National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Emerson Secure KM
(identified 2, 4, 8-Port models)

Report Number: CCEVS-VR-VID10704-2016

Dated: March 24, 2016

Version: 1.0

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

Department of Defense
National Security Agency
9800 Savage Road
Fort Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Chris Thorpe

Daniel Faigin

Ken Stutterheim

Tony Chew

Brad O'Neill

Common Criteria Testing Laboratory

CSC Global Cybersecurity, Security Testing & Certification Lab
Computer Sciences Corporation
7459A Candlewood Drive
Hanover, Maryland 21076

1. EXECUTIVE SUMMARY

This report is intended to assist the end-user of this product and any security certification Agent for the end-user with determining the suitability of this Information Technology (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 by the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Emerson Secure KM Switch, the Target of Evaluation (TOE), performed by CSC Global Cybersecurity, Security Testing & Certification Lab. 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 was performed by CSC Global Cybersecurity, Security Testing & Certification Lab of Hanover, MD in accordance with the United States evaluation scheme and completed on February 26, 2016. The information in this report is largely derived from the ST, the Evaluation Technical Report (ETR) and the functional testing report. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, dated September 2012; and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1, Revision 4, September 2012; and the NIAP Peripheral Sharing Switch (PSS) Protection Profile (PP) version 3.0.

The Emerson Secure Peripheral Sharing Switches (PSS) allows the secure sharing of a single set of peripheral components such as keyboard and Mouse/Pointing devices among multiple computers through standard USB interfaces.

The Evaluation Team performed an analysis of the NIAP Technical Decisions and determined that Technical Decision TD0083 applies to this TOE.

The TOE is also compliant with all International interpretations with effective dates on or before April 28, 2015.

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) using the Common Evaluation Methodology (CEM) and NIAP approved Protection Profiles in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

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 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;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Emerson Secure KM, selected 2, 4, and 8 port models
Protection Profile	NIAP Peripheral Sharing Switch for Human Interface Devices Protection Profile, Version 3.0, February 13, 2015
Security Target	Emerson Network Power Secure KM Switch, Security Target, Rev 3.18
Dates of evaluation	April 28, 2015 – February 26, 2016
Evaluation Technical Report	Emerson Evaluation Technical Report: Emerson Secure KM Switch, Document Version 1.0, February 2016
Assurance Activity Report	Emerson Network Power Secure KM Switch Assurance Activity Report, Document Version 1.0, February 2016
Conformance Result	This evaluation has the following CC conformance claims: • Part 2 extended • Part 3 conformant
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1, Revision 4, September 2012: 1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012. 2. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012. 3. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012.
Common Evaluation Methodology (CEM) version	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 4, September 2012
Sponsor	Emerson
Developer	Emerson
Evaluators	CSC Global Cybersecurity, Security Testing & Certification Lab : Brian Pleffner, John F. Daniels, Cheryl Dugan, Brittany Conti
Validation Team	The Aerospace Corporation: Daniel Faigin, Tony Chew, Kenneth Stutterheim The MITRE Corporation: Chris Thorpe, Brad O'Neill

3. SECURITY POLICY

The TOE implements the Data Separation Security Function Policy (SFP) as outlined in Section 4 of the claimed Protection Profile. Isolated USB device emulators are used for the keyboard and mouse. There is one USB device emulator per each connected computer. The use of isolated USB device emulators assures that connected computers will not interact electrically or logically with shared TOE or peripheral resources. Data exchange from computer emulators to device emulators is uses a proprietary protocol called UNIDIR. The UNIDIR protocol is limited to basic HID transactions. No other data may flow between emulators as it is not supported by the limited protocol. Keyboard and mouse data flows are not combined or connected to any other TOE data flow. The keyboard and mouse (KM) functions are completely isolated from all other functions (audio, DPP etc.). There are no shared microcontrollers or any other electronic components. No other external interfaces are coupled to the keyboard and mouse data flow paths.

a. Wireless keyboards are not allowed per applicable user guidance.

b. Wireless mice are not allowed per applicable user guidance.

c. TOE Keyboard and mouse USB console ports are interchangeable.

