TAICS

TAICS TS-0015-4(E) v1.0:2019

Cybersecurity Test Specification for Video Surveillance System-Part 4: Network Attached Storage

2019/05/30

社團法人台灣資通產業標準協會

Taiwan Association of Informationand Communication Standards

Cybersecurity Test Specification for Video Surveillance System- Part 4: Network Attached Storage

Published Date: 2019/05/30

Approved Date: 2018/05/30

Acknowledgements

This specification is formulated by the TAICS-TC5 Network and Information Security Technical Committee.

TC5 President: Kuang-Chun Hung, General Manager, Onward Security Inc.

TC5 Vice President: Cheng-Yu Tsai, Section Chief, Institute for Information Industry

TC5 IoT Security Working Group Leader: Dr. Chuan-Kai Kao, Section Chief, Institute for Information Industry

The list of association members participating in this specification formulation is as follows:

National Chung-Shan Institute of Science and Technology, Industrial Technology Research Institute, Electronics Testing Center, Taiwan, Institute for Information Industry, Telecom Technology Center, Chunghwa Telecom, D-Link Corporation, Onward Security, HTC Corporation, Digicentre Company Limited, National Central University, A Test Lab Technology Corporation, Synology Inc., Trend Micro Inc., Gapertise Inc. and ArcRan Inc.

This specification is supported by the National Communications Commission and Industrial Development Bureau, MOEA, R.O.C..

Contents

Foreword

This is an industry specification regulated and published by the Taiwan Association of Information and Communication Standards (TAICS) with the approval of the TAICS council.

This specification does not suggest all the safety precautions. The related safety maintenance and health operations shall be established and the relevant regulations shall be obeyed before applying this specification.

Part of this specification may involve patents, trademarks, and copyrights. The association is not responsible for the identification of any patents, trademarks, and copyrights.

Introduction

Due to frequent occurrences of cybersecurity issues of video surveillance systems recent years, comprehensive quality improvement of cybersecurity has become a major task for Industrial Development Bureau of MOEA. In order to elevate product development competency, ensure the quality of video surveillance related devices and cascade local industries with global marketplace, planning and implementation of a series of video surveillance system cybersecurity standards, in referring to both national and international up-to-date cybersecurity standards and/or regulations, has thus been initiated.

"Cybersecurity Test Specification for Video Surveillance System- Part 4: Network Attached Storage" (hereafter referred to as "this/the specification") is formulated by TAICS, in accordance with "TAICS TS-0014-4 Cybersecurity Standard for Video Surveillance System- Part 2: Network Attached Storage"[1] and in parallel with "TAICS TS-0015-1 Cybersecurity Test Specification for Video Surveillance System – Part 1: General Requirements", as the technical guidance for the devices manufacturers, system integrators and IoT cybersecurity testing laboratories. This specification specifies all related test items, test conditions, test methods and its respective criteria.

1. Scope

This specification is applicable to network attached storage in video surveillance systems (See Figure 1).

