TAICS

TAICS TS-0014-2(E) v2.0:2019

Cybersecurity Standard for Video Surveillance System- Part 2: IP Camera

2019/03/26

社團法人台灣資通產業標準協會

Taiwan Association of Informationand Communication Standards

Cybersecurity Standard for Video Surveillance System- Part 2: IP Camera

Published date： 2019/03/26

Approved date： 2018/06/07

Acknowledgements

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

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

TC Vice president: Cheng-Yu Tsai, Section Chief, Institute for Information Industry

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

The list of association members participating in this standard 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 standard is supported by the National Communications Commission and Industrial Development Bureau, MOEA, R.O.C..

Contents

Foreword

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

This standard 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 standard.

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

Introduction

Internet of things (IoT) is the fastest developing industry across the world, and related applications are constantly being innovated. Information security is undeniably the key to the success of IoT technology. Therefore, the Industrial Development Bureau, Ministry of Economic Affairs (MOEA), first sets goals for the environmental standards for IoT security, including video surveillance systems, internet of vehicles (IoV) systems, IoT general systems, auxiliary applications, industrial control systems, medical equipment systems, and point of sale security standards. These standards promote the overall quality of domestic industries and product competitiveness and ensure that consumers are assured information security when they use monitoring devices. The list of all TAICS TS-0014 series standards is available on the TAICS website.

In view of this, “TAICS TS-0014-2 Cybersecurity Standard for Video Surveillance System-Part 2: IP Camera” (hereafter referred to as “this/the standard”) is formulated and used with “TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System-Part 1: General Requirements” [1]. It ensures the security of IP cameras in five aspects, namely (1) physical security, (2) system security, (3) communication security, (4) authentication and authorization mechanism security, and (5) privacy protection. The standard also establishes benchmarks for security quality of IP cameras in Taiwan, enables equipment manufacturers or system service providers to have a basis for product development, promotes the overall competitiveness of the quality of domestic industries and products, and ensures that consumers are assured information security when they use IP cameras.

1. Scope

This standard is applicable to embedded cameras with networking functions in video surveillance systems (See Figure 1).

