Test Report issued under the responsibility of:

www.nemko.com

TEST REPORT
ETSI EN 303645

Cyber Security for Consumer Internet of Things: Baseline Requirements

Report Number. ..... :	REP110466
Date of issue ..... :	2025. 08. 13.
Total number of pages ..... :	29
Name of Testing Laboratory preparing the Report ..... :	Nemko Korea Co., Ltd. 165-51, Yurim-ro, Cheoin-gu, Yongin-si, Gyeonggi-do, 17042, Korea, Republic of
Applicant's name ..... :	Hanwha Vision Co., Ltd.
Address ..... :	6. Pangyo-ro 319 beon-gil Bundang-gu, seongnam-si, Gyeonggi-do, 13488, Republic of Korea
Test specification:	
Standard ..... :	ETSI-EN-303-645:2020
Test procedure ..... :	CB Scheme
Non-standard test method ..... :	N/A
TRF template used ..... :	IECEE OD-2020-F1:2023, Ed.1.6
Test Report Form No. ..... :	ETSI_EN_303645A
Test Report Form(s) Originator .... :	TÜV NORD CERT GmbH
Master TRF ..... :	2024-02-23

If this Test Report Form is used by non-IECEE members, the IECEE/IEC logo and the reference to the CB Scheme procedure shall be removed.

This report is not valid as a CB Test Report unless signed by an approved IECEE Testing Laboratory and appended to a CB Test Certificate issued by an NCB in accordance with IECEE 02.

General disclaimer:

The test results presented in this report relate only to the object tested.
This report shall not be reproduced, except in full, without the written approval of the Issuing NCB. The authenticity of this Test Report and its contents can be verified by contacting the NCB, responsible for this Test Report.

Test item description ..... :	8MP AI IR Vandal Dome Camera
Trademark(s) ..... :	Hanwha Vision
Manufacturer ..... :	Name: Hanwha Vision Vietnam Company Limited Address: Lot O-2, Que Vo Industrial Zone Expanded Area, Nam Son Ward, Bac Ninh City, Bac Ninh Province, Vietnam
Model/Type reference ..... :	XNV-A9084R
Ratings ..... :	PoE Power Consumption: Maximum 11.2 W, Typical 8.4 W
Version / release ..... :	Software Version: Firmware Platform Version 25.0 / Hardware Version: N/A
	Variants Model: (Software Version: Firmware Platform Version 25.0)

Product Name	**Model**
5MP AI IR Vandal Dome Camera	XNV-A8084R
8MP AI IR Dome Camera	XND-A9084RV
5MP AI IR Dome Camera	XND-A8084RV
8MP AI IR Bullet Camera	XNO-A9084R
5MP AI IR Bullet Camera	XNO-A8084R
8MP AI Box Camera	XNB-A9004
5MP AI Box Camera	XNB-A8004
2MP AI Box Camera	XNB-A6004
Multi-channel Camera	PNM-C19183RVTP
	PNM-C20000QB
	PNM-C32083RQZ
	PNM-C16083RQZ
	PNM-C32083RVQ
	PNM-C16083RVQ
	PNM-C34404RQPZ
5MP AI Box Camera	XNB-A8004B
2MP PTZ Camera	TNP-A6550RW
8MP PTZ Camera	TNP-A9430RW
4MP PTZ Camera	TNP-A7430RW
2MP Dome Camera	QND-C6084R
5MP Dome Camera	QND-C8084R
8MP Dome Camera	QND-C9084R
2MP Vandal Dome Camera	QNV-C6084R
5MP Vandal Dome Camera	QNV-C8084R
8MP Vandal Dome Camera	QNV-C9084R
2MP Fixed Dome Camera	QND-C6014R
	QND-C6024R
2MP Fixed Vandal Dome Camera	QNV-C6014R

	QNV-C6024R
2MP Fixed Bullet Camera	QNO-C6014R
	QNO-C6024R
8MP AI Box Camera	PNB-A9082
	PNB-A9092
8MP AI IR Vandal Dome Camera	PNV-A9082RZ
4MP AI IR Vandal Dome Camera	PNV-A7082RZ
8MP AI IR Dome Camera	PND-A9082RV
4MP AI IR Dome Camera	PND-A7082RV
8MP AI IR Bullet Camera	PNO-A9092R
	PNO-A9082R
4MP AI IR Bullet Camera	PNO-A7082R
8MP AI IR Vandal Dome Camera	XNV-A9085R
5MP AI IR Vandal Dome Camera	XNV-A8085R
8MP AI IR Dome Camera	XND-A9085RV
5MP AI IR Dome Camera	XND-A8085RV
13MP Panoramic Camera	PMN-C13022RV
6MP Fisheye Camera	XNF-A8014R
	XNF-A8014RV
12MP Fisheye Camera	XNF-A9014R
	XNF-A9014RV
2MP AI IR Bullet Camera	XNO-A6084R
2MP AI IR Vandal Dome Camera	XNV-A6084R
2MP AI IR Dome Camera	XND-A6084R
8MP AI Box Camera with ANPR	PNB-A9092LP
8MP AI IR Bullet Camera with ANPR	PNO-A9092RLP

Responsible Testing Laboratory (as applicable), testing procedure and testing location(s):			
☒	**CB Testing Laboratory:**	Nemko Korea Co., Ltd.	
Testing location/ address.....:		165-51, Yurim-ro, Cheoin-gu, Yongin-si, Gyeonggi-do, 17042, Korea, Republic of Korea	
Tested by (name, function, signature).....:		Junbum Kim Evaluator	
Approved by (name, function, signature)...:		Jungmoo Lee Lead Evaluator	
☐	**Testing procedure: CTF Stage 1:**	N/A	
Testing location/ address.....:			
Tested by (name, function, signature).....:			
Approved by (name, function, signature)...:			
☐	**Testing procedure: CTF Stage 2:**	N/A	
Testing location/ address.....:			
Tested by (name + signature).....:			
Witnessed by (name, function, signature) .:			
Approved by (name, function, signature)...:			
☐	**Testing procedure: CTF Stage 3:**	N/A	
☐	**Testing procedure: CTF Stage 4:**	N/A	
Testing location/ address.....:			
Tested by (name, function, signature).....:			
Witnessed by (name, function, signature) .:			
Approved by (name, function, signature)...:			
Supervised by (name, function, signature) :			

List of Attachments (including a total number of pages in each attachment):

1. Attachment 1 (2 pages): Network diagram and photos of appliance

Summary of testing:

-. The evaluation of the device was based on the document and sample, as relevant, provided by manufacturer.
-. All tests were conducted XNV-A9084R
-. The documentation from Hanwha Vision was improved by the Non-Conformity correspondence and test descriptions which verified that various implementations were according to the ETSI/EN 303 645 V2.1.1 (2020-06) standard.
-. The User Manual reference used for the evaluation was:
[Online Help_XND-A9084RV,XND-A8084RV,XNV-A9084R,XNV-A8084R,XNO-A9084R,XNO-A8084R_EN.PDF]
-. This report is not related to KS Q ISO/IEC 17025 and KOLAS accreditation.