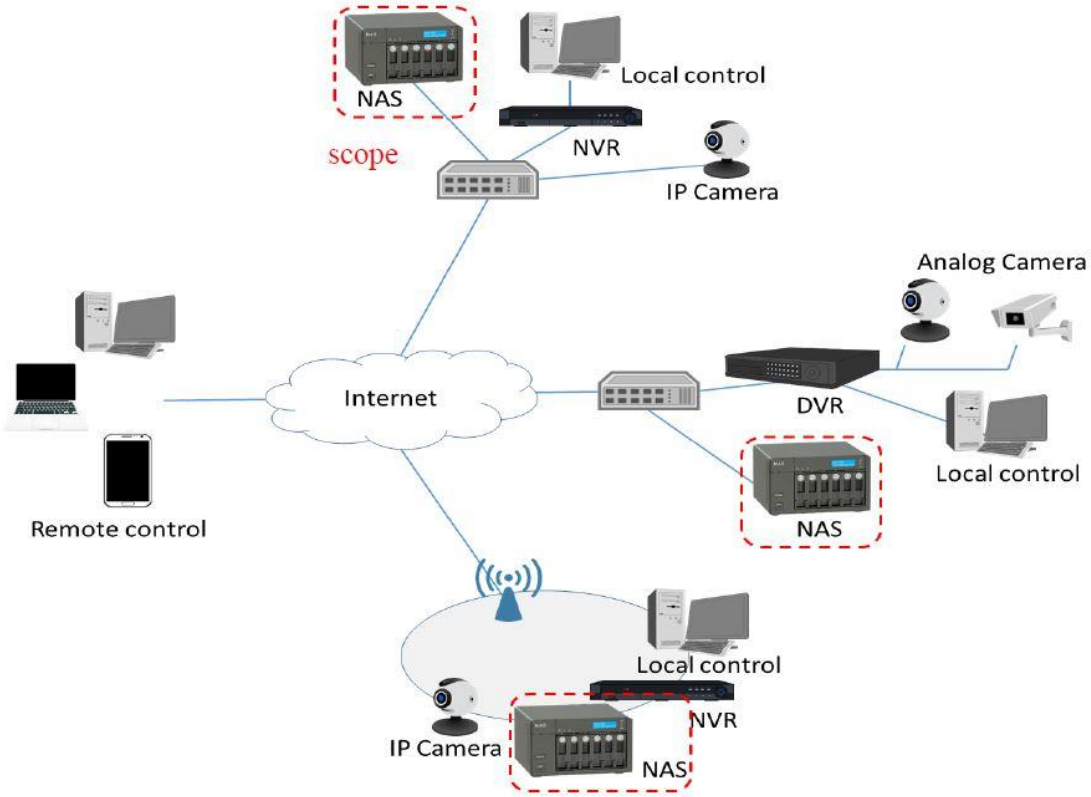

Figure 1 Scope

2. Normative Reference

The following documents are referred to in the text in such a way that some or all of their content constitutes the requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

(1) ANSI/CAN/UL 2900-1 Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements

(2) CNS 27001:2013 Information Technology-Security Technology-Information Security Management System- Requirements

(3) NIST SP 800-92 Guide to Computer Security Log Management

(4) TAICS TS-0015-1 v1.0:2018 Cybersecurity Test Specification for Video Surveillance System- Part 1: General Requirements

3. Terms and Definitions

All terms defined within “TAICS TS-0014-4 v 1.0: 2019 Cybersecurity Standard for Video Surveillance System- Part 4: Network Attached Storage” shall be applicable to the specification.

4. Test Items by Security Levels

Within this section, all security test items shall be defined and categorized in accordance with each individual section of “TAICS TS-0014-4 Cybersecurity Standard for Video Surveillance System- Part 4: Network Attached Storage”, respectively.

Test items by security levels are defined in Table 1, where the first column refers to security aspects, namely (1) physical security, (2) system security, (3) communication security, (4) authentication and authorization mechanism security, (5) privacy protection and (6) application security. The second column refers to the security test requirements in each security aspect. The third column refers to security levels, each of which is a combination of test items that must be executed to cope with various security risks.

Security levels are defined in accordance with (1) its severity of risk impact and (2) the complexity for realization and are categorized into three levels. Products shall fulfill the requirements of lower levels before upgrading to higher levels.

Table 1 Test items by security levels

Security Aspects	Security Requirements	Security Levels		
		Level 1	Level 2	Level 3
Physical Security	5.1.1. Access Control of Physical Interfaces	-	-	-
	5.1.2. Warning of Physical Abnormal Behavior	-	5.1.2.2	-
	5.1.3. Physical Protection	-	-	-
	5.1.4. Secure Boot	-	-	-
	5.1.5. Physical Backup	5.1.5.1	5.1.5.2	5.1.5.3
System Security	5.2.1. Operating System and Security of Network Services	-	-	-
	5.2.2. Security of Network Service Ports	-	-	-
	5.2.3. Update Security	-	-	-

Security Aspects	Security Requirements	Security Levels		
		Level 1	Level 2	Level 3
	5.2.4. Security of Sensitive Data in Storage	-	-	-
	5.2.5. Security of Website Management Interface	-	-	-
	5.2.6. Security of Management Applications	-	-	-
	5.2.7. Logs and Warnings	5.2.7.2	-	-
	5.2.8. Security of Storage	-	5.2.8.1 5.2.8.2	-
	5.2.9. Security of System Backup	5.2.9.1	-	5.2.9.2
Communication Security	5.3.1. Security of Sensitive Data in Transmission	-	-	-
	5.3.2. Communication Protocols and Configuration Security	-	-	-
	5.3.3. Wi-Fi Communication Security	-	-	-
Authentication and Authorization Mechanism Security	5.4.1. Security Authentication	-	-	-
	5.4.2. Password Authentication	-	-	-
	5.4.3. Security Authorization	-	-	-
Privacy Protection	5.5.1. Protection of Access of Privacy	-	-	-
	5.5.2. Privacy Transmission Protection	-	-	-
Application Security	5.6.1. Application Security	-	5.6.1.1	5.6.1.2

5. Security Test Specification

5.1 Physical Security

Inspect network attached storage device under test (DUT) and review submitted documents in fulfilling physical security test requirements, and conduct test items defined below accordingly.

5.1.1 Access control of physical interfaces

5.1.1.1 Tests shall be conducted according to "TAICS TS-0015-1: Cybersecurity Test Specification for Video Surveillance System – Part 1 General Requirements", Section 5.1.1.

5.1.1.2 Storage media protection mechanism

(a) Compliance:

"TAICS TS-0014-4: Cybersecurity Standard for Video Surveillance System- Part 4: Network Attached Storage", Section 5.1.1.2.

