Dahua EAL2+
Network Camera Series
Security Target
Version 2.8

Document History

Version	Date	Comment	Author
0.1	2021-01-26	First draft	Zhejiang Dahua Technology Co., Ltd
0.3	2021-04-21	After workshop	Pere Quetglas
0.4	2021-04-26	After workshop	Pere Quetglas
0.5	2021-04-30	After workshop	Zhejiang Dahua Technology Co., Ltd
0.6	2021-05-04	Added crypto support and other	Pere Quetglas
0.7	2021-05-06	New approach for crypto support	Pere Quetglas
0.8	2021-05-08	Revise the review comments, mainly contains 1) Cryptographic Support 2) Add TOE Summary Specification	Zhejiang Dahua Technology Co., Ltd
0.9	2021-05-10	Minor updates	Pere Quetglas
1.0	2021-05-18	Updated after evaluation round	Pere Quetglas
1.1	2021-05-19	Updated after evaluation round	Pere Quetglas
1.2	2021-05-20	Updated table of TOE models. Table taken from ST v0.8.1, 2021-05-20	Zhejiang Dahua Technology Co., Ltd
1.3	2021-06-07	Updated table of TOE models.	Zhejiang Dahua Technology Co., Ltd
1.4	2021-06-11	Answer ADV Action item list A.TDS.11 Cryptographic key destruction	Zhejiang Dahua Technology Co., Ltd
1.5	2021-07-05	1) Answer ADV Action item list FAU_GEN.1.2 Correct description 2) Correct user role: Administrator and User. Delete Advanced Operator	Zhejiang Dahua Technology Co., Ltd
1.6	2021-08-07	1) Correct the list of TOE In section 1.4.1.2 2) Update the version of TOE User Manual in Table 5 3) Update the firmware to meet the "the outcome (success or failure) of the event" in 6.1.1 FAU_GEN.1.2	Zhejiang Dahua Technology Co., Ltd
1.7	2021-08-16	Updated table of TOE models	Zhejiang Dahua Technology Co., Ltd
1.8	2021-09-10	Update Section 1.4.1 Firmware version， update section 6.1.6，delete DH algorithms	Zhejiang Dahua Technology Co., Ltd
1.9	2021-10-19	ST reference updated	Zhejiang Dahua Technology Co., Ltd
2.0	2021-10-21	1) Update 6.1.2.1, add 6.1.2.5 about Onvif account lock 2) Update 1.4.1 firmware version and file name	Zhejiang Dahua Technology Co., Ltd
2.1	2021-10-28	1) Update 6.1.2, FIA_AFL.1 Use a unique identifier FIA_AFL.1/non-ONVIF、FIA_AFL/ONVIF 2) Update 6.1.3,3 FMT_SMR 1.1 added ONVIF	Zhejiang Dahua Technology Co., Ltd
2.2	2021-11-03	1) Update FIA_AFL.1/* 2) Update FMT_SMR.1/*	Pere Quetglas
2.3	2021-12-30	Back to ST1.9 version, delete ONVIF related content only	Zhejiang Dahua Technology Co., Ltd
2.4	2022-04-07	Update chapter 6.1.1.1,chapter 6.1.2.2,chapter 1.4.1.5 and chapter 1.1	Zhejiang Dahua Technology Co., Ltd
2.5	2022-04-16	1) remove the “/TLS” iteration of Section 6.1.6.1 in order to make it consistent with the SFR definition. 2) Firmware version update 3) Added description to the model IPC 5 Series and the model SDT5X Series	Zhejiang Dahua Technology Co., Ltd
2.6	2022-06-06	update the ST to include the hardening guide in the physical scope of the TOE.	Zhejiang Dahua Technology Co., Ltd
2.7	2022-07-22	Update 1.4.1 firmware version and file name	Zhejiang Dahua Technology Co., Ltd
2.8	2022-10-27	Update 6.1.1.1	Zhejiang Dahua Technology Co., Ltd

Contents

1 ST Introduction 6
1.1 ST Reference 6
1.2 TOE Reference 6
1.3 TOE Overview 6
1.3.1 TOE Type 6
1.3.2 Usage and Major Security Features of a TOE 6
1.3.3 Required Non-TOE Hardware/Software/Firmware 8
1.4 TOE Description 8
1.4.1 Physical Scope 8
1.4.2 Logical Scope 14

2 Conformance Claim 17

3 Security Problem Definition 18
3.1 Threats 18
3.2 Organizational Security Policies 19
3.3 Assumptions 19

4 Security Objectives 20
4.1 Security Objectives for the TOE 20
4.2 Security Objectives for the Operational Environment 20
4.3 Security Objectives Rationale 21