The evaluation process has been through the following phases:

1. Document Review Evaluation
2. Test Raport Evaluation
3. Test Demonstration Evaluation

The product has been assessed against all of the 67 provisions in the ETSI EN 303 645, of which:

Pass: 50

Fail Mandatory: 0

Fail Recommended: 8

Not applicable: 9

The product has successfully completed both functional and conceptual evaluations.

Version of software tools used during testing:

Software Tool	Version
Nessus	10.8.5
Wireshark	4.4.7
Nmap	7.95
SSLscan	2.1.5
Hping	3.0.0
TCPDump	4.99.5
Kali linux	6.12.33
binwalk	2.4.3
Burpsuite	2025.6.3

ETSI EN 303 645 is used in conjunction with ETSI TS 103 701 and ETSI TR 103 621.

Tests performed (name of test, test clause and date test performed):	**Testing location: (CBTL, SPTL, CTF, Subcontractor)**
All testing according to this standard tested at:	Nemko Korea Co., Ltd. 165-51, Yurim-ro, Cheoin-gu, Yongin-si, Gyeonggi-do, 17042, Korea, Republic of

Summary of compliance with National Differences

- IECEE Member countries that are also CENELEC members
  Compliance with Group Differences evaluated ☐ **yes** ☐ **No** ☒ N/A
- IECEE Member countries with published National Differences which were evaluated:
- IECEE Member countries that did not publish any National Differences:

To support compliance with published National Differences, attach a compilation of relevant ND and/or GD TRFs to the CB Test Report

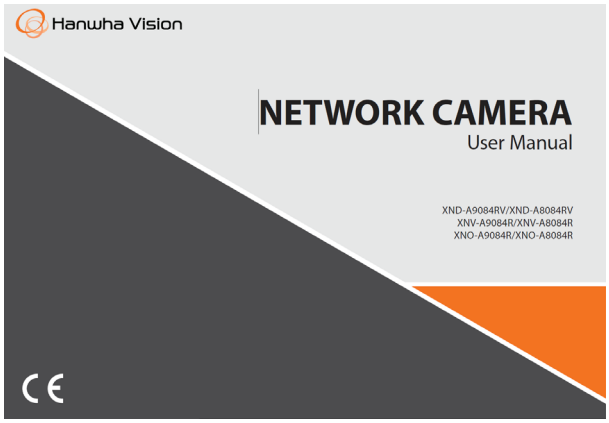
Use of uncertainty of measurement for decisions on conformity (decision rule) :

☒ No decision rule is specified by the IEC standard, when comparing the measurement result with the applicable limit according to the specification in that standard. The decisions on conformity are made without applying the measurement uncertainty ("simple acceptance" decision rule, previously known as "accuracy method").

☐ Other: … (to be specified, for example when required by the standard or client, or if national accreditation requirements apply)

Information on uncertainty of measurement:
The uncertainties of measurement are calculated by the laboratory based on application of criteria given by OD-5014 for test equipment and application of test methods, decision sheets and operational procedures of IECEE.
IEC Guide 115 provides guidance on the application of measurement uncertainty principles and applying the decision rule when reporting test results within IECEE scheme, noting that the reporting of the measurement uncertainty for measurements is not necessary unless required by the test standard or customer.
Calculations leading to the reported values are on file with the NCB and testing laboratory that conducted the testing.

Copy of marking plate:



The artwork below may be only a draft. The use of certification marks on a product must be authorized by the respective NCBs that own these marks.

Test item particulars.....:	
Classification of installation and use.....:	Fixed dome installation, Outdoor, Commercial/Industrial use
Network connection .....:	Ethernet LAN (10/100BASE-T), IPv4/IPv6, TCP/IP, HTTP/HTTPS, RTSP, ONVIF, IEEE 802.1X authentication
Possible test case verdicts:	
- test case does not apply to the test object.....:	N/A
- test object does meet the requirement.....:	P (Pass)
- test object does not meet the requirement.....:	F (Fail)
The status column indicates the status of a provision. The following notations are used:	
- mandatory requirement .....:	M
- recommendation.....:	R
- mandatory requirement and conditional.....:	MC
- recommendation and conditional .....:	RC
The status column indicates the status of a provision. The following conditions are used:	
- passwords are used.....:	(1)
- pre-installed passwords are used.....:	(2)
- software components are not updateable .....:	(3)
- the device is constrained .....:	(4)
- the device is not constrained .....:	(5)
- telemetry data being collected .....:	(6)
- personal data is processed on the basis of consumers' consent.....:	(7)
- the device allowing user authentication .....:	(8)
- the device supports automatic updates and/or update notifications.....:	(9)
- hard-coded unique per device identity is used for security purposes.....:	(10)
- updates are delivered over a network interface...:	(11)
- an update mechanism is implemented .....:	(12)
- debug interface is physically accessible .....:	(13)
Testing.....:	
Date of receipt of test item .....:	2024-11-13
Date (s) of performance of tests.....:	2024-11-14 to 2025-08-08

General remarks:
"(See Enclosure #)" refers to additional information appended to the report. "(See appended table)" refers to a table appended to the report. **Throughout this report a comma / point is used as the decimal separator.**
Manufacturer's Declaration per sub-clause 4.2.5 of IECEE 02:

The application for obtaining a CB Test Certificate includes more than one factory location and a declaration from the Manufacturer stating that the sample(s) submitted for evaluation is (are) representative of the products from each factory has been provided ..... :	☐ **Yes** ☒ **Not applicable**

When differences exist; they shall be identified in the General product information section.