(b) Purpose:

Verify whether the access to DUT's storage media, e.g. hard disc drive, from external devices shall be conducted.

(c) Sample Condition:

None.

(d) Test Setup:

None.

(e) Test Method:

(1) Dismantle storage media from DUT and use a Test Computer to retrieve video from the storage media.

(2) Under un-authorized condition, verify the readability of video within the storage media.

(f) Expected Result:

(1) Video shall not be readable.

5.1.2 Warning of physical abnormal behavior

5.1.2.1 Tests shall be conducted according to “TAICS TS-0015-1: Cybersecurity Test Specification for Video Surveillance System- Part 1: General Requirements”, Section 5.1.2.

5.1.3 Physical protection

5.1.3.1 Tests shall be conducted according to “TAICS TS-0015-1: Cybersecurity Test Specification for Video Surveillance System- Part 1: General Requirements”, Section 5.1.3.

5.1.4 Secure Boot

5.1.4.1 Tests shall be conducted according to “TAICS TS-0015-1: Cybersecurity Test Specification for Video Surveillance System- Part 1: General Requirements”, Section 5.1.4.

5.1.5 Physical backup

5.1.5.1 Physical backup elementary security Test

(a) Compliance:

“TAICS TS-0014-4: Cybersecurity Standard for Video Surveillance System- Part 4: Network Attached Storage”, Section 5.1.5.1.

(b) Purpose:

Verify whether external backup storage interfaces shall exist on DUT.

(c) Sample Condition:

None.

(d) Test Setup:

None.

(e) Test Method:

(1) Visual inspection shall be conducted on the outer appearance of DUT for external storage devices and/or related interface connection.

(f) Expected Result:

(1) DUT shall be designed with external storage devices and/or related interface connection

5.1.5.2 Physical backup intermediate security Test

(a) Compliance:

"TAICS TS-0014-4: Cybersecurity Standard for Video Surveillance System- Part 4: Network Attached Storage", Section 5.1.5.2.

(b) Purpose:

Verify whether storage redundancy mechanism, e.g. RAID 1 or higher, shall exist on DUT.

(c) Sample Condition:

None.

(d) Test Setup:

Refer to Figure 2.

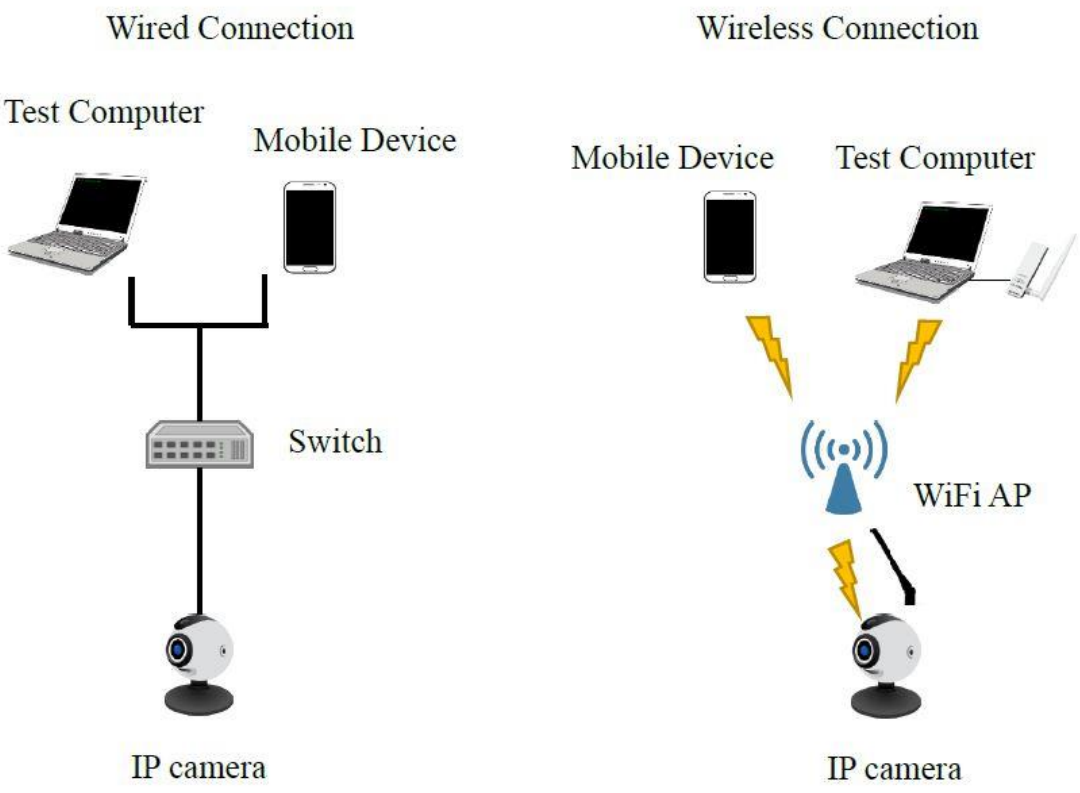

Figure 2 Test Setup

(e) Test Method:

(1) Connect DUT with a Test Computer or Mobile Device.

