TAICS

TAICS TS-0015-2(E) v2.0:2019

Cybersecurity Test Specification for Video Surveillance System-Part 2: IP Camera

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 2: IP Camera

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 2: IP Camera" (hereafter referred to as "this/the specification") is formulated by TAICS, in accordance with "TAICS TS-0014-2 Cybersecurity Standard for Video Surveillance System-Part 2: IP Camera" [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 embedded cameras with networking functions in video surveillance systems (See Figure 1).

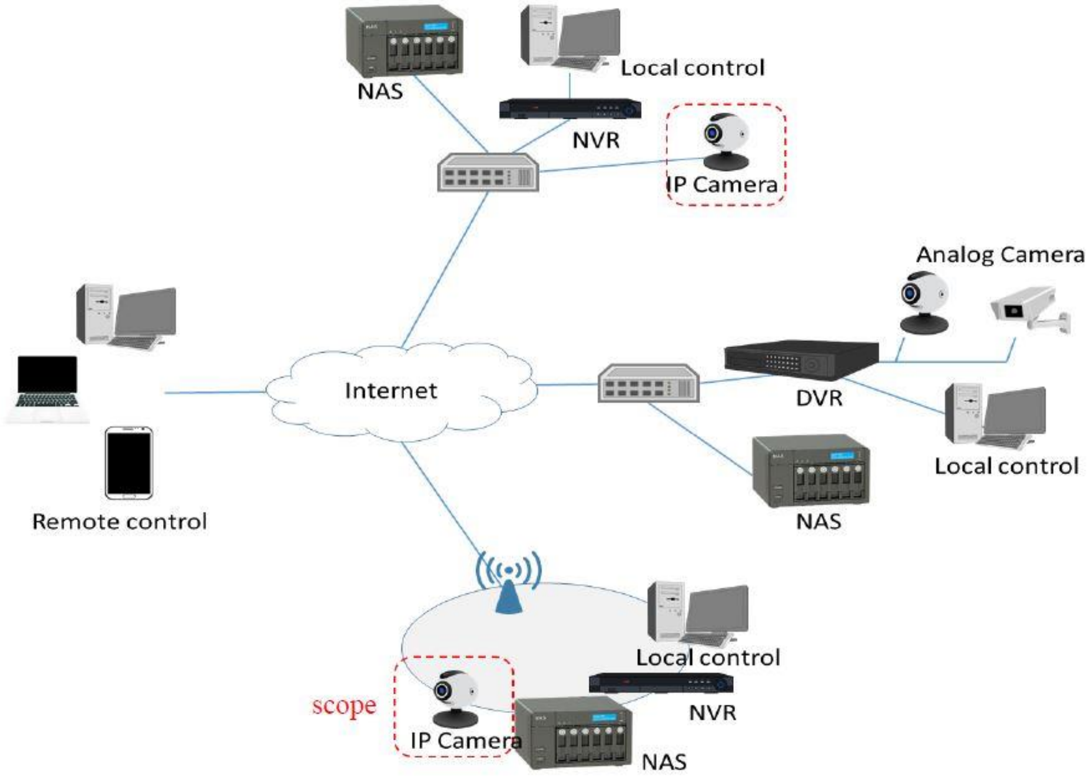

Figure 1 Scope

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

(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-0014-2 v 2.0: 2019 Cybersecurity Standard for Video Surveillance System- Part 2: IP Camera” 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-0014-2 Cybersecurity Standard for Video Surveillance System- Part 2: IP Camera", 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	-	5.1.1.2	-
	5.1.2. Warning of Physical Abnormal Behavior	-	-	-
	5.1.3. Physical Protection	-	5.1.3.2	-
	5.1.4. Secure Boot	-	-	-
System Security	5.2.1. Operating System and Security of Network	-	-	-
	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	-	-	-
Communication Security	5.3.1. Security of Sensitive Data in Transmission	-	-	-
	5.3.2. Communication Protocols and Configuration Security	-	-	5.3.2.2
	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. Privacy Authorization	-	-	-
Privacy Protection	5.5.1. Protection of Access of Private Data	-	5.5.1.2	-
	5.5.2. Privacy Transmission Protection	-	-	-

5. Security Test Specification

5.1 Physical Security

Inspect IP Camera 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 Physical interface redundancy

(a) Compliance:

"TAICS TS-0014-2: Cybersecurity Standard for Video Surveillance System- Part 2: IP Camera", Section 5.1.1.2.

(b) Purpose:

Verify whether external access to DUT's storage media shall be conducted.

(c) Sample Condition:

None.

(d) Test Setup:

None.

(e) Test Method:

(1) Scenario 1:

(i) Visual inspection shall be conducted on the outer appearance of DUT. No physical slot for inserting memory card, e.g. SD Card, shall exist, excluding wall mounting side.