Name and address of factory (ies) ..... :	Name: Hanwha Vision Vietnam Company Limited Address: Lot O-2, Que Vo Industrial Zone Expanded Area, Nam Son Ward, Bac Ninh City, Bac Ninh Province, Vietnam

General product information and other remarks:

Model Differences:
- The representative model, XNV-A9084R, and its variants were confirmed to have no security differences, as verified through the manufacturer's submitted model difference document. All variants use the same Firmware Platform Version 25.0. The models PNM-C32083RQZ, PNM-C16083RQZ, PNM-C32083RVQ, PNM-C16083RVQ, and PNM-C34404RQPZ have identical security features except that Secure Storage is implemented with TPM 2.0.

5	**CYBER SECURITY PROVISIONS FOR CONSUMER IoT**		P
5.1	**No universal default passwords**		P
5.1-1 MC (1)	Where passwords are used and in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user.	Passwords are created by the user Users can set passwords according to the password policy below ※ Password policy 1. Minimum password length - 8 characters: Combination of at least 3 out of 4 types of combination characters - 10 characters: Combination of at least 2 out of 4 types of combination characters 2. Complexity: 1) Combination of at least 2~3 out of 4 types of combination characters according to minimum length 2) Cannot use more than 4 consecutive characters (e.g. 1234, abcd, etc.). - The criteria for consecutive characters are based on ASCII code - 4 consecutive characters for English uppercase letters - 4 consecutive characters for English lowercase letters - 4 consecutive characters for numbers - No special characters - Keyboard layout is not consecutive 3) Cannot use the same character more than 4 times (e.g. !!!!, 1111, aaaa, etc.). 4) Cannot use the same character string as the ID. 5) Cannot use spaces. ※ 4 types of combination characters - English uppercase letters (A~Z), English lowercase letters (a~z), numbers (0~9), 32 special characters ~ ` ! @ # $ % ^ & * ( ) _ - + = { } [ ] | \ ; : ‘ “ < > . , ? /	P
5.1-2 MC (2)	Where pre-installed unique per device passwords are used, these shall be generated with a mechanism that reduces the risk of automated attacks against a class or type of device.	There is no pre-installed unique password. Evaluator's note: Passwords defined by the user.	N/A

5.1-3 M	Authentication mechanisms used to authenticate users against a device shall use best practice cryptography, appropriate to the properties of the technology, risk and usage.	Since the password itself is not transmitted during user authentication and is authenticated using the Digest authentication (RFC-7616) method, the password is safely protected during authentication. When users log in, they can log in via HTTP (port 80)/HTTPS (port 443)/ONVIF (port 80)/RTSP (port 554), and since the TLS option is provided by default for each service, transmission encryption can be applied when using HTTP over TLS and RTSP over TLS. From Non Conformity 5.1-3 Updated to OpenSSL 3.4.0. # openssl version OpenSSL 3.4.0 22 Oct 2024 (Library: OpenSSL 3.4.0 22 Oct 2024) Evaluator's note: From provision 5.4-1 The password for using the service/function within the device is encrypted with a symmetric key encryption algorithm of AES-128 or higher. From provision 5.5-1: TLS 1.2 and TLS 1.3 is used. From provision 5.6-1 HTTP is not enabled by default and can be activated at the user's discretion for compatibility purposes.	P
5.1-4 MC (8)	Where a user can authenticate against a device, the device shall provide to the user or an administrator a simple mechanism to change the authentication value used.	A password change function is provided. Webviewer > Settings > Change Password	P
5.1-5 MC (5)	When the device is not a constrained device, it shall have a mechanism available which makes bruteforce attacks on authentication mechanisms via network interfaces impracticable.	If a user fails to log in 5 consecutive times, their account will be locked for 30 seconds.	P

5.2	Implement a means to manage reports of vulnerabilities		P
5.2-1 M	The manufacturer shall make a vulnerability disclosure policy publicly available. This policy shall include, at a minimum: • contact information for the reporting of issues; and • information on timelines for: 1) initial acknowledgement of receipt; and 2) status updates until the resolution of the reported issues.	We have established a dedicated team (S-CERT) that can respond professionally to security vulnerabilities, and we operate with the goal of responding quickly (analysis and countermeasure preparation, etc.) when vulnerabilities occur. When a security vulnerability related to a product is discovered, S-CERT (secure.cctv@hanwha.com) receives the security vulnerability report along with detailed information such as product information, reproduction method, and symptoms. The Security Breach Incident Response Council is immediately convened to analyze the vulnerability content and impact and prepare the best solution to resolve the problem. Reporters of security vulnerabilities can receive an initial response within 2 business days, and can receive a response regarding the manufacturer's future response measures and plans related to the vulnerability within 10 business days. Website: https://www.hanwhavision.com/ko/support/cybersecurity/	P
5.2-2 R	Disclosed vulnerabilities should be acted on in a timely manner.	The firmware with improved vulnerabilities and the vulnerability details will not be disclosed until 90 days from the date of receipt or a date mutually agreed upon with the reporter. For transparent and efficient management of security vulnerabilities, Hanwha Vision has been participating in the CVE program as an organization that can directly register and manage CVE vulnerabilities as a CNA since September 2023, and is operating a bug bounty program for internal customers. https://www.hanwhavision.com/en/support/cybersecurity/ From Non- Conformity 5.2-2a We are completing it within 90 days from the date the vulnerability was disclosed. However, if additional issues arise within this period, we will complete it and respond by a date mutually agreed upon with the reporter.	P
5.2-3 R	Manufacturers should continually monitor for, identify and rectify security vulnerabilities within products and services they sell, produce, have produced and services they operate during the defined support period.	We collect and analyze not only CVEs of our own products, but also new open source vulnerabilities (known CVEs) that may affect our products, and monitor related open source vulnerabilities. Information on this is provided through weekly mailings. CVEs are collected through https://nvd.nist.gov/vuln.	P