(2) By following user manual instructions, activate respective control management tools.

(3) Under DUT in operation condition, dismantle one storage device from the unit and inspect the functionality of DUT.

(f) Expected Result:

(1) Video surveillance functions shall stay in normal operations.

5.1.5.3 Physical backup advanced security Test

(a) Compliance:

"TAICS TS-0014-4: Cybersecurity Standard for Video Surveillance System- Part 4: Network Attached Storage", Section 5.1.5.3.

(b) Purpose:

Verify whether backup mechanism supporting hot spare function to raise the fault tolerance shall be performed on DUT.

(c) Sample Condition:

Description of hot spare function shall be provided.

(d) Test Setup:

None.

(e) Test Method:

(1) Under DUT in normal operations, dismantle one RAID disc drive from the unit.

(2) Inspect DUT for both functionality and effectiveness.

(f) Expected Result:

(1) DUT shall stay in normal operations with no impact on both functionality and effectiveness.

5.2 System Security

Inspect network attached storage device under test (DUT) and review submitted documents in fulfilling system security test requirements, and conduct test items defined below accordingly.

5.2.1 Operation system and security of Internet services

5.2.1.1 Tests shall be conducted according to “TAICS TS-0015-1: Cybersecurity Test Specification for Video Surveillance System- Part 1: General Requirements”, Section 5.2.1.

5.2.2 Service of Internet service ports

5.2.2.1 Tests shall be conducted according to “TAICS TS-0015-1: Cybersecurity Test Specification for Video Surveillance System- Part 1: General Requirements”, Section 5.2.2.

5.2.3 Update security

5.2.3.1 Tests shall be conducted according to “TAICS TS-0015-1: Cybersecurity Test Specification for Video Surveillance System- Part 1: General Requirements”, Section 5.2.3.

5.2.4 Security of Sensitive Data in Storage

5.2.4.1 Tests shall be conducted according to “TAICS TS-0015-1: Cybersecurity Test Specification for Video Surveillance System- Part 1: General Requirements”, Section 5.2.4.

5.2.5 Security of website management interface

5.2.5.1 Tests shall be conducted according to “TAICS TS-0015-1: Cybersecurity Test Specification for Video Surveillance System- Part 1: General Requirements”, Section 5.2.5.

5.2.6 Security of Management Applications

5.2.6.1 Tests shall be conducted according to “TAICS TS-0015-1: Cybersecurity Test Specification for Video Surveillance System- Part 1: General Requirements”, Section 5.2.6.

5.2.7 Logs and warnings

5.2.7.1 Tests shall be conducted according to “TAICS TS-0015-1: Cybersecurity Test Specification for Video Surveillance System- Part 1: General Requirements”, Section 5.2.7.

5.2.7.2 Security log with image file write-in

(a) Compliance:

“TAICS TS-0014-4: Cybersecurity Standard for Video Surveillance System- Part 4: Network Attached Storage”, Section 5.2.7.2.

(b) Purpose:

Verify whether the write-in record of image file in security log shall be performed on DUT.

(c) Sample Condition:

None.

(d) Test Setup:

Refer to Figure 3.