5 Extended Components Definition 24
5.1 Definition of the Family FPT_TFU – Trusted Firmware Update 24
5.2 Definition of the Family FPT_INI – Trusted Software Initialization 24

6 Security Requirements 26
6.1 Security Functional Requirements 26
6.1.1 Security Audit (FAU) 26
6.1.2 Identification and Authentication (FIA) 27
6.1.3 Security Management (FMT) 28
6.1.4 Protection of the TSF (FPT) 28
6.1.5 TOE Access (FTA) 29
6.1.6 Trusted Path/Channels (FTP) 30
6.1.7 Cryptographic support (FCS) 31
6.2 SFRs Rationale 32
6.3 SFR Dependencies 33
6.4 Security Assurance Requirements 34

7 TOE Summary Specification 36
7.1 Security Audit 36
7.2 Identification and Authentication 36
7.3 Security Management 36
7.4 Protection of the TSF 37
7.5 TOE Access 37
7.6 Trusted Path/Channels 37
7.7 Cryptographic Support 37

A Abbreviations and Glossary 39

B References 40

1 ST Introduction

1.1 ST Reference

ST Title	Dahua EAL2+ Network Camera Series Security Target
ST Version	2.8
ST Publication Date	2022-10-27

Table 1 ST Reference

1.2 TOE Reference

TOE Developer	Zhejiang Dahua Technology Co.,Ltd
TOE Name	Dahua Network Camera Series
TOE Version	1.0

Table 2 TOE Reference

1.3 TOE Overview

1.3.1 TOE Type

The TOE is a Network camera device produced by Zhejiang Dahua Technology Co., Ltd. TOE device is composed of hardware and firmware and provides video and configuration management functions.

The TOE can be divided into two categories: IPC and dome camera. The biggest difference between IPC and dome camera is that the dome camera has PTZ (Pan/Tilt/Zoom) function, while IPC does not.

1.3.2 Usage and Major Security Features of a TOE

The usage environment of TOE is a segregated LAN, optionally connected to Internet, which may include one or more TOE devices, video storage devices (such as NVR, DVR, etc.), PC hosts supporting web browser, hosts supporting the installation of TOE management software and TOE management platform. The following figure is a sample network topology diagram of a TOE device.

The TOE device provides video and management functions. Non-TOE devices, such as PC with a web browser, can access devices, preview video streams, and configure and manage TOE through the web. NVR can connect devices, store or forward video streams through network protocols. The client / platform can also connect to the device and implement functions such as configuration management, preview, storage, and forwarding (different clients / platforms may support different functions).

