National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Haivision Systems Inc., 4445 Garand,
Montreal, Quebec, Canada H4R 2H9

Makito Video Encoders

Report Number:	**CCEVS-VR-VID10501-2013**
Dated:	**June 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

Table of Contents

Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Haivision Makito 2.1, provided by Haivision Systems, Inc. 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 COACT, Inc. Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in May 2013. The information in this report is largely derived from the associated test reports, all written by COACT, Inc. The evaluation team determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements set forth in the Network Device Protection Profile (NDPP) Version 1.1.

The Target of Evaluation (TOE) is identified as the Makito Video Encoders:

Blades: B-290E-DVI, B-290E-DVI-S, B-290E-HDSDI, B-280E-SDI

Firmware Option: SW-290E-KLV

Chassis: F-280-1, F-290-1, F-290-1DH, F-MB6B-RAC, F-MB6X-RAC, F-MB6B-DC, F-MB6B-MED, F-MB21B-R

Appliances: S-290E-AIR, S-290E-DVI, S-290E-HDSDI, S-280E-SDI

Firmware Version: 2.1.1-3

Each of the Haivision Video Encoders is a full-featured, high-performance IP audio/video encoder that is capable of encoding H.264 video at resolutions of up to 1080p60, with a latency of less than 55 milliseconds. The TOE can also support computer display input at resolutions up to 1920x1080@60 Hz or 1280x1024@75 Hz.

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 3) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 3), as interpreted by the assurance activities contained in the NDPP v1.1. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation and validation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme policies and practices as described on their web site www.niap-ccevs.org.

The validation team provided guidance on technical issues and evaluation processes, and reviewed the individual work units of the ETR and the Assurance Activity reports for the NDPP assurance activities. 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 and test summary reports are consistent with the evidence produced.

The technical information included in this report was obtained from the Haivision Makito 2.1 Security Target and analysis performed by the Validation Team.

1. Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

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	Makito Video Encoders with firmware version 2.1.1-3.	
	Product Reference #	Description
	Blades	
	B-290E-DVI	Makito HD-DVI H.264 Encoder blade
	B-290E-DVI-S	Makito HD-DVI H.264 Encoder blade with serial port
	B-290E-HDSDI	Makito HD-SDI H.264 Encoder blade
	B-280E-SDI	Barracuda SD-SDI H.264 Encoder blade
	Firmware Options	
	SW-290E-KLV	KLV metadata support, a licensable feature providing Key Length Value encoding functionality
	FCO-SV-SW-CONFIG	A specific firmware version can be requested by including this part number in the purchase order.

Item	Identifier	
		Please specify the 2.1.1-3 release as part of the configuration information in order to receive the firmware described in this Security Target.
	Chassis	
	F-280-1	Single-slot Barracuda enclosure with AC power supply
	F-290-1DH	Dual height, single-slot Makito enclosure with AC power supply
	F-290-1	Single-slot Makito enclosure with AC power supply
	F-MB6B-RAC	Second generation 6-slot chassis with redundant AC power supply (can hold any B- blade)
	F-MB6X-RAC	Same as F-MB6B-RAC, but with new power supplies for MakitoX series (can hold any B-blade)
	F-MB6B-DC	Second generation 6-slot chassis with DC power supply (can hold any B- blade)
	F-MB6B-MED	Second generation 6-slot chassis with medical-grade AC power supply (can hold any B- blade)
	F-MB21B-R	Second generation 21-slot chassis with redundant power supplies (can hold any B-blade)
	Appliances	
	S-280E-SDI	Barracuda SD-SDI H.264 Encoder appliance (B-280E-SDI) in single-card enclosure (F-280-1)
	S-290E-HDSDI	Makito HD-SDI H.264 Encoder appliance (B-290EHDSDI) in single-card enclosure (F-290-1)
	S-290E-DVI	Makito HD-DVI H.264 Encoder appliance (B-290EDVI) in single-card enclosure (F-290-1)
	S-290E-DVI-S	Makito HD-DVI H.264 Encoder appliance (B-290EDVI-S) in single-card, dual-height enclosure (F-290-1DH)
	S-290E-AIR	Makito Air Ruggedized HD/SD H.264 Video Encoder with SW-290E-KLV
Protection Profile	*Security Requirements for Network Devices, Version 1.1, 08 June 2012* (including the optional TLS, HTTPS, and SSH requirements)	
Security Target	Haivision Makito 2.1 Security Target, Document Number: HVS-PD-ST-MAK211, Version 1.1, May 29, 2013	
Evaluation Technical Report	Haivision Makito Video Encoders Evaluation Technical Report, May 31, 2013, Document No. F1-0613-001	
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 3	
Conformance Result	CC Part 2 extended, CC Part 3 conformant	