5.3	Keep software updated		P
5.3-1 R	All software components in consumer IoT devices should be securely updateable.	A feature is provided on the webpage to safely update components of the firmware. From non-conformity 5.3-1 All software components are built into a single firmware binary with electronic signature (secure boot, secure update) and firmware encryption, and can be safely updated.	P
5.3-2 MC (5)	When the device is not a constrained device, it shall have an update mechanism for the secure installation of updates.	Secure update via electronic signature is implemented to safely update firmware components, and secure boot is implemented to determine whether the firmware has been tampered with at each boot. If tampering is detected, updates and booting will no longer proceed. In addition, the firmware is encrypted and can only be downloaded through the homepage operated by our company. This provides confidentiality and integrity of the firmware installed on the product. The rollback prevention function will be applied to products subject to this certification to prevent updates to lower versions. Evaluator's note: From provision 5.3-7: The firmware is provided encrypted with AES-256. In addition, a digital signature is included in the firmware, and the signature value is verified during the update, so that users can trust that the firmware has not been tampered with. The digital signature is generated as a private key through a key server, and the public key is safely managed in the Secure element.	P
5.3-3 MC (12)	An update shall be simple for the user to apply.	1. After downloading the firmware from our official website, log in to the product webpage, and then click Settings > System > Upgrade/Restart > Upgrade Upgrade Firmware button. There is no further user intervention required, and the webpage will be reconnected once the upgrade is complete. 2. The user can automatically update the firmware through the cloud service. By navigating to Cloud Portal > Devices > Device Management > Cloud Connector Firmware Update, Device Firmware Update, the user can use the Firmware Update button, and no additional user operation is required.	P
5.3-4 RC (12)	Automatic mechanisms should be used for software updates.	The user can perform automatic updates through the camera’s cloud service.	P

5.3-5 RC (12)	The device should check after initialization, and then periodically, whether security updates are available.	Through the firmware status check function of Wisenet Device Manager, it is possible to verify whether the device firmware is up to date. Evaluator's note: Since this function requires the user to click to check the status, the device does not perform the check after initialization.	F
5.3-6 RC (9, 12)	If the device supports automatic updates and/or update notifications, these should be enabled in the initialized state and configurable so that the user can enable, disable, or postpone installation of security updates and/or update notifications.	The firmware update can be scheduled, and at the specified time the firmware will be automatically downloaded and updated. This feature can be enabled or disabled	P
5.3-7 MC (12)	The device shall use best practice cryptography to facilitate secure update mechanisms.	The firmware is provided encrypted with AES-256. In addition, a digital signature is included in the firmware, and the signature value is verified during the update, so that users can trust that the firmware has not been tampered with. The digital signature is generated as a private key through a key server, and the public key is safely managed in the Secure element. Evaluator's note: From provision 5.3-2 Secure update via electronic signature is implemented to safely update firmware components, and secure boot is implemented to determine whether the firmware has been tampered with at each boot. If tampering is detected, updates and booting will no longer proceed. In addition, the firmware is encrypted and can only be downloaded through the homepage operated by our company. This provides confidentiality and integrity of the firmware installed on the product. The rollback prevention function will be applied to products subject to this certification to prevent updates to lower versions.	P

5.3-8 MC (12)	Security updates shall be timely.	The security vulnerability reporter will receive an initial response within 2 business days, and a response regarding the manufacturer's future response measures and plans related to the vulnerability within 10 business days. The firmware with improved vulnerabilities and the vulnerability information will be provided within 90 days of receipt or by a date mutually agreed upon with the reporter, and will not be disclosed until provided. https://www.hanwhavision.com/en/support/cybersecurity/ The development team is responsible for firmware releases, and a separate SQE team is responsible for testing. Once the security changes are verified, they will be updated on the offWicial website.	P
5.3-9 RC (12)	The device should verify the authenticity and integrity of software updates.	The firmware components can be securely updated through a secure update mechanism implemented using digital signatures, and secure boot is implemented to verify the integrity of the firmware at every boot. If any tampering is detected, the update and boot process will be halted. In addition, the firmware is encrypted and can only be downloaded from our official website. This ensures the confidentiality and integrity of the firmware installed on the product. The authenticity of secure boot is verified using a public key pre-written into OTP for signature verification, while the authenticity of secure update is verified using a public key protected by a Secure Element. From Non-Conformity 5.3-9a 1) Public key exchange for firmware transmission: During firmware updates, the public key is exchanged over HTTPS (HTTP over TLS) and is used for symmetric key exchange for encrypted firmware transmission. ※ The HTTPS option is enabled by default. 2) Public keys used for secure boot and secure update: The RSA key pair is generated in the initial key server, and the private key is structured so that it cannot be exported externally under any circumstances. During production, the public key is injected into the product with the build firmware. - Secure boot: Public key injected into OTP - Secure update: Public key injected into the Secure Element	P

5.3-10 M (11, 12)	Where updates are delivered over a network interface, the device shall verify the authenticity and integrity of each update via a trust relationship.	'Secure update and secure boot through electronic signature are implemented to ensure safe use of firmware components, and the electronic signature value is verified at each update and boot to determine whether the firmware has been tampered with. If there is no problem after verifying the electronic signature value, the update and boot will begin, and if tampering is confirmed, the update and boot will no longer proceed. From Non-Conformity 5.3-10a 1) Public key exchange for firmware transmission: Public keys are exchanged via HTTPS (HTTP over TLS) when updating firmware, and are used to exchange symmetric keys for firmware transmission encryption. ※ The HTTPS option is initially activated. 2) Public key used by Secure Boot and Secure Update: An RSA KEY pair is generated within the initial key server, and the private key is structured so that no one can export it to the outside. The public key is injected into the product as a build firmware during production. - Secure Boot: Injected into OTP - Secure Update: Injected into Secure Element	P
5.3-11 RC (12)	The manufacturer should inform the user in a recognizable and apparent manner that a security update is required together with information on the risks mitigated by that update.	If a security vulnerability occurs, the reason why a security update is required and the patched firmware version can be checked through the RSS Feed function.	P
5.3-12 RC (12)	The device should notify the user when the application of a software update will disrupt the basic functioning of the device.	When updating through the device's cloud service, if the update interferes with the basic functions of the camera, a warning message will be displayed. When the user clicks Cloud Portal > Devices > Device Information > Update available here, a popup will appear.	P
5.3-13 M	The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period.	In accordance with the long-term firmware support policy, we support firmware updates in stages. We actively support firmware updates for up to two years after the product launch to improve security vulnerabilities related to access control and video information protection. We provide firmware updates to reflect improvements to security vulnerabilities reported by external organizations or known issues with potential attack potential from two years to the end of production. For up to five years after the product is discontinued, we provide enhanced security firmware to maintain security stability in the event of a serious security vulnerability.	P