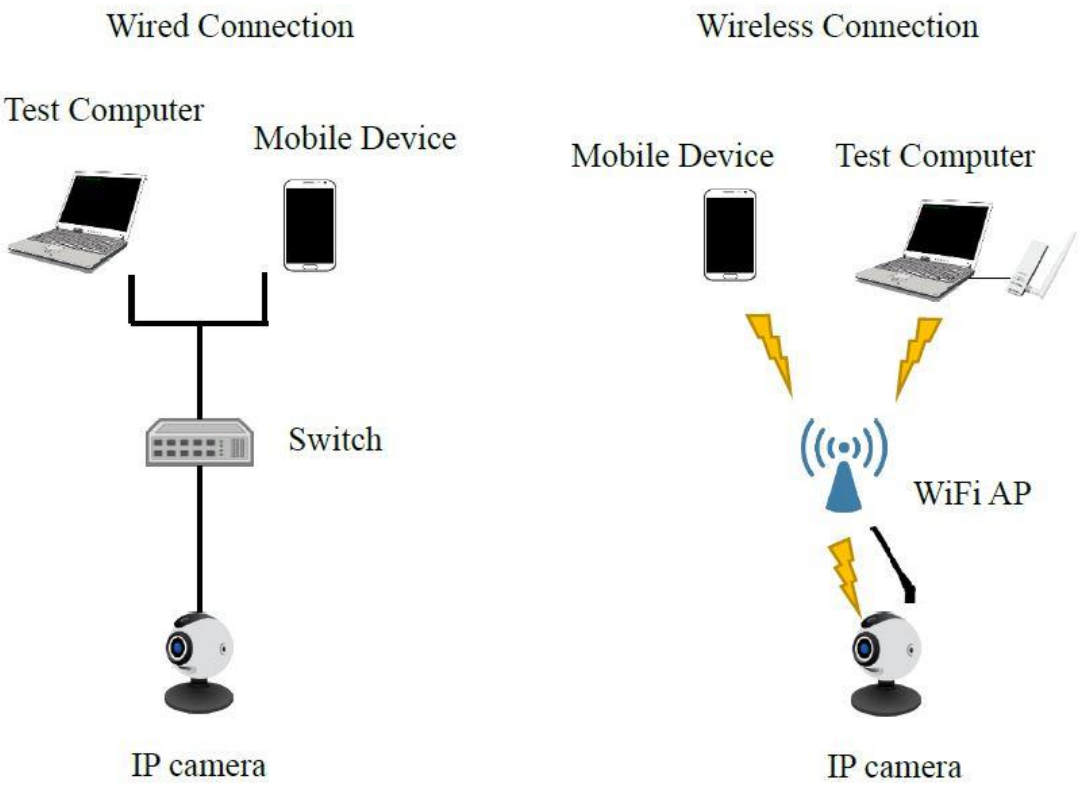

Figure 3 Test Setup

(e) Test Method:

(1) Connect DUT with a Test Computer or Mobile Device.

(2) By following user manual instructions, activate respective control management tools to read security events log.

(3) Trigger image file write-in event.

(4) Inspect security log for the existence of image file write-in event.

(5) Inspect security log for records with exact time recording, user identity and execution results.

(6) Reset DUT.

(7) Inspect the existence of all security records.

(f) Expected Results:

(1) DUT shall provide user the availability of write-in function of image file in security event log.

(2) Information of security event log shall include exact time, i.e. year, month, day, hour, minute and second, together with user identity and execution results.

(3) Reset of DUT shall not create impact to previous records.

5.2.8 Storage security

5.2.8.1 Effective storage space utilization

(a) Compliance:

"TAICS TS-0014-4: Cybersecurity Standard for Video Surveillance System- Part 4: Network Attached Storage", Section 5.2.8.1.

(b) Purpose:

Verify whether a warning mechanism shall be provided on DUT to issue alerts when available storage space is less than a preset value.

(c) Sample Condition:

Description of insufficient storage space warning mechanism shall be provided.

(d) Test Setup:

Refer to figure 4.