Item	Identifier
Sponsor	Haivision Systems Inc.
Developer	Haivision Systems Inc.
Common Criteria Testing Lab (CCTL)	COACT, Inc., Columbia, MD
CCEVS Validators	Ken Elliott, The Aerospace Corporation Bradford O'Neill, Mitre Corporation

2. Architectural Information

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

2.1 TOE Introduction

The TOE is a full-featured, high-performance IP audio/video encoder that is capable of encoding H.264 video at resolutions of up to 1080p60, with a latency of less than 55 milliseconds. The TOE can also support computer display input at resolutions up to 1920x1080@60 Hz or 1280x1024@75 Hz.

The TOE can take any one of several forms, based on a combination of blades, firmware options, and chassis/appliances described in the tables below. Please note the following:

- Each blade is identical except for the number and type of physical interfaces.
- The KLV firmware option refers to non-TSF related functionality (factory installed).
- Firmware version is 2.1.1-3.
- Chassis serve only to enclose the blades and to provide power distribution.
- Appliances are a combination of one blade in a single-slot enclosure.

The differences in the blades include the number of ports, interfaces, and throughput. Although these blades have different specifications (in terms of performance and capabilities), they all provide the same security functions described in the ST. They are therefore considered to be the same for the purposes of the ST description.

2.2 Physical Boundaries

There is no difference between the products and the TOE. The physical boundary of each product that comprises the TOE is the enclosure.

The TOE relies on external IT entities in the operating environment for its secure management.

The TOE supports syslog and can utilize an external audit server to store audit records.

The TOE supports NTP and must use an external time server to initialize its date and time at startup in order to time stamp audit records, validate certificates, and manage password aging.

A remote administrative user can use a web browser to access the Web GUI interface, or use a telnet or an SSH client to access the CLI. A local administrative user can use a terminal client on the serial port to access the CLI. Neither the web browser or the SSH client is part of the TOE.

The TOE does not support external authentication servers to authenticate administrative users.

3. Security Policy

This section summarizes the security functionality of the TOE:

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

3.1 Security Audit

The TOE is designed to be able to generate audit logs for a wide range of security relevant events. The TOE is configured in the evaluated configuration to send the logs to a designated syslog server.

3.2 Cryptographic Support

The TOE includes Cryptographic functions that provides key management, random bit generation, encryption/decryption, digital signature and secure hashing and asymmetric key generation features in support of higher level cryptographic protocols including TLS, HTTPS, and SSH.

The TOE algorithms were validated through the Cryptographic Algorithm Validation Program (CAVP). The certificate numbers are provided below.