5.3-14 RC (3, 4)	For constrained devices that cannot have their software updated, the rationale for the absence of software updates, the period and method of hardware replacement support and a defined support period should be published by the manufacturer in an accessible way that is clear and transparent to the user.	This is not a constrained device (the device itself has limited power/memory/network bandwidth, etc.) Evaluators note: Device is not a constrained device.	N/A
5.3-15 RC (3, 4)	For constrained devices that cannot have their software updated, the product should be isolable and the hardware replaceable.	This is not a constrained device (the device itself has limited power/memory/network bandwidth, etc.) Evaluators note: Device is not a constrained device.	N/A
5.3-16 M	The model designation of the consumer IoT device shall be clearly recognizable, either by labelling on the device or via a physical interface.	There is a label for the product model under the device, and the model name can be checked at the top of the web viewer.	P
5.4	**Securely store sensitive security parameters**		P
5.4-1 M	Sensitive security parameters in persistent storage shall be stored securely by the device.	User authentication information is encrypted, and the encryption key is managed by Secure Element. 1. The login account password for web viewer / RTP, RTSP / ONVIF streaming is encrypted with a symmetric key encryption algorithm of AES-128 or higher or a hash encryption algorithm of SHA256 or higher. 2. The password for using the service/function within the device is encrypted with a symmetric key encryption algorithm of AES-128 or higher. - SNMPv3 password - SDCARD encryption password - NAS / DDNS / 802.1x / SNMP / FTP password - Password used to encrypt the configuration file when exporting the configuration file	P

5.4-2 MC (10)	Where a hard-coded unique per device identity is used in a device for security purposes, it shall be implemented in such a way that it resists tampering by means such as physical, electrical or software.	The Subject Name of the device certificate contains the device's unique MAC information, and is signed by Hanwha Techwin/Hanwha Vision's private Root CA certificate to ensure authenticity and integrity. The device certificate/private key is provided as RSA-2048 bit.	P
5.4-3 M	Hard-coded critical security parameters in device software source code shall not be used.	The use of hard-coded CSP (private key, secret key, password) in the source code is prohibited during operation, and important information is managed separately through Secure Element, not the source code. Important information is to be safely injected during the manufacturing process. From Non-Conformity 5.4-3 Private keys, secret keys, and passwords are not hardcoded.	P
5.4-4 M	Any critical security parameters used for integrity and authenticity checks of software updates and for protection of communication with associated services in device software shall be unique per device and shall be produced with a mechanism that reduces the risk of automated attacks against classes of devices.	The CSP (private key, secret key, password) used in the product is unique to each device. The secret key and private key are generated with a safe key length and randomness and injected into the product. The secret key uses AES 128 bits or higher, and the private key uses RSA 2048 bits or higher. For reference, the public key is used for secure update and secure boot signature verification. (※ The CSP used for secure update and secure boot verification must be unique for each device and must be generated safely, but this provision can be satisfied when the public key is used for secure update verification.) Evaluator's note: From test scenario the key generation is verified. 1. create privatekey openssl genrsa -out camera-firmsign-basic-priv_0.key 2048 2. create publickey (to privatekey) openssl rsa -in camera-firmsign-basic-priv_0.key -pubout > camera-firmsign-basic-pub_0.pem	P

5.5	Communicate securely		P
5.5-1 M	The consumer IoT device shall use best practice cryptography to communicate securely.	1. When transmitting and receiving video using a web viewer, apply encrypted communication based on HTTPS/WSS 2. When transmitting and receiving video between devices by connecting a storage device/SSM+WisenetViewer to the camera, apply encrypted communication based on RTSP over HTTPS 3. When transmitting and receiving video between devices by connecting a mobile app to the camera, apply encrypted communication based on RTSP over HTTPS or SRTP When applying TLS, the versions used are TLS 1.2 and 1.3, and provide secure Cipher suites to provide confidentiality and integrity of important information during communication. In addition, mutual authentication function is provided between our devices, enabling end-to-end identity verification during TLS communication. From Non-Conformity 5.5-1 Updated to OpenSSL 3.4.0. # openssl version OpenSSL 3.4.0 22 Oct 2024 (Library: OpenSSL 3.4.0 22 Oct 2024)	P
5.5-2 R	The consumer IoT device should use reviewed or evaluated implementations to deliver network and security functionalities, particularly in the field of cryptography. Reviews and evaluations can involve an independent internal or external entity.	We use the open source library OpenSSL for TLS communication and encryption key generation, but we do not conduct a separate cryptographic review of the library. Our development code is checked for and improved for security vulnerabilities through the commercial static analysis tool Coverity, and developer peer review is performed.	P
5.5-3 R	Cryptographic algorithms and primitives should be updateable.	Firmware updates are available, so encryption algorithms can be updated as needed (e.g. if encryption is deemed weak, it can be deleted/modified via firmware update).	P
5.5-4 R	Access to device functionality via a network interface in the initialized state should only be possible after authentication on that interface.	All network interfaces are inaccessible to the device right away when initialized. Access is only possible after setting a password through the web viewer and passing authentication on the interface.	P

5.5-5 M	Device functionality that allows security-relevant changes in configuration via a network interface shall only be accessible after authentication. The exception is for network service protocols that are relied upon by the device and where the manufacturer cannot guarantee what configuration will be required for the device to operate.	When changing security-related functions of the environment configuration via the network interface, access is only possible after authentication. ※ For example, changing passwords, setting permissions, configuring network keys, etc.	P
5.5-6 R	Critical security parameters should be encrypted in transit, with such encryption appropriate to the properties of the technology, risk and usage.	The encryption protocols used when transmitting CSP via a remote network interface are as follows. (※ Remote shell access such as Telnet or SSH is not provided) HTTPS (with TLS 1.2/1.3), RTSP over HTTPS (with TLS 1.2/1.3), SRTP-based encrypted communication The versions used when applying TLS are TLS 1.2 and 1.3, and provide secure cipher suites to provide confidentiality and integrity of important information during communication. Encryption algorithms deemed vulnerable (such as RC4, DES, 3DES, MD5, etc.) are not used. However, MD5-based Digest used in RFC-7616 is an exception because it is an ONVIF (surveillance camera standard protocol, RFC-2617) protocol.	P

