TAICS

TAICS TS-0015-1(E) v1.0:2019

Cybersecurity Test Specification for Video Surveillance System- Part 1: General Requirements

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 1: General Requirements

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 specificationis 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 1: General Requirements” (hereafter referred to as “this/the specification”) is formulated by TAICS, in accordance with “TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements” [1], 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

Video surveillance systems, whose purpose is to monitor specific locations for security maintenance, mainly consist of IP cameras, digital video recorders, network video recorders, and network-attached storage. These systems further comprise (1) dedicated monitoring infrastructure for the installed cameras, local or remote computer devices, mobile devices, and cloud servers and (2) a functional networking environment, including Wi-Fi access points, routers and switches. With all these integrated, it creates a complete video surveillance system.

2. Normative References

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

3. Terms and Definitions

All terms defined within “TAICS TS-0014-1 v1.0: 2019 Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements” and below are applicable to the specification.

3.1. Cipher Suite

A cipher suite is a set of algorithms that help secure a network connection that uses Transport Layer Security (TLS) or its now-deprecated predecessor Secure Socket Layer (SSL). The set of algorithms that cipher suites usually contain includes: an identity validation algorithm, an encryption algorithm, a message authentication code (MAC) algorithm, and a key exchange algorithm.

3.2 Port Scan

Network ports, also known as communication or connecting ports, serve as an interface for data transmission and reception between interconnecting devices and external sources. Port scan is a kind of practice being adopted by hackers in detecting network ports and service access and, even further, looking for possible vulnerabilities in reaching unauthorized access points.

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-0014-1 Cybersecurity Standard for Video Surveillance System-Part 1: General Requirements", 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, and (5) privacy protection. 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	5.1.1.1	-	-
	5.1.2. Warning of Physical Abnormal Behavior	-	5.1.2.1 5.1.2.2	-
	5.1.3. Physical Protection	5.1.3.1	-	-
	5.1.4. Secure Boot	-	-	5.1.4.1
System Security	5.2.1. Operating System and Network Services Security	5.2.1.1	-	5.2.1.2
	5.2.2. Security of Network Service Ports	5.2.2.1	-	-
	5.2.3. Update Security	5.2.3.1 5.2.3.2 5.2.3.3	-	-
	5.2.4. Security of Sensitive Data in Storage	5.2.4.1(a) 5.2.4.2(a)	5.2.4.1(b) 5.2.4.2(b) 5.2.4.3	5.2.4.4

Security Aspects	Security Requirements	Security Levels		
		Level 1	Level 2	Level 3
	5.2.5. Security of Website Management Interface	5.2.5.1	-	-
	5.2.6. Security of Management Applications	5.2.6.1 5.2.6.2 5.2.6.3	-	-
	5.2.7. Logs and Warnings	5.2.7.1 5.2.7.2 5.2.7.3	5.2.7.4	-
Communication Security	5.3.1. Security of Sensitive Data in Transmission	5.3.1.1	-	5.3.1.2
	5.3.2. Communication Protocols and Configuration Security	5.3.2.1 5.3.2.2	5.3.2.3	-
	5.3.3. Wi-Fi Communication Security	5.3.3.1 5.3.3.2	5.3.3.3	5.3.3.4
Authentication and Authorization Mechanism Security	5.4.1. Security Authentication	5.4.1.1 5.4.1.2	5.4.1.3 5.4.1.4	5.4.1.5 5.4.1.6
	5.4.2. Password Authentication	5.4.2.1 5.4.2.2 5.4.2.3 5.4.2.4	-	5.4.2.5 5.4.2.6
	5.4.3. Security Authorization	5.4.3.1 5.4.3.2	-	-
Privacy Protection	5.5.1. Protection of Access of Privacy	5.5.1.1 5.5.1.2 5.5.1.3	-	-
	5.5.2. Privacy Transmission Protection	5.5.2.1	-	5.5.2.2

5. Security Test Specification

5.1 Physical Security

Inspect the video surveillance 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 Access control of physical interfaces Test

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System-Part 1: General Requirements", Section 5.1.1.1.

(b) Purpose:

Verify whether the access to the debug mode of the operating system shall be conducted through physical interface of DUT.

(c) Sample Condition:

(1) DUT shall remain in factory default environment conditions.
(2) Methods to access the debug mode of DUT's operating system shall be described in detail within submitted documents.

(d) Test Setup:

None.

(e) Test Method:

(1) Access the debug mode of DUT's operating system according to submitted documents, and activate respective control management tools.
(2) Tests shall be conducted through a USB port.
(3) Access to the debug mode of DUT's operating system shall be verified.
(4) If Password authentication procedure is required for such access, tests of section 5.4.2.1, 5.4.2.2, 5.4.2.3 and 5.4.2.4 shall be conducted for security verification purpose.

(5) Tests shall be conducted through a UART port.

(6) Again, access to the debug mode of DUT's operating system shall be verified

(7) If Password authentication procedure is required for such access, tests of section 5.4.2.1, 5.4.2.2, 5.4.2.3 and 5.4.2.4 shall be conducted for security verification purpose.

(f) Expected Results:

(1) While the debug mode of DUT's operating system is being accessed through a USB port, authentication mechanism is required.

(2) The above authentication mechanism shall comply with the expected results of section 5.4.2.1, 5.4.2.2, 5.4.2.3 and 5.4.2.4.

(3) While the debug mode of DUT's operating system is being accessed through a UART port, authentication mechanism is required.

(4) The above authentication mechanism shall comply with the expected results of section 5.4.2.1, 5.4.2.2, 5.4.2.3 and 5.4.2.4.

(5) DUT with no interface to access the debug mode of its operating system complies with this subject clause.

5.1.2 Warning of physical abnormal behavior

5.1.2.1 Physical port device plug-unplug recording

(a) Compliance:

"TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.1.2.1.

(b) Purpose:

Verify whether the recording of plugs and unplugs of DUT's physical ports shall be conducted.

(c) Sample Condition:

None.

(d) Test Setup:

None.

(e) Test Method:

(1) DUT shall be connected to a Test Computer or appropriate Mobile Device.
(2) According to submitted documents, activate respective control management tools.
(3) Conduct plug-unplug tests on USB ports and inspect the records for compliance.
(4) Conduct plug-unplug tests on RJ 45 ports and inspect the records for compliance.

(f) Expected Results:

(1) DUT shall possess complete plug-unplug records of USB ports.
(2) DUT shall possess complete plug-unplug records of RJ45 ports.
(3) DUT shall possess plug-unplug records of all physical ports in correct timing.

5.1.2.2 Warning of Physical Abnormal Behavior

(a) Compliance:

"TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.1.2.2.

(b) Purpose:

Verify whether DUT shall be equipped with warning mechanism in response to the occasions when the network connection is isolated on the physical layer.

(c) Sample Condition:

None.

(d) Test Setup:

Refer to Figure 1.

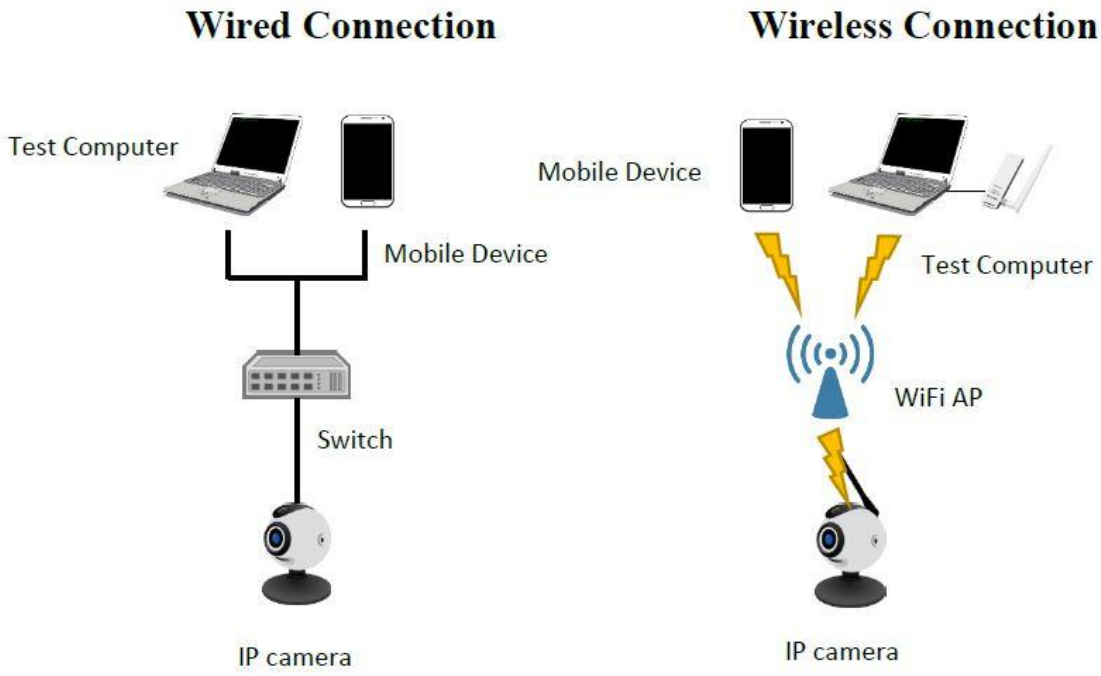

Figure 1 Test Setup

(e) Test Method:

(1) Follow DUT's user manual instructions.

(2) Unplug network cables and/or physically mask the antenna in causing DUT to be internet disconnected and/or signal interrupted.

(3) Inspect DUT in accordance with submitted operating manual for the effectiveness of its alarm mechanism.

(f) Expected Result:

(1) DUT shall be issuing effective alarms at network disconnections.

5.1.3 Physical Protection

5.1.3.1 Enclosure Design Security Test

(a) Compliance:

"TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System-Part 1: General Requirements", Section 5.1.3.1.

(b) Purpose:

Verify whether physical enclosure security mechanism shall be designed for default password reset prevention.

(c) Sample Condition:

None.

(d) Test Setup:

None.

(e) Test Method:

(1) Visual inspection of DUT's enclosure shall be conducted. Default password reset mechanism shall be designed to prevent intrusion without tools.

(f) Expected Result:

(1) DUT's enclosure is designed with mechanism to prevent intrusion without tools in conducting defult password reset.

5.1.4 Secure Boot

5.1.4.1 DUT shall be designed to fulfill the functions of secure boot.

(a) Compliance:

"TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System-Part 1: General Requirements", Section 5.1.4.1.

(b) Purpose:

Verify whether DUT shall be conducted, during initial power-on stage, to ensure its completion and legitimacy.

(c) Sample Condition:

Initial submitted documents shall include secure boot function design for review.

(d) Test Setup:

None.

(e) Test Method:

(1) Review submitted documents to confirm secure boot functions being design-in.
(2) Verify that during initial power-on stage, DUT shall ensure the signatures of both firmware and operating system to be validated.

(f) Expected Results:

(1) While “power-on” being activated, secure boot functions shall only be executed through security zone.
(2) Signature validation of both firmware and operating system at the “power-on” stage shall be clearly identified within submitted documents.

5.2 System Security

Inspect the video surveillance device under test (DUT) and review submitted documents in fulfilling system security test requirements, and conduct test items defined below accordingly.

5.2.1 Operating System and Network Services Security

5.2.1.1 Verification of Operating system shall be conducted and no CVE with scoring 9.0 or above under CVSS v3 exists.

(a) Compliance:

"TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System-Part 1: General Requirements", Section 5.2.1.1.

(b) Purpose:

Verify whether both operating system and network services of DUT shall be designed against major CVSS v3 vulnerabilities and exposures.

(c) Sample Condition:

(1) DUT shall remain in factory default environment conditions.

(d) Test Setup:

Refer to Figure 2. The linkage between the Test Computer and DUT can be wired or wireless. Test setup includes a Test Computer (connecting to video surveillance device for testing purpose), wired connection (Ethernet or Optical fiber cables) and wireless connection.

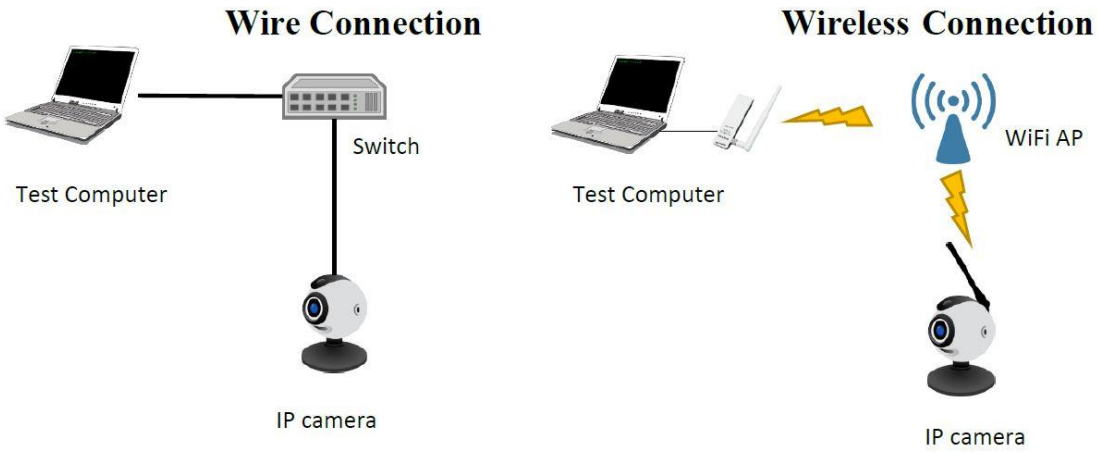

Figure 2 Test Setup

(e) Method:

(1) Connect a Test Computer with DUT accordingly.

(2) Activate vulnerability scanning tool to diagnose both the operating system and network services of DUT.

(3) Scanning tool shall generate reports in identifying all vulunerabilities of DUT. No CVE with scoring 9.0 or above under CVSS v3 shall be identified.

(f) Expected Results:

(1) No CVE with scoring 9.0 or above under CVSS v3 shall be observed in both operating system and network services.

(2) While security vulnerability and exposure being observed with no scoring under CVSS v3 scoring system, DUT shall be evaluated according to CVSS v2 instead.

5.2.1.2 Verification of both operating system and network services shall be conducted in identifying the existence of CVE scoring 7.0 or above against CVSS v3.

(a) Compliance:

"TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.2.1.2.

(b) Purpose:

Verify whether both the operating system and network services of DUT shall be designed against known high risk CVE of CVSS v3.

(c) Sample Condition:

DUT shall remain in factory default environment conditions.

(d) Test Setup:

Refer to Figure 3.

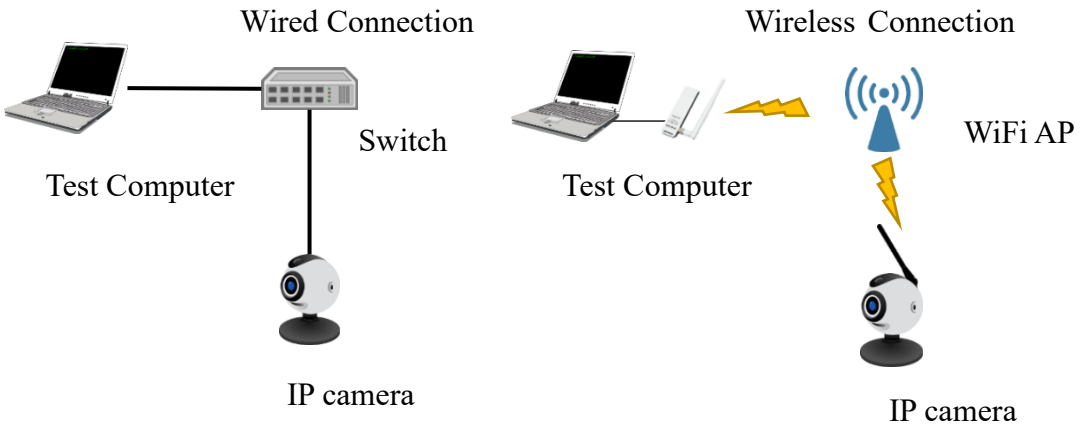

Figure 3 Test Setup

(e) Test Method:

(1) Connect DUT with a Test Computer.
(2) Activate vulunerability scanning tool to diagnose both the operating system and network services of DUT.
(3) Scanning tool shall generate reports in identifying all vulunerabilities of DUT. No CVE with scoring 7.0 or above against CVSS v3 shall be identified.

(f) Expected Results:

(1) No CVE with scoring 7.0 or above against CVSS v3 shall be observed.
(2) While security vulnerability and exposure being observed with no scoring under CVSS v3 scoring system, DUT shall be evaluated according to CVSS v2 instead.

5.2.2 Security of Network Service Ports

5.2.2.1 Minimal Network Services

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.2.2.1.

(b) Purpose:

Verify whether unknown network services ports shall exist.

(c) Sample Condition:

(1) DUT shall remain in factory default environment conditions.

(2) Define and declare network services applied and their respective network service ports within submitted documents.

(d) Test Setup:

Refer to Figure 4.

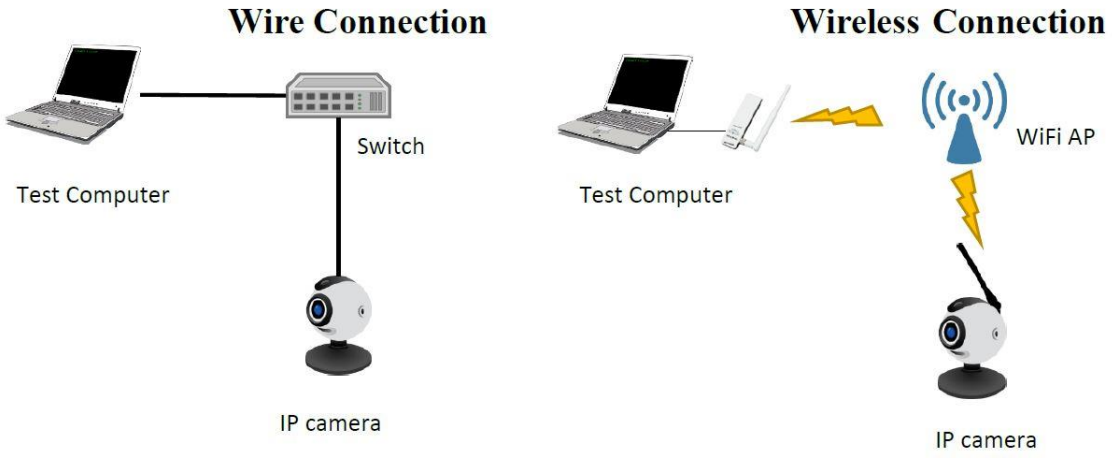

Figure 4 Test Setup

(e) Test Method:

(1) Connect DUT with a Test Computer.

(2) Activate network port scanning tool and apply both TCP and UDP in scanning all ports, from 0 to 65535.

(3) Scanning report shall identify all network services content and its respective ports.

(4) Compare testing results with declared documents and identify the difference.

(f) Expected Result:

(1) Test report shall be identical to declared documents for compliance.

5.2.3 Update Security

5.2.3.1 (a)Firmware Files Security Test

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.2.3.1(a).

(b) Purpose:

Verify whether DUT's firmware updated file shall reveal sensitivity data.

(c) Sample Condition:

(1) Scenario 1:

(i)Applicable to security strength tests on firmware encryption protection.

(ii)Applicable to DUT with offline update functions.

(iii)Firmware files need to be submitted for testing purpose.

(iv)Written documents of encryption algorithm being applied is needed for review.

(2) Scenario 2:

(i)Applicable to sensitive data tests in plain text or ciphered form on firmware files.

(ii)Firmware files need to be submitted for testing purpose.

(iii)If submitted firmware files are encrypted, decryption algorithm shall be provided.

(iv)Declaration of all servers intend to connect with DUT shall be provided.

(d) Test Setup:

Refer to Figure 5.