(ii) Visual inspection shall be conducted on the outer appearance of DUT. No USB devices insertion slot shall exist, excluding wall mounting side.

(2) Scenario 2:

(i) Remove memory card from DUT and use a Test Computer to retrieve video in the memory card.

(ii) Under un-authorized condition, verify the readability of video in the memory card.

(iii) Remove USB devices from DUT and use a Test Computer to retrieve video in the USB devices.

(iv) Under un-authorized condition, verify the readability of video in the USB devices.

(f) Expected Results:

(1) Scenario 1:

(i) No insertion slot for removable storage devices exists.

(ii) No USB insertion slot exists.

(2) Scenario 2:

(i) Under un-authorized condition, video in removable memory card shall not be readable.

(ii) Under un-authorized condition, video in USB storage devices 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.

5.1.3.2 Physical protection

(a) Compliance:

"TAICS TS-0014-2: Cybersecurity Standard for Video Surveillance System- Part 2: IP Camera", Section 5.1.3.2.

(b) Purpose:

Verify whether DUT's physical enclosure shall not be dismantled without hindrance.

(c) Sample Condition:

None.

(d) Test Setup:

None.

(e) Test Method:

(1) Visual inspection of DUT's enclosure to be of one-piece form factor.

(2) Visual inspection of DUT's enclosure to be designed with tamper-proof security screws assembly.

(f) Expected Result:

(1) DUT shall be designed with one-piece form factor enclosure or tamper-proof security screws assembly.

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.

5.2 System Security

System security of IP Camera shall be investigated against submitted documents and tested in accordance with the test items defined within this section.

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.

5.3 Communication Security

Inspect IP Camera 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 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.

5.3.2.2 Network device information inquiry

(a) Compliance:

"TAICS TS-0014-2: Cybersecurity Standard for Video Surveillance System- Part 2: IP Camera", Section 5.3.2.2.

(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 of DUT shall be submitted with description of all supported network services.

(d) Test Setup:

Refer to Figure 2.

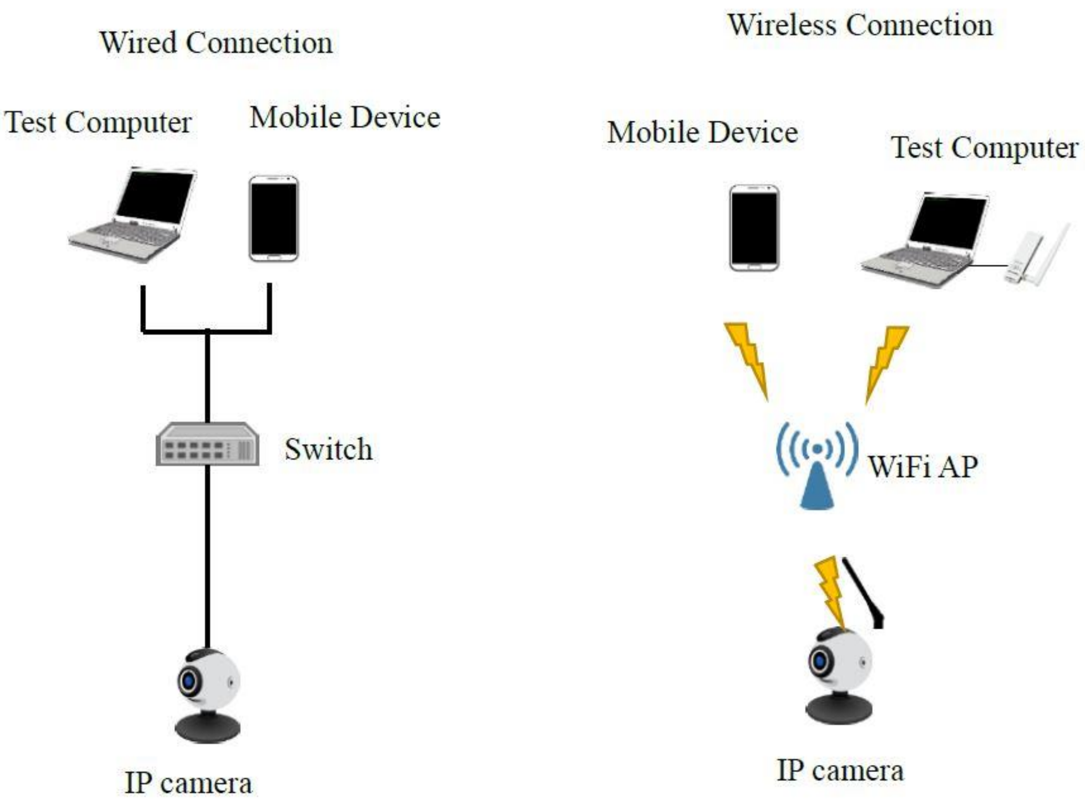

Figure 2 Test Setup

(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) Apply UPnP protocol scanning tool to identify DUT equipped with the protocol service and with default setting as OFF.