5.5-7 M	The consumer IoT device shall protect the confidentiality of critical security parameters that are communicated via remotely accessible network interfaces.	The encryption protocols used when transmitting CSP via a remote network interface are as follows. (※ Remote shell access such as Telnet or SSH is not provided) HTTPS (with TLS 1.2/1.3), RTSP over HTTPS (with TLS 1.2/1.3), SRTP-based encrypted communication The versions used when applying TLS are TLS 1.2 and 1.3, and provide secure cipher suites to provide confidentiality and integrity of important information during communication. Encryption algorithms deemed vulnerable (such as RC4, DES, 3DES, MD5, etc.) are not used. However, MD5-based Digest used in RFC-7616 is an exception because it is an ONVIF (surveillance camera standard protocol, RFC-2617) protocol. From Non-Conformity 5.5-1 Updated to OpenSSL 3.4.0. # openssl version OpenSSL 3.4.0 22 Oct 2024 (Library: OpenSSL 3.4.0 22 Oct 2024)	P

5.5-8 M	The manufacturer shall follow secure management processes for critical security parameters that relate to the device.	To ensure the security of the encryption algorithm, the encryption key or passphrase is safely generated, used, updated, distributed, destroyed, stored, and transmitted. - The private key storage for secure boot and secure update is accessible only to authorized users, and is stored and used so as not to be exposed to the outside. (Accessible to the key server only in the CI environment) - The device certificate and private key are generated through the certificate generation server, and the manufacturing line connects to the certificate generation server, in an encrypted state for each device, and then decrypts it in the device and then encrypts it and stores it in the Secure Element. - Encryption is applied to the OTP area or Secure Element in the SOC and stored. From Non-Conformtiy 5.5-8 The private key managed by the key server is managed (stored) by configuring the key server in a virtual environment for creating electronic signatures for secure boot and secure update, and if the key needs to be destroyed, it is destroyed by deleting the activated virtual environment. The corresponding public key is safely stored in the camera's secure storage and is used to verify the electronic signature included in the firmware. The SSL certificate/private key used for TLS communication is uniquely generated and signed for each device through Hanwha Vision Root CA, and the existing device certificate/private key is destroyed when the updated device certificate/private key is inserted. Important information (device certificate/private key, SMTP, FTP server access password, etc.) stored in the camera is encrypted and stored using the TPM's secret key.	P
5.6	**Minimize exposed attack surfaces**		P
5.6-1 M	All unused network and logical interfaces shall be disabled.	The purpose of port usage is as follows. 80/tcp: When connecting to HTTP with the HTTPS option activated, Redirection to HTTPS and HTTP port used when the HTTP option is activated 443tcp: HTTP port used when the HTTPS option is activated 554/tcp: RTSP port used 3702/udp: Used for competitor/our camera discovery in ONVIF 7701/udp: Used for our camera discovery purposes	P

5.6-2 M	In the initialized state, the network interfaces of the device shall minimize the unauthenticated disclosure of security-relevant information.	All products are checked for security-related information that may be exposed through the network interface without authentication in the initialization state. ※ Kernel or open source version information, device environment configuration information, etc.	P
5.6-3 R	Device hardware should not unnecessarily expose physical interfaces to attack.	When the camera cover is removed, the JTAG and UART interfaces are exposed on the PCB. Evaluator's note: Interfaces are not physically accessible.	P
5.6-4 MC (13)	Where a debug interface is physically accessible, it shall be disabled in software.	Both JTAG and UART are enabled, but UART is protected by account authentication and JTAG by entering a password key. From provision 5.6-3 Interfaces are not physically accessible. Evaluator's note: Both JTAG and UART are enabled, but UART is protected by account authentication and JTAG by entering a password key. Also Interfaces are not physically accessible.	P
5.6-5 R	The manufacturer should only enable software services that are used or required for the intended use or operation of the device.	Only services required for the intended use/operational purpose are enabled by default. From Non-Conformity 5.6-1 HTTPS is set as default when initialized. Currently, the initially open ports are 80, 443, 554, 8587, and port 8587 will be deleted during mass production. The purpose of port usage is as follows. 80: When connecting to HTTP with the HTTPS option activated, Redirection to HTTPS and HTTP port used when the HTTP option is activated 443: HTTP port used when the HTTPS option is activated 554: RTSP port used	P
5.6-6 R	Code should be minimized to the functionality necessary for the service/device to operate.	Unnecessary codes in services/devices are removed. Unused codes are detected using commercial static analysis tools (Coverity).	P

5.6-7 R	Software should run with least necessary privileges, taking account of both security and functionality.	Daemon/process runs with root privileges. From Non-Conformity 5.6-7 User/Guest permissions are all disabled before being granted by an administrator. User permissions have only the minimum permissions of administrator permissions (excluding adding users), profile settings, video settings, focus settings, camera settings, and audio IN/OUT. Guests only have the right to view the live screen.	P
5.6-8 R	The device should include a hardware-level access control mechanism for memory.	No hardware level (CPU) memory access control features are used. Evaluator's note: No hardware-level access control mechanism	F
5.6-9 R	The manufacturer should follow secure development processes for software deployed on the device.	We are conducting security checks/security verification activities according to our development process. We are conducting code reviews during the development stage and conducting regular penetration tests.	P
5.7	**Ensure software integrity**		P
5.7-1 R	The consumer IoT device should verify its software using secure boot mechanisms.	Secure update and secure boot through electronic signature are implemented to ensure safe use of firmware components, and the electronic signature value is verified at each update and boot to determine whether the firmware has been tampered with. If there is no problem after verifying the electronic signature value, the update and boot will begin, and if tampering is confirmed, the update and boot will no longer proceed.	P
5.7-2 R	If an unauthorized change is detected to the software, the device should alert the user and/or administrator to the issue and should not connect to wider networks than those necessary to perform the alerting function.	If the product detects tampering with the firmware during secure boot, the booting will not occur. There is no separate function to notify the administrator or user. If the product detects tampering with the firmware during secure update, the update will fail and the original version of the firmware will operate. Evaluator's note: No alert the user and/or administrator.	F
5.8	**Ensure personal data is secure**		P
5.8-1 R	The confidentiality of personal data transiting between a device and a service, especially associated services, should be protected, with best practice cryptography.	No personal information is specifically transmitted to the cloud when the device and cloud service are connected. Evaluator's note: No personal data, see provision 5.8-2 for sensitive personal data	P