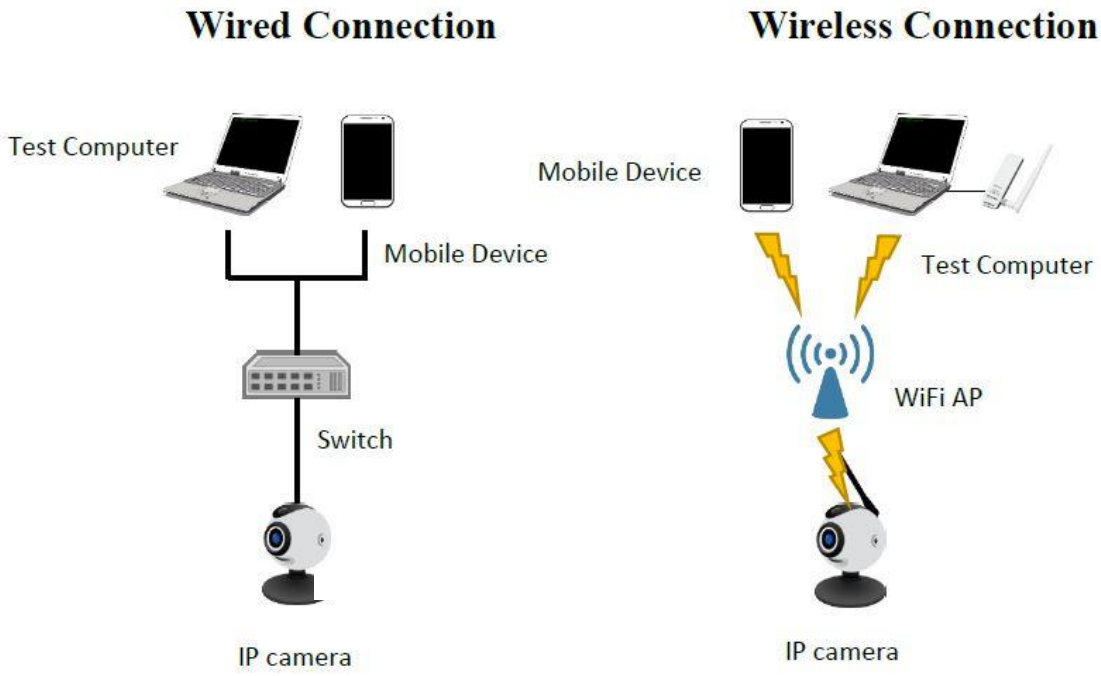

Figure 5 Test Setup

(e) Test Method:

(1) Scenario 1:

(i)Apply appropriate firmware analysis tools to DUT for firmware extraction.

(ii)Inspect firmware updated files for possible file system being resolved.

(iii)Review submitted documents of encryption algorithm for confirmation.

(2) Scenario 2:

(i) Apply appropriate firmware analysis tools to DUT for firmware extraction.

(ii) Extract file system.

(iii) Verify whether the security function of system password shall comply with “One-way Hash” validation according to FIPS 140-2 Annex A.

(iv) Verify whether key shall be extracted.

(v) Verify whether non-public email shall be exposed.

(vi) Except for IP of those servers being declared, verify whether unknown IP information of others shall exist.

(vii) Except for URL of those servers being declared, verify whether unknown URL information of others shall exist.

(f) Expected Results:

(1) Scenario 1

(i) Firmware update files shall resolve no file system directory related information.

(ii) Encryption algorithms comply with FIPS 140-2 Annex A [2].

(2) Scenario 2

(i) No password related information shall be detected within DUT's embedded program codes, installation files and related documents. Or else, password authentication schemes in compliance with Section 5.4.2 also fulfill the request.

(ii) No encrypted and/or decrypted key shall be detected within DUT's embedded program codes, installation files and related document. Or else, decrypted and encrypted key shall not be recoverable.

(iii) No non-public email information exists.

(iv) No unknown IP server connection exists.

(v) No unknown URL server connection exists.

DUT shall comply with either one of the scenarios above in fulfilling the subject clause requirement.

5.2.3.1 (b)Firmware update path protection

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.2.3.1(b).

(b) Purpose:

Verify whether firmware's online update shall adopt secure channel whose certificate proves its legitimacy and effectiveness.

(c) Sample Condition:

(1) DUT shall support online update functions.

(2) Declaration of all servers intending to connect with DUT shall be provided.

(3) DUT's supplier shall provide necessary assistance in triggering online update functions during tests.

(4) DUT shall remain in factory default environment conditions.

(d) Test Setup:

Refer to Figure 6. Test shall be conducted against DUT and firmware update server, simultaneously.

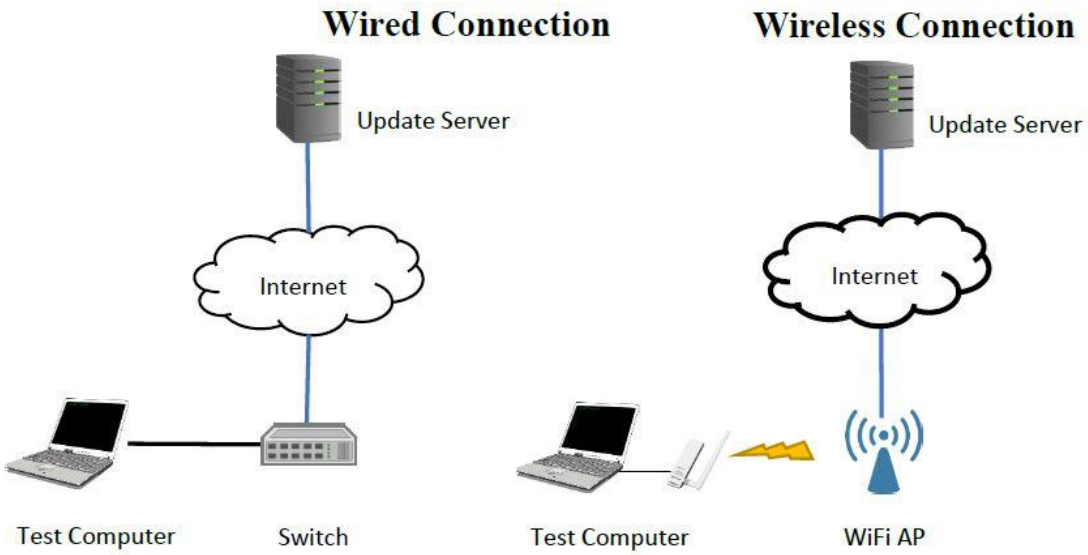

Figure 6 Test Setup

(e) Test Method:

(1) Activate security tunnel scanning tool and conduct scanning against firmware update server.

(2) Review and make comparison of scanning results, conduct inspection on cipher suite of server against criteria of Appendix A.

(3) Connect the Test Computer or Mobile Device with video surveillance device and activate updating process.

(4) Record and monitor the path of packets between firmware update server and DUT. Identify secure tunnel has been adopted.

(5) Repeat updating process.

(6) Intercept certificate on the path between firmware update server and DUT while transmitting, and make replacement of either the key or related information, such as issuing body, expiration date, incorrect formatting and/or signature.

(7) Transmit tampered certificate to DUT and monitor the packets during hand-shaking process on secure tunnel to verify the effectiveness of DUT's validation process.

(f) Expected Results:

(1) Secure tunnel shall be adopted for online firmware update and shall support cipher suite suggested in Appendix A only.

(2) Once certification key and/or related information being tampered, secure tunnel shall not be established.

5.2.3.2 Completeness and Credibility of Firmware Update files

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.2.3.2.

(b) Purpose:

Verify whether DUT shall be capable of performing integrity and non-repudiation check on firmware updated file.

(c) Sample Condition:

(1) Mechanism of digital signature utilization shall be submitted.

(2) All firmware files shall be provided.

(d) Test Setup:

Refer to Figure 7.

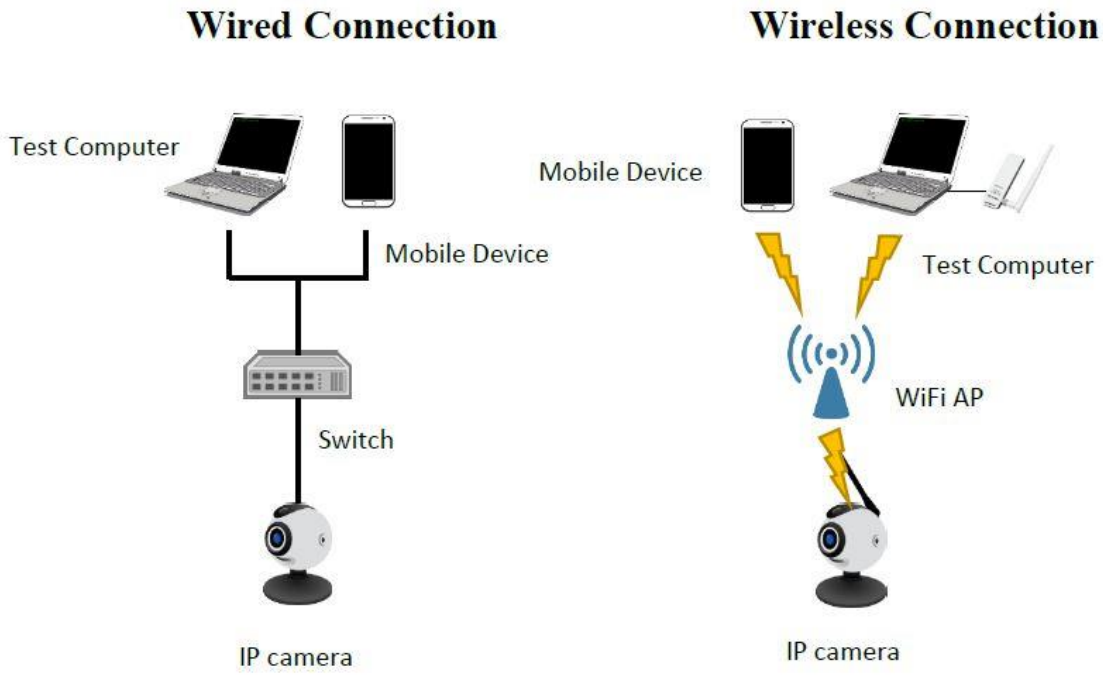

Figure 7 Test Setup

(e) Test Method:

(1) Digital signature re-assignment of updated firmware file.

(2) Activate firmware updating process and monitor update result.

(f) Expected Result:

(1) Firmware update failure shall be observed.

5.2.3.3 firmware recovery

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.2.3.3.

(b) Purpose:

Verify whether DUT shall be capable of continuing its normal operations after abnormal interrupts during updating process.

(c) Sample Condition:

(1) Scenario 1

DUT shall support offline manual updating mechanism.

(2) Scenario 2

DUT shall support online updating mechanism.

(d) Test Setup:

(1) Scenario 1

Refer to Figure 8.

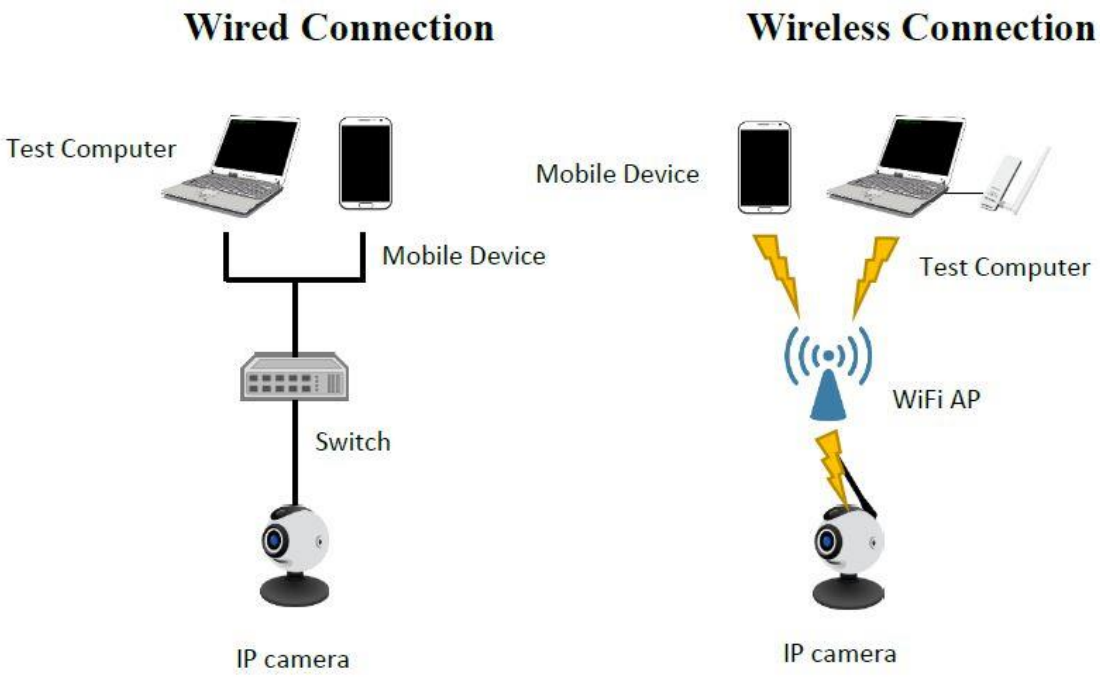

Figure 8 Test Setup

(2) Scenario 2

Refer to Figure 9.

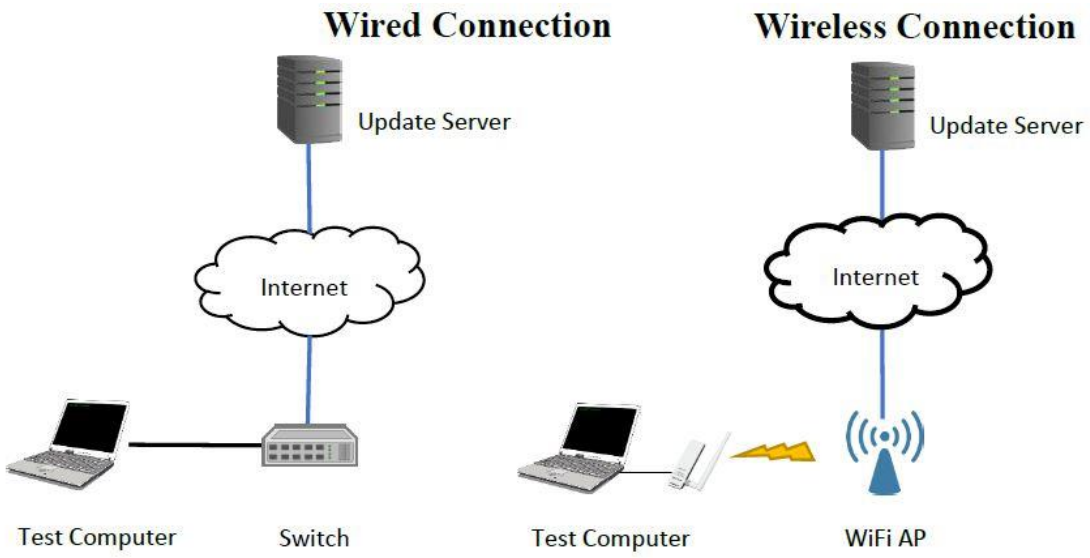

Figure 9 Test Setup

(e) Test Method:

(1) Scenario 1

(i) Connect DUT with a Test Computer.

(ii) Activate offline manual updating functions.

(iii) Trigger interruption to DUT during the updating process.

(2) Scenario 2

(i) Connect DUT with a Test Computer.

(ii) Activate online manual updating functions.

(iii) Trigger interruption to DUT during the updating process.

(f) Expected Result:

(1) System shall be recovered to normal operation after updating process being interrupted.

5.2.4 Security of sensitive data in storage

5.2.4.1 Access control of sensitive data

(a) Elementary Level Test:

(1) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.2.4.1.

(2) Purpose:

Verify whether DUT shall be equipped with authority control mechanism for sensitive data access.

(3) Sample Condition:

Written documents of sensitive data storage and management shall be submitted for review.

(4) Test Setup:

None.

(5) Test Method:

(i)Review submitted documents for assessment of compliance.

(6) Expected Results:

(i)Access control of password shall be consistent with that in submitted self-declaration documents.

(ii) Access control of encrypted/decrypted keys shall be consistent with that in submitted self-declaration documents.

(iii) Access control and management scheme shall designate roles with at least two layers of authorization limits.

(b) Intermediate Level Test:

(1) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.2.4.1.

(2) Purpose:

Verify whether DUT shall be equipped with authority control mechanism for sensitive data access.

(3) Sample Condition:

(i)Written documents of sensitive data storage and management shall be submitted for review.

(ii)The administrator privileges shall be provided for testing purpose.

(iii)The accessible interfaces for the operating system shall be provided.

(4) Test Setup:

Refer to Figure 10.

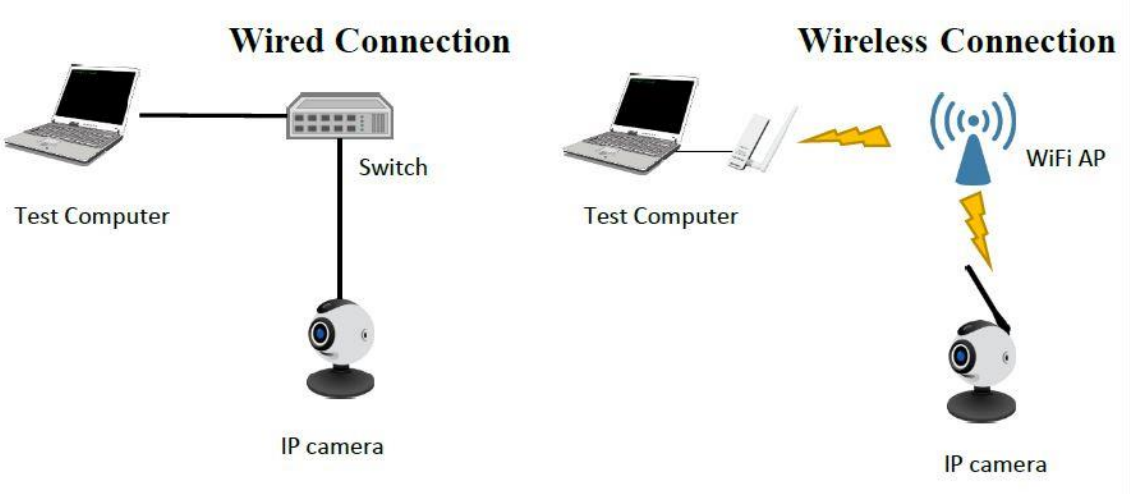

Figure 10 Test Setup

(5) Test Method:

(i) Connect DUT with a Test Computer.

(ii) Cross-check password storage and authorization limits with submitted documents for compliance.

(iii) Cross-check encryption/decryption key storage and authorization limits with submitted documents for compliance.

(6) Expected Results:

(i) Access control of password shall be consistent with that in submitted self-declaration documents.

(ii) Access control of encrypted/decrypted key shall be consistent with that in submitted self-declaration documents.

(iii) Access control scheme shall designate roles with at least two layers of authorization limits.

5.2.4.2 Sensitive Data Storage Encryption

(a) Elementary Stage Test:

(1) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.2.4.2.

(2) Purpose:

Verify whether encryption protection of sensitive data in storage shall be conducted.

(3) Sample Condition:

Written documents of encryption algorithms for sensitive date in storage shall be submitted for review.

(4) Test Setup:

None.

(5) Test Method:

(i)Review submitted documents for assessment of compliance.

(6) Expected Results:

(i) Security mechanism for password and related information shall be defined in accordance with "One-way Hash" function of FIPS 140-2 Annex A.

(ii) Security mechanism for encryption/decryption key shall be defined in accordance with the encryption algorithm of FIPS 140-2 Annex A.

(b) Intermediate Stage Test:

(1) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.2.4.2.

(2) Purpose:

Verify whether encryption protection of sensitive data in storage shall be conducted.

(3) Sample Condition:

(i) Written documents of sensitive data storage and management shall be submitted for review.

(ii) The administrator privileges shall be provided for testing purpose.

(iii) The accessible interfaces for operating system shall be provided.

(4) Test Setup:

Refer to Figure 11.