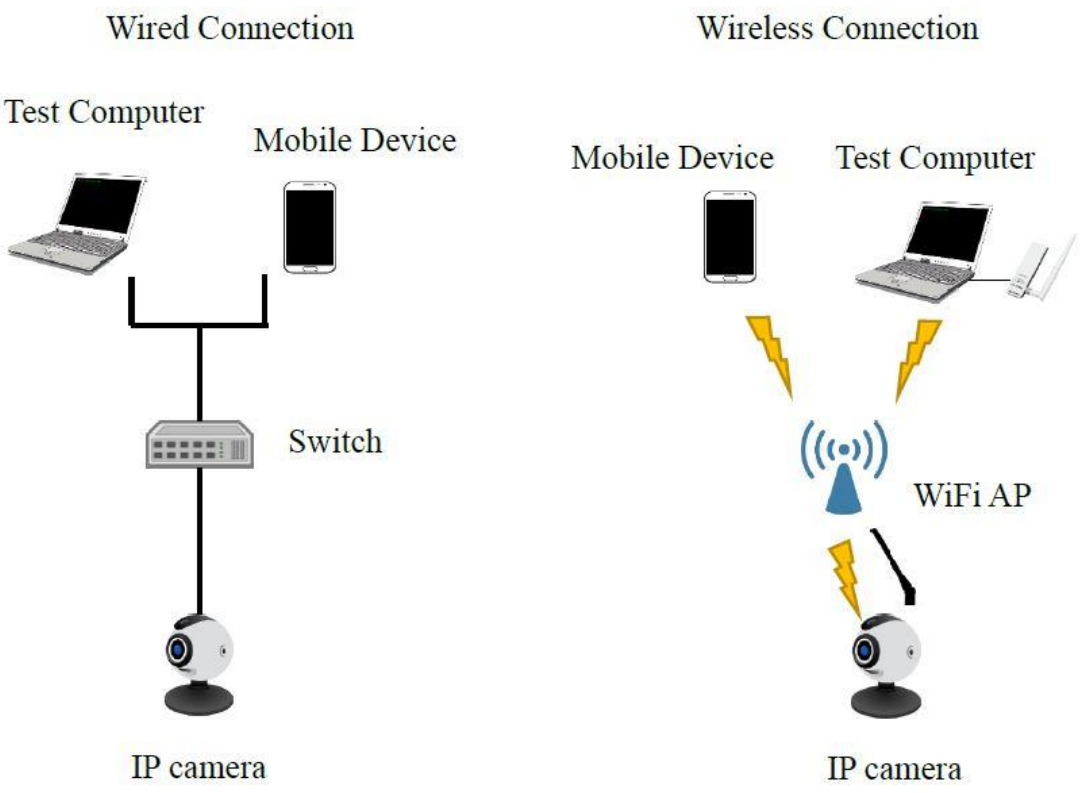

Figure 4 Test Setup

(e) Test Method:

(1) Connect DUT with a Test Computer or Mobile Device.

(2) By following user manual instructions, activate respective control management tools.

(3) Input data into DUT storage space till available storage space is less than a preset value.

(4) Abnormal warning is being activated.

(f) Expected Result:

(1) DUT shall provide warning mechanism for insufficient storage space alerts.

5.2.8.2 Tamper-proof warning mechanism

(a) Compliance:

"TAICS TS-0014-4: Cybersecurity Standard for Video Surveillance System- Part 4: Network Attached Storage", Section 5.2.8.2.

(b) Purpose:

Verify whether tamper-proof warning mechanism shall be performed on DUT.

(c) Sample Condition:

Authorization of system administrators shall be provided.

(d) Test Setup:

Refer to Figure 5.

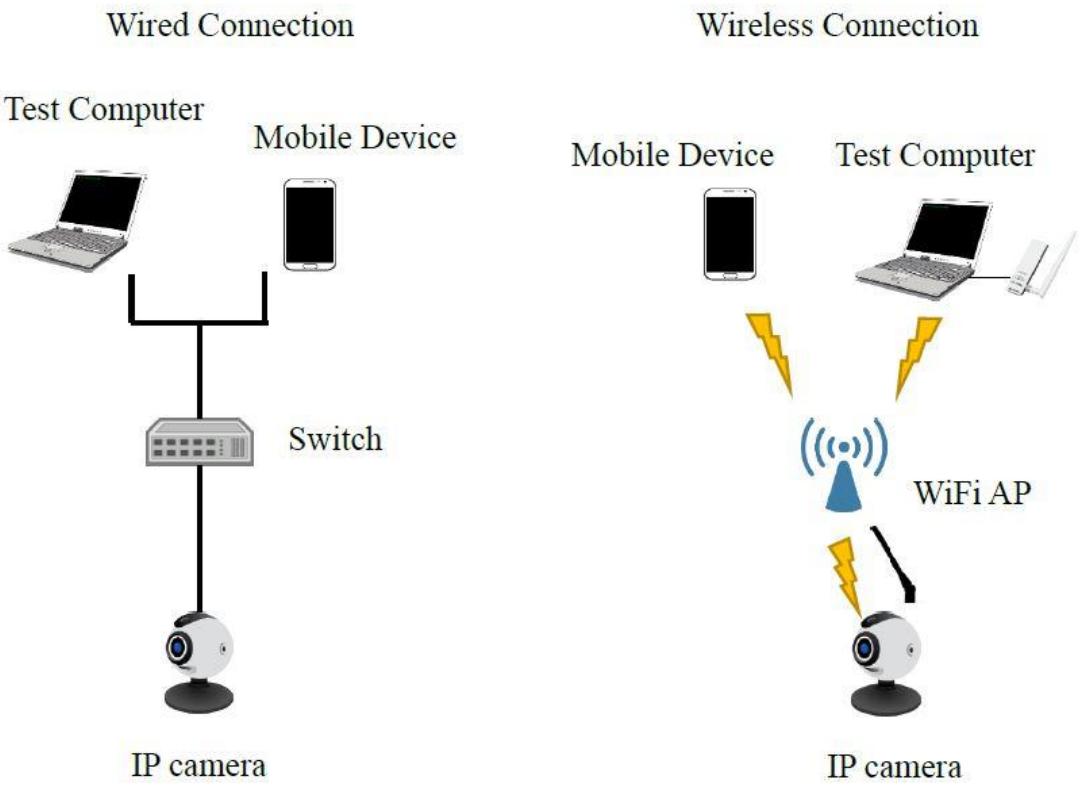

Figure 5 Test Setup

(e) Test Method:

(1) Connect DUT with a Test Computer or Mobile Device.

(2) By following user manual instructions, activate respective control management tools.

(3) Manipulate recorded image files within DUT storage.

(4) Abnormal warning is being activated.

(f) Expected Result:

(1) DUT shall provide warning mechanism for tampered record alerts.