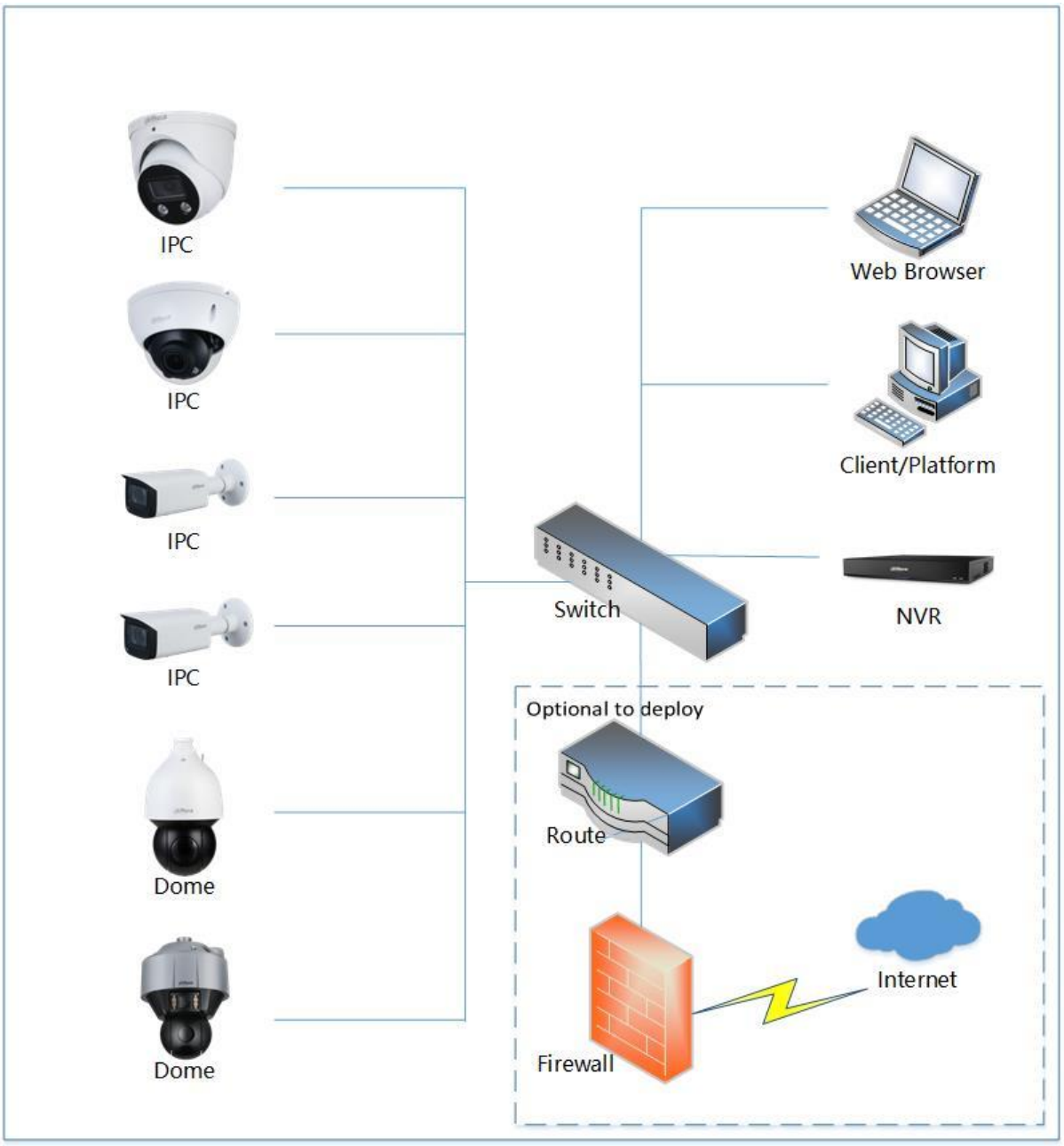


Figure 1 TOE network deployment diagram

TOE provides the following main security functions：

- Audit Logs
- Identification and Authentication
- Security Management
- Protection of the TSF
- Trusted Path/Channels
- Trusted Firmware Updates
- TOE Access
- Cryptographic Support

1.3.3 Required Non-TOE Hardware/Software/Firmware

According to the non-TOE other components shown in Figure 1 Deployment diagram of TOE network, it can include a Web browser, video storage device, client / platform.

Component	Required	Description
Web Browser (PC)	Yes	Support connection with TOE devices through RTSP, TCP, HTTP, HTTPS and other network protocols. It can support real-time video stream viewing and configuration management of TOE devices.
Client/Platform	No	Support TOE connection, different clients / platforms support different functions, which can be summarized as TOE configuration management, video preview, video storage and forwarding, etc.
NVR	No	Support to connect to TOE device through private protocol, ONVIF protocol, RTSP and other network protocols. Mainly used to store and forward video and image data.
Switch	Yes	Build a LAN environment for TOE
Route/Firewall	No	If the TOE needs to connect to the Internet, routers and firewalls must be deployed to the usage environment in order provide the routing to Internet and to defend against network attacks.

Table 3 Non-TOE components

1.4 TOE Description

1.4.1 Physical Scope

The TOE includes a total of six different camera series:

Series	Devices	Firmware/Software
IPC 5 Series	1.4.1.1	Version V2.820.19EL001.0.R, Build Date: 2022-06-30 File: DH_IPC-HX5XXX-Volt_MultiLang_PN_Stream3_V2.820.19EL001.0.R.220630.zip
IPC 3 Series	1.4.1.2	**Version** V2.800.19EL002.0.R, Build Date: 2022-07-15 **File**: DH_IPC-HX3XXX-Leo_MultiLang_PN_Stream3_V2.800.19EL002.0.R.220715.zip
	1.4.1.3	**Version**: V2.800.19EL002.0.R, Build Date: 2022-07-15 **File**: DH_IPC-HX5(4)(3)XXX-Leo_MultiLang_PN_Stream3_V2.800.19EL002.0.R.220715.zip
	1.4.1.4	**Version**: V2.820.19EL002.0.R, Build Date: 2022-06-30 **File**: DH_IPC-HX3XXX-Dalton_MultiLang_PN_Stream3_V2.820.19EL002.0.R.220630.zip
SD5A Series	1.4.1.5	**Version**: V2.810.1A6W000.0.R, Build Date: 2022-06-30 **File**: General_SD-Prometheus_MultiLang_PN_Stream3_V2.810.1A6W000.0.R.220630.zip
SDT5X Series	1.4.1.6	**Version** V2.810.1A6W000.0.R, Build Date: 2022-06-30 **File:** DH_SD-Fafnir_MultiLang_PN_Stream3-LingxiV2_V2.810.1A6W000.0.R.220630.zip

Table 4 TOE series, devices and firmware

1.4.1.1 IPC 5 Series devices

IPC 5 Series includes the following devices:

