test Plan. To disambiguate portions of a particular test, the evaluation team included all test steps taken. The evaluation team repeated a representative portion of the Sponsor test cases and developed a number of additional tests. The additional test coverage was determined based on the analysis of the Developer test coverage and the ST.

Each TOE Security Function was exercised at least once, and the evaluation team verified that each test passed.

9.3. Vulnerability Analysis

The evaluation team devised penetration testing to confirm that the TOE was resistant to penetration attacks performed by an attacker with a moderate attack window. The evaluation team conducted testing using the same test configuration that was used for the independent team testing. In addition to the documentation review used in the independent testing, the team used the knowledge gained during independent testing to devise the penetration testing.

9.4. Vulnerability Search

The evaluation team performed a thorough search of public vulnerability databases in order to identify potential vulnerabilities that could affect the evaluated TOE. No vulnerabilities were found related to the evaluated TOE or similar products.

10. Evaluated Configuration

The evaluated configuration of the NCS Technologies Stratus CM 4110 and Stratus CM 4120, as defined in the Security Target, consists of two hardware components (Control Module and Remote Control) and two firmware components (Control Module and Remote Control Firmware).

The NCS Technologies Stratus CM 4110 and Stratus CM 4120 are delivered to the end user with an instructional supplement describing the actions necessary to download and obtain the user guide. The user guide describes the steps required to configure the TOE to be in the Common Criteria evaluated configuration.

11. Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1.

InfoGard has determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 2. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed in April of 2013.

12. Validator Comments

The TOE was successfully evaluated in the defined evaluated configuration and scope described in Security Target. The validation team recommends certification of the TOE at EAL 2 augmented with ALC_FLR.2.

Potential users of this product should note the following:

- The product includes the capability to attach a CAC reader. This capability is not included in the evaluated configuration and is disabled in the delivered product. Enabling this capability through manipulation of dip switches on the product will cause the product to be taken out of the evaluated configuration, making the certification of that product instance invalid.
- The product includes an intrusion detection mechanism that is not considered as a security protections. The user should not rely on the intrusion detection mechanism for the protection of the product either during the delivery process or during operation of the TOE.

13. Security Target

NCS Technologies Model Stratus CM 4110 and Stratus CM 4120 Security Target, Version 1.778, Date 4/26/2013

14. Glossary

KVM Switch Keyboard, Video, Mouse - A KVM (keyboard, video, mouse) switch allows a single keyboard, video monitor and mouse to be switched to any of a number of computers when typically a single person interacts with all the computers but only one at a time.

Peripheral Data Refers to data entered via a member of a peripheral port group i.e.: data entered by the mouse or keyboard and displayed through the monitor.

Peripheral Port Group A collection of device ports treated as a single entity by the TOE.

Plug and Play A standardized interface for the automatic recognition and installation of interface cards and devices on a PC.

Switched Computers Refers to the computers connected to the TOE and connected to the Peripheral port group upon the switching function of the TOE.

State Information The current or last known status or condition, of a process, transaction, or setting. "Maintaining state" means keeping track of such data over time.

User The human operator of the TOE.

15. Bibliography

Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and General Model, July 2009, Version 3.1, Revision 3, CCMB-2009-07-001.

Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation - Part 2: Security Functional Components, July 2009, Version 3.1, Revision 3, CCMB-2009-07-002.

Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation - Part 3: Security Assurance Components, July 2009, Version 3.1, Revision 3, CCMB-2009-07-003.

Common Criteria Project Sponsoring Organisations. Common Criteria Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, July 2009, Version 3.1, Revision 3, CCMB-2009-07-004.

Common Criteria, Evaluation and Validation Scheme, Publication #3, Guidance to Validators, Version 2.0, 8 September 2008.

NCS Technologies Model Stratus CM 4110 and Stratus CM 4120 Security Target, Version 1.778, April 26, 2013

Evaluation Technical Report Peripheral Sharing Switch (PSS), Version V1.1, April 18, 2013