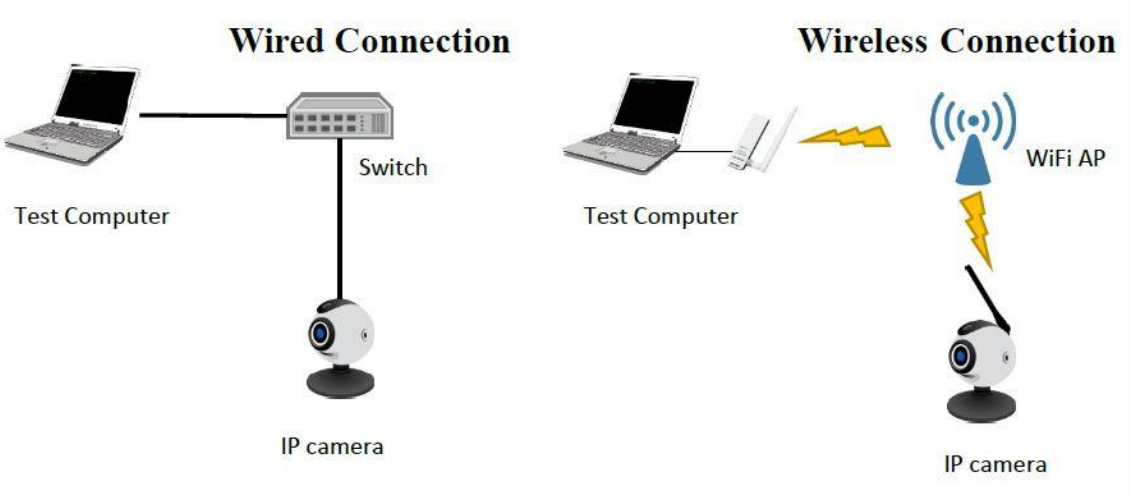

Figure 11 Test Setup

(5) Test Method:

(i) Review submitted documents for compliance.

(ii) Connect DUT with a Test Computer.

(iii) Inspection shall be conducted on security mechanism of password and related information.

(iv) Inspection shall be conducted on security mechanism of encryption/decryption key.

(6) Expected Results:

(i) Security mechanism for password and related information shall be defined in accordance with “One-way Hash” function of FIPS 140-2 Annex A.

(ii) Security mechanism for encryption/decryption key shall be defined in accordance with “One-way Hash” function of FIPS 140-2 Annex A.

5.2.4.3 Key Management Procedure

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.2.4.3.

(b) Purpose:

Verify whether reliable procedures shall be conducted on key management.

(c) Sample Condition:

Written documents of key management procedures shall be submitted.

(d) Test Setup:

None.

(e) Test Method:

(1) Review key management procedures for compliance.

(f) Expected Result:

(1) DUT shall possess specific procedures of key generation, exchange, storage, use, destruction and replacement. All procedures shall achieve the objective of monitoring, assurance and well management of keys.

5.2.4.4 Sensitive data storage isolation

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.2.4.4.

(b) Purpose:

Verify whether storage isolation between sensitive data and those from normal operating system shall be conducted.

(c) Sample Condition:

(1) Written documents of sensitive data storage and management shall be submitted for review.

(2) Written documents shall be provided in specifying secure domain for the storage of each individual security application for review.

(d) Test Setup:

None.

(e) Test Method:

(1) Review submitted functional related documents.

(f) Expected Result:

(1) Submitted documents shall clearly define secure domain for the storage of sensitive data.

5.2.5 Security of Website Management Interface

5.2.5.1 Cybersecurity risk evaluation of Website Management Interface

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.2.5.1.

(b) Purpose:

Verify whether known CVE shall exist in Website Management Interface.

(c) Sample Condition:

Administrator privileges shall be provided for testing purpose.

(d) Test Setup:

Refer to Figure 12.

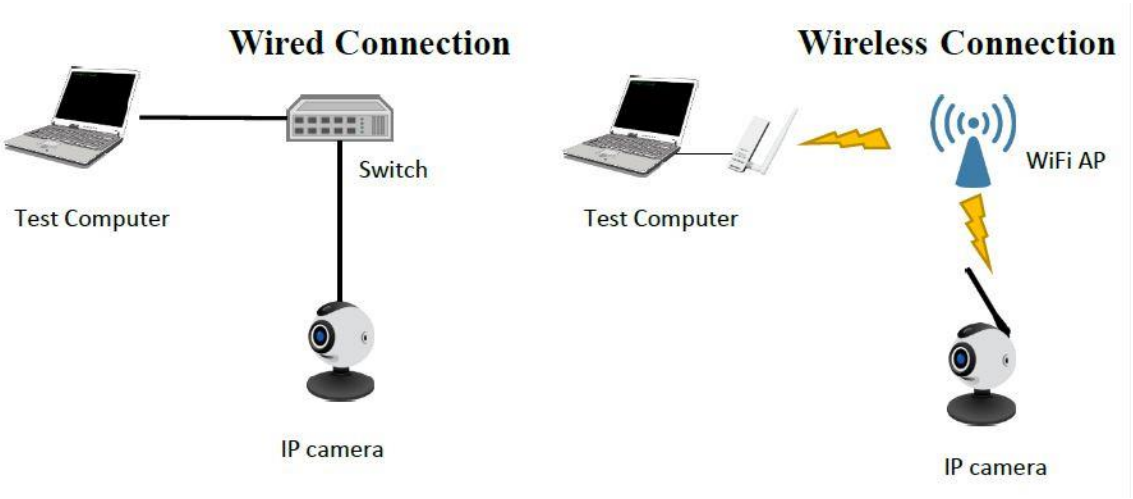

Figure 12 Test Setup

(e) Test Method:

(1) Connect DUT with a Test Computer.

(2) Activate website management interface, inspection shall be conducted for utilizing HTTP within the website.

(3) Activate website CVE scanning tool for website management interface verification.

(4) Review scanning report and evaluate the possible risks of Injection and Cross-Site Scripting (XSS).

(f) Expected Result:

(1) Website Management Interface of DUT shall not be exposed to the risks of Injection and XSS attack with referring to OWASP web Top 10 [3].

5.2.6 ONVIF API Security of Control Program

5.2.6.1 Authentication Mechanism of API

(a) Strength Evaluation of API Authentication Mechanism

(1) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.2.6.1.

(2) Purpose:

Verify whether API calling shall be conducted with authentication mechanism, and the authentication mechanism shall be resistant to replay attacks.

(3) Sample Condition:

Applicable to Test Computer or Mobile Device with control program interface (i.e. ONVIF API) only.

(4) Test Setup:

Refer to Figure 13.

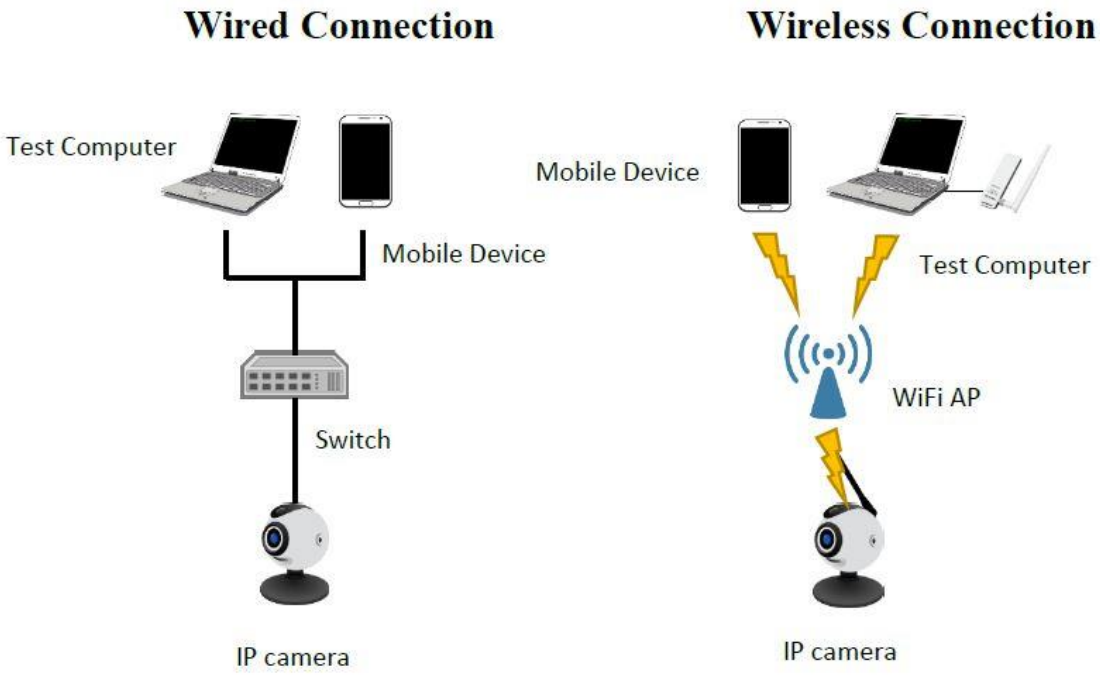

Figure 13 Test Setup

(5) Test Method:

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

(ii) Follow user manual instructions to activate ONVIF API control program.

(iii)Through linkage between the control program and DUT, conduct online packet sniffing of linkage.

(iv) Conduct video surveillance related operations and inspect sniffed packets to verify the existence of authentication mechanism.

(v) If authentication mechanism is required, apply the above sniffed, authenticated packets onto DUT for another authentication process.

(vi) Monitor the result from authentication process.

(6) Expected Results:

(i) Authentication is required for DUT access.

(ii) Replay attack prevention shall be achieved.

(b) Error Message from Authentication Mechanism of API

(1) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.2.6.1.

(2) Purpose:

Verify whether error messages shall cause the leakage of sensitive data.

(3) Sample Condition:

User accounts shall be created on DUT.

(4) Test Setup:

Refer to Figure 14.

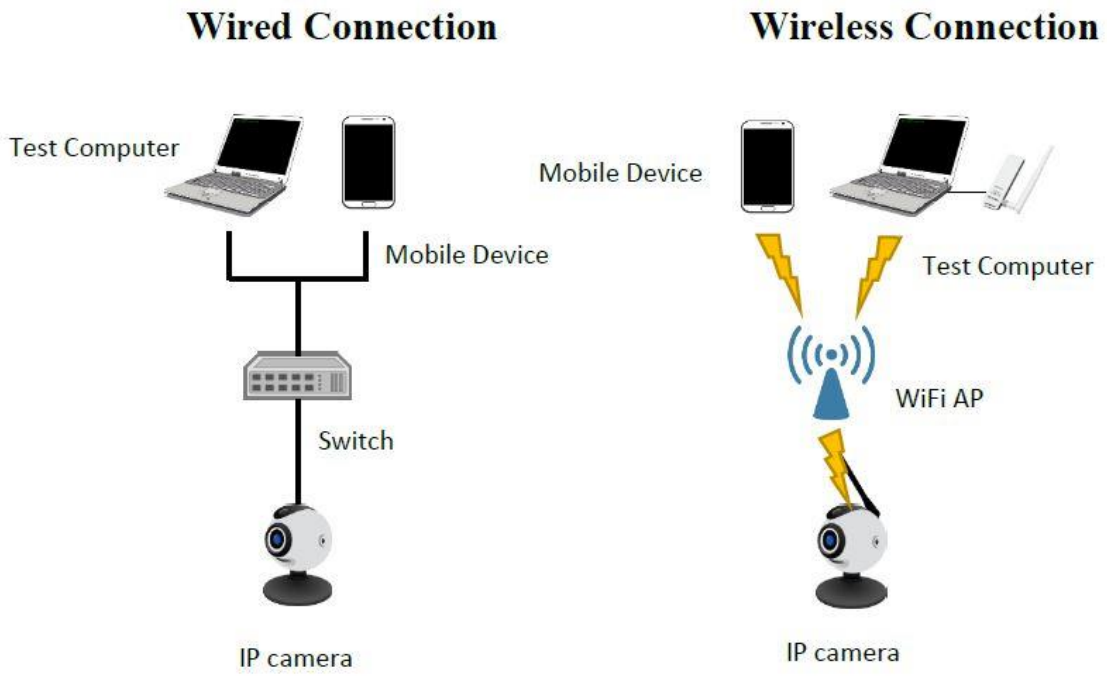

Figure 14 Test Setup

(5) Test Method:

(i) Connect DUT with a Test Computer.

(ii) Follow user manual instructions to activate ONVIF API control program.

(iii) Create linkage between the control program and DUT.

(iv) Conduct video surveillance related operations and inspect sniffed packets to verify the existence of authentication mechanism.

(v) Input existing user account with incorrect password and inspect error messages in return from authentication process.

(vi) Input non-existing account and inspect error messages in return again.

(6) Expected Result:

(i) From error messages returning from DUT, no legitimate user name shall be identified.

5.2.6.2 Strength Evaluation of API Password Authentication

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.2.6.2.

(a) Purpose:

Verify whether the API password authentication of DUT shall be enough to ensure sufficient security strength.

(b) Sample Condition:

(1) Applicable to DUT with API password authentication mechanism only.

(2) Description of account lockup design shall be submitted.

(c) Test Setup:

Refer to Figure 15.

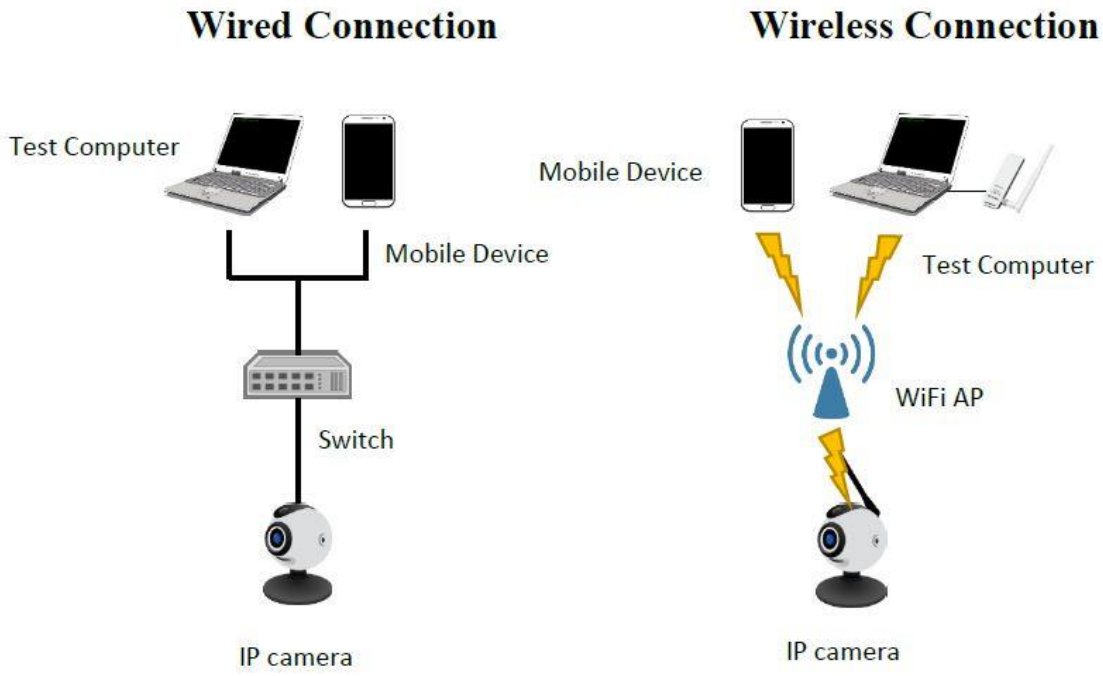

Figure 15 Test Setup

(d) Test Method:

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

(2) Conduct security evaluation on password authentication mechanism of DUT by following section 5.4.2.1, 5.4.2.2, 5.4.2.3 and 5.4.2.4.

(e) Expected Result:

(1) Password authentication mechanism of DUT shall comply with the expected results of section 5.4.2.1, 5.4.2.2, 5.4.2.3 and 5.4.2.4.

5.2.6.3 API Access Control Mechanism

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.2.6.3.

(b) Purpose:

Verify whether API Access Control Mechanism shall exist on DUT.

(c) Sample Condition:

(1) Declaration of API authorization limits for each different role.

(2) Applicable to DUT with control program interface only.

(3) User accounts and respective passwords shall be established, including both administrators and general users.

(d) Test Setup:

Refer to Figure 16.

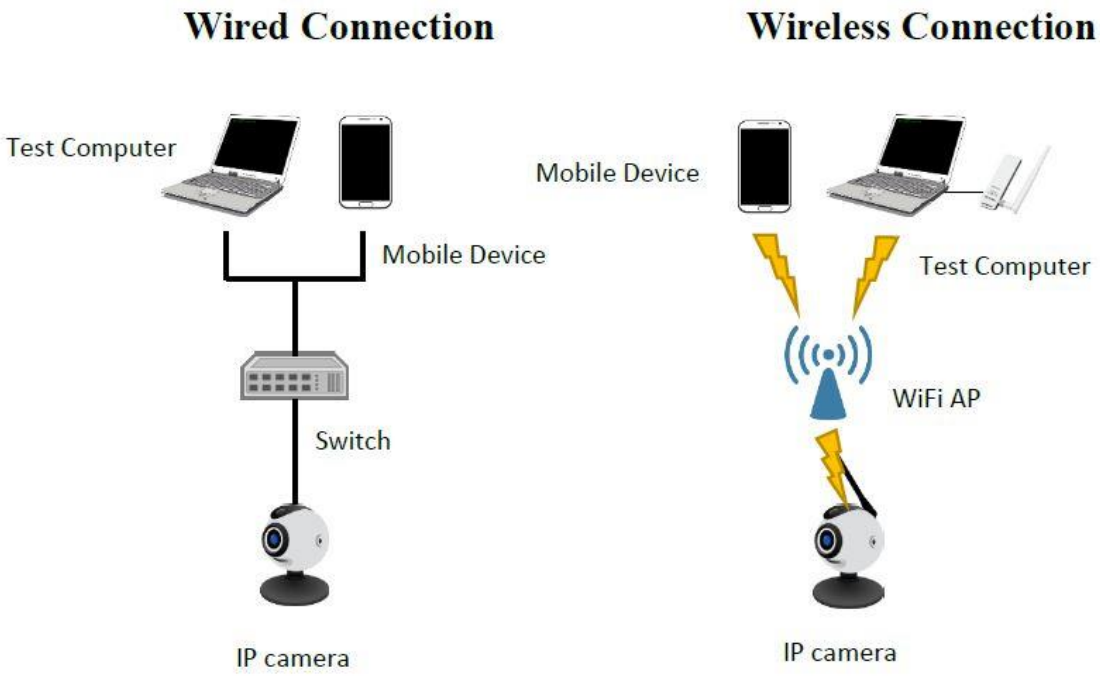

Figure 16 Test Setup

(e) Test Method:

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

(2) Follow user manual instructions to activate the control program of the Test Computer or Mobile Device.

(3) With different roles being adopted, access DUT by utilizing ONVIF API.

(4) Cross-check type of accounts with respective authorization limits comparing with declaration documents.

(f) Expected Results:

(1) Authorization limits of all defined roles of ONVIF API are consistent with DUT's declaration documents.

(2) At least two different authorization limits on roles shall be defined.

5.2.7 Logs and warnings

5.2.7.1 Security events log

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.2.7.1.

(b) Purpose:

Verify whether security event logs shall exist for queries.

(c) Sample Condition:

None.

(d) Test Setup:

Refer to Figure 17.