DH-IPC-HDW5541H-ASE-PV, as the reference model, and

DH-IPC-HFW5241E*-SE; DH-IPC-HFW5241T*-SE; DH-IPC-HFW5241T*-ASE; DH-IPC-HFW5242T*-ASE-MF; DH-IPC-HDBW5241R*-S; DH-IPC-HDBW5241R*-ASE; DH-IPC-HDBW5242R*-ASE-MF; DH-IPC-HDW5241TM*-ASE; DH-IPC-HFW5241E*-ZE; DH-IPC-HFW5241E*-ZHE; DH-IPC-

HFW5241E*-Z5E; DH-IPC-HFW5241E*-Z12E; DH-IPC-HFW5242E*-ZE-MF; DH-IPC-HDBW5241E*-ZE; DH-IPC-HDBW5241E*-ZHE; DH-IPC-HDBW5241E*-Z5E; DH-IPC-HDBW5242E*-ZE-MF; DH-IPC-HDPW5241G*-ZE; DH-IPC-HDPW5242G*-ZE-MF; DH-IPC-HDW5241T*-ZE; DH-IPC-HDW5242T*-ZE-MF; DH-IPC-HF5241E*-E; DH-IPC-HF5242E*-E-MF; DH-IPC-HFW5442E*-SE; DH-IPC-HFW5442T*-SE; DH-IPC-HFW5442T*-ASE; DH-IPC-HDBW5442R*-S; DH-IPC-HDBW5442R*-ASE; DH-IPC-HDW5442TM*-ASE; DH-IPC-HFW5442E*-ZE; DH-IPC-HFW5442E*-ZHE; DH-IPC-HFW5442E*-Z4E; DH-IPC-HDBW5442E*-ZE; DH-IPC-HDBW5442E*-ZHE; DH-IPC-HDBW5442E*-Z4E; DH-IPC-HDPW5442G*-ZE; DH-IPC-HDW5442T*-ZE; DH-IPC-HF5442E*-E; DH-IPC-HFW5541E*-SE; DH-IPC-HFW5541T*-SE; DH-IPC-HFW5541T*-ASE; DH-IPC-HDBW5541R*-S; DH-IPC-HDBW5541R*-ASE; DH-IPC-HDW5541TM*-ASE; DH-IPC-HFW5541E*-ZE; DH-IPC-HFW5541E*-Z5E; DH-IPC-HDBW5541E*-ZE; DH-IPC-HDBW5541E*-Z5E; DH-IPC-HDPW5541G*-ZE; DH-IPC-HDW5541T*-ZE; DH-IPC-HF5541E*-E; DH-IPC-HDW5241H*-AS-PV; DH-IPC-HDW5541H*-AS-PV; DH-IPC-HFW5241T*-AS-PV; DH-IPC-HFW5541T*-AS-PV; DH-IPC-HDBW5241R1*-AS-PV; DH-IPC-HDBW5541R1*-AS-PV; DH-IPC-HDW5241H*-ASE-PV; DH-IPC-HDW5541H*-ASE-PV; DH-IPC-HFW5241T*-AS-LED; DH-IPC-HFW5442T*-AS-LED; DH-IPC-HFW5241T*-ASE-NI; DH-IPC-HFW5442T*-ASE-NI; DH-IPC-HDBW5241R*-ASE-NI; DH-IPC-HDBW5442R*-ASE-NI; DH-IPC-HDW5241TM*-AS-LED; DH-IPC-HDW5442TM*-AS-LED; DH-IPC-HFW5242H*-ZE-MF; DH-IPC-HFW5242H*-ZHE-MF; DH-IPC-HFW5242H*-Z6E-MF; DH-IPC-HFW5442H*-ZE; DH-IPC-HFW5442H*-ZHE; DH-IPC-HFW5442H*-Z4E; DH-IPC-HDBW5242H*-ZE-MF; DH-IPC-HDBW5242H*-ZHE-MF; DH-IPC-HDBW5242H*-Z6E-MF; DH-IPC-HDBW5442H*-ZE; DH-IPC-HDBW5442H*-ZHE; DH-IPC-HDBW5442H*-Z4E; DH-IPC-HDW3549H*-AS-PV; DH-IPC-HDW3449H*-AS-PV; DH-IPC-HDW3249H*-AS-PV; DH-IPC-HFW3549T1*-AS-PV; DH-IPC-HFW3449T1*-AS-PV; DH-IPC-HFW3249T1*-AS-PV; DH-IPC-HFW5842E*-SE-S2; DH-IPC-HFW5842T*-ASE-S2; DH-IPC-HDBW5842R1*-ASE-S2; DH-IPC-HDW5842TM*-SE-S2; DH-IPC-HFW5842E*-ZE-S2; DH-IPC-HFW5842E*-Z4E-S2; DH-IPC-HDBW5842E*-ZE-S2; DH-IPC-HDBW5842E*-Z4E-S2; DH-IPC-HF5842F*-ZE-S2; DH-IPC-HDW5842T*-ZE-S2; DH-IPC-HFW5442H*-ZHE-S2; DH-IPC-HFW5442H*-Z4HE-S2; DH-IPC-HFW5842H*-ZHE-S2; DH-IPC-HFW5842H*-Z4HE-S2; DH-IPC-HDBW5442H*-ZHE-S2; DH-IPC-HDBW5442H*-Z4HE-S2; DH-IPC-HDBW5842H*-ZHE-S2; DH-IPC-HDBW5842H*-Z4HE-S2; DH-IPC-HFW5449T*-ASE-LED; DH-IPC-HDBW5449R1*-ASE-LED; DH-IPC-HDW5449TM*-SE-LED; DH-IPC-HFW5449T1*-ZE-LED; DH-IPC-HDBW5449R1*-ZE-LED; DH-IPC-HFW5849T1*-ASE-LED; DH-IPC-HFW5449T1*-ASE-D2; DH-IPC-HDW5449H*-ASE-D2; DH-IPC-HFW3449T1*-AS-PV-S3; DH-IPC-HFW3549T1*-AS-PV-S3; DH-IPC-HDW3449H*-AS-PV-S3; DH-IPC-HDW3549H*-AS-PV-S3; DH-IPC-HFW3849T1*-AS-PV-S3; DH-IPC-HDW3849H*-AS-PV-S3; DH-IPC-HFW3449T1*-ZAS-PV-S3; DH-IPC-HFW3549T1*-ZAS-PV-S3; DH-IPC-HFW3849T1*-ZAS-PV-S3; DH-IPC-HDBW3449R1*-ZAS-PV-S3; DH-IPC-HDBW3549R1*-ZAS-PV-S3; DH-IPC-HDBW3849R1*-ZAS-PV-S3; IPC-HFW5241E-SE-0280B; IPC-HFW5241E-SE-0360B; IPC-HFW5241E-SE-0600B; IPC-HFW5241E-S-0280B; IPC-HFW5241E-S-0360B; IPC-HFW5241E-S-0600B; IPC-HFW5241T-SE-0280B; IPC-HFW5241T-SE-0360B; IPC-HFW5241T-SE-0600B; IPC-HFW5241T-SE-0800B; IPC-HFW5241T-SE-1200B; IPC-HFW5241T-S-0280B; IPC-HFW5241T-S-0360B; IPC-HFW5241T-S-0600B; IPC-HFW5241T-S-0800B; IPC-HFW5241T-S-1200B; IPC-HFW5241T-ASE-0280B; IPC-HFW5241T-ASE-0360B; IPC-HFW5241T-ASE-0600B; IPC-HFW5241T-ASE-0800B; IPC-HFW5241T-ASE-1200B; IPC-HFW5241T-ASE-0360B-S2; IPC-HFW5242T-ASE-MF-0280B; IPC-HFW5242T-ASE-MF-0360B; IPC-HFW5242T-ASE-MF-0600B; IPC-HDBW5241R-S-0280B; IPC-HDBW5241R-S-0360B; IPC-HDBW5241R-S-0600B; IPC-HDBW5241R-ASE-0280B; IPC-HDBW5241R-ASE-0360B; IPC-HDBW5241R-ASE-0600B; IPC-HDBW5241R-ASE-0280B-S2; IPC-HDBW5242R-ASE-MF-0280B; IPC-HDBW5242R-ASE-MF-0360B; IPC-HDBW5242R-ASE-MF-0600B; IPC-HDW5241TM-ASE-0280B; IPC-HDW5241TM-ASE-0600B; IPC-HDW5241TM-ASE-0360B; IPC-HDW5241TM-AS-0360B; IPC-HDW5241TM-AS-0600B; IPC-HDW5241TM-AS-0280B; IPC-HFW5241E-ZE-27135-S2; IPC-HFW5241E-ZE-27135; IPC-HFW5241E-ZHE-27135; IPC-