4. ARCHITECTURAL INFORMATION

4.1. Logical Scope and Boundary

Secure KMs are used to enable a single user having a single set of peripherals to operate in an environment having multiple isolated computers. KM switches keyboard, mouse, audio, and other peripheral devices to one user selected computer.

The following subsections summarize the various KM TOE features and services that were verified in the current evaluation.

4.1.1. Keyboard and mouse security

Isolated keyboard and mouse USB device emulators per connected computer to prevent direct interface between the TOE shared peripheral devices and connected computers.

TOE uses host (computer) emulators to interface with connected keyboard and mouse peripheral devices, thus isolating external peripherals from TOE internal circuitry and from connected computers.

Keyboard user data is not stored on TOE non-volatile memory. All USB stacks are implemented in the TOE using SRAM (Static Random Access Memory) – a volatile memory that clears data once TOE is powered down.

4.1.2. TOE external interface security

The TOE supports only the following external interfaces protocols:

- USB keyboard and mouse;
- Analog audio output;
- User authentication device or other assigned USB devices (TOE model specific);
- Power (AC or DC)

4.1.3. Audio Subsystem security

The TOE audio data flow path is electrically isolated from all other functions and interfaces to prevent signaling data leakages to and from the audio paths.

4.1.4. User authentication device subsystem security

TOE supports User Authentication Device function (called DPP). These products are configured by default as FDF (Fixed Device Filtration) with filter set to qualify only the following devices:

- Standard smart-card reader USB token or biometric authentication device having USB smart-card class interface complying with USB Organization standard CCID Revision 1.1 or ICCID Revision 1.0.
- An administrator after successfully logging-in to the TOE administrative function may switch the TOE to CDF (Configurable Device Filtration) mode trough loading any white-list/black-list or traffic rules.

  Note that device must be bus powered.

4.1.5. User control and monitoring security

TOE is controlled and monitored by the user through front panel illuminated push-buttons and switches. These controls and indications are coupled to the TOE system controller function.

4.1.6. Tampering protection

Always-on anti-tampering system mechanically coupled to the TOE enclosure to detect and attempt to access the TOE internal circuitry.

TOE is equipped with special holographic Tampering Evident Labels that located in critical location on the TOE enclosure.

4.1.7. Self-testing and Log

TOE is equipped with self testing function that operating at TOE power up prior to normal use. The self-test function is running independently at each one of the TOE microcontrollers following power up.

TOE is equipped with event log non-volatile memory that stores information about abnormal security related events.

4.2. Administrative and User configuration of the KM TOE

The KM TOE enable user configuration of various operational parameters. This access may be performed using one of the following methods (as further explained in the relevant TOE user guidance):

1. Using predefined keyboard shortcuts;
2. Using connected computer and text editor application; and
3. Using special USB configuration loading cable and special configuration utility software.

The KM TOE enable administrator configuration of various operational and security parameters. Access requires password authentication. This access may be performed using one of the following methods (as further explained in the relevant TOE administrator guidance):

1. Using connected computer and text editor application; and
2. Using special USB configuration loading cable and special configuration utility software.

4.3. Physical Scope and Boundary

The TOE is a peripheral sharing switch configured as a KM.

The physical boundary of the TOE consists of:

- One EMERSON Secure KM Switch, typically consisting of a system controller board and power supply;

- The firmware embedded inside the TOE that is permanently programmed into the TOE multiple microcontrollers;
- The log, state and settings data stored in the TOE;
- The TOE power supply that is shipped with the product (or integrated inside some of the products having 4 ports or more);
- The TOE computer interface cables that are shipped with the product.

The TOE also includes the user documentation identified elsewhere in this ST. The latest version of the documentation may be found at the Emerson website: http://www.emersonnetworkpower.com/en-US/Support/Warranty/Infrastructure-Management/Hardware-Support/Pages/Cybex-Supporting-Documentation.aspx.

The evaluated TOE configuration does not include any peripherals or computer components, but does include supplied computer interface cables attached to the TOE.

It also should be noted that some TOE models support only a partial set of peripheral devices.