5.2.9 System backup security

5.2.9.1 Image file backup function

(a) Compliance:

"TAICS TS-0014-4: Cybersecurity Standard for Video Surveillance System- Part 4: Network Attached Storage", Section 5.2.9.1.

(b) Purpose:

Verify whether the backup of image files shall be available on DUT.

(c) Sample Condition:

Description of image file backup function shall be provided.

(d) Test Setup:

Refer to Figure 6.

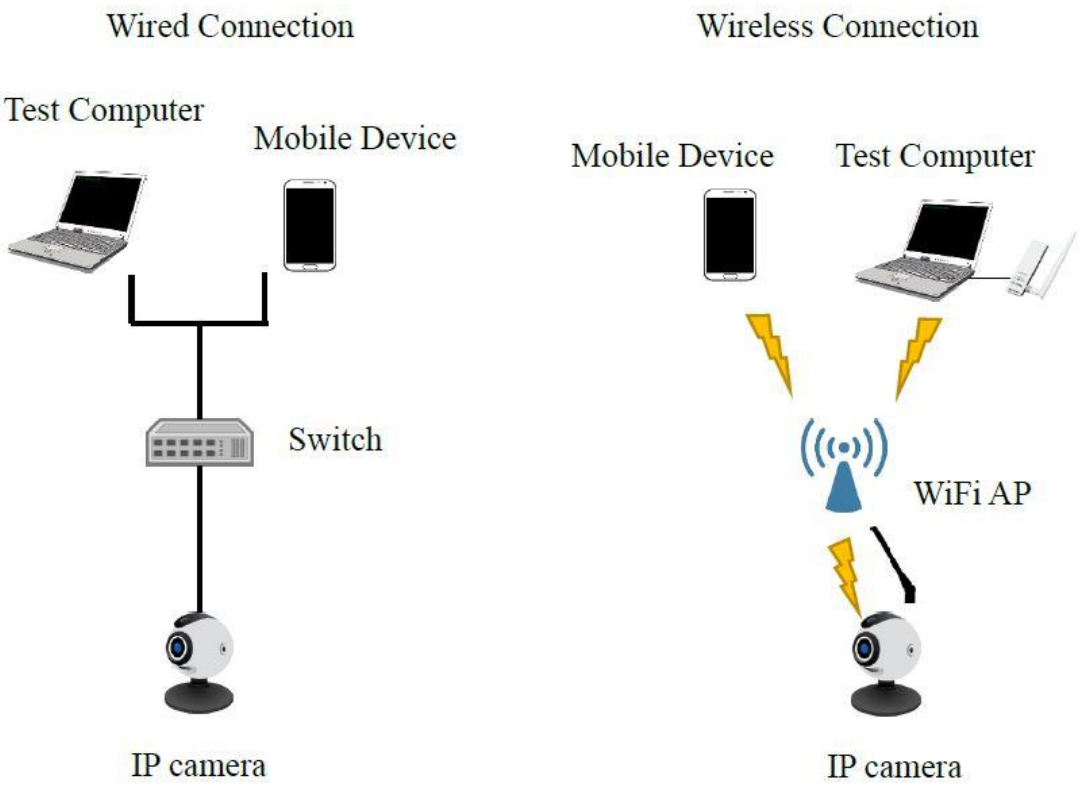

Figure 6 Test Setup

(e) Test Method:

(1) Connect DUT with a Test Computer or Mobile Device.

(2) By following user manual instructions, activate respective control management tools.

(3) Activate backup function and inspect its functionality.

(f) Expected Result:

(1) Backup function shall be in normal operations.

5.2.9.2 Backup files security protection

(a) Compliance:

"TAICS TS-0014-4: Cybersecurity Standard for Video Surveillance System- Part 4: Network Attached Storage", Section 5.2.9.2.

(b) Purpose:

Verify whether the confidentiality of backup image files shall be performed on DUT.

(c) Sample Condition:

Detailed description of encryption algorithms of sensitive data in storage shall be submitted for review.

(d) Test Setup:

None.

(e) Test Method:

(1) Review submitted documents for compliance.

(2) Verify encryption algorithms for backup documents.

(f) Expected Result:

(1) Encryption algorithm shall adopt FIPS 140-2 Annex A [2] approved methodology.

5.3 Communication Security

Communication security of network attached storage shall be investigated against submitted documents and tested in accordance with the test items defined within this section.

5.3.1 Security of Sensitive Data in Transmission

5.3.1.1 Tests shall be conducted according to “TAICS TS-0015-1: Cybersecurity Test Specification for Video Surveillance System- Part 1: General Requirements”, Section 5.3.1.

5.3.2 Communication Protocols and Configuration Security

5.3.2.1 Tests shall be conducted according to “TAICS TS-0015-1: Cybersecurity Test Specification for Video Surveillance System- Part 1: General Requirements”, Section 5.3.2.