(4) Apply SNMP protocol scanning tool to identify DUT equipped with the protocol service and with default setting as OFF.

(5) Apply Bonjour protocol scanning tool to identify DUT equipped with the protocol service and with default setting as OFF.

(f) Expected Results:

(1) For DUT supporting UPnP protocol, the default setting shall be OFF.

(2) For DUT supporting SNMP protocol, the default setting shall be OFF.

(3) For DUT supporting Bonjour protocol, the default setting shall be OFF.

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 IP Cameras 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

Inspect IP Camera 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 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.

5.5.1.2 Video privacy leakage protection

(a) Compliance:

"TAICS TS-0014-2 Cybersecurity Standard for Video Surveillance System- Part 2: IP Camera ", Section 5.5.1.2.

(b) Purpose:

Verify whether the function of non-disclosure video display zone designation within full surveillance range shall be conducted.

(c) Sample Condition:

None.

(d) Test Setup:

Refer to Figure 3.

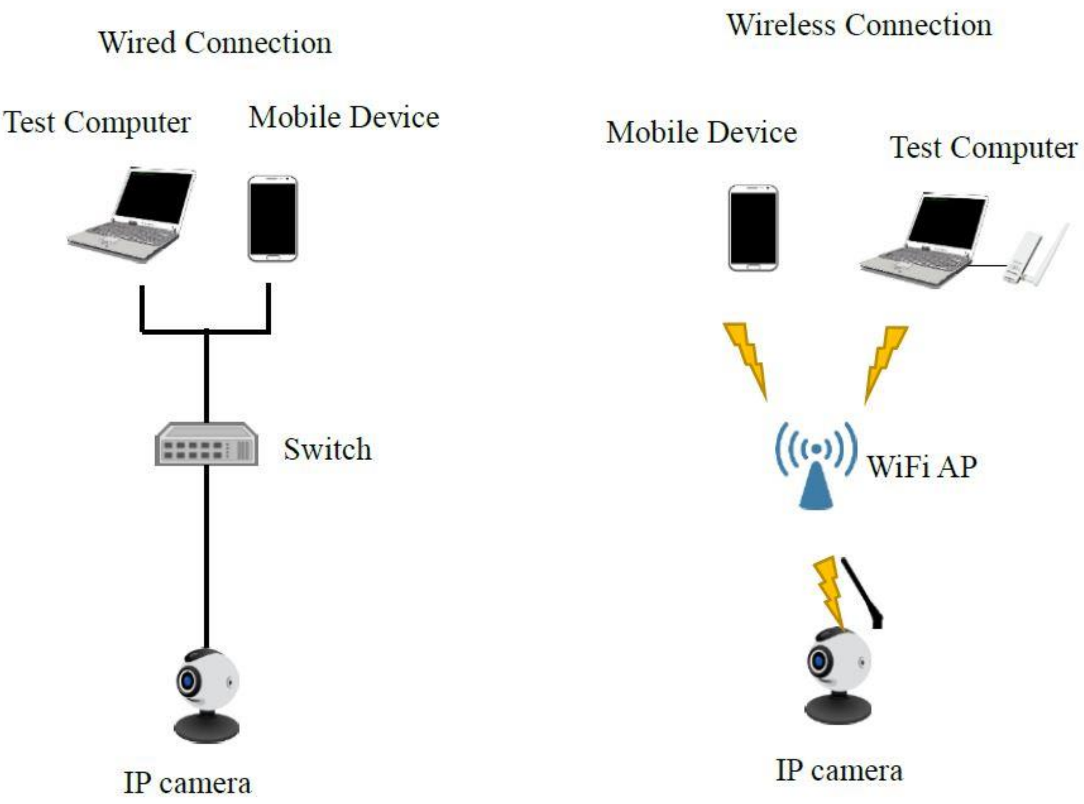

Figure 3 Test Setup

(e) Test Method:

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

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

(3) Visual inspection on website control management or control program, and verify the availability of user applicable privacy mask function.

(4) Apply privacy mask function, if applicable, investigate designated non-disclosure zone with video being masked accordingly.

(f) Expected Result:

(1) Video of designated non-disclosure zone shall be masked.

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.

References

[1] TAICS TS-0014-2 v2.0:2018 Cybersecurity Standard for Video Surveillance System-Partv 2: IP Camera

Revision Record

Version	Date	Summary
v1.0	2017/12/26	v1.0 Chinese version published
v2.0	2018/06/08	v.2.0 Chinese version published
v2.0(E)	2019/05/30	v.2.0 English version published
-	-	-
-	-	-
-	-	-
-	-	-

台灣資通產業標準協會

Taiwan Association of Information and Communication Standards

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