Table 2 - Supported Cryptographic Algorithms

Function	Algorithm	Options	CAVP Cert #
Random Number Generation	[SP 800-90] DRBG	CTR DRBG (AES)	298

Encryption / Decryption	[FIPS Pub 197] AES	128/256 CBC, CTR	2349
Message Digests	[FIPS Pub 180-3]	SHA-1, SHA-2 (256)	2025
Keyed Hash	[FIPS Pub 198] HMAC	SHA-1, SHA-2 (256)	1456
Digital Signature	[FIPS Pub 186-2] RSA	SigGen9.31, SigGenPKCS1.5, SigVer9.31, SigVerPKCS1.5	1232
Asymmetric Key Generation	[FIPS Pub 186-3] RSA	186-3KeyGen: FIPS186-3_Fixed_e , FIPS186-3_Fixed_e_Value PGM(ProbRandom: (2048 , 3072) PPTT:(C.2)	1211

3.3 User Data Protection

There is no private user data per se transiting through the TOE. Users of the TOE are passive viewers/listeners of common media streams (MPEG-TS, RTP, RTMP, or QuickTime) encoded in real-time from the TOE audio, video, and metadata inputs, and transmitted unprotected on the network.

The input signal is the same for all viewers/listeners and is considered to be the organization’s data for which confidentiality, authenticity and integrity is not the responsibility of the TOE. Viewers/listeners of the media streams do not have to be identified users of the TOE. The knowledge of the multicast address (and the protocols) provides access to the content. If RTSP is enabled on the TOE, the knowledge of the URL of the media stream is enough to provide access to it.

3.4 Identification and Authentication

The TSF maintains local administrative user name/password/role databases for interactive management sessions.

Security Administrators manage all administrative users’ account with the CLI account command or the WCI Accounts page. Password policies are managed with the CLI *policy* (password) command or the WCI Policies page.

Password policies are not enforced by the TSF when Security Administrators create accounts or reset the password of other users’ accounts. Instead, the password is forced to expire and the account owner is required to change its password upon next login.

Administrative users can change their own password using the CLI *passwd* command or the WCI My Account page (or their own Account page for Security Administrators), constrained by the password policies.

Administrative users can also manage their SSH authorized public keys using the CLI *pubkey* command or the WCI My Account page (or their own Account page for Security

Administrators). Security Administrators can manage any administrative user's public keys with the CLI *account* command or the WCI Accounts page.

3.5 Security Management

TOE Security Administrators can create login accounts and assign them to one of the following roles: Administrator, Operator, or Guest. The CLI account command or the WCI Accounts page is used to create an administrative user account and assign it a role.

The TOE Administrator role maps to the Security Administrator role described in the security target and the applicable Protection Profile.

The Administrators manage the TSF and the media streams. The Operators manage the media streams, and the Guests can only read the media stream configuration and monitor the status of the TOE.

All roles are permitted to log on the TOE using the CLI or the web interface (WCI), but their actions on the TOE are limited by their role.

3.6 Protection of the TSF

The TSF Data is mostly stored on a flash-memory based Linux file system, in files and databases that are readable and writable by the root user only.

The root account is not used to log in to the TOE and is locked down at the factory.

The ability to manage the TSF data is provided to the Security Administrators through the sudo Linux command for a limited set of operations.

The TOE flash-memory based file system is supported by a micro-SD device that can be ejected if the TOE enclosure is opened. The environment shall then provide physical security to the TOE as stipulated by the A.PHYSICAL assumption.

The firmware is based on the Linux operating system and proprietary applications that can be upgraded from digitally signed packages only.

3.7 TOE Access

The TOE presents a warning and consent message before establishing an interactive session with any user role (Administrator, Operator, or Guest) and terminates the session if it remains idle for a configured period of time.

An interactive session is established either via local CLI using the serial port, or remotely via CLI with SSH or a web browser using HTTPS.

3.8 Trusted Path / Channels

The TSF can be configured to transmit its audit records to a remote audit server. The TSF also supports remote interactive CLI and web interface sessions.

The cryptographic support for the CC evaluated configuration is set with the CLI policy (crypto) command or WCI Policies page. Setting the crypto compliance policy to Makito21st (Makito 2.1 Security Target) sets, upon next reboot, the FIPS mode of operation of the cryptographic module, along with other cryptographic restrictions for TLS, SSH, and HTTPS.