4.3.1. Evaluated Environment

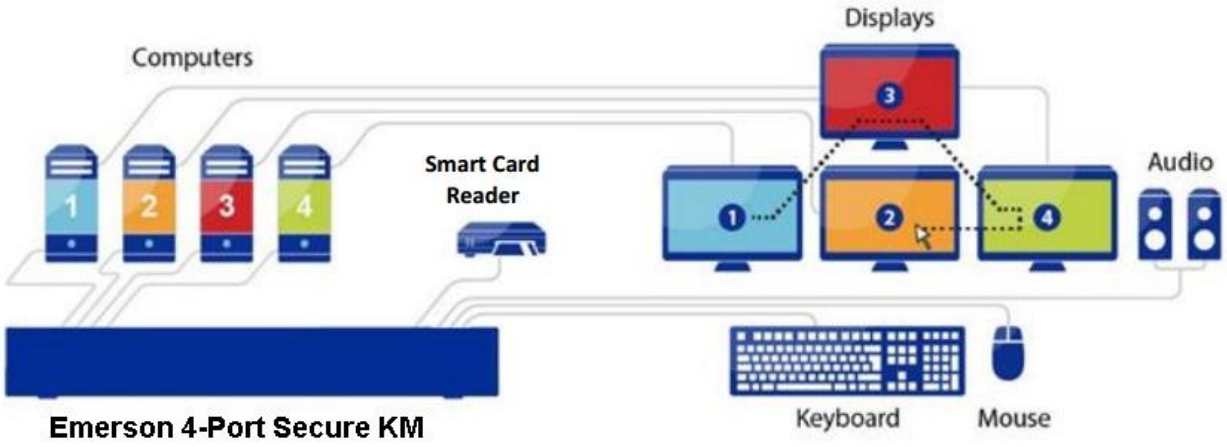
This table identifies hardware components and indicates whether or not each component is in the TOE or Environment.

Evaluated TOE and Environment Components

TOE / Environment	Component	Description
TOE	Selectable product from Evaluated KM Products table.	TOE Hardware and firmware
Environment	Standard USB or PS/2 Mouse	Console USB user mouse port
Environment	Standard USB or PS/2 keyboard	Console USB user keyboard port
Environment	Standard USB User Authentication Device. Any other predefined USB device based on the Configurable Device Filtration (CDF) settings.	Console user authentication device interface
Environment	Standard computer display (VGA, DVI, HDMI, DisplayPort depending on TOE product)	Console user display interface

<table>
<tr><td>TOE</td><td>Emerson KVM Cables (as needed):<table><tr><th>P/N</th><th>Description</th></tr><tr><td>CWR05117</td><td>KVM Cable short (1.8 m), USB Type-A to USB Type-B, Black</td></tr><tr><td>CWR05116</td><td>KVM Cable short (1.8 m), Audio out, DPP, Black</td></tr><tr><td>CWR05205</td><td>KVM Cable short (1.8 m), DVI-A to VGA, USB, Black</td></tr><tr><td>CWR05114</td><td>KVM Cable short (1.8 m), DVI-D to DVI-D Single-Link, USB, Black</td></tr><tr><td>CWR05115</td><td>KVM Cable short (1.8 m), DVI-D to DVI-D Dual-Link, USB, Black</td></tr><tr><td>HWR08154</td><td>KVM Cable short (1.8m), HDMI to HDMI, USB, Black</td></tr><tr><td>CWR05113</td><td>KVM Cable short (1.8 m), DVI-D to DVI-D Single-Link, USB, Audio out, DPP, Black</td></tr><tr><td>CWR06011</td><td>Cable Ethernet CAT 5-E, Blue, 1.8m</td></tr><tr><td>CWR06246</td><td>KVM Cable short (1.8 m), DP to DP, USB A to USB B, Black</td></tr></table></td><td>Cables for connection of computers to TOE computers</td></tr>
<tr><td>TOE</td><td>Special Administrator Programming Cable (as needed):<table><tr><th>P/N</th><th>Description</th></tr><tr><td>HWR06579</td><td>USB Type-A to USB Type-A Configuration loading Cable, 1.8m, Black</td></tr></table></td><td>USB-A to USB-A Conf. Loading Cable</td></tr>
<tr><td>Environment</td><td>Standard amplified stereo speakers or analog headphones</td><td>Audio output console port</td></tr>
<tr><td>Environment</td><td>Standard PC, Server, portable computer , tablet, thin-client or zero-client running any operating system; or</td><td>Connected computers</td></tr>
</table>