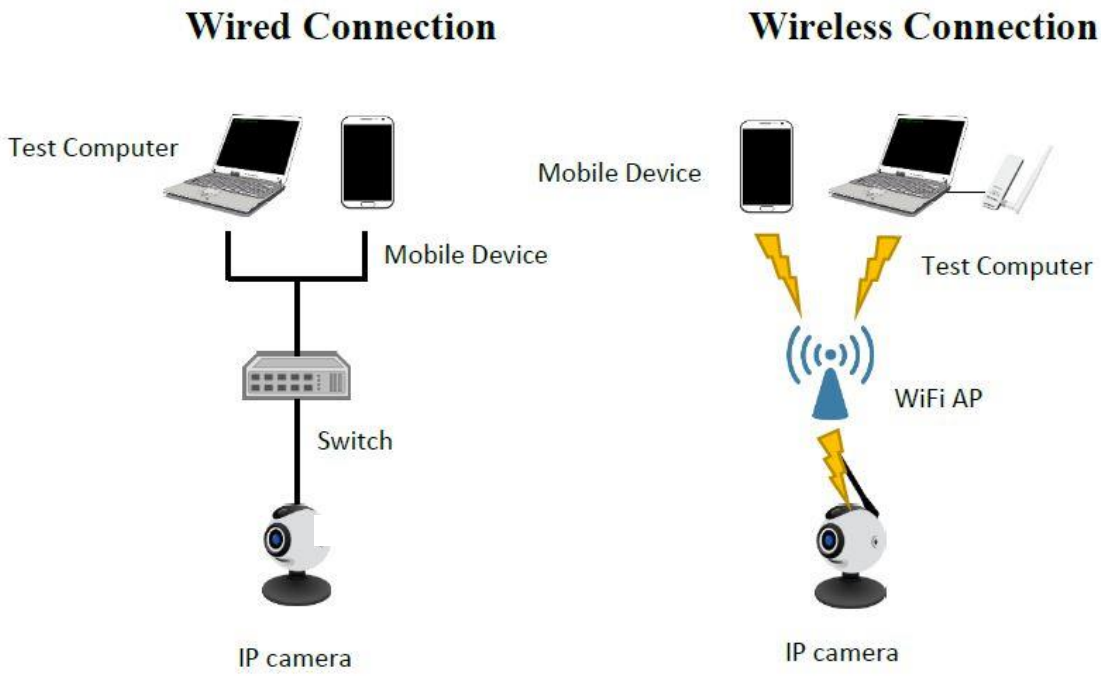

Figure 17 Test Setup

(e) Test Method:

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

(2) Activate respective control management tools by following user manual instructions and create linkage in reviewing security events log record.

(3) Inspect log records and check the existence of user login records.

(4) Log inspection shall be conducted with data input of time, user identity and event description.

(5) Reset DUT.

(6) Inspect log records again in confirming the existence of history records.

(f) Expected Results:

(1) DUT shall be designed with security events log functions for users.

(2) Security event log shall include time (with year, month, day, hour, minute and second), user identity and event description.

(3) Reset of DUT shall not affect log content.

5.2.7.2 Access control of Security Events Log Access

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.2.7.2.

(b) Purpose:

Verify whether access control shall be conducted for security events log.

(c) Sample Condition:

(1) User accounts and respective authentication factors, e.g. password, shall be established, including both administrators and general users.

(2) Authorization limit description for security events log access shall be submitted.

(d) Test Setup:

Refer to Figure 18.

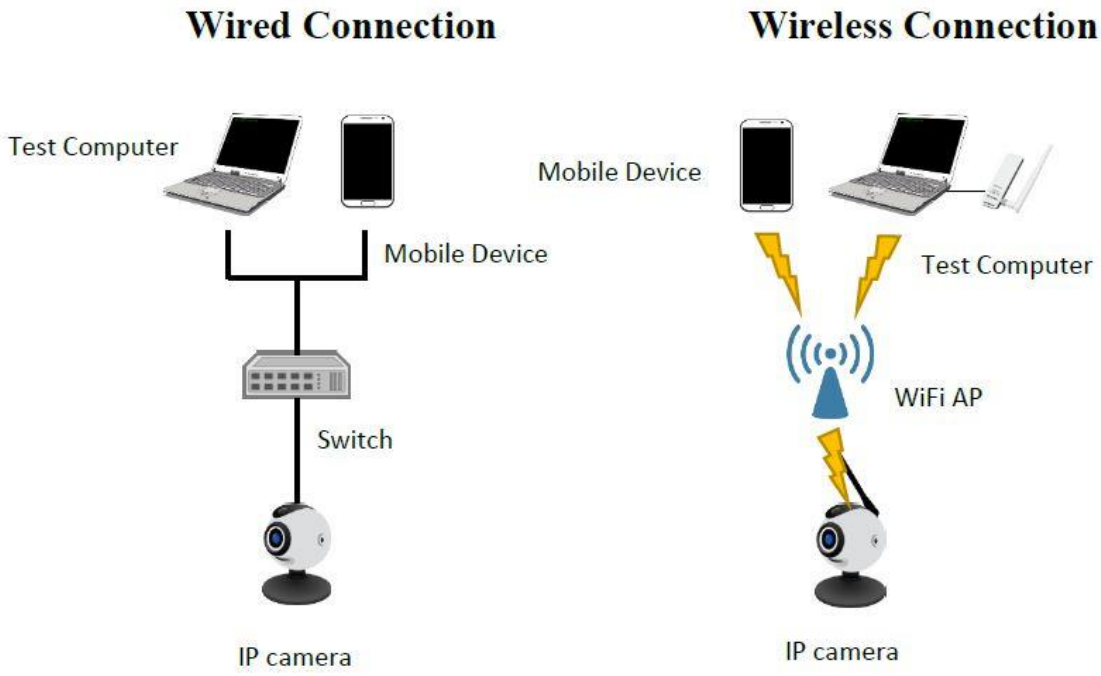

Figure 18 Test Setup

(e) Test Method:

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

(2) Activate respective control management tools by following user manual instructions and create linkage in reviewing security events log records.

(3) Review account identities with respect to security events log access and cross-check the declaration documents for compliance.

(f) Expected Results:

(1) Authorization mechanism of security event log access shall be consistent with that in declaration documents.

(2) At least two different authorization limits on roles shall be defined.

5.2.7.3 Log rotation function of security events log files

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.2.7.3.

(b) Purpose:

Verify whether log rotation function of DUT shall be conducted to avoid the running out of disk space.

(c) Sample Condition:

Administrator privileges shall be provided.

(d) Test Setup:

Refer to Figure 19.

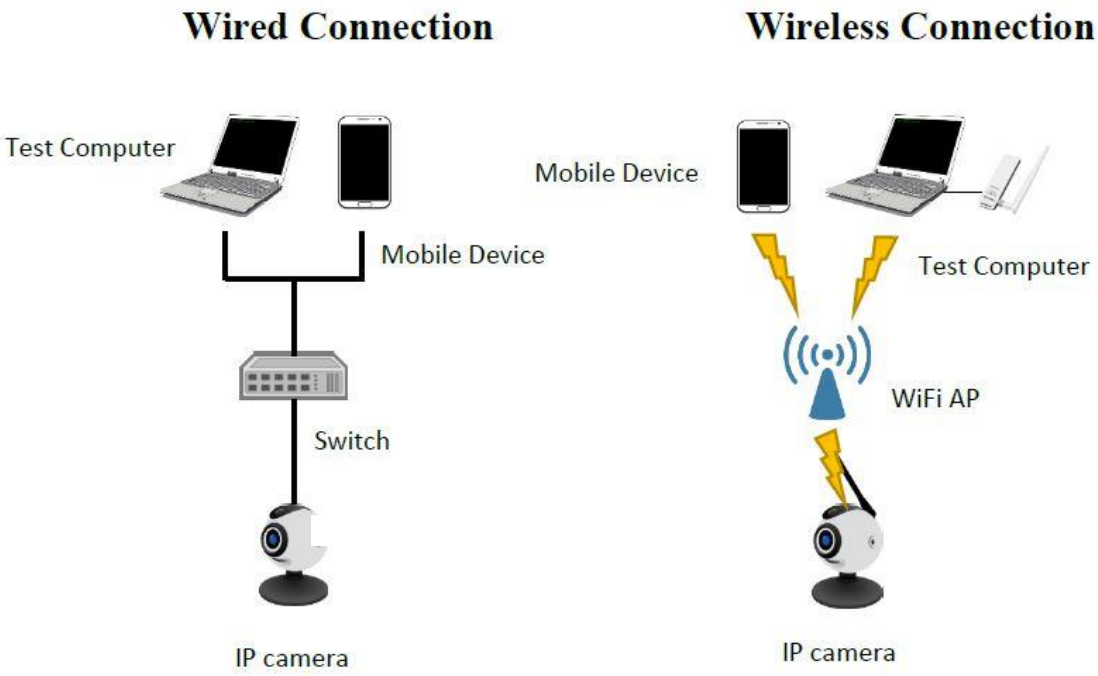

Figure 19 Test Setup

(e) Test Method:

(1) Trigger security events continuously in causing disk space exhaustion.
(2) Inspect whether security events are recorded properly.

(f) Expected Results:

(1) Insufficient disk space situation shall not occur.
(2) DUT continues with event logging, with no abnormal situation occurring.

5.2.7.4 Abnormal warning function

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.2.7.4.

(b) Purpose:

Verify whether security events log files shall be available.

(c) Sample Condition:

(1) Authorization limit of administrators shall be provided.

(2) Warnings of disk space exhaustion of security event logs shall be provided.

(d) Test Setup:

Refer to Figure 20.

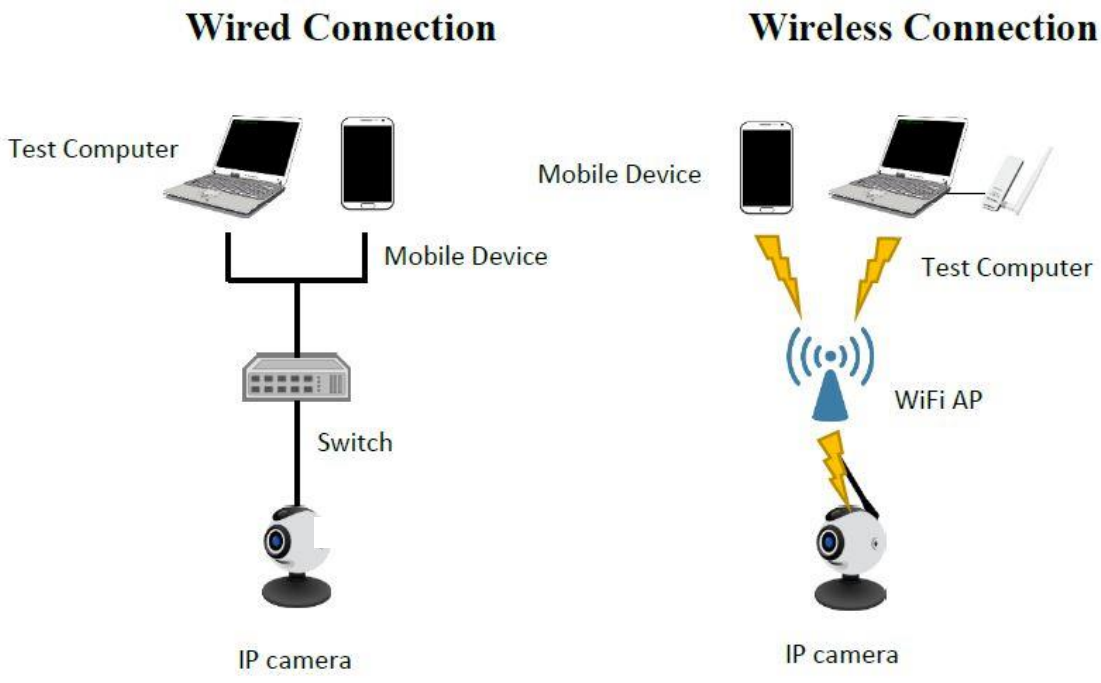

Figure 20 Test Setup

(e) Test Method:

(1) Trigger security events continuously until disk space exhaustion.

(2) Inspection shall be conducted with warnings activated.

(f) Expected Result:

(1) Warnings shall be activated with disk space exhaustion of security event logs.

5.3 Communication Security

Inspect the video surveillance device under test (DUT) and review submitted documents in fulfilling communication security test requirements, and conduct test items defined below accordingly.

5.3.1 Security of Sensitive Data in Transmission

5.3.1.1 Elementary Security Test of Sensitive Data in Transmission

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.3.1.1.

(b) Purpose:

(1) Verify whether sensitive data transmission shall be conducted in sufficient secure tunnel by default.
(2) Verify whether the certificate of secure tunnel shall stay valid to assure its effectiveness and legitimacy.

(c) Sample Condition:

(1) DUT shall remain in factory default environment conditions.
(2) Compatible video surveillance devices shall be provided for verification purpose.
(3) For video surveillance devices, in connection with DUT, with self-signed certificate, intermediate certificate editor interface shall be provided.

(d) Test Setup:

Refer to Figure 21.

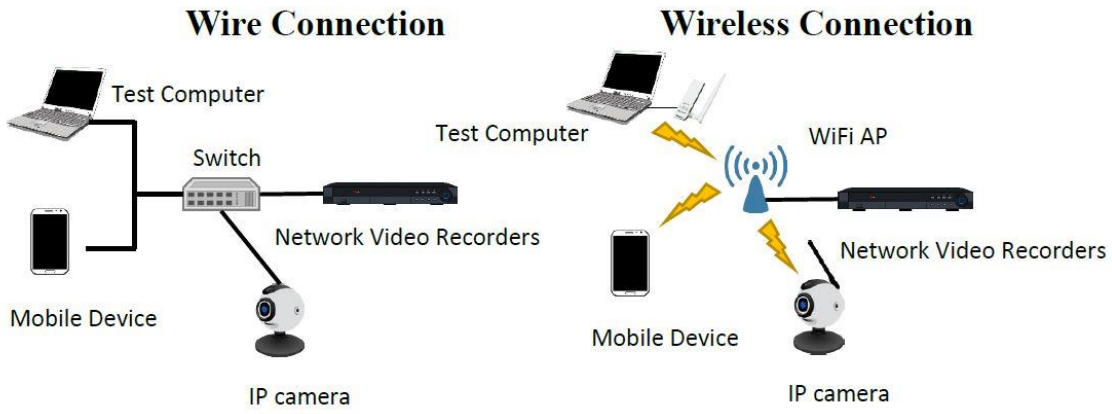

Figure 21 Test Setup

(e) Test Method:

(1) Apply secure tunnel scanning to DUT.

(2) Compare DUT's scanned results with those of cipher suite provided in Appendix A.

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

(4) Enter account and password into respective control management interface and conduct packet sniffing.

(5) Inspection shall be conducted to verify sniffed packets out of secure tunnel.

(6) Connect DUT with other security surveillance devices and activate secure tunnel establishment procedure.

(7) While other devices issuing certificate to DUT, intercept and replace certificate's public key and/or information with changed issuer, changed effective date, incorrect format and incorrect signature.

(8) Send out tampered certificate to DUT. Monitor packets under hand-shaking process within secure tunnel on its acceptance.

(f) Expected Results:

(1) Secure tunnel shall support cipher suites suggested in Appendix A only.

(2) Under default condition, account and password transmission with the Test Computer shall adopt secure tunnel.

(3) Under default condition, account and password transmission with the Mobile Device shall adopt security tunnel.

(4) Secure tunnel certificate for tampered sensitive data shall not be accepted by DUT.

5.3.1.2 Intermediate Security Test of Sensitive Data in Transmission

(a) Compliance:

TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.3.1.2.

(b) Purpose:

Verify whether strong encryption algorithm shall be available for sensitive data transmission within secure tunnel.

(c) Sample Condition:

None.

(d) Test Setup:

Refer to Figure 22.

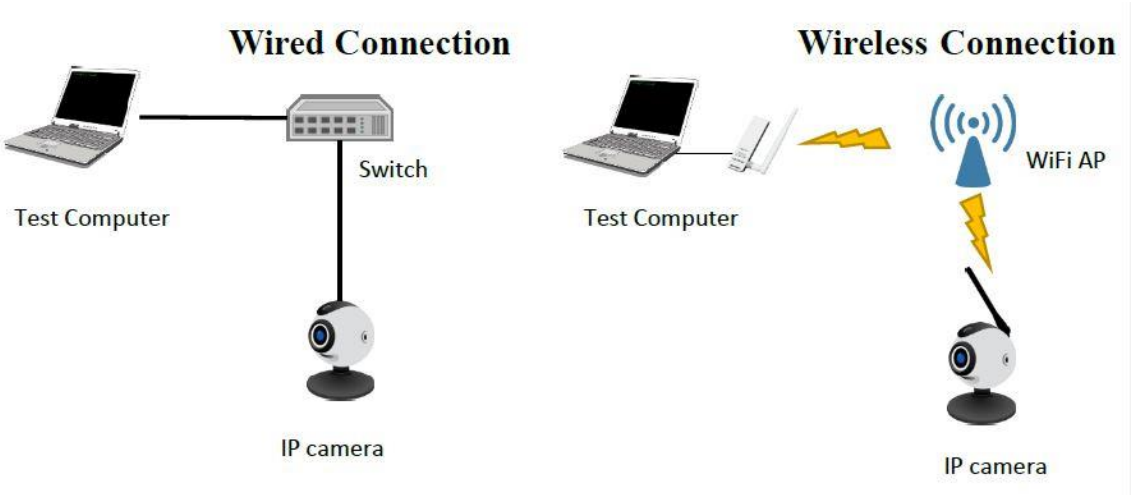

Figure 22 Test Setup

(e) Test Method:

(1) Connect a Test Computer with DUT.
(2) Apply secure tunnel scanning tool to DUT.
(3) Compare DUT's scanned results with those of cipher suite provided in Appendix A to verify its support of AES-256 equivalent or higher encryption algorithm.

(f) Expected Result:

(1) Secure tunnel supports AES-256 equivalent or higher encryption algorithm.

5.3.2 Communication protocols and configuration security

5.3.2.1 Network devices discovery function

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.3.2.1.

(b) Purpose:

Verify whether DUT is operating under network settings to cope with cybersecurity risks.

(c) Sample Condition:

(1) Applicable to DUT supporting either UPnP, SNMP or Bonjour services.
(2) DUT shall remain in factory default environment conditions.
(3) Written documents shall be submitted with description of all supported network services.

(d) Test Setup:

Refer to Figure 23.

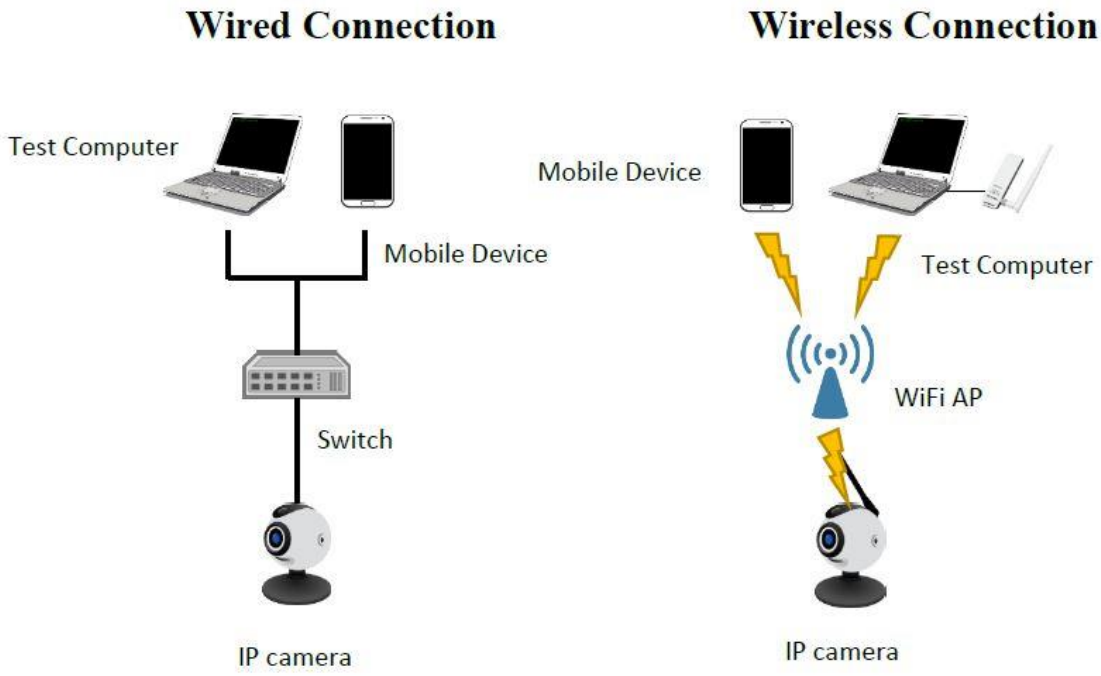

Figure 23 Test Setup

(e) Test Method:

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

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

(3) For DUT supporting UPnP protocol, visual inspection shall be conducted on either the control program or website control management for the existence of user applicable ON/OFF interface.