4. Assumptions

The following assumptions about the operational environment are made regarding its ability to provide security functionality.

- **A.NO_GENERAL_PURPOSE** - It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- **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 administrative users are trusted to follow and apply all administrator guidance in a trusted manner.

5. Documentation

The following end user documentation was used as evidence for the evaluation of the Haivision Makito 2.1 Video Encoders.

5.1 Security Target

- Haivision Makito 2.1 Security Target, Document Number: HVS-PD-ST-MAK211, Version 1.1, May 29, 2013

5.2 Guidance Documentation

- Makito 2.1 Hardening Guide, Document Number: HVS-PD-IG-MAK211, Version 1.1, May 29, 2013
- Release Notes - Barracuda, Software Version: 2.1.1, April 8, 2013
- Release Notes - Makito, Software Version: 2.1.1, April 8, 2013
- Barracuda Compact SD H.264 Video Encoder, User’s Guide Version 2.1.1, Document Number: HVS-07BAR-UG01-211, Issue 02, 2013
- Makito Compact HD H.264 Video Encoder User’s Guide Version 2.1.1, Document Number: HVS-07MAK-UG01-211, Issue 02, 2013

6. IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

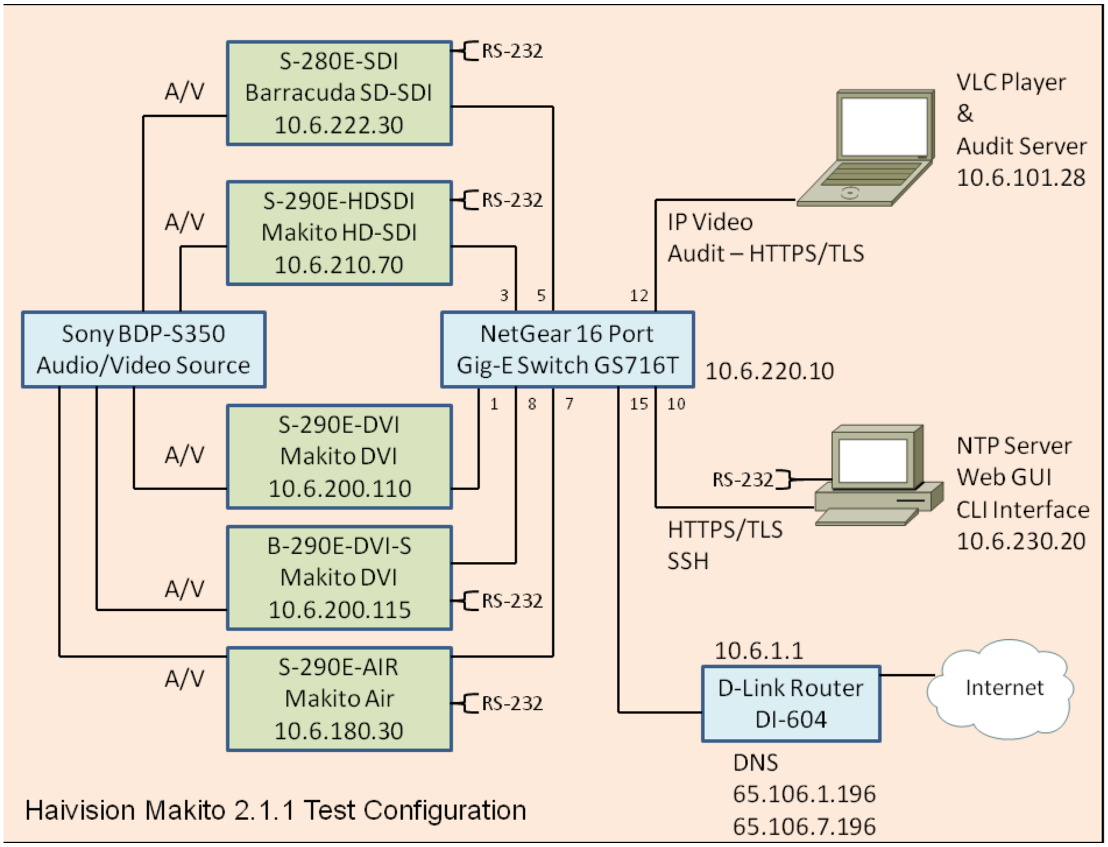
6.1 Developer Testing

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

6.2 Evaluation Team Testing

The evaluation team verified the product according the Makito 2.1 Hardening Guide, Document Number: HVS-PD-IG-MAK211, Version 1.1, May 29, 2013 document and performed the tests and documentation analysis as specified in the NDPP v1.1. These assurance activities are summarized in the Haivision Makito 2.1.1 Test Summary Report, May 30, 2013, Document No. F1-0613-002. The test configuration in the CCTL test lab is shown below.

Figure 1 - Evaluated Test Configuration



7. Evaluated Configuration.

The evaluated configuration, as defined in the Security Target, is Makito Video Encoders including:

Blades: B-290E-DVI, B-290E-DVI-S, B-290E-HDSDI, B-280E-SDI

Firmware Option: SW-290E-KLV

Chassis: F-280-1, F-290-1, F-290-1DH, F-MB6B-RAC, F-MB6X-RAC, F-MB6B-DC, F-MB6B-MED, F-MB21B-R

Appliances: S-290E-AIR, S-290E-DVI, S-290E-HDSDI, S-280E-SDI

Firmware Version: 2.1.1-3

8. Results of the Evaluation