HFW5241E-Z5E-0735; IPC-HFW5241E-ZE-0560; IPC-HFW5242E-ZE-MF-2712; IPC-HFW5242E-ZE-MF-2712-ATC; IPC-HDBW5241E-ZE-27135-DC12AC24V-S2; IPC-HDBW5241E-ZE-27135-DC12AC24V; IPC-HDBW5241E-ZHE-27135-DC12AC24V; IPC-HDBW5241E-Z5E-0735-DC12AC24V; IPC-HDBW5242E-ZE-MF-2712-DC12AC24V; IPC-HDBW5242E-ZE-MF-2712-DC12AC24V-ATC; IPC-HDPW5241G-ZE-27135; IPC-HDPW5241G-Z-27135; IPC-HDPW5242G-ZE-MF-2712; IPC-HDPW5242G-Z-MF-2712; IPC-HDW5241T-ZE-27135; IPC-HDW5242T-ZE-MF-2712; IPC-HF5241E-E; IPC-HF5242E-E-MF; IPC-HFW5442E-SE-0280B; IPC-HFW5442E-SE-0360B; IPC-HFW5442E-SE-0600B; IPC-HFW5442E-S-0360B; IPC-HFW5442E-S-0280B; IPC-HFW5442E-S-0600B; IPC-HFW5442T-SE-0280B; IPC-HFW5442T-SE-0360B; IPC-HFW5442T-SE-0600B; IPC-HFW5442T-S-0360B; IPC-HFW5442T-S-0280B; IPC-HFW5442T-S-0600B; IPC-HFW5442T-ASE-0280B; IPC-HFW5442T-ASE-0360B; IPC-HFW5442T-ASE-0600B; IPC-HFW5442T-ASE-0280B-S2; IPC-HFW5442T-ASE-0360B-S2; IPC-HDBW5442R-S-0280B; IPC-HDBW5442R-S-0360B; IPC-HDBW5442R-S-0600B; IPC-HDBW5442R-ASE-0280B; IPC-HDBW5442R-ASE-0360B; IPC-HDBW5442R-ASE-0600B; IPC-HDBW5442R-ASE-0280B-S2; IPC-HDBW5442R-ASE-0360B-S2; IPC-HDW5442TM-ASE-0360B; IPC-HDW5442TM-ASE-0600B; IPC-HDW5442TM-ASE-0280B; IPC-HDW5442TM-AS-0280B; IPC-HDW5442TM-AS-0360B; IPC-HDW5442TM-AS-0600B; IPC-HFW5442E-ZE-2712; IPC-HFW5442E-ZE-2712-S2; IPC-HFW5442E-ZHE-2712; IPC-HFW5442E-Z4E-0832; IPC-HDBW5442E-ZE-2712-DC12AC24V; IPC-HDBW5442E-ZE-2712-DC12AC24V-S2; IPC-HDBW5442E-ZHE-2712-DC12AC24V; IPC-HDBW5442E-Z4E-0832-DC12AC24V; IPC-HDPW5442G-ZE-2712; IPC-HDPW5442G-Z-2712; IPC-HDW5442T-ZE-2712; IPC-HFW5541E-SE-0280B; IPC-HFW5541E-SE-0360B; IPC-HFW5541E-SE-0600B; IPC-HFW5541E-S-0280B; IPC-HFW5541E-S-0360B; IPC-HFW5541E-S-0600B; IPC-HFW5541T-SE-0280B; IPC-HFW5541T-SE-0360B; IPC-HFW5541T-SE-0600B; IPC-HFW5541T-SE-0800B; IPC-HFW5541T-SE-1200B; IPC-HFW5541T-S-0800B; IPC-HFW5541T-S-0600B; IPC-HFW5541T-S-0280B; IPC-HFW5541T-S-0360B; IPC-HFW5541T-S-1200B; IPC-HFW5541T-ASE-0280B; IPC-HFW5541T-ASE-0360B; IPC-HFW5541T-ASE-0600B; IPC-HFW5541T-ASE-0800B; IPC-HFW5541T-ASE-1200B; IPC-HFW5541T-ASE-0360B-S2; IPC-HDBW5541R-S-0280B; IPC-HDBW5541R-S-0360B; IPC-HDBW5541R-S-0600B; IPC-HDBW5541R-ASE-0280B; IPC-HDBW5541R-ASE-0360B; IPC-HDBW5541R-ASE-0600B; IPC-HDBW5541R-ASE-0280B-S2; IPC-HDW5541TM-ASE-0360B; IPC-HDW5541TM-ASE-0600B; IPC-HDW5541TM-ASE-0280B; IPC-HDW5541TM-AS-0600B; IPC-HDW5541TM-AS-0360B; IPC-HDW5541TM-AS-0280B; IPC-HFW5541E-ZE-27135; IPC-HFW5541E-ZE-27135-S2; IPC-HFW5541E-Z5E-0735; IPC-HDBW5541E-ZE-27135-DC12AC24V; IPC-HDBW5541E-ZE-27135-DC12AC24V-S2; IPC-HDBW5541E-Z5E-0735-DC12AC24V; IPC-HDPW5541G-ZE-27135; IPC-HDPW5541G-Z-27135; IPC-HDW5541T-ZE-27135; IPC-HDW5241H-AS-PV-0280B; IPC-HDW5241H-AS-PV-0360B; IPC-HDW5241H-AS-PV-0600B; IPC-HDW5541H-AS-PV-0280B; IPC-HDW5541H-AS-PV-0360B; IPC-HDW5541H-AS-PV-0600B; IPC-HFW5241T-AS-PV-0280B; IPC-HFW5241T-AS-PV-0360B; IPC-HFW5241T-AS-PV-0600B; IPC-HFW5241T-AS-PV-0800B; IPC-HFW5541T-AS-PV-0280B; IPC-HFW5541T-AS-PV-0360B; IPC-HFW5541T-AS-PV-0600B; IPC-HFW5541T-AS-PV-0800B; IPC-HDBW5241R1-AS-PV-0280B; IPC-HDBW5241R1-AS-PV-0600B; IPC-HDBW5241R1-AS-PV-0360B; IPC-HDBW5541R1-AS-PV-0280B; IPC-HDBW5541R1-AS-PV-0360B; IPC-HDBW5541R1-AS-PV-0600B; IPC-HDW5241H-ASE-PV-0600B; IPC-HDW5241H-ASE-PV-0360B; IPC-HDW5241H-ASE-PV-0280B; IPC-HDW5541H-ASE-PV-0600B; IPC-HDW5541H-ASE-PV-0360B; IPC-HDW5541H-ASE-PV-0280B; IPC-HFW5249T-AS-LED-0280B; IPC-HFW5249T-AS-LED-0360B; IPC-HFW5249T-AS-LED-0600B; IPC-HFW5249T-AS-LED-0800B; IPC-HFW5449T-AS-LED-0280B; IPC-HFW5449T-AS-LED-0360B; IPC-HFW5449T-AS-LED-0600B; IPC-HFW5249T-ASE-NI-0360B; IPC-HFW5449T-ASE-NI-0360B; IPC-HDBW5249R-ASE-NI-0360B; IPC-HDBW5449R-ASE-NI-0360B; IPC-HDW5249TM-AS-LED-0280B; IPC-HDW5249TM-AS-LED-0360B; IPC-HDW5249TM-AS-LED-0600B; IPC-HDW5449TM-AS-LED-0280B; IPC-HDW5449TM-AS-LED-0360B; IPC-HDW5449TM-AS-LED-0600B; IPC-HFW5242H-ZE-MF-2718; IPC-HFW5242H-ZHE-MF-