Typical TOE Installation



4.3.2. KM TOE details

Evaluated KM Products

No	Model	P/N MPN	Description	Eval. Version
2-Port				
1.	SCKM120	CGA08587 520-925-501	Emerson - Cybex SC KM 120, 2-port Secure KM, PP 3.0	30303-00C4
4-Port				
2.	SCKM140	CGA08554 520-926-501	Emerson - Cybex SC KM 140, 4-port Secure KM, PP 3.0	30303-00C4
3.	SCKM145	CGA08555 520-959-501	Emerson - Cybex SC KM 145, 4-port Secure KM + DPP, PP 3.0	30333-00C4
8-Port				
4.	SCKM180	CGA08556 520-927-501	Emerson - Cybex SC KM 180, 8-port Secure KM, PP 3.0	30303-00C4
5.	SCKM185	CGA08564 520-960-501	Emerson - Cybex SC KM 185, 8-port Secure KM + DPP, PP 3.0	30333-00C4

5. ASSUMPTIONS AND CLARIFICATION OF SCOPE

5.1. Assumptions

The ST identified the following security assumptions:

Table: Secure Usage Assumptions

Assumption	Definition
A.NO_TEMPEST	It is assumed that the computers and peripheral devices connected to the TOE are not TEMPEST approved.
A.NO_SPECIAL_ANALOG_CAPABILITIES	It is assumed that the computers connected to the TOE are not equipped with special analog data collection cards or peripherals such as: Analog to digital interface, high performance audio interface, Digital Signal Processing function, and analog video capture function.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators and users are trusted to follow and apply all guidance in a trusted manner.
A.TRUSTED_CONFIG	Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.

5.2. Threats

The ST identified the following threats addressed by the TOE:

Table: Threats

Threat	Definition
T.DATA_LEAK	A connection via the PSS between computers may allow unauthorized data flow through the PSS or its connected peripherals.
T.SIGNAL_LEAK	A connection via the PSS between computers may allow unauthorized data flow through bit-by-bit signaling.
T.RESIDUAL_LEAK	A PSS may leak (partial, residual, or echo) user data between the intended connected computer and another unintended connected computer. More specifically, a PSS may leak user keyboard entries to a PSS-connected computer other than

	the selected computer in real-time or at a later time.
T.UNINTENDED_SWITCHING	A threat in which the user is connected to a computer other than the one to which they intended to be connected.
T.UNAUTHORIZED_DEVICES	The use of an unauthorized peripheral device with a specific PSS peripheral port may allow unauthorized data flows between connected devices or enable an attack on the PSS or its connected computers.
T.AUTHORIZED_BUT_UNTRUSTED_DEVICES	The use of an authorized peripheral device with the PSS may still cause unauthorized data flows between connected devices or enable an attack on the PSS or its connected computers. Such threats are possible due to known or unknown device vulnerabilities or due to additional functions within the authorized peripheral device.
T.MICROPHONE_USE	Microphone connected to the TOE used for audio eavesdropping or to transfer data across an air-gap through audio signaling.
T.AUDIO_REVERSED	Audio output device used by an attacker as a low-gain microphone for audio eavesdropping. This threat is an abuse of the computer and TOE audio output path to reverse the analog data flow from the headphones to the computer. The computer then amplifies and filters the weak signal, and then digitizes and streams it to another location.
T.LOGICAL_TAMPER	An attached device (computer or peripheral) with malware, or otherwise under the control of a malicious user, could modify or overwrite code embedded in the TOE's volatile or non-volatile memory to allow unauthorized information flows between connected devices.
T.PHYSICAL_TAMPER	A malicious human agent could physically tamper with or modify the TOE to allow unauthorized information flows between connected devices.
T.REPLACEMENT	A malicious human agent could replace the TOE during shipping, storage, or use with an alternate device that does not enforce the TOE security policies.
T.FAILED	Detectable failure of a PSS may cause an unauthorized information flow, weakening of PSS security functions, or unintended switching.