The results of the assurance requirements are summarized in this section. The details of the evaluation results are recorded in the Evaluation Technical Report (proprietary) and Test Summary Report provided by the CCTL. 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 version 3.1 R3 of the CC and the CEM. Additionally the evaluators performed the assurance activities specified in the Network Devices Protection Profile (NDPP). The evaluation determined the Haivision Makito 2.1 Video Encoder TOE to be Part 2 extended, and meets the SARs contained the PP.

Below lists the assurance requirements the TOE was required to be evaluated at Evaluation Assurance Level 1. All assurance activities and work units received a passing verdict. The following components are taken from CC part 3:

- ADV_FSP.1 Basic functional specification
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative user guidance
- ALC_CMC.1 Labeling of the TOE
- ALC_CMS.1 TOE CM coverage
- ASE_CCL.1 Conformance claims
- ASE_ECD.1 Extended components definition
- ASE_INT.1 ST Introduction
- ASE_OBJ.1 Security objectives for the operational environment
- ASE_REQ.1 Stated security requirements
- ASE_TSS.1 TOE summary specification
- ATE_IND.1 Independent testing – conformance
- AVA_VAN.1 Vulnerability analysis

9. Validator Comments / Recommendations

The validators have no comments or specific recommendations

10. Annexes

Not applicable

11. Security Target

Haivision Makito 2.1 Security Target, Document Number: HVS-PD-ST-MAK211, Version 1.1, May 29, 2013

12. 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 as interpreted by the supplemental guidance in the NDPP Assurance Activities to determine whether or not the claims made are justified.

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.

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.

13. Bibliography

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

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

2. Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 3, dated: July 2009.

3. Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 3, dated: July 2009

4. Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation*

Methodology, Version 3.1, Revision 3, dated: July 2009.

5. Information Assurance Directorate, *Protection Profile for Network Devices*, Version 1.1, June 8, 2012
6. COACT, Inc. Haivision Makito Video Encoders Evaluation Technical Report, May 31, 2013, Document No. F1-0613-001 (Proprietary)
7. COACT, Inc. Haivision Makito 2.1.1 Test Summary Report, Document No. F1-0613-002, May 30, 2013
8. Haivision Makito 2.1 Security Target, Document Number: HVS-PD-ST-MAK211, Version 1.1, May 29, 2013