(4) Apply UPnP protocol scanning tool to identify whether DUT is equipped with the protocol service and also user applicable ON/OFF selection.

(5) For DUT supporting SNMP protocol, visual inspection shall be conducted on either the control program or website control management for the existence of user applicable ON/OFF interface.

(6) Apply SNMP protocol scanning tool to identify whether DUT is equipped with the protocol service and also user applicable ON/OFF selection.

(7) For DUT supporting Bonjour protocol, visual inspection shall be conducted on either the control program or website control management for the existence of user applicable ON/OFF interface.

(8) Apply Bonjour protocol scanning tool to identify whether DUT is equipped with the protocol service and also user applicable ON/OFF selection.

(f) Expected Results:

(1) For DUT supporting UPnP protocol, ON/OFF function shall be provided for user selection.

(2) For DUT supporting SNMP protocol, ON/OFF function shall be provided for user selection.

(3) For DUT supporting Bonjour protocol, ON/OFF function shall be provided for user selection.

5.3.2.2 Network Interface Access Setup

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.3.2.2.

(b) Purpose:

Verify whether DUT shall be designed with secure remote access to the debug mode of operating system.

(c) Sample Condition:

(1) DUT shall remain in factory default environment conditions.

(2) Debug mode access instructions shall be provided for verification purpose.

(d) Test Setup:

Refer to Figure 24.

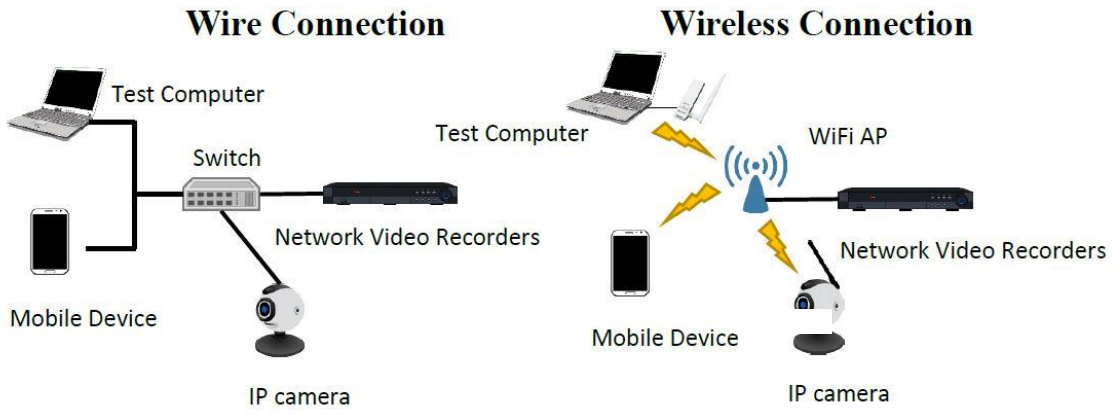

Figure 24 Test Setup

(e) Test Method:

(1) Connect DUT with a Test Computer.

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

(3) Verify the accessibility to the debug mode of operating system through network connection.

(4) Connect DUT to a Test Computer through a USB port.

(5) Again, verify the accessibility to the debug mode of operating system through the USB Port.

(6) If password and authentication is necessary before the access, security tests according to Section 5.4.2.1, 5.4.2.2, 5.4.2.3 and 5.4.2.4 shall be conducted.

(f) Expected Results:

(1) No remote access to the debug mode of DUT's operating system shall exist.

(2) If remote access to the debug mode of DUT's operating system exists, authentication process shall be adopted.

(3) With the existence of both remote access to and authentication process for the debug mode of DUT's operating system, respective authentication mechanism shall comply with the expected results of Section 5.4.2.1, 5.4.2.2, 5.4.2.3 and 5.4.2.4.

5.3.2.3 Abnormal Input of Communication Protocol

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.3.2.3.

(b) Purpose:

Verify whether unknown security vulnerabilities of communication protocol shall exist.

(c) Sample Condition:

None.

(d) Test Setup:

Refer to Figure 25.

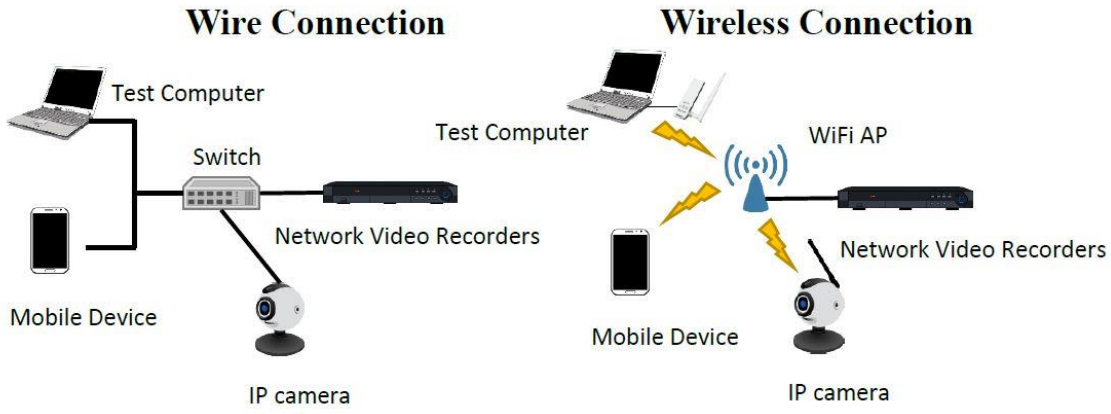

Figure 25 Test Setup

(e) Test Method:

(1) Connect DUT with a Test Computer.
(2) Activate Fuzzy testing tool.
(3) Referring to Appendix B, e.g. B1, B2, B3, and according to the protocol types being specified, apply abnormal input tests on each column (1) with 100,000 independent records, or (2) with 8 hours time duration at the minimum.
(4) Ensure only one single test case being conducted during the time period.
(5) While DUT is under test, verify whether DUT shall be in normal operation condition.

(f) Expected Result:

(1) During the test, DUT shall not crash due to specific abnormal packets.

5.3.3 Wi-Fi Communication Security

Test items within this section refer to “Wireless IP Camara Cybersecurity Test Guide” [4], issued by National Communications Commission (NCC).

5.3.3.1 Wi-Fi Configuration Setup Security

(a) Compliance:

“TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements”, Section 5.3.3.1.

(b) Purpose:

Verify whether incorrect Wi-Fi settings shall exist on DUT.

(c) Sample Condition:

(1) Applicable to DUT with Wi-Fi protected setup function only.
(2) DUT shall remain in factory default environment conditions.

(d) Test Setup:

Refer to Figure 26.

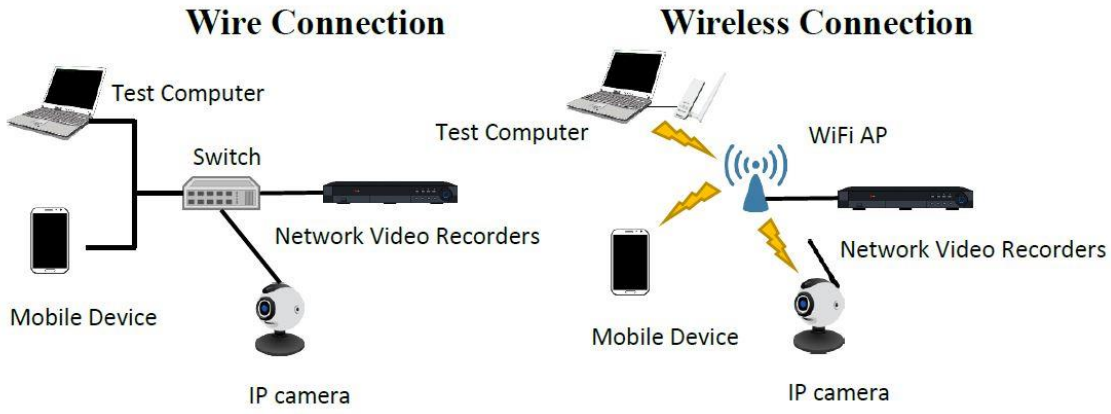

Figure 26 Test Setup

(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) Visual inspection shall be conducted on the control program or webpage control management and confirm that user operable ON/OFF interface of WPS PIN exists.

(f) Expected Results:

(1) User operable ON/OFF function of WPS PIN exists.
(2) Default setting of WPS PIN shall be OFF.

5.3.3.2 Wi-Fi security mechanism setup

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.3.3.2.

(b) Purpose:

Verify whether insecure settings of Wi-Fi channel protection shall exist.

(c) Sample Condition:

(1) Applicable to DUT supporting Wi-Fi function only.
(2) DUT shall remain in factory default environment conditions.

(d) Test Setup:

Refer to Figure 27.

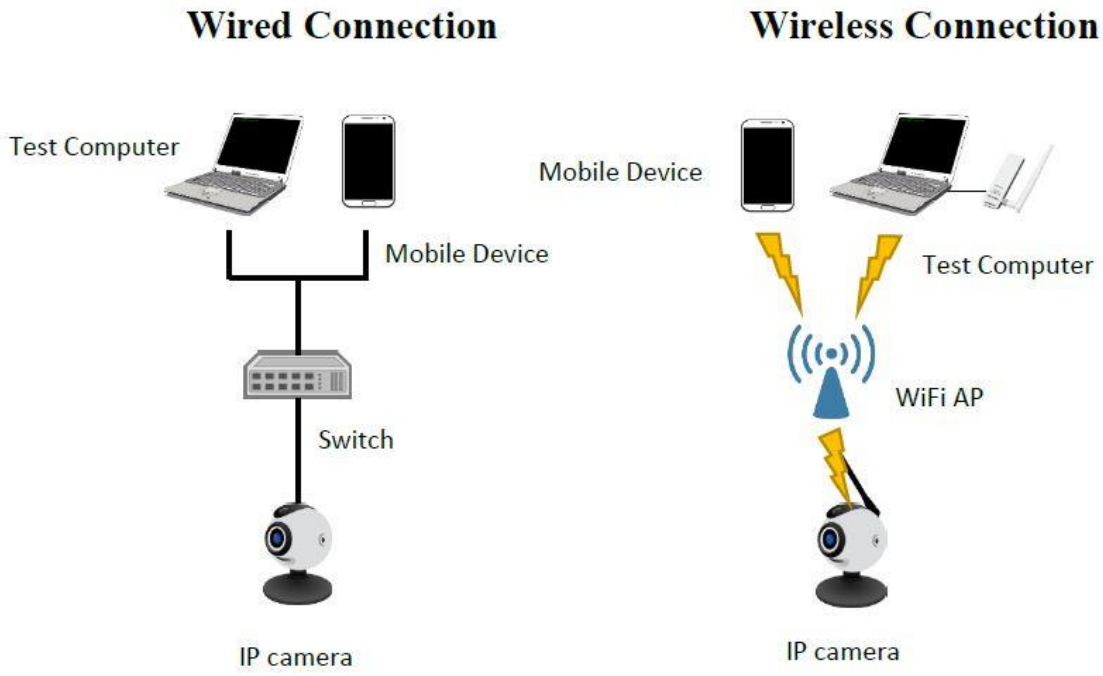

Figure 27 Test Setup

(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) Establish connection with DUT and conduct packet sniffing on Wi-Fi channel.

(4) Based upon packet sniffing results, verify that WPA2 encryption method is adopted.

(f) Expected Result:

(1) Default Wi-Fi encryption setting shall be WPA2.

5.3.3.3 Abnormal input of Wi-Fi communication protocol

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.3.3.3.

(b) Purpose:

Verify whether unknown security vulnerability shall exist in Wi-Fi communication protocol on DUT.

(c) Sample Condition:

None.

(d) Test Setup:

Refer to Figure 28.

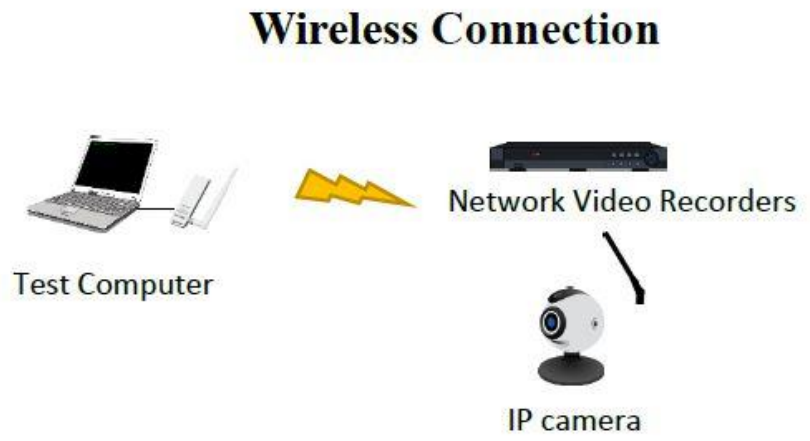

Figure 28 Test Setup

(e) Test Method:

(1) Link DUT with Wi-Fi connection with a Test Computer simulated as Wi-Fi AP.
(2) Activate Fuzzy testing tool.
(3) Conduct abnormal input tests on IEEE 802.11x communication protocol by applying each column (1) with 100,000 independent records, or (2) with 8 hours time duration at the minimum.
(4) Ensure only one single test case being conducted during the time period.
(5) While DUT under test, verify whether DUT shall be in normal operation condition.

(f) Expected Result:

(1) During the test, DUT shall not crash due to specific abnormal packets.

5.3.3.4 Wi-Fi authentication security mechanism setup

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.3.3.4.

(b) Purpose:

Verify whether DUT shall support IEEE 802.1x authentication.

(c) Sample Condition:

None.

(d) Test Setup:

Refer to Figure 30.

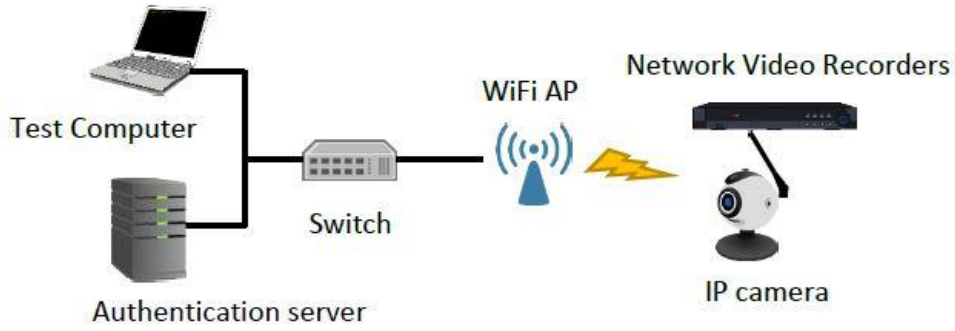

Figure 30 Test Setup

(e) Test Method:

(1) Activate DUT's IEEE 802.1x functions.
(2) Connect DUT through IEEE 802.1x with Wi-Fi AP.

(f) Expected Result:

(1) Wi-Fi connection through IEEE 802.1x shall be established.

5.4 Authentication and Authorization Mechanism Security

Inspect the video surveillance device under test (DUT) and review submitted documents in fulfilling authentication and authorization mechanism security test requirements, and conduct test items defined below accordingly.

5.4.1 Authentication mechanism security

5.4.1.1 Authentication mechanism strength

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.4.1.1.

(b) Purpose:

Verify whether reliable authentication mechanism shall be conducted on DUT.

(c) Sample Condition:

None.

(d) Test Setup:

Refer to Figure 30.

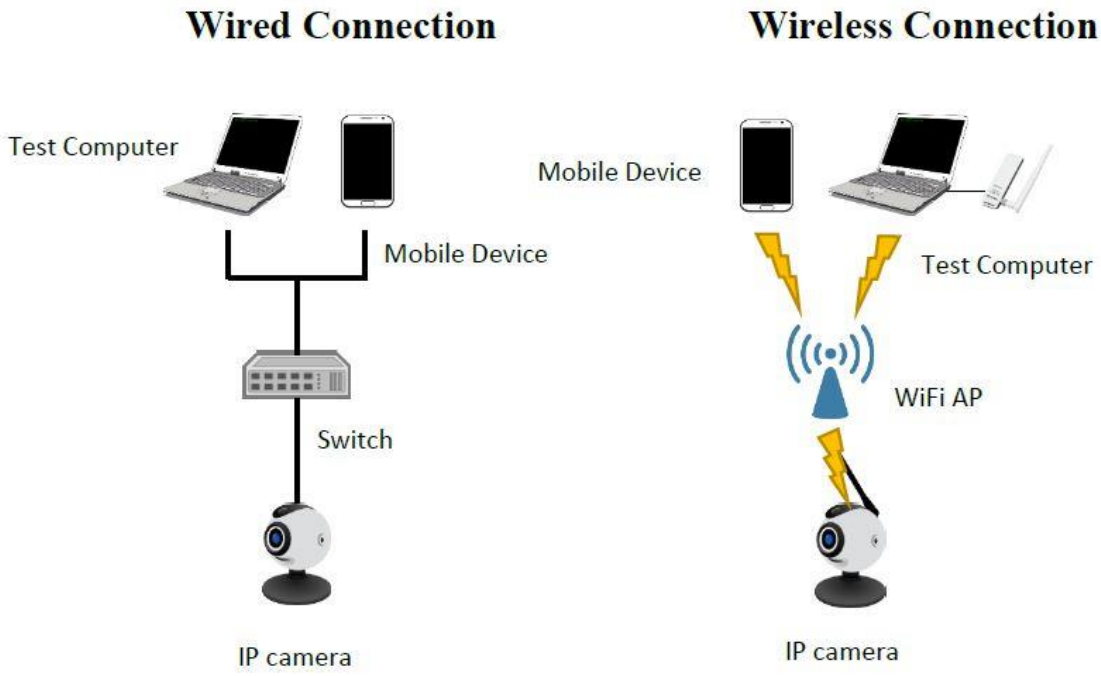

Figure 30 Test Setup

(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) Conduct authentication process and packet sniffing in parallel. Inspect authentication mechanism in operation.

(4) Apply the above sniffed, authenticated packets onto DUT for another authentication process.

(5) Monitor the result from authentication process.

(6) After logging out and re-logging in on DUT, conduct inspection on authentication functionality.

(f) Expected Results:

(1) Regardless through the webpage control management or control program in accessing video surveillance devices, authentication mechanism shall be in operation.

(2) Authentication mechanism shall possess the ability in preventing replay attacks.

(3) In order to access DUT after log-out, log-in is always necessary.

5.4.1.2 Error message of authentication

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.4.1.2.

(b) Purpose:

Verify whether error messages shall cause the leakage of sensitive data.

(c) Sample Condition:

None.

(d) Test Setup:

Refer to Figure 31.

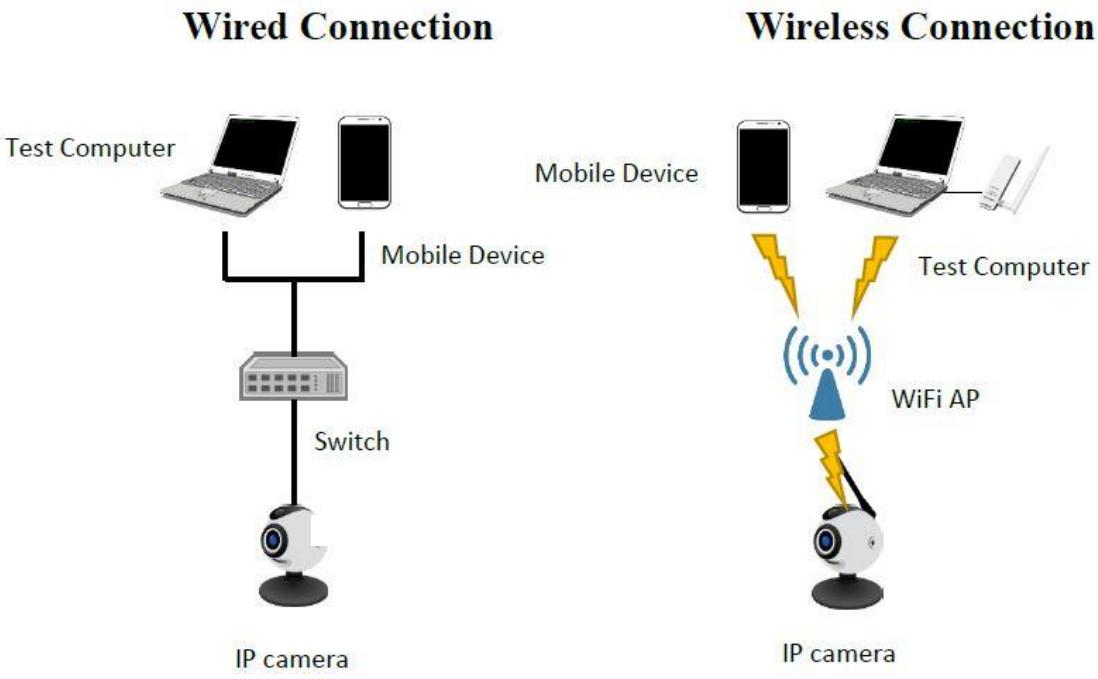

Figure 31 Test Setup

(e) Test Method:

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

(2) By following user manual instructions, activate respective control management tools for conducting authentication process.