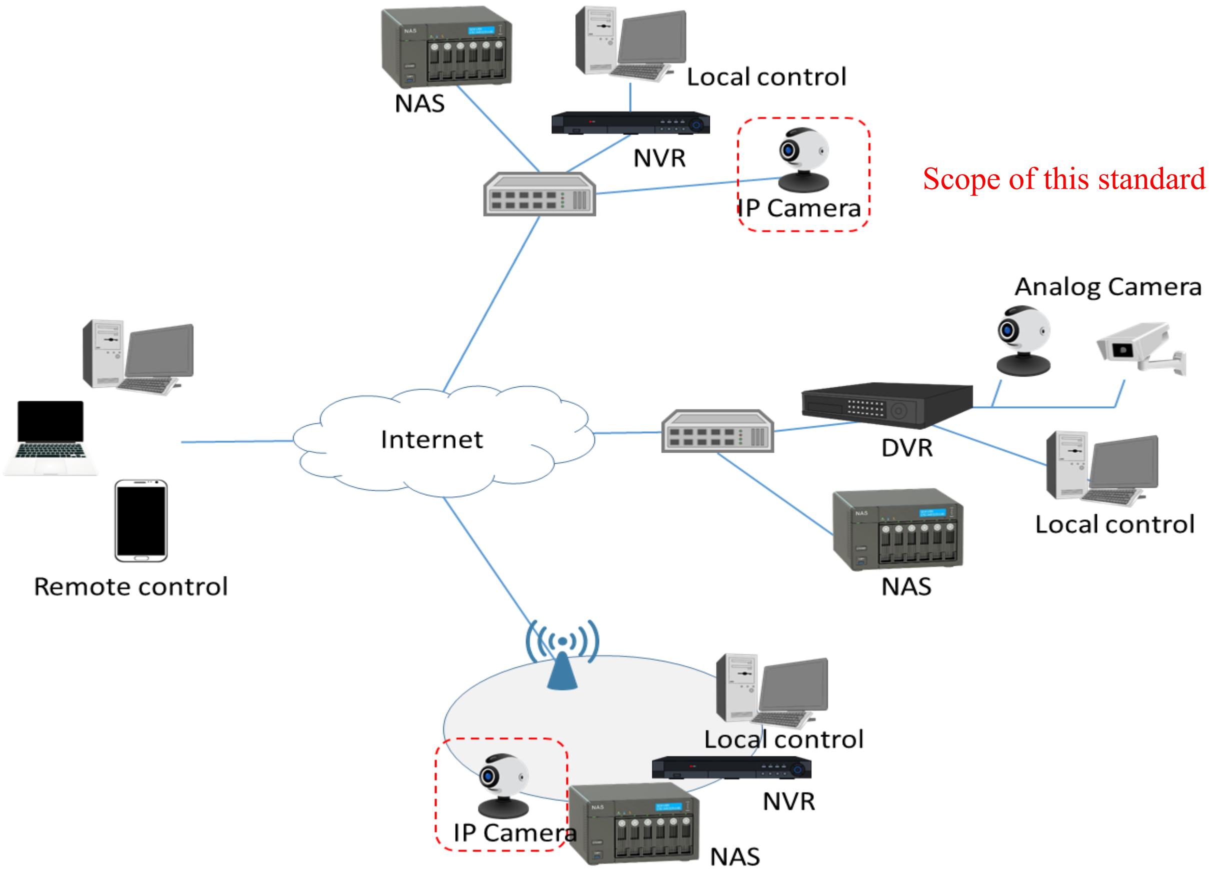

Figure 1 Schematic of the scope

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-0014-1 v1.0:2019 Cybersecurity Standard for Video Surveillance System- Part 1: General Requirements

3. Terms and Definitions

The following terms and definitions and those described in "TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System - Part 1: General Requirements" are applicable in this standard.

3.1 One-Piece Forming

The shell of the product is not composed of components, but is manufactured directly without division.

3.2 Tamper-Proof Screw

Tamper-proof screw refers to screws that use special header and punch-pin designs. They cannot be removed by a general cross or one-handed wrench.

3.3 Privacy Mask

Privacy mask refers to areas not displayed on the screen when users do not want certain areas within the surveillance range of the IP camera to be shown.

4. Security Levels

Security levels are a combination of security requirements that address various security risks at product deployment. Thus, security levels can be utilized to reduce or eliminate the threats to information security.

4.1 Brief Introduction

A summary of security levels is presented 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 goals of security requirements in each security aspect. The third column refers to security levels, each of which is a combination of security requirements that must be met to cope with various security risks, whose details are described in chapter 5.

Table 1 Summary of security levels

Security aspects	Goals of 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 Services	-	-	-
	5.2.2. Security of Network Service Ports	-	-	-
	5.2.3. Update security	-	-	-
	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	-	-	-

Security aspects	Goals of security requirements	Security levels		
		Level 1	Level 2	Level 3
	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. Security Authorization	-	-	-
Privacy protection	5.5.1. Protection of Access of Private Data	-	5.5.1.2	-
	5.5.2. Privacy Transmission Protection	-	-	-

4.1.1 Security aspects

Section 4.1.1 of TAICS TS-0014-1 is applicable to this standard.

4.1.2 Goals of security requirements

Section 4.1.2 of TAICS TS-0014-1 is applicable to this standard.

4.1.3 Formation of security levels

Section 4.1.3 of TAICS TS-0014-1 is applicable to this standard.

5. Security Requirements

This chapter describes common methods for satisfying the security functions of video surveillance in detail. IP cameras (each being referred to as "target product" hereafter) shall meet all the stated requirements accordingly.

5.1 Physical Security

5.1.1 Access control of physical interfaces

5.1.1.1 The target product shall meet the requirements in section 5.1.1 of "TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System - Part 1: General Requirements".

5.1.1.2 The slot used by removable storage media shall be removed, or the removable storage media shall support a storage media protection mechanism, that is, the storage media of the target product shall not be accessed by other machines except the local machine.

5.1.2 Warning of physical abnormal behavior

5.1.2.1 Target product shall meet the requirements in section 5.1.2 of "TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System - Part 1: General Requirements".

5.1.3 Physical protection

5.1.3.1 Target product shall meet the requirements in section 5.1.3 of "TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System - Part 1: General Requirements".

5.1.3.2 The target product shall adopt an antidemolition protection design, such as one-piece forming or tamper-proof security screws.

5.1.4 Secure Boot

5.1.4.1 Target product shall meet the requirements in section 5.1.4 of "TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System - Part 1: General Requirements".