5.3.3 Wi-Fi Communication Security

5.3.3.1 Tests shall be conducted according to “TAICS TS-0015-1: Cybersecurity Test Specification for Video Surveillance System- Part 1: General Requirements”, Section 5.3.3.

5.4 Authentication and Authorization mechanism security

Authentication and authorization mechanism security of network attached storage shall be investigated against submitted documents and tested in accordance with the test items defined within this section.

5.4.1 Security authentication

5.4.1.1 Tests shall be conducted according to “TAICS TS-0015-1: Cybersecurity Test Specification for Video Surveillance System- Part 1: General Requirements”, Section 5.4.1.

5.4.2 Password authentication

5.4.2.1 Tests shall be conducted according to “TAICS TS-0015-1: Cybersecurity Test Specification for Video Surveillance System- Part 1: General Requirements”, Section 5.4.2.

5.4.3 Security Authorization

5.4.3.1 Tests shall be conducted according to “TAICS TS-0015-1: Cybersecurity Test Specification for Video Surveillance System- Part 1: General Requirements”, Section 5.4.3.

5.5 Privacy Protection

Privacy protection of network attached storage shall be investigated against submitted documents and tested in accordance with the test items defined within this section. Privacy information, in general, includes all video and acoustic information being collected from video surveillance devices throughout this specification.

5.5.1 Privacy access protection

5.5.1.1 Tests shall be conducted according to “TAICS TS-0015-1: Cybersecurity Test Specification for Video Surveillance System- Part 1: General Requirements”, Section 5.5.1.

5.5.2 Privacy Transmission Protection

5.5.2.1 Tests shall be conducted according to “TAICS TS-0015-1: Cybersecurity Test Specification for Video Surveillance System- Part 1: General Requirements”, Section 5.5.2.

5.6 Application Security Requirements

Inspect network attached storage device under test (DUT) and review submitted documents in fulfilling application security test requirements, and conduct test items defined below accordingly.

5.6.1 Application security

5.6.1.1 Applications tampering prevention

(a) Compliance:

"TAICS TS-0014-4: Cybersecurity Standard for Video Surveillance System- Part 4: Network Attached Storage", Section 5.6.1.1.

(b) Purpose:

Verify whether the activation prevention of tampered applications preinstalled by factory shall be conducted on DUT.

(c) Sample Condition:

None.

(d) Test Setup:

Authorization of system administrators shall be provided.

(e) Test Method:

(1) Connect DUT with a Test Computer or Mobile Device.

(2) By following user manual instructions, activate respective control management tools.

(3) Replace the original application execution file and check the operability of the new application executable.

(4) Replace the original webpage source code and check the operability of the new webpage source code.

(f) Expected Results:

(1) Replacing application shall not be activated.

(2) Replacing website source code shall not be activated.

5.6.1.2 Application of origin

(a) Compliance:

"TAICS TS-0014-4: Cybersecurity Standard for Video Surveillance System- Part 4: Network Attached Storage", Section 5.6.1.2.

(b) Purpose:

Verify whether origin indication of referenced third party libraries shall be performed on DUT.

(c) Sample Condition:

Listing of application adopted from third party libraries, with function library name and version, shall be provided for verification.

(d) Test Setup:

None.

(e) Test Method:

(1) Review submitted third party libraries list.

(2) Verify the existence of function libraries by applying CVSS v3 evaluation with severity rating of 9.0 or above CVE.

(f) Expected Result:

(1) CVE with severity rating 9.0 or above of CVSS v3 shall not exist.

Appendix A
(Normative)
Security Specification Description (Template)

This document shall be filled and submitted together with DUT for testing reference.

Table 1: Security Specification Sheet

Item	Description	Filled in by applicant
1. Backup Function	Detail description with step by step method of backup function, or supporting document delivering. *Example:* *1. Log-in control program;* *2. Select "setup";* *3. Select "SSH"* *4. …*	
2. Hot Spare Function	Detail description of step by step method of hot spare function, or supporting document delivering. *Example:* *1. Log-in control program;* *2. Select "setup";* *3. Select "Hot spare function"*	

	4. …	
3. Third party libraries list	List all third-party function library. *Example:* *1. openssl ver. 1.1.1*	

References

[1] TAICS TS-0014-4 Cybersecurity Standard for Video Surveillance System-Part 4: Network Attached Storage.

[2] National Institute of Standards and Technology (NIST), Annex A: Approved Security Functions for FIPS PUB 140-2: Security Requirements for Cryptographic Modules, May 10, 2017

Revision Record

Version	Date	Summary
v1.0	2018/06/08	v1.0 Chinese version published
v1.0(E)	2019/05/30	v1.0 English version published
-	-	-
-	-	-
-	-	-
-	-	-
-	-	-

地　址・台北市中正區重慶南路二段51號8樓之一
電　話・+886-2-23567698
Email・secretariat@taics.org.tw
www.taics.org.tw