(3) Log in with existing user account using incorrect password, and inspect error messages from authentication process.

(4) Log in with non-existent user account, inspect error messages from authentication process.

(f) Expected Result:

(1) From error messages, user account shall not be retrievable.

5.4.1.3 Certificate uploading interface

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.4.1.3.

(b) Purpose:

Verify whether DUT shall be equipped with certificate uploading function.

(c) Sample Condition:

(1) Certificate uploading procedures shall be provided.

(2) Compatible video surveillance devices shall be provided for testing purpose.

(d) Test Setup:

Refer to Figure 32.

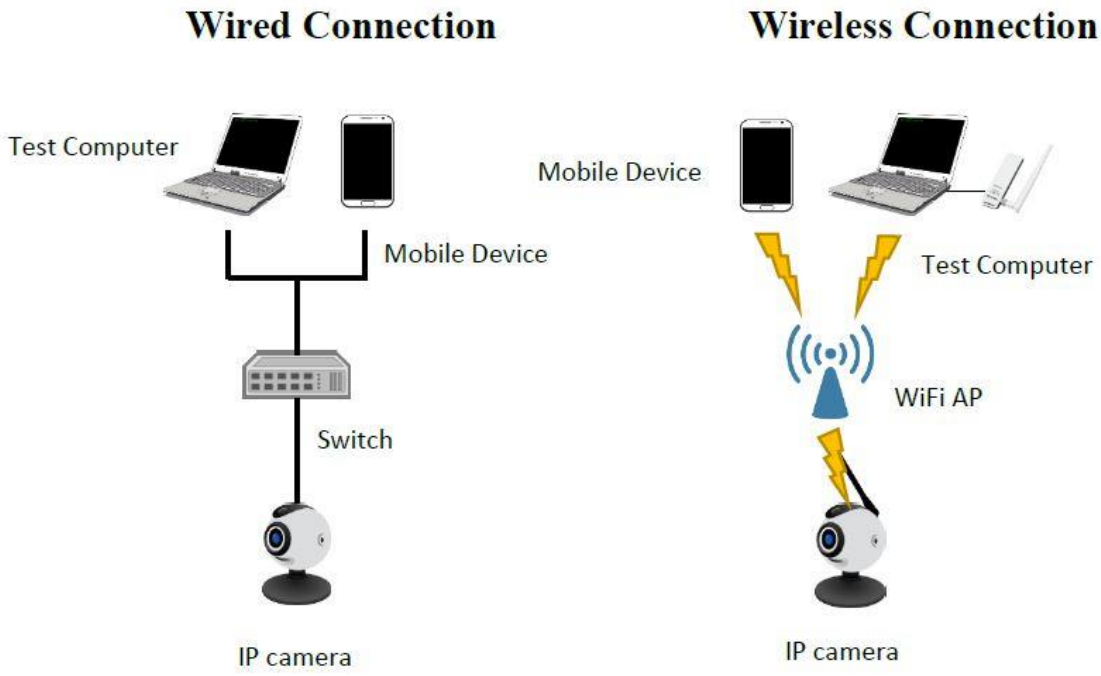

Figure 32 Test Setup

(e) Test Method:

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

(2) By following user manual instructions, activate respective control management tools for conducting certificate uploading.

(3) Connect to other video surveillance devices with certificate recognition capability. Verify whether the uploaded certificate shall be recognized.

(f) Expected Result:

(1) Uploaded certificate from DUT shall be recognized by its connected devices.

5.4.1.4 Uniqueness of key

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.4.1.4.

(b) Purpose:

Verify whether key shall be unique

(c) Sample Condition:

DUT compatible video surveillance devices shall be provided.

(d) Test Setup:

Refer to Figure 33.

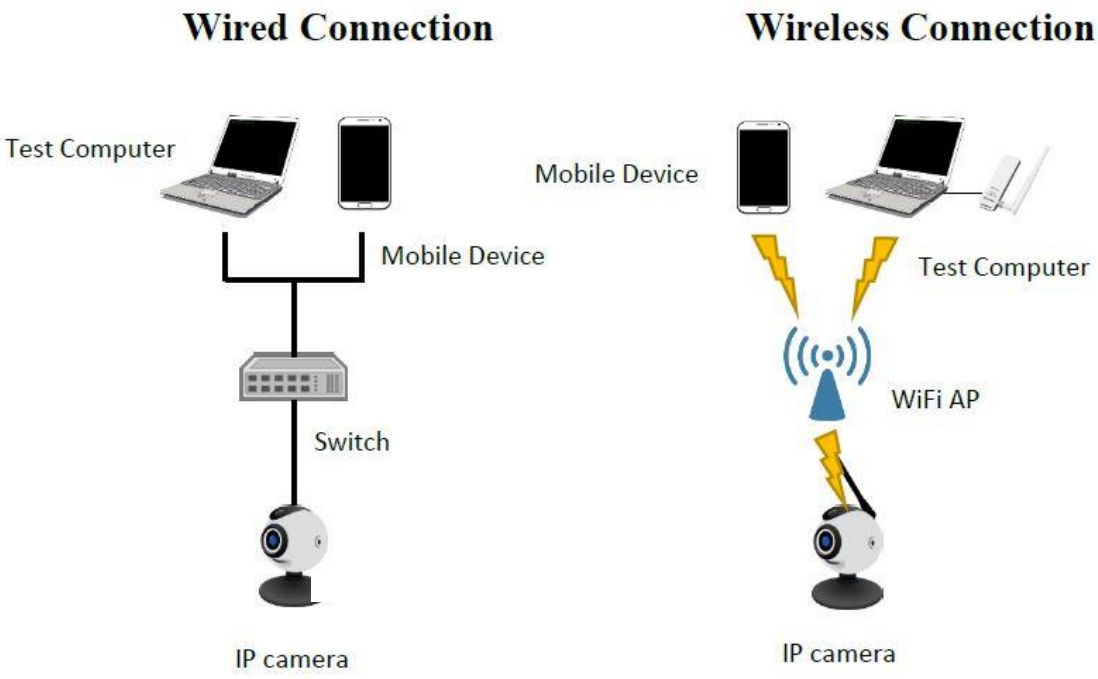

Figure 33 Test Setup

(e) Test Method:

(1) Connect DUT with a Test Computer or Mobile Device.
(2) By following user manual instructions, activate respective control management tools for conducting authentication process.
(3) Conduct packet sniffing and capture certificate of DUT. Investigate its respective fingerprint.
(4) Reset DUT to be in factory default environment conditions.
(5) Repeat steps 2 and 3.
(6) Connect DUT with other video surveillance devices in conducting authentication process.
(7) Conduct packet sniffing and capture certificate of DUT. Investigate its respective fingerprint.

(8) Reset DUT to be in factory default environment conditions.

(9) Repeat steps 6 to 8.

(f) Expected Results:

(1) If test equipment applies graphic management interface in connecting with DUT, fingerprint of certificate shall be different before and after the reset of factory default environment conditions.

(2) If test equipment applies secure shell (SSH) protocol in connecting with DUT, fingerprint of certificate shall be different before and after the reset of factory default environment conditions.

(3) If testing is conducted with DUT connecting with other video surveillance devices, fingerprint of certificate shall be different before and after the reset of factory default environment conditions.

5.4.1.5 Multi-factor authentication mechanism

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.4.1.5.

(b) Purpose:

Verify whether DUT's authentication mechanism shall support multi-factor authentication mechanism.

(c) Sample Condition:

(1) User account and respective authentication factors, e.g. password, shall be established and multi-factors authentication mechanism shall be activated.

(2) Operational procedures of multi-factors authentication mechanism shall be provided.

(d) Test Setup:

Refer to Figure 34.

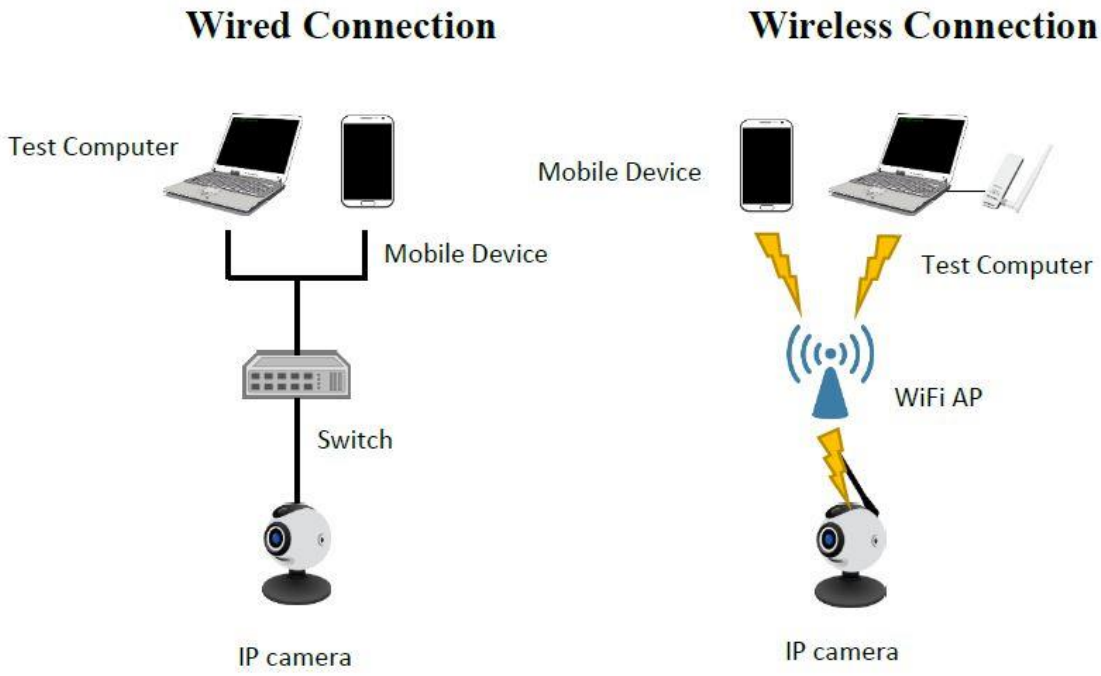

Figure 34 Test Setup

(e) Test Method:

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

(2) By following user manual instructions, activate respective control management tools for conducting authentication process.

(3) Apply mulit-factor authentication operations and verify authentication mechanism with one factor at a time.

(4) Use Short Message Service to acquire password in checking its availability.

(5) By using mobile devices as the authentication factor of “something you have”, verify the feasibility of multiple mobile devices in acquiring authentication factors at the same time.

(f) Expected Results:

(1) Multi-factor authentication can be achieved between DUT and webpage control management or control program.

(2) Different types of authentication factors are applicable to different stages of authentication operations.

(3) While applying authentication factors, Short Message Service is not a feasible practice for acquiring password.

(4) By using mobile devices as the authentication factors of "something you have", authentication factor can acquire from one single mobile device.

5.4.1.6 Device authentication

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.4.1.6.

(b) Purpose:

Verify whether DUT shall be capable of performing device authentication to all connected video surveillance devices and its device authentication mechanism shall be capable of preventing replay attacks.

(c) Sample Condition:

DUT compatible video surveillance devices shall be provided.

(d) Test Setup:

Refer to Figure 35.

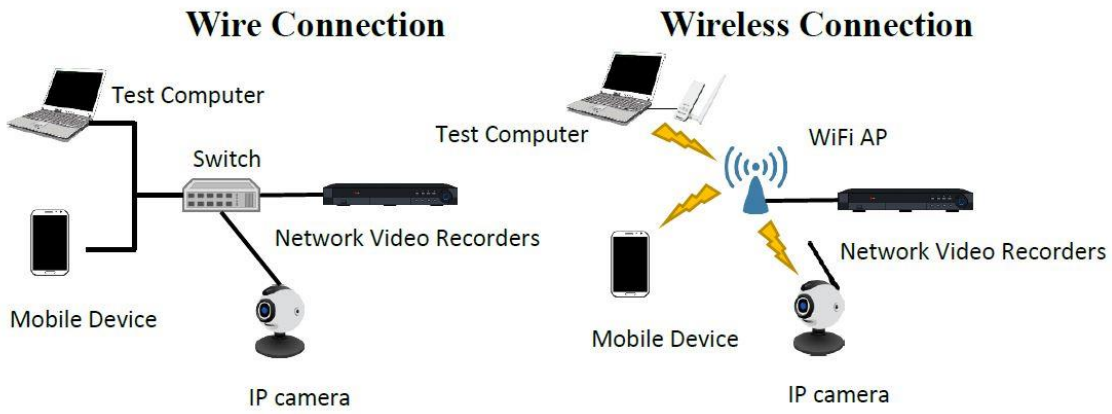

Figure 35 Test Setup

(e) Test Method:

(1) Connect DUT with other video surveillance devices.

(2) Connect other surveillance devices with a Test Computer or Mobile Device.

(3) Check authentication request from connecting devices.

(4) Activate authentication process and conduct packet sniffing.

(5) Apply the above sniffed, authenticated packets onto DUT for another authentication process.

(6) Inspect results from authentication process.

(f) Expected Results:

(1) While DUT is connecting with other video surveillance devices, authentication process is required.

(2) Device authentication mechanism shall be capable of preventing replay attacks.

5.4.2 Password authentication

5.4.2.1 Default password of API

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.4.2.1.

(b) Purpose:

(1) Scenario 1:

Verify whether DUT shall be set with identical default password.

(2) Scenario 2:

Verify whether DUT shall be required to change password during initial online.

(c) Sample Condition:

(1) Applicable to DUT supporting password authentication mechanism only.
(2) DUT shall remain in factory default environment conditions.

(d) Test Setup:

Refer to Figure 36.

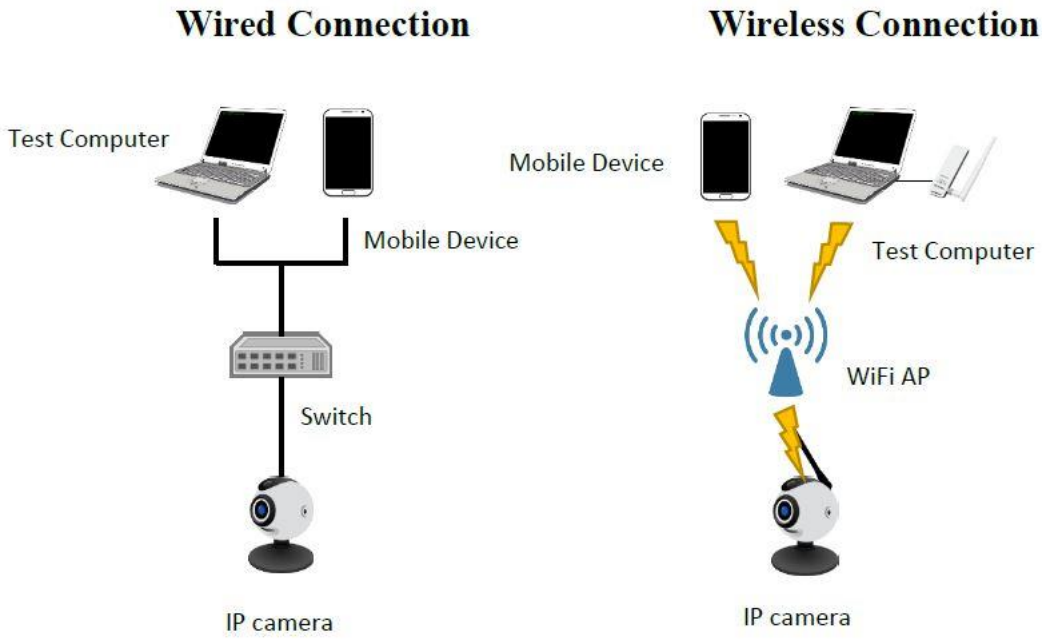

Figure 36 Test Setup

(e) Test Method:

(1) Scenario 1:

(i) Two units of DUT, at least, shall be provided.

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

(iii)Through webpage control management or control program, by following user manual instructions, enter the default password of DUT.

(iv) Compare default passwords of the two units.

(2) Scenario 2:

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

(ii) Enter DUT's password through webpage control management or control program.

(iii) Verify DUT's accessibility before new password being set.

(f) Expected Results:

(1) Scenario 1:

Passwords of the two units shall be different.

(2) Scenario 2:

DUT shall not be workable before new password being set.

Tests shall fulfill either one of the expected results for compliance.

5.4.2.2 Password length

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.4.2.2.

(b) Purpose:

Verify whether the length of DUT's password shall be long enough to ensure its security strength.

(c) Sample Condition:

Applicable to DUT supporting password authentication mechanism only.

(d) Test Setup:

Refer to Figure 37.

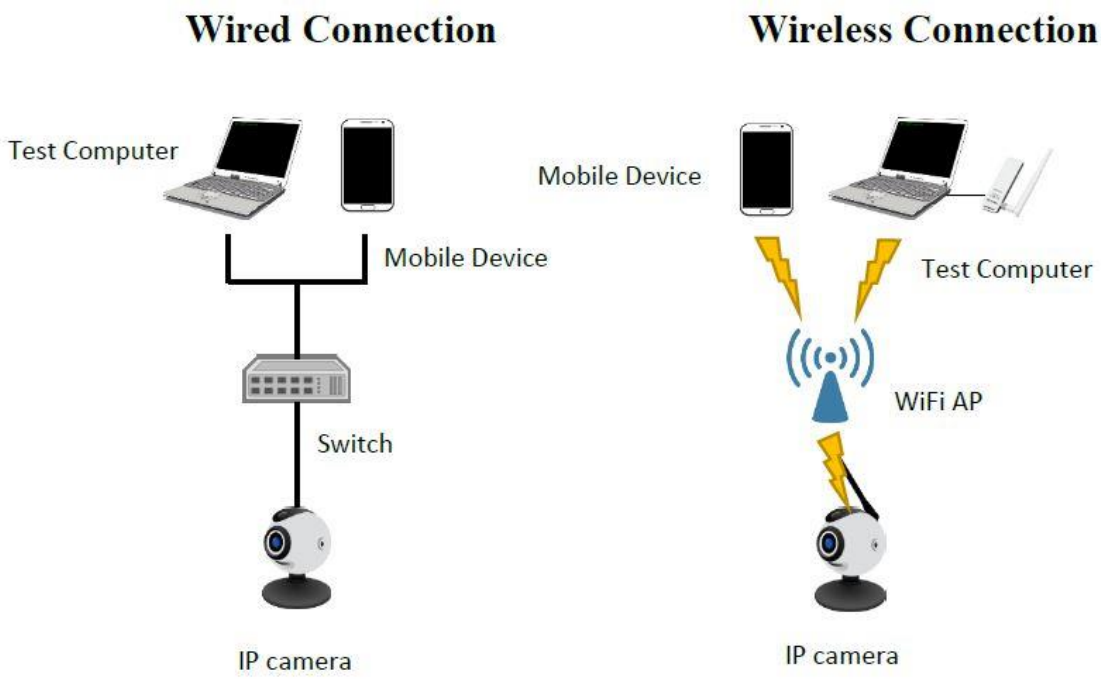

Figure 37 Test Setup

(e) Test Method:

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

(2) Create or change password by using webpage control management or control program.