2718; IPC-HFW5242H-Z6E-MF-0848; IPC-HFW5442H-ZE-2712; IPC-HFW5442H-ZH-CER-2712-DC12DC24V; IPC-HFW5442H-ZHE-2712; IPC-HFW5442H-Z4E-0832; IPC-HDBW5242H-ZE-MF-2718-DC12AC24V; IPC-HDBW5242H-ZHE-MF-2718-DC12AC24V; IPC-HDBW5242H-Z6E-MF-0848-DC12AC24V; IPC-HDBW5442H-ZE-2712-DC12AC24V; IPC-HDBW5442H-ZH-CER-2712-DC12DC24AC24V; IPC-HDBW5442H-ZHE-2712-DC12AC24V; IPC-HDBW5442H-Z4E-0832-DC12AC24V; IPC-HDW3549H-AS-PV-0360B; IPC-HDW3549H-AS-PV-0280B; IPC-HDW3449H-AS-PV-0280B; IPC-HDW3449H-AS-PV-0360B; IPC-HDW3249H-AS-PV-0280B; IPC-HDW3249H-AS-PV-0360B; IPC-HFW3549T1-AS-PV-0280B; IPC-HFW3549T1-AS-PV-0360B; IPC-HFW3549T1-AS-PV-0600B; IPC-HFW3449T1-AS-PV-0280B; IPC-HFW3449T1-AS-PV-0360B; IPC-HFW3449T1-AS-PV-0600B; IPC-HFW3249T1-AS-PV-0280B; IPC-HFW3249T1-AS-PV-0360B; IPC-HFW3249T1-AS-PV-0600B; IPC-HFW5842E-SE-0280B-S2; IPC-HFW5842E-SE-0360B-S2; IPC-HFW5842E-SE-0600B-S2; IPC-HFW5842T-ASE-0280B-S2; IPC-HFW5842T-ASE-0360B-S2; IPC-HFW5842T-ASE-0600B-S2; IPC-HDBW5842R1-ASE-0280B-S2; IPC-HDBW5842R1-ASE-0360B-S2; IPC-HDBW5842R1-ASE-0600B-S2; IPC-HDW5842TM-SE-0280B-S2; IPC-HDW5842TM-SE-0360B-S2; IPC-HDW5842TM-SE-0600B-S2; IPC-HFW5842E-ZE-2712-S2; IPC-HFW5842E-Z4E-0832-S2; IPC-HDBW5842E-ZE-2712-S2; IPC-HDBW5842E-Z4E-0832-S2; IPC-HF5842F-ZE-2712-S2; IPC-HDW5842T-ZE-2712-S2; IPC-HFW5442H-ZHE-2712-S2; IPC-HFW5442H-Z4HE-0832-S2; IPC-HFW5842H-ZHE-2712-S2; IPC-HFW5842H-Z4HE-0832-S2; IPC-HDBW5442H-ZHE-2712-S2; IPC-HDBW5442H-Z4HE-0832-S2; IPC-HDBW5842H-ZHE-2712-S2; IPC-HDBW5842H-Z4HE-0832-S2; IPC-HFW5449T-ASE-LED-0280B; IPC-HFW5449T-ASE-LED-0360B; IPC-HFW5449T-ASE-LED-0600B; IPC-HDBW5449R1-ASE-LED-0280B; IPC-HDBW5449R1-ASE-LED-0360B; IPC-HDBW5449R1-ASE-LED-0600B; IPC-HDW5449TM-SE-LED-0280B; IPC-HDW5449TM-SE-LED-0360B; IPC-HDW5449TM-SE-LED-0600B; IPC-HFW5449T1-ZE-LED-2712; IPC-HDBW5449R1-ZE-LED-2712; IPC-HFW5849T1-ASE-LED-0280B; IPC-HFW5849T1-ASE-LED-0360B; IPC-HFW5849T1-ASE-LED-0600B; IPC-HFW5449T1-ASE-D2-0280B; IPC-HFW5449T1-ASE-D2-0360B; IPC-HFW5449T1-ASE-D2-0600B; IPC-HDW5449H-ASE-D2-0280B; IPC-HDW5449H-ASE-D2-0360B; IPC-HDW5449H-ASE-D2-0600B; IPC-HFW3449T1-AS-PV-0280B-S3; IPC-HFW3449T1-AS-PV-0360B-S3; IPC-HFW3549T1-AS-PV-0280B-S3; IPC-HFW3549T1-AS-PV-0360B-S3; IPC-HDW3449H-AS-PV-0280B-S3; IPC-HDW3449H-AS-PV-0360B-S3; IPC-HDW3549H-AS-PV-0280B-S3; IPC-HDW3549H-AS-PV-0360B-S3; IPC-HFW3849T1-AS-PV-0280B-S3; IPC-HFW3849T1-AS-PV-0360B-S3; IPC-HDW3849H-AS-PV-0280B-S3; IPC-HDW3849H-AS-PV-0360B-S3; IPC-HFW3449T1-ZAS-PV-27135-S3; IPC-HFW3549T1-ZAS-PV-27135-S3; IPC-HFW3849T1-ZAS-PV-27135-S3; IPC-HDBW3449R1-ZAS-PV-27135-S3; IPC-HDBW3549R1-ZAS-PV-27135-S3; IPC-HDBW3849R1-ZAS-PV-27135-S3