5.3. Organizational Security Policies

The Protection Profile claimed identifies no Organizational Security Policies (OSPs) to which the TOE must comply.

5.4. Security Objectives

The following table, Security Objectives for the TOE, identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified.

Security Objective	Definition as applied to KM type TOE
O.COMPUTER_INTERFACE_ISOLATION	The TOE must prevent unauthorized data flow to assure that the TOE and/or its connected peripheral devices would not be exploited in an attempt to leak data. The TOE computer interface shall be isolated from all other TOE computer interfaces while TOE is powered.
O.COMPUTER_INTERFACE_ISOLATION_ TOE_UNPOWERED	The same level of isolation defined in the dataflow objectives must be maintained at all times, including periods while TOE is unpowered.
O.USER_DATA_ISOLATION	User data such as keyboard entries should be switched (i.e., routed) by the TOE only to the computer selected by the user. The TOE must provide isolation between the data flowing from the peripheral device to the selected computer and any non-selected computer.
O.NO_USER_DATA_RETENTION	The TOE shall not retain user data after it is powered down.
O.PURGE_TOE_KB_DATA_WHILE_ SWITCHING	The TOE shall purge all user keyboard data from computer interfaces following channel switching and before interacting with the new connected computer.
O.NO_DOCKING_PROTOCOLS	The use of docking protocols such as DockPort, USB docking, Thunderbolt etc. is not allowed in the TOE.
O.NO_OTHER_EXTERNAL_INTERFACES	The TOE may not have any wired or wireless external interface with external entities (external entity is an entity outside the TOE evaluated system, its connected computers and peripheral devices).
O.NO_ANALOG_AUDIO_INPUT	Shared audio input peripheral functions (i.e., analog audio microphone input or line input) are not allowed in the TOE.
O.UNIDIRECTIONAL_AUDIO_OUT	The TOE shall be designed to assure that reverse audio signal attenuation will be at least 30 dBv measured with 200 mV and 2V input pure sinus wave at the extended audio frequency range including negative swing signal. The level of the reverse audio signal received by the selected computer shall be minimal to assure that the signal level generated by headphones will be well under the noise floor level.

O.COMPUTER_TO_AUDIO_ISOLATION	The audio dataflow shall be isolated from all other TOE functions. Signal attenuation between any TOE computer interface and any TOE audio interface shall be at least 45 dBv measured with 2V input pure sinus wave at the extended audio frequency range including negative swing signal.
O.USER_AUTHENTICATION_ISOLATION	The user authentication function shall be isolated from all other TOE functions.
O.USER_AUTHENTICATION_RESET	Upon switching computers, the TOE shall reset (turn off and then turn on) the power supplied to the user authentication device for at least 1 second
O.USER_AUTHENTICATION_ADMIN	TOE CDF configuration may only performed by an administrator.
O.AUTHORIZED_SWITCHING	The TOE shall allow only authorized switching mechanisms to switch between connected computers and shall explicitly prohibit or ignore unauthorized switching mechanisms.
O.NO_AMBIGUOUS_CONTROL	Only one switching method shall be operative at any given time to prevent ambiguous commands.
O.CONTINUOUS_INDICATION	The TOE shall provide continuous visual indication of the computer to which the user is currently connected.
O.KEYBOARD_AND_MOUSE_TIED	The TOE shall ensure that the keyboard and mouse devices are always switched together
O.NO_CONNECTED_COMPUTER_ CONTROL	The TOE shall not allow TOE control through a connected computer.
O.PERIPHERAL_PORTS_ISOLATION	The TOE shall prevent data flow between peripheral devices of different SPFs and the TOE peripheral device ports of different SPFs shall be isolated.
O.DISABLE_UNAUTHORIZED_ PERIPHERAL	The TOE shall only allow authorized peripheral device types (See Annex C) per peripheral device port; all other devices shall be identified and then rejected or ignored by the TOE.
O.DISABLE_UNAUTHORIZED_ ENDPOINTS	The TOE shall reject unauthorized peripheral devices connected via a USB hub. Alternatively, the TOE may reject all USB hubs.
O.KEYBOARD_MOUSE_EMULATED	The TOE keyboard and pointing device functions shall be emulated (i.e., no electrical connection other than the common ground is allowed between peripheral devices and connected computers).
O.KEYBOARD_MOUSE_ UNIDIRECTIONAL	The TOE keyboard and pointing device data shall be forced to unidirectional flow from the peripheral device to the switched computer only.