(3) Enter password with less than 8 digits, check result feedback of the process.

(f) Expected Result:

(1) Password with less than 8 digits shall not be accepted.

5.4.2.3 Password complexity

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.4.2.3.

(b) Purpose:

Verify whether the password complexity of DUT shall be enough to ensure sufficient security strength.

(c) Sample Condition:

Applicable to DUT supporting password authentication mechanism only.

(d) Test Setup:

Refer to Figure 38.

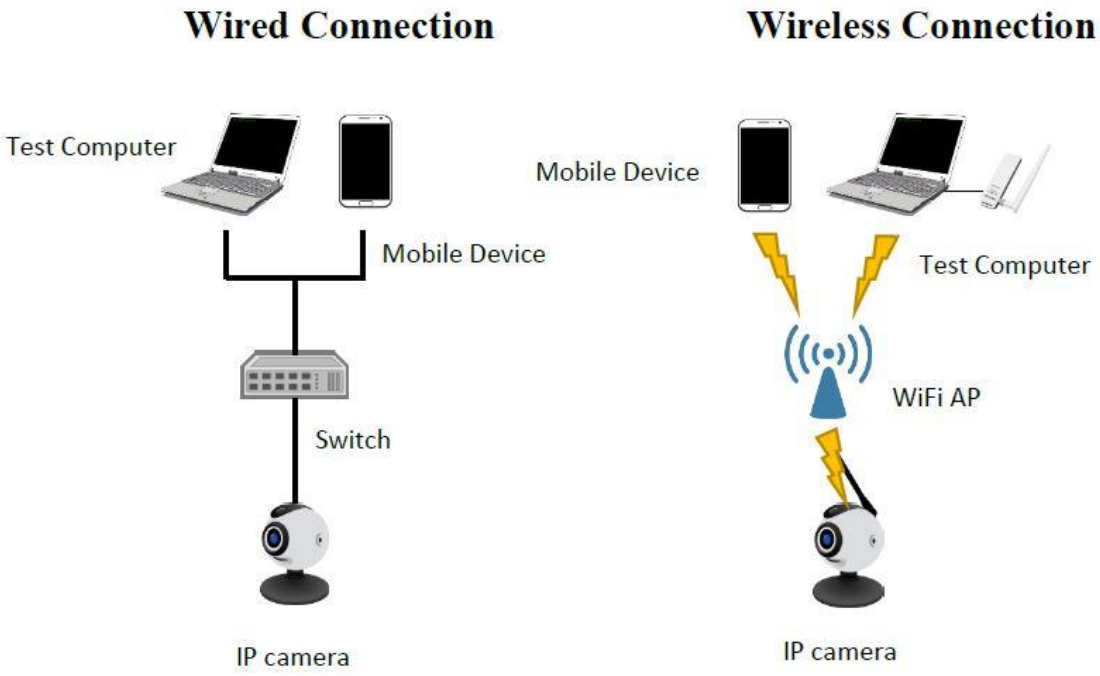

Figure 38 Test setup

(e) Test Method:

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

(2) Create or change password by using webpage control management or control program.

(3) Enter only one or two types of the following listed digits and check result feedback of the process.

(4) 1. English uppercase letters (A to Z)；

(5) 2. English lowercase letters (a to z)；

(6) 3. Decimal numbers (0 to 9)；

(7) 4. Non-alphabetic characters (e.g., !、$、#、%)

(f) Expected Result:

(1) Password can not be created or changed.

5.4.2.4 Password entry limits of frequency or number of times

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.4.2.4.

(b) Purpose:

Verify whether password authentication mechanism shall be performed to prevent brute-force attacks.

(c) Sample Condition:

(1) Applicable to DUT with authentication mechanism only.

(2) User accounts and respective authentication factors, e.g. password, shall be established.

(3) Design description of account locking mechanism shall be provided.

(d) Test Setup:

Refer to Figure 39.

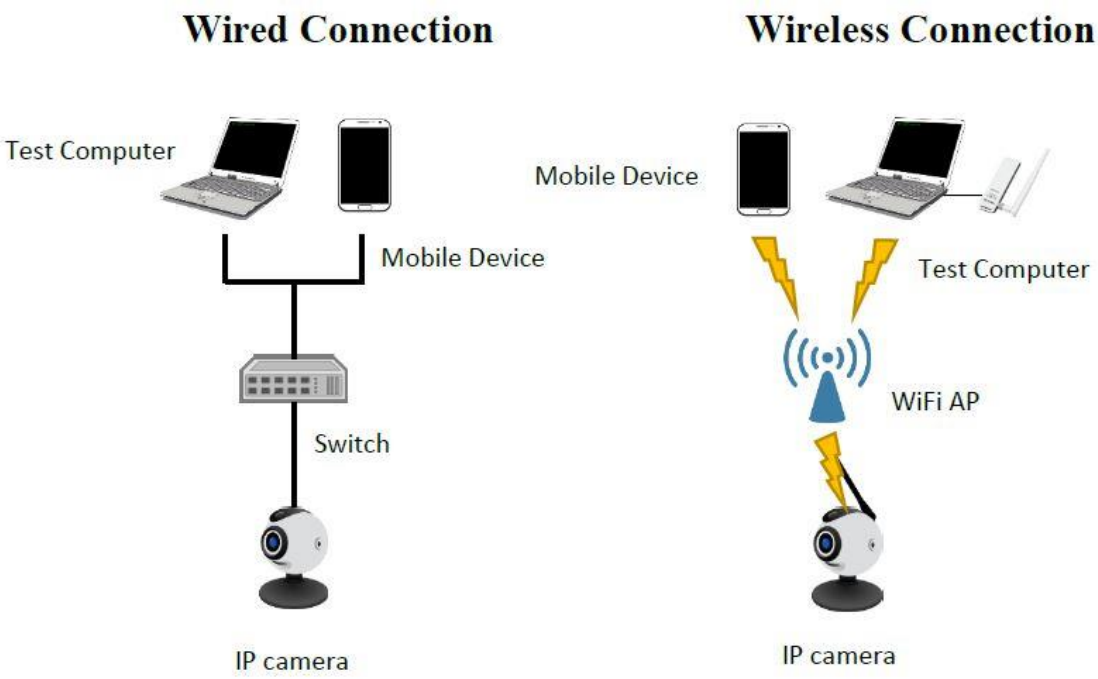

Figure 39 Test Setup

(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 conduct authentication process.

(3) Enter different incorrect passwords continuously.

(4) Before resetting DUT's account locking counter to zero, verify whether the account locking mechanism shall be activated after five continuous incorrect password entries.

(5) After account locked, continuously conduct password entries with different and incorrect passwords. Verify whether the account shall be unlocked within manufacturer's declared account locked time limit.

(6) After any failed login of one account, re-enter incorrect and different passwords. Verify whether the counter of failed login shall be reset within manufacturer's declared account locked counter reset time limit.

(f) Expected Results:

(1) Account shall be locked with more than five failed password entries.

(2) Within manufacturer's declared account locked time limit, account shall not be unlocked.

(3) Within manufacturer's declared account locked counter reset time limit, counter shall not be reset.

5.4.2.5 Password with consecutive characters

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.4.2.5.

(b) Purpose:

Verify whether DUT's password shall not contain consecutive characters to ensure its security strength.

(c) Sample Condition:

Applicable to DUT supporting password authentication mechanism only.

(d) Test Setup:

Refer to Figure 40.

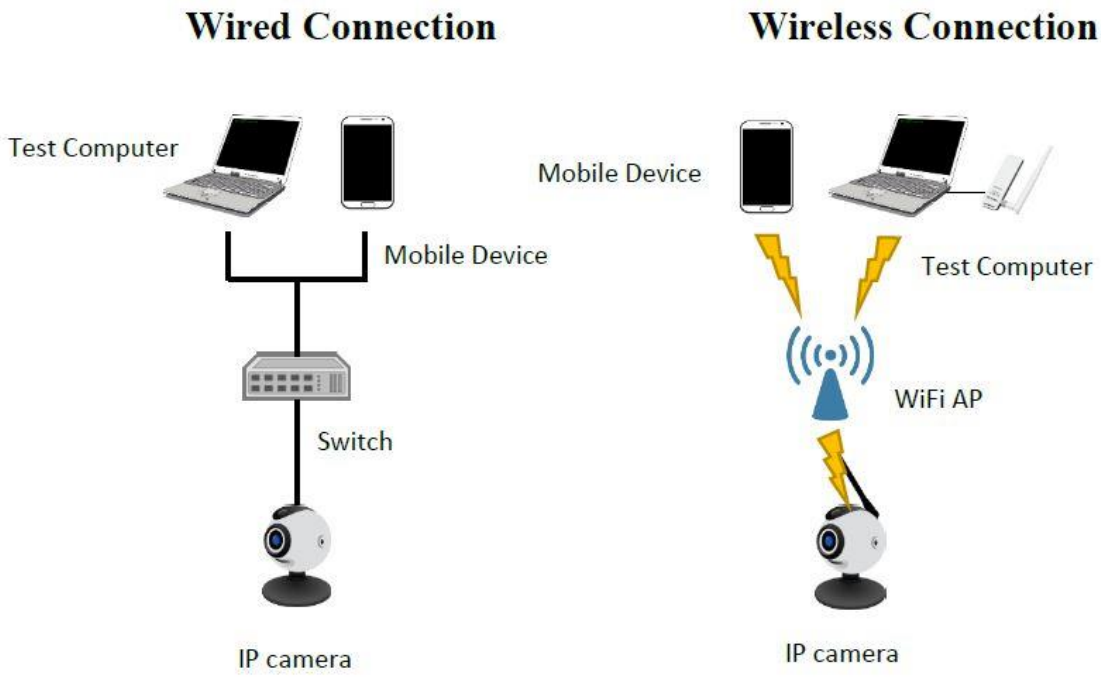

Figure 40 Test Setup

(e) Test Method:

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

(2) Create or change password by using webpage control management or control program.

(3) Enter password with more than three consecutive characters from user account name and check the feedback results of creating or changing password.

(f) Expected Result:

(1) Enter password with more than three consecutive characters from user account name shall fail to be accepted.

5.4.2.6 Password history record

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.4.2.6.

(b) Purpose:

Verify whether DUT's password history record function shall be performed to ensure its security strength.

(c) Sample Condition:

Applicable to DUT with password authentication mechanism only.

(d) Test Setup:

Refer to Figure 41.

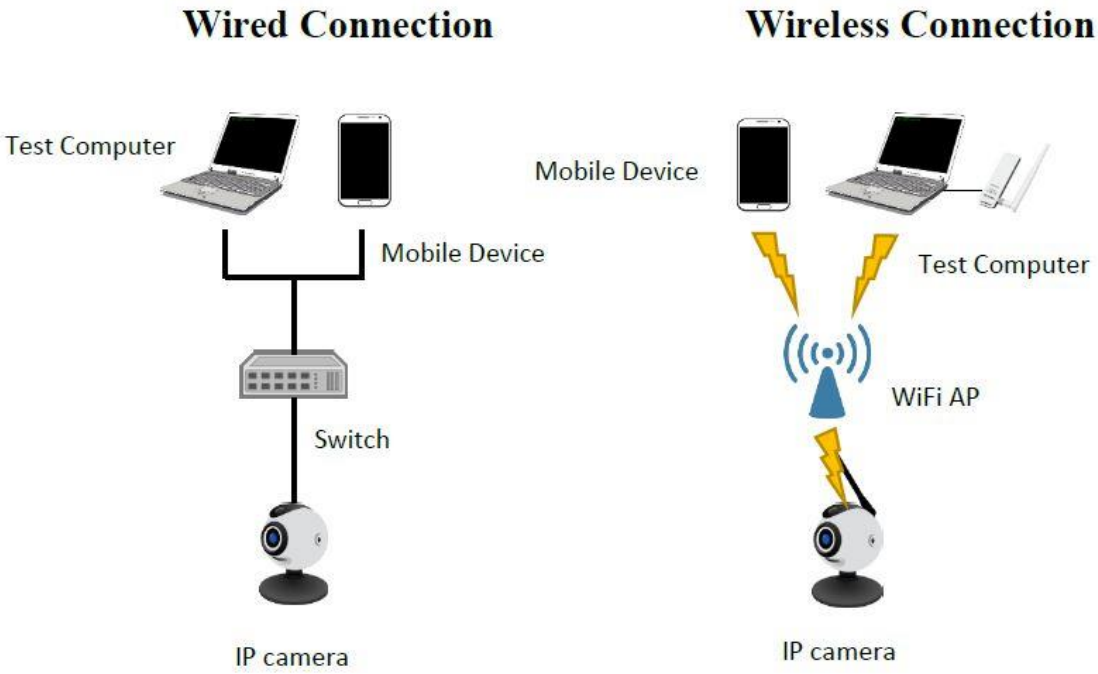

Figure 41 Test Setup

(e) Test Method:

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

(2) Create or change password by using webpage control management or control program.

(3) Change password through webpage control management or control program with password from history record to verify the acceptance.

(f) Expected Result:

(1) Duplicated changed password shall not be accepted.

5.4.3 Security Authorization

5.4.3.1 Access control mechanism

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.4.3.1.

(b) Purpose:

Verify whether the access control mechanism of DUT shall be performed in resource access.

(c) Sample Condition:

(1) User accounts and respective authentication factors, e.g. password, shall be established.

(2) Authorization limit description for resource access of DUT shall be provided.

(d) Test Setup:

Refer to Figure 42.

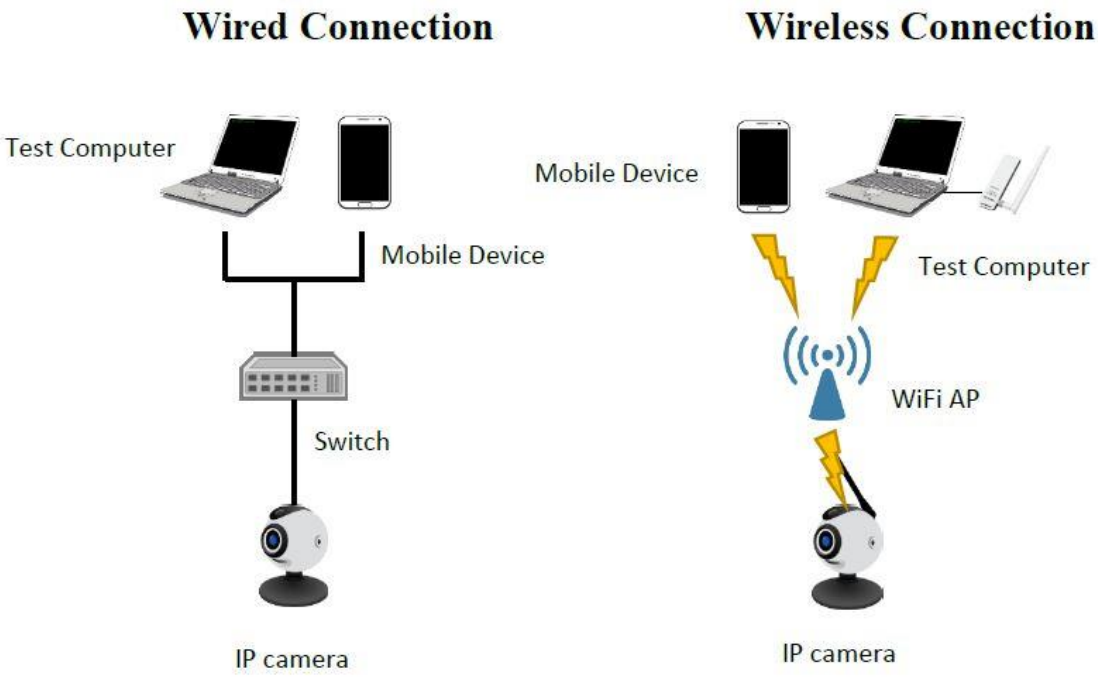

Figure 42 Test Setup

(e) Test Method:

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

(2) Log in to DUT through webpage control management or control program with different roles.

(3) Access DUT resources and make comparison between different roles and their respective authorization limits in accordance with the manufacturer's declaration.

(4) For webpage control management, conduct resource access on identically the same webpage by adopting different roles with different authorization limits.

(f) Expected Results:

(1) User's authorization limit shall be consistent with manufacturer's declaration documents.

(2) At least two different authorization limits on roles shall be defined.

5.4.3.2 Authorization time limit

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.4.3.2.

(b) Purpose:

Verify whether time limit of authorization shall be conducted.

(c) Sample Condition:

User accounts and respective authentication factors, e.g. passwords, shall be established.

(d) Test Setup:

Refer to Figure 43.

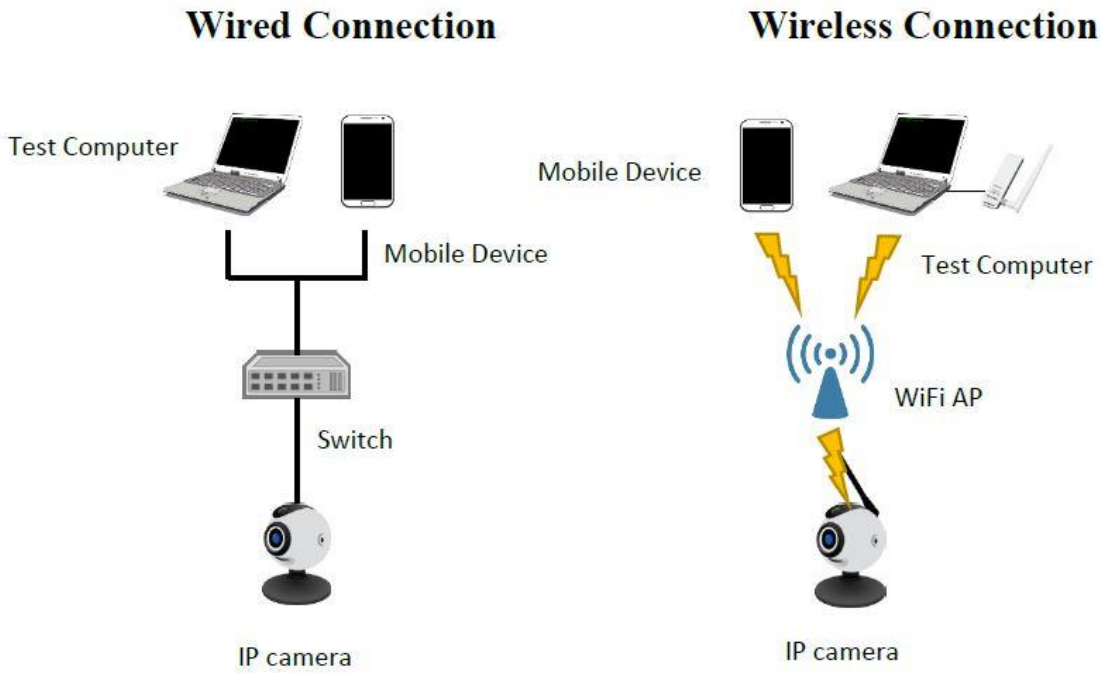

Figure 43 Test Setup

(e) Test Method:

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

(2) Log in to DUT through webpage control management or control program.

(3) Check the control management or control program of DUT, and verify whether DUT is designed with operating interface for setting idle time limit.

(4) Keep DUT in idle stage till exceeding the time limit.

(5) Check re-authentication procedure required for resource access.

(f) Expected Results:

(1) DUT is equipped with authorization mechanism and provides idle time limiting function for user setting.

(2) While remote access stays idle beyond the time limit, authentication procedure shall be re-established before further resource access.

5.5 Privacy Protection

Inspect the video surveillance device under test (DUT) and review submitted documents in fulfilling privacy protection test requirements, and conduct test items defined below accordingly. 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 Privacy access protection control

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.5.1.1.

(b) Purpose:

Verify whether access control on privacy information of DUT shall exist.

(c) Sample Condition:

(1) Declaration of authorization limit of privacy information access shall be submitted.
(2) Applicable to DUT with capability of creating multiple passwords only.

(d) Test Setup:

Refer to Figure 44.