5.8-2 M	The confidentiality of sensitive personal data communicated between the device and associated services shall be protected, with cryptography appropriate to the properties of the technology and usage.	When a device and cloud service are connected, sensitive personal information (video) transmitted to the cloud is set to Secure by default, with HTTPS and TLS (TCP over TLS, MQTT over TLS) options used. Refer to the link below> https://support.hanwhavisionamerica.com/hc/en-us/articles/26365028589211-Cloud-Solution-What-are-the-network-requirements-for-Hanwha-Vision-Cloud	P
5.8-3 M	All external sensing capabilities of the device shall be documented in an accessible way that is clear and transparent for the user.	External detection function: Image sensor, built-in microphone, external microphone connection function It provides functions related to video and microphone settings, and the voice recording function is disabled by default Related setting functions are guided to users through "online help" Settings > Video and Audio > Video Settings / Audio Settings Evaluator's note From Online help Audio setup Pg.28 Camera setup Pg.32	P
5.9	**Make systems resilient to outages**		P
5.9-1 R	Resilience should be built in to consumer IoT devices and services, taking into account the possibility of outages of data networks and power.	It is difficult to provide system resilience in the event of network and power outages, as there is no separate standby power supply. Evaluator's note: No resilience built in to device.	F
5.9-2 R	Consumer IoT devices should remain operating and locally functional in the case of a loss of network access and should recover cleanly in the case of restoration of a loss of power.	The network operates on PoE, so if the network is disconnected, power loss occurs, and local operation is not possible when power is lost. When power is supplied again, it can be operated again from the previous saved state after reboot. Evaluator's note: Device is not remain operating and locally functional.	F
5.9-3 R	The consumer IoT device should connect to networks in an expected, operational and stable state and in an orderly fashion, taking the capability of the infrastructure into consideration.	Surveillance cameras are mainly used in closed networks, and are designed and implemented to support stable network operation even when used in public networks. ※ Compliance with standards for network connection (initialization/termination) ※ Protection against simultaneous mass reconnection requests	P

5.10	**Examine system telemetry data**		N/A
5.10-1 RC (6)	If telemetry data is collected from consumer IoT devices and services, such as usage and measurement data, it should be examined for security anomalies.	We treated it as N/A because we do not collect telemetry data. Evaluator's note: No telemetry data is collected.	N/A
5.11	**Make it easy for users to delete user data**		P
5.11-1 M	The user shall be provided with functionality such that user data can be erased from the device in a simple manner.	You can easily delete user data through factory reset. This may include user accounts and user information (passwords, keys, configuration information, etc.) added by the administrator. Settings > Factory Reset	P
5.11-2 R	The consumer should be provided with functionality on the device such that personal data can be removed from associated services in a simple manner.	Appropriate security options are provided as Secure by default, and matters affecting the operating environment (e.g. compatibility items) are provided as a hardening guide, allowing users to decide with security in mind. There is no personal information stored on the device or stored in the cloud when the device is connected to a cloud service. Evaluator's note: There is no functionality on the device such that personal data can be removed from associated services	F
5.11-3 R	Users should be given clear instructions on how to delete their personal data.	Not supported. Evaluator's note: Not supported.	F
5.11-4 R	Users should be provided with clear confirmation that personal data has been deleted from services, devices and applications.	Not supported. Evaluator's note: Not supported.	F

5.12	**Make installation and maintenance of devices easy**		P
5.12-1 R	Installation and maintenance of consumer IoT should involve minimal decisions by the user and should follow security best practice on usability.	Appropriate security options are provided as Secure by default, and matters affecting the operating environment (e.g. compatibility items) are provided as a hardening guide, allowing users to decide with security in mind. From Non-Conformity 5.12-1 The following security features are provided by default on the device without any separate settings for the user: - Force complex password settings - Remove initial password - Restrict input in case of consecutive password failures - Disable remote services (Telnet, SSH) - Encrypt environment setting information - Encrypt firmware and secure update - Watermarking and encryption of extracted video formats - Maintain logs during initialization - Non-Plug-in web viewer based on HTML5 streaming - Individual device authentication (device/user authentication) - Disable SUNAPI/ONVIF in factory default state - Secure Boot	P
5.12-2 R	The manufacturer should provide users with guidance on how to securely set up their device.	Appropriate security options are provided as Secure by default, and matters affecting the operating environment (e.g. compatibility items) are provided as a hardening guide, allowing users to decide with security in mind.	P
5.12-3 R	The manufacturer should provide users with guidance on how to check whether their device is securely set up.	Appropriate security options are provided as Secure by default, and matters affecting the operating environment (e.g. compatibility items) are provided as a hardening guide, allowing users to decide with security in mind.	P
5.13	**Validate Input Data**		P
5.13-1	The consumer IoT device software shall validate data input via user interfaces or transferred via Application Programming Interfaces (APIs) or between networks in services and devices.	Data input verification is being conducted using the Fuzzing Testing Tool or Manual TC. From Non-Conformity 5.13-1 We provide the user interface of the product web page (Web viewer) and the API of SUNAPI/ONVIF. We verify all data that can be input from the web page and API. As a verification method, we test injection attacks or forgery attacks on secure coding and API through Coverity (commercial static analysis) tool.	P