O.TAMPER_EVIDENT_LABEL	The TOE shall be identifiable as authentic by the user and the user must be made aware of any procedures or other such information to accomplish authentication. This feature must be available upon receipt of the TOE and continue to be available during the TOE deployment. The TOE shall be labeled with at least one visible and one invisible unique identifying tamper-evident marking that can be used to authenticate the device. The TOE manufacturer must maintain complete list of manufactured TOE articles and their respective identification markings' unique identifiers.
O.ANTI_TAMPERING	The TOE shall be physically enclosed so that any attempts to open or otherwise access the internals or modify the connections of the TOE would be evident. This shall be accomplished through the use of an always-on active anti-tampering system that serves to permanently disable the TOE should its enclosure be opened. The TOE shall use an always-on active anti-tampering system to permanently disable the TOE in case physical tampering is detected.
O.ANTI_TAMPERING_BACKUP_POWER	The anti-tampering system must have a backup power source to enable tamper detection while the TOE is unpowered.
O.ANTI_TAMPERING_BACKUP_FAIL_ TRIGGER	A failure or depletion of the anti-tampering system backup power source shall trigger TOE to enter tampered state.
O.ANTI_TAMPERING_INDICATION	The TOE shall have clear user indications when tampering is detected.
O.ANTI_TAMPERING_PERMANENTLY_ DISABLE_TOE	Once the TOE anti-tampering is triggered, the TOE shall become permanently disabled. No peripheral-to-computer data flows shall be allowed.
O.NO_TOE_ACCESS	The TOE shall be designed so that access to the TOE firmware, software, or its memory via its accessible ports is prevented.
O.SELF_TEST	The TOE shall perform self-tests following power up or powered reset.
O.SELF_TEST_FAIL_TOE_DISABLE	Upon critical failure detection the TOE shall disable normal operation of the whole TOE or the respective failed component.
O.SELF_TEST_FAIL_INDICATION	The TOE shall provide clear and visible user indications in the case of a self-test failure.

Notes:

1. Objective O.USER_AUTHENTICATION_TERMINATION is not applicable to for the models covered by this security target in accordance with the referenced PP, as it does not support an emulated user authentication device function.

2. Objectives O.UNIDIRECTIONAL_VIDEO, O.UNIDIRERCTIONAL_EDID and O.DISPLAYPORT_AUX_FILTERING FILTERING are not applicable for the models covered by this security target in accordance with the referenced PP, as they does not support video.

5.5. Security Objectives for the Operational Environment

The following IT security objectives for the environment are to be addressed by the Operational Environment by technical means.

Environment Security Objective	Definition
OE. NO_TEMPEST	The operational environment will not require the use of TEMPEST approved equipment.
OE. NO_SPECIAL_ANALOG_ CAPABILITIES	The operational environment will not require special analog data collection cards or peripherals such as: Analog to digital interface, high performance audio interface, Digital Signal Processing function, and analog video capture function.
OE.PHYSICAL	The operational environment will provide physical security, commensurate with the value of the TOE and the data it contains.
OE.TRUSTED_ADMIN	The operational environment will ensure that appropriately trained and trusted TOE Administrators and users are available to administer, configure and use the TOE.

5.6. 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:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the Protection Profile for Peripheral Sharing Switches.
2. Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, 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.

3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.
4. The evaluated configuration of the TOE includes the products identified in Section 4.3.2 using the identified version in the same section for each product. The TOE includes all the code that enforces the policies identified.