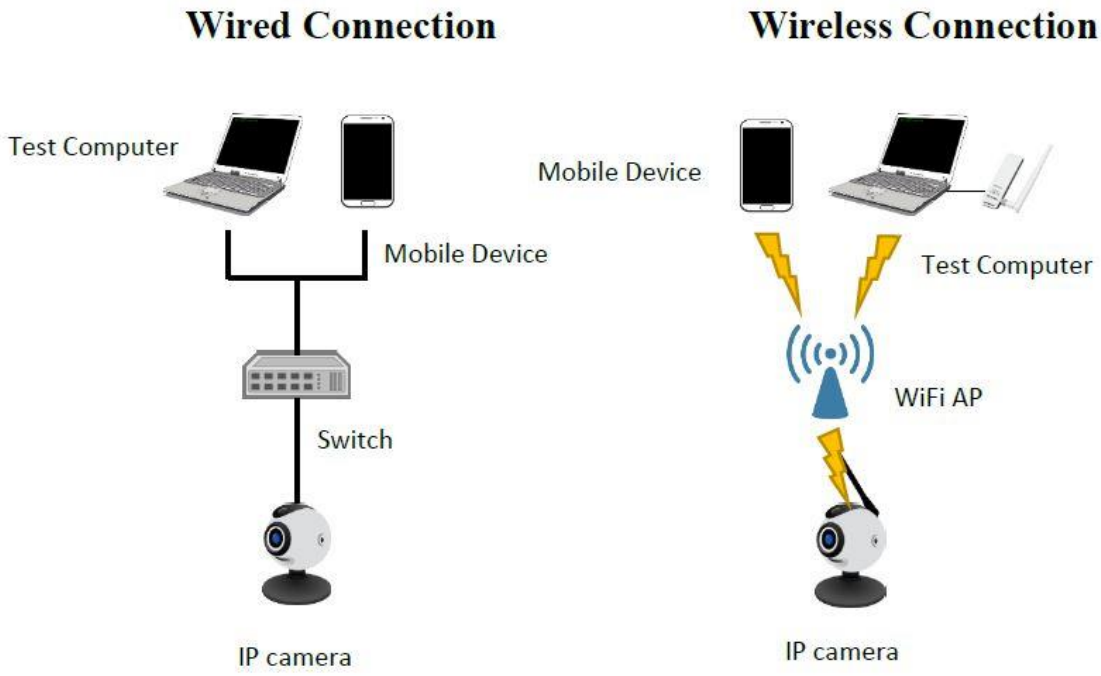

Figure 44 Test Setup

(e) Test Method:

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

(2) Log in to DUT, by different roles, through webpage control management or control program.

(3) Access video and conduct inspection and comparison of account identities and respective privacy access authorization with that in submitted declaration.

(4) While webpage control management, provided by DUT, with account logged in already, verify the accessibility to privacy information, without switching user accounts, beyond current account's authorization limit.

(f) Expected Result:

(1) User's privacy access authorization limit shall be consistent with that in submitted declaration.

5.5.1.2 Privacy information deletion

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.5.1.2.

(b) Purpose:

Verify whether users shall possess the authority in deleting their own privacy access authorization.

(c) Sample Condition:

(1) User accounts and respective authentication factors, e.g. password, shall be established and shall include both administrator and general user accounts.

(2) Video of each account shall be established.

(d) Test Setup:

Refer to Figure 45.

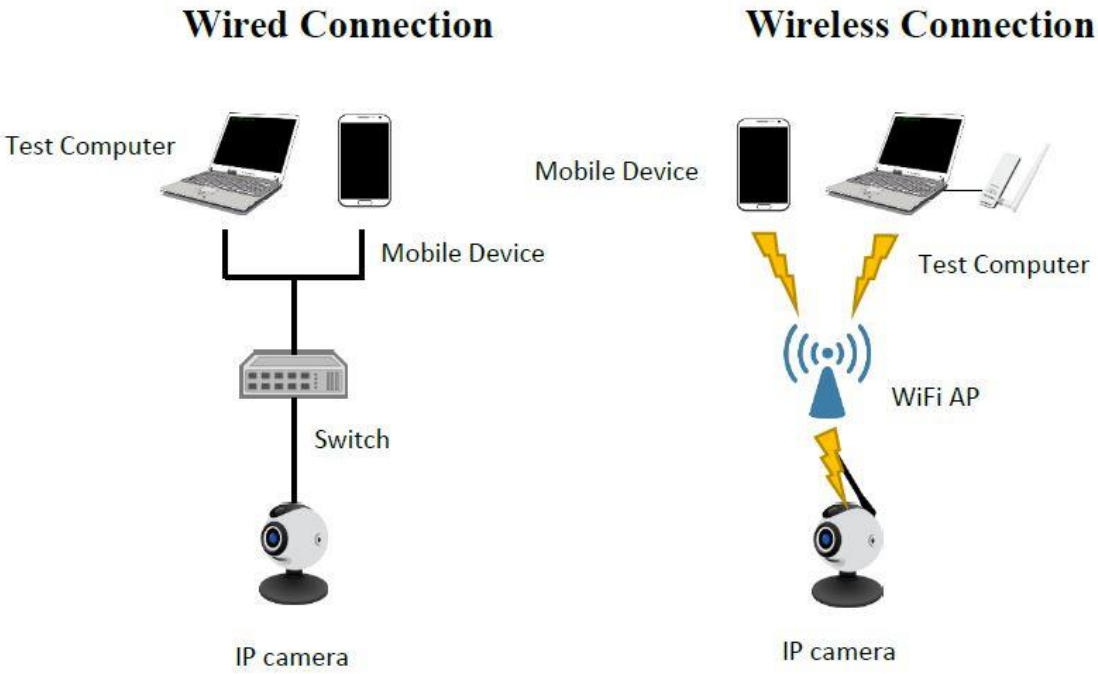

Figure 45 Test Setup

(e) Test Method:

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

(2) Log in to DUT, by different roles, through webpage control management or control program.

(3) Visually inspect webpage control management or control program and verify whether user interface to delete video shall be provided.

(4) Apply deleting function and check the elimination of privacy information simultaneously.

(f) Expected Results:

(1) Privacy information deletion function applicable to users shall be supported.

(2) Privacy information shall be eliminated.

5.5.1.3 Log-in warning mechanism

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.5.1.3.

(b) Purpose:

Verify whether privacy leakage prevention shall be conducted on DUT.

(c) Sample Condition:

None.

(d) Test Setup:

Refer to Figure 46.

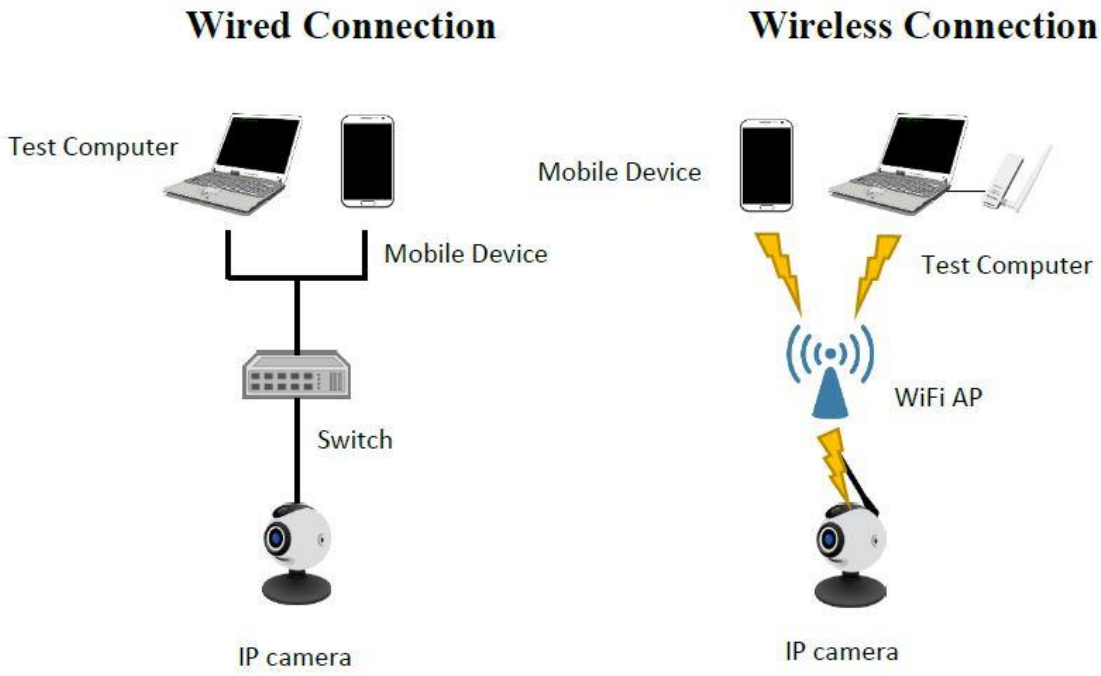

Figure 46 Test Setup

(e) Test Method:

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

(2) Log in to DUT, by different roles, through webpage control management or control program.

(3) By following user manual instructions, verify that warning messages shall be received no matter log-in is successful or not.

(f) Expected Result:

(1) With every new access occurred, DUT shall send out warning messages always.

5.5.2 Privacy Transmission Security Protection

5.5.2.1 Privacy Transmission Elementary Security Protection

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.5.2.1.

(b) Purpose:

(1) Verify whether sufficient strength of security tunnel for privacy transmission shall exist.

(2) Verify the effectiveness and legitimacy of security tunnel.

(c) Sample Condition:

None.

(d) Test Setup:

Refer to Figure 47.

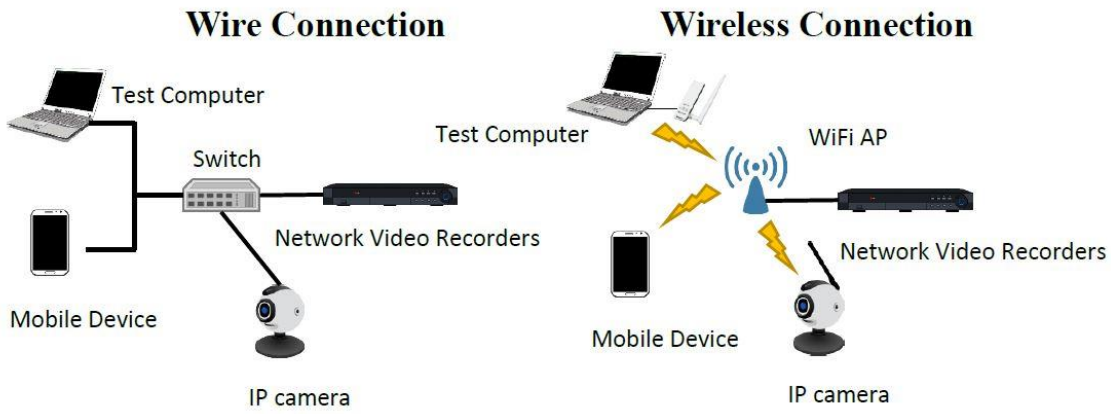

Figure 47 Test Setup

(e) Test Method:

(1) Apply security tunnel scanning tool to DUT.

(2) Make comparison between scanned results with those of cipher suites of Appendix A.

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

(4) Activate video surveillance functions through respective control management and conduct packet sniffing simultaneously.

(5) Identify all sniffed packets are adopting security tunnel.

(6) Connect DUT with other video surveillance devices and activate security tunnel establishment for video transmission.

(7) While other video surveillance devices submitting certificate to DUT, intercept and replace certificate public key and/or information with changed issuer, changed effective date, incorrect format and incorrect signature.

(8) Send out tampered certificate toward DUT, monitor packets during handshaking process of security tunnel establishment in progress and verify whether DUT certificate shall be accepted.

(f) Expected Results:

(1) Secure tunnel supports cipher suites as suggested in Appendix A.

(2) Between the Test Computer and DUT, video transmission shall adopt security channel by default.

(3) Between the Mobile Device and DUT, video transmission shall adopt security channel by default.

(4) Certificate of tampered video information shall fail to be accepted by DUT.

5.5.2.2 Privacy information transmission intermediate security protection

(a) Compliance:

"TAICS TS-0014-1: Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements", Section 5.5.2.2.

(b) Purpose:

Verify whether security tunnel for privacy information transmission with strong encryption algorithm shall be performed.

(c) Sample Condition:

None.

(d) Test Setup:

Refer to Figure 48.

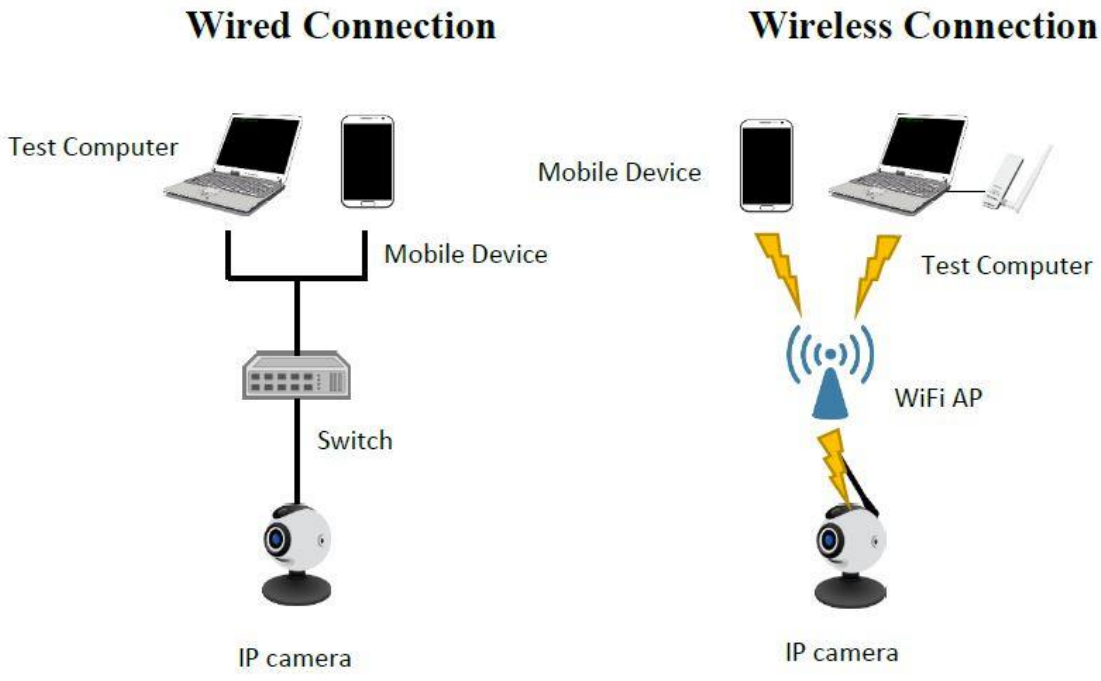

Figure 48 Test Setup

(e) Test Method:

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

(2) Apply security tunnel scanning tool to DUT. Make comparison between scanned results with those of cipher suite suggested within Appendix A to be identically the same and, even further, in supporting AES-256 equivalent or higher encryption algorithm.

(f) Expected Result:

(1) Security tunnel shall support AES-256 equivalent or higher encryption algorithm.

Appendix A

(Normative)

Security Tunnel Applicable Cipher Suite

Cipher suite being adopted by security tunnel (TLS) shall fulfill criteria listed below:

- TLSv1.2
- TLS_ECDHE_ECDSA_WITH_AES256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
- TLS_ECDHE_ECDSA_WITH_AES128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES256_SHA384
- TLS_ECDHE_RSA_WITH_AES256_SHA384
- TLS_ECDHE_ECDSA_WITH_AES128_SHA256
- TLS_ECDHE_RSA_WITH_AES128_SHA256
- TLSv1.3
- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_CCM_SHA256
- TLS_AES_128_CCM_8_SHA256

Appendix B
(Normative)
Communication Protocols for Video Surveillance Devices

B.1 Real-time Transport Protocol (RTP) & Real-time Transport Control Protocol (RTCP):

The RTP and RTCP are defined in RFC 3550 [5] and are commonly applied to video streaming systems, video conferencing, and push-to-talk systems. They define the standard format of packets used to deliver audio and video through the network. RTCP is not used for data transmission, but it supports RTP to pack and send media data. RTCP provides statistics and transmission control information periodically by out-of-band on an RTP conference connection. The main function of this protocol is to provide feedback on the quality of service.

B.2 Real Time Streaming Protocol (RTSP):

The RTSP is defined in RFC 2326 [6] and is used for controlling data for immediate use, such as playing, recording, and pausing video/audio multimedia. This, immediate video/audio control can be achieved between the user end and media server.

B.3 The Transport Layer Security (TLS):

The TLS protocol is defined in RFC 5246[7]. It establishes a security channel between two applications through the network and can prevent eavesdropping and tampering during data exchange.

Appendix C

(Normative)

Product General Description (Template)

This document shall be submitted together with test sample(s) to testing Laboratory for reference purpose.

Table 1 Product Genenral Description

Manufacturer	xxx
Device Name	xxx
Brand Name	xxx
Model No.	xxx
Software/firmware version	xxx
Communication Interface	Wi-Fi, RJ-45
Network Services	https (443)
Connected Server(IP)	SAMBA (8.8.8.x)
ONVIF API Authorization Limit	RemoveIPAddressFilter: Administrator
Security Event Log Access Authorization	USER A: Read only
Security Event Log Record Expiration time period	90 Days
Roles & Access authorization limits	Administrator: Accessible to all executable webpage control management services

Privacy authorization limits	Administrator: Accessible to all user video information
Outer Appearance	<picture>

Appendix D
(Normative)
Security Specification Description (Template)

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

Table 2 Security specification description sheet

Item	Description	Filled in by applicant
1. Debug mode	Detail description of step by step method of operating system debug mode, or supporting document delivering. *Example:* 1. *Log-in control program;* 2. *Select "setup";* 3. *Select "SSH"* 4. ...	
2. Encryption algorithm	List all encryption algorithm and its respective application. *Example:* *Remote encryption linkage: RSA-2048* *Encryption storage httpskey: AES-128*	
3. Digital	List all digital signature algorithm.	

signature algorithm	*Example:* *Security Actication:RSA* *Firmware signature:DSS*	
4. Security Events Log available warning mechanism	Description of warning mechanism of security events log, while insufficient storage space occurring, or supporting document delivering. *Example:* *while insufficient storage space occurring…,*	
5. Key Management procedure	List detail procedure of key management stages, or submit supporting document. Remark: For intermediate security level test, above document shall be provided. *Example:* 1. *Create: …。* 2. *Exchange: …。* 3. *Storage: …。* 4. *Utlization: …。* 5. *Destroy: …。* 6. *Replacement: …。*	

6. Certificate upload	Detail description of security tunnel certificate self-creation, or supporting document delivering. Remark: For intermediate security test, above document shall be provided. *Example:* *1. Log in control program.* *2. Select "Setup".* *3. ...*	
7. Multi-factor Authentication mechanism	Detail description of multi-factor authentication mechanism, or supporting document delivering. Remark:For advance security level test, above document shall be provided. *Example:* *1. Log in control program.* *2. Select "Setup".* *3. ...*	
8. Secure domain	Description shall include secure domain types, brand, model number, applicable function and secure information. Or supporting	

	document delivering. Remark: For Advance security test, above document shall be provided. *Example:* *Type: HSM* *Brand name: xxx* *Model number: xxx* *Applicable Method:While establish security tunnel, transmit request packet to HSM…* *Secure information: Log-in password, https key, secure boot key.*	
9. Account lock mechanism	Description of account lock mechanism, while incorrect password entered. *Example:* *Account lock after 5 times password entries failure.* *Un-lock after one minute lockup.* *Reset lock counter after two minutes lockup.*	

References

[1] TAICS TS-0014-1 v1.0:2018 Cybersecurity Standard of Video Surveillance System-Part 1: General Requirements.

[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.

[3] Open Web Application Security Project (OWASP) org., OWASP Top 10 – 2017 [viewed 2018-05-16]. Available at https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf.

[4] National Communications Commission, “Wireless IP Camera Cybersecurity Test Guide”, 2018.

[5] RFC 3550, RTP: A Transport Protocol for Real-Time Applications.

[6] RFC 2326, Real Time Streaming Protocol (RTSP).

[7] RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2.

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