6	DATA PROTECTION PROVISIONS FOR CONSUMER IoT		N/A
6.1 M	The manufacturer shall provide consumers with clear and transparent information about what personal data is processed, how it is being used, by whom, and for what purposes, for each device and service. This also applies to third parties that can be involved, including advertisers.	We do not process information that is judged to be personal data. Evaluator's note: This product is only used locally, and the recorded video is also processed solely by the user on the local device. No personal data is collected, and since the video is not processed by any related services, it is marked as N/A.	N/A
6.2 MC (7)	Where personal data is processed on the basis of consumers' consent, this consent shall be obtained in a valid way.	We do not process information that is judged to be personal data. Evaluator's note: This product is used only locally, and real-time video is also processed solely by the user on the local system. No other personal information is collected, and since the video is not processed by related services, it is marked as N/A.	N/A
6.3 M	Consumers who gave consent for the processing of their personal data shall have the capability to withdraw it at any time.	We do not process information that is judged to be personal data. Evaluator's note: This product is used only locally, and real-time video is also processed solely by the user on the local system. No other personal information is collected, and since the video is not processed by related services, it is marked as N/A.	N/A
6.4 RC (6)	If telemetry data is collected from consumer IoT devices and services, the processing of personal data should be kept to the minimum necessary for the intended functionality.	We treated it as N/A because we do not collect telemetry data. Evaluator's note: No telemetry data is collected	N/A
6.5 MC (6)	If telemetry data is collected from consumer IoT devices and services, consumers shall be provided with information on what telemetry data is collected, how it is being used, by whom, and for what purposes.	We treated it as N/A because we do not collect telemetry data. Evaluator's note: No telemetry data is collected	N/A

List of test equipment used:

N/A

A completed list of used test equipment shall be provided in the Test Reports when a Customer's Testing Facility according to CTF stage 1 or CTF stage 2 procedure has been used.

Note: This page may be removed when CTF stage 1 or CTF stage 2 are not used. See also clause 4.8 in OD 2020 for more details.

Clause	Measurement / testing	Testing / measuring equipment / material used, (Equipment ID)	Range used	Last Calibration date	Calibration due date

Statement of Measurement Uncertainty

N/A

The Test Report shall include a statement concerning the uncertainty of the measurement systems used for the tests conducted when it is required by the standard, client or other authorities.
In such cases, the table below may be used for reporting U of M.

(This page may be removed from the final Test Report when not required. See also clause 4.8 in OD 2020 for more details.)

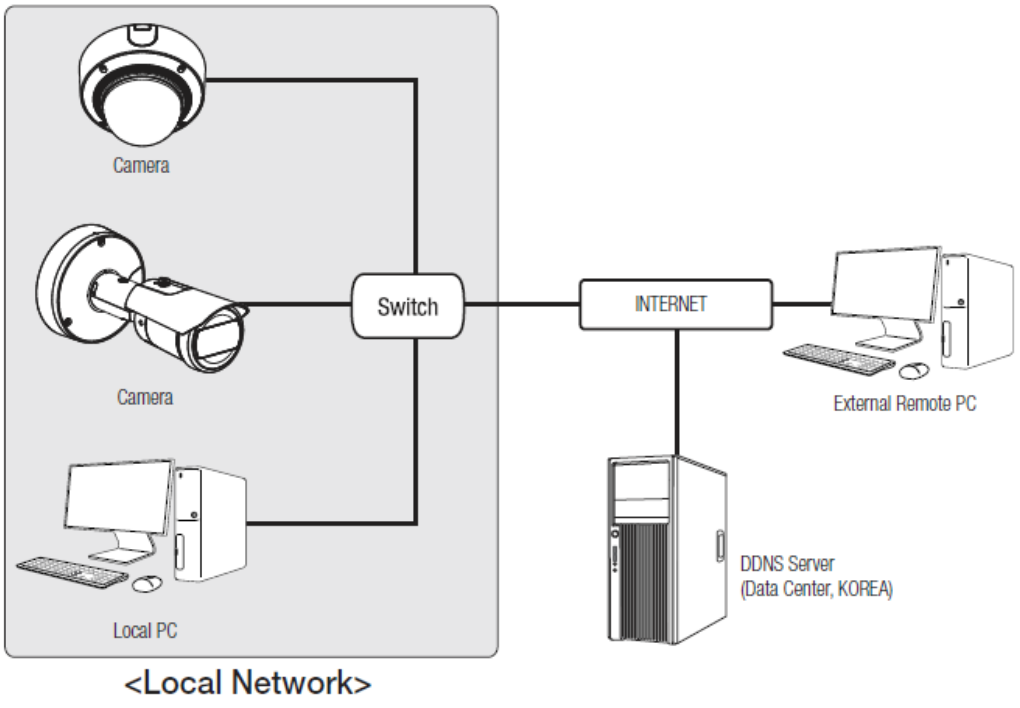
Clause #	Parameter/ Measurement / test method	Requirement % or k	Calculated U of M*

*Note: Calculations leading to the reported value are on file with the NCB

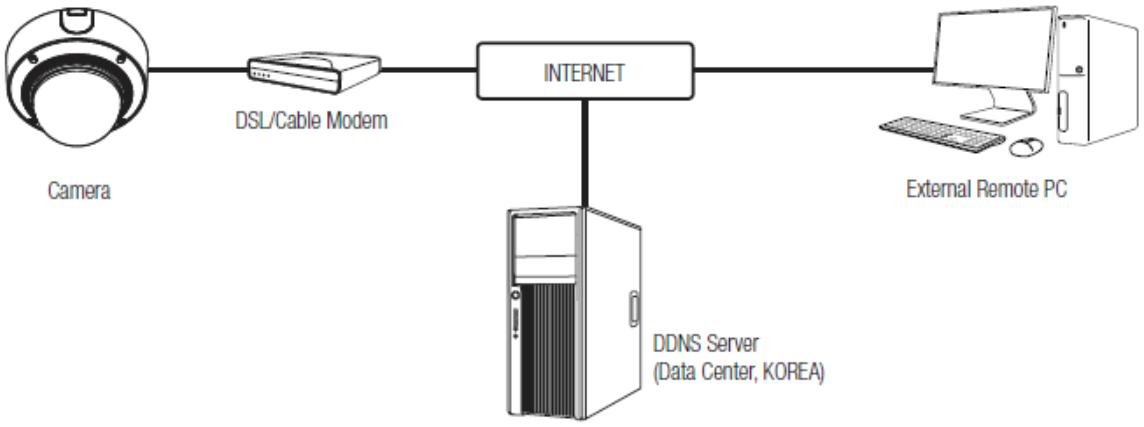
= END OF REPORT =

ATTACHMENT 1 (Network diagram and photos of appliance)

< Network diagram >



<Local Network>



ATTACHMENT 1 (Network diagram and photos of appliance)

< Overview 1 >

< Overview 2 >

= END OF ATTACHMENT 1 REPORT =