6. DOCUMENTATION

The following guidance documents are provided with the TOE upon delivery in accordance with the PP:

1. Emerson. *Secure KM Switch 2/4 Port User Manual*, Document Number HDC10364, Rev E, August 13, 2015.
2. Emerson. *Secure KM Switch 8 Port User Manual*. Document Number HDC11607, Rev E. September 24, 2015.
3. Emerson. *Emerson KM Configuration Manual*. Document Number HDC10961, Rev C. January 28, 2016.
4. Emerson. *Emerson DPP Configuration Utility Manual*. Document Number HDC10955, Rev C. January 28, 2016
5. Emerson. *Emerson Administrator Guide*. Document Number HDC10958, Rev C. August 13, 2015.

All documentation delivered with the product is relevant to and within the scope of the TOE. The documentation can be downloaded from Emerson website: http://www.emersonnetworkpower.com/en-US/Support/Warranty/Infrastructure-Management/Hardware-Support/Pages/Cybex-Supporting-Documentation.aspx at any time.

7. IT PRODUCT TESTING

This section describes the testing efforts of the evaluation team.

7.1. Evaluation team independent testing

The evaluation team conducted independent testing at the Emerson facilities in Huntsville, Alabama. The evaluation team installed and configured the TOE according to vendor installation instructions and the evaluated configuration as identified in the Security Target. The testing configuration and the testing results were documented in the Assurance Activity Report (AAR) and the Test Report (TR) identified in the Bibliography.

The evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. 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 Protection Profile test procedures as a basis for creating each of the Independent tests as required by the Assurance Activities.

Each Assurance Activity was tested as required by the conformant Protection Profiles and the evaluation team verified that each test passed.

7.2. Vulnerability analysis

The evaluation team performed a vulnerability analysis of the TOE evidence and a search of publicly available information to identify potential vulnerabilities in the TOE. Based on the results of this effort, there were no identifiable vulnerabilities found at the time of certification.

8. 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 3.1R4. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1R4.

CSC Global Cybersecurity, Security Testing & Certification Lab has determined that the product meets the security criteria in the Security Target, which specifies conformance to the NIAP Peripheral Sharing Switch for Human Interface Devices Protection Profile, Version 3.0, February 13, 2015. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation effort was finished on February 26, 2016.

9. VALIDATOR COMMENTS

This evaluation was one of the first evaluations performed against the updated Peripheral Sharing Switch (PSS) Protection Profile (PP) version 3.0. The updates to the protection profile required some significant changes to the document. During the initial evaluation and validation processes for this updated PP, several issues necessitated review by the PSS Technical Rapid Response Team (TRRT). The TRRT has formally posted two technical decisions related to the PSS PP (TD0083 and TD0086) and they are posted on the NIAP website. Only TD0083 applies to this TOE. It should be noted that the nature of a PSS presents challenges when reviewing validation evidence against detailed assurance activities. Since most of the evidence is pictorial in nature several iterations, between the validators and the lab, were required to agree the appropriateness of presentation of the evidence.

In addition to the items mentioned above some additional product administration and usability features are worth considering:

- An administrator mode is supported in the product, but its usability and features are limited. The administrator should make sure they enable multiple users and change default passwords.
- An audit feature is supported, but is of a limited nature given the product.
- The product uses a unique syntax where both the left and right control buttons are pressed at the same time to invoke special modes. The notation CTRL (Left), CTRL (Right), X or CTRL | CTRL | X is used to indicate this.

10. ANNEXES

None

11. SECURITY TARGET

Emerson. *Emerson Network Power Secure KM Switch, Security Target*, Document Number HDC11603. Rev 3.18. January 28, 2016

12. GLOSSARY

- **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.
- **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.
- **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.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **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.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

13. BIBLIOGRAPHY

1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012.
2. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012.
3. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012.
4. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 4, September 2012.
5. Emerson. Emerson Network Power Secure KM Switch, Security Target, Document Number HDC11603. Rev 3.18. January 28, 2016
6. CSC Global Cybersecurity, Security Testing & Certification Lab. *Emerson Evaluation Technical Report: Emerson Secure KM Switch*, Document Version 1.0, February 26, 2016
7. CSC Global Cybersecurity, Security Testing & Certification Lab. *Emerson Network Power Secure KM Switch Assurance Activity Report*, Document Version 1.0, February 26, 2016
8. CSC Global Cybersecurity, Security Testing & Certification Lab. *Tests Results Emerson Secure KM*, Document Version 1.2, January 28, 2016