5.2 System Security

5.2.1 Operation system and security of Internet services

5.2.1.1 Target product shall meet the requirements in section 5.2.1 of "TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System - Part 1: General Requirements".

5.2.2 Service of Internet service ports

5.2.2.1 Target product shall meet the requirements in section 5.2.2 of "TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System - Part 1: General Requirements".

5.2.3 Update security

5.2.3.1 Target product shall meet the requirements in section 5.2.3 of "TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System - Part 1: General Requirements".

5.2.4 Security of Sensitive Data in Storage

5.2.4.1 Target product shall meet the requirements in section 5.2.4 of "TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System - Part 1: General Requirements".

5.2.5 Security of website management interface

5.2.5.1 Target product shall meet the requirements in section 5.2.5 of "TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System - Part 1: General Requirements".

5.2.6 Security of Management Applications

5.2.6.1 Target product shall meet the requirements in section 5.2.6 of "TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System - Part 1: General Requirements".

5.2.7 Logs and warnings

5.2.7.1 Target product shall meet the requirements in section 5.2.7 of "TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System - Part 1: General Requirements".

5.3 Communication Security

5.3.1 Security of Sensitive Data in Transmission

5.3.1.1 Target product shall meet the requirements in section 5.3.1 of “TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System - Part 1: General Requirements”.

5.3.2 Communication Protocols and Configuration Security

5.3.2.1 Target product shall meet the requirements in section 5.3.2 of “TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System - Part 1: General Requirements”.

5.3.2.2 The “Network device information inquiry” function of the target product, including UPnP, SNMP, and Bonjour, which can be turned on/off by users, shall be turned off by default.

5.3.3 Wi-Fi communication security

5.3.3.1 Target product shall meet the requirements in section 5.3.3 of “TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System - Part 1: General Requirements”.

5.4 Authentication and Authorization mechanism security

5.4.1 Security authentication

5.4.1.1 Target product shall meet the requirements in section 5.4.1 of "TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System - Part 1: General Requirements".

5.4.2 Password authentication

5.4.2.1 Target product shall meet the requirements in section 5.4.2 of "TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System - Part 1: General Requirements".

5.4.3 Security Authorization

5.4.3.1 Target product shall meet the requirements in section 5.4.3 of "TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System - Part 1: General Requirements".

5.5 Privacy Protection

5.5.1 Protection of access of privacy

5.5.1.1 Target product shall meet the requirements in section 5.5.1 of "TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System - Part 1: General Requirements".

5.5.1.2 The target product shall support privacy masks to avoid the risk of privacy leakage triggered by normal operation.

Note: Status indicator lights can be installed on the target product to inform users that the surveillance function is running and to avoid the leakage of private videos.

5.5.2 Privacy Transmission Protection

5.5.2.1 Target product shall meet the requirements in section 5.5.2 of "TAICS TS-0014-1 Cybersecurity Standard for Video Surveillance System - Part 1: General Requirements".

Appendix A
(Informative)
Technical Requirements and Comparison of Standards

Table A.1 Technical requirements and comparison of standards

Technique requirements	Term corresponds to OWASP [2]	Term corresponds to ONVIF [3, 4]
5.1.1.2	I10: Poor Physical Security Ensuring data storage medium cannot be easily removed. Ensuring stored data is encrypted at rest.	-
5.1.3.2	I10: Poor Physical Security Ensuring device cannot be easily disassembled.	-
5.3.2.2	I3: Insecure Network Services Ensuring network ports or services are not exposed to the internet via UPnP for example.	-
5.5.1.2	-	-

References

[1] TAICS TS-0014-1(E) v1.0:20182018 Video Surveillance System Cybersecurity Standard – Part1: General Requirement

[2] Open Web Application Security Project (OWASP) org., Top IoT Vulnerabilities [viewed 2018-05-16]. Available at https://www.owasp.org/index.php/Top_IoT_Vulnerabilities

[3] Open Network Video Interface Forum(ONVIF), Core Specification Version 16.12, Dec., 2016.

[4] Open Network Video Interface Forum(ONVIF), Advanced Security Service Version 1.3, Feb., 2016.

Revision Record

Version	Date	Abstract
v1.0	2017/11/26	v1.0 Chinese version published
v2.0	2018/06/08	v2.0 Chinese version published
v2.0(E)	2019/03/26	v2.0 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