Application note: There are only three cases for the uniform matching character (*) in the model: none, P, N. For example， DH-IPC-HDW5541H*-ASE-PV can be extended to DH-IPC-HDW5541H-ASE-PV，DH-IPC-HDW5541HP-ASE-PV，DH-IPC-HDW5541HN-ASE-PV.

1.4.1.2 IPC 3 Series (1) devices

IPC 3 Series (1) includes the following devices:

DH-IPC-HDBW3241RP-ZS as the reference model, and

DH-IPC-HDBW3241E*-S; DH-IPC-HDBW3241E*-AS; DH-IPC-HDBW3241R*-ZS; DH-IPC-HDBW3241R*-ZAS; DH-IPC-HFW3241T*-ZS; DH-IPC-HFW3241T*-ZAS; DH-IPC-HFW3241E*-SA; DH-IPC-HFW3241E*-AS; DH-IPC-HFW3241M*-AS-I2; DH-IPC-HDW3241TM*-AS; DH-IPC-HDW3241T*-ZAS; DH-IPC-HDBW3241F*-AS-M; IPC-HDBW3241E-S-0280B; IPC-HDBW3241E-S-0360B; IPC-HDBW3241E-S-0600B; IPC-HDBW3241E-AS-0280B; IPC-HDBW3241E-AS-0360B; IPC-HDBW3241E-AS-0600B; IPC-HDBW3241R-ZS-27135; IPC-HDBW3241R-ZAS-27135; IPC-HFW3241T-ZS-27135; IPC-HFW3241T-ZAS-27135; IPC-HFW3241E-SA-0280B; IPC-HFW3241E-SA-

0360B; IPC-HFW3241E-SA-0600B; IPC-HFW3241E-AS-0280B; IPC-HFW3241E-AS-0360B; IPC-HFW3241E-AS-0600B; IPC-HFW3241M-AS-I2-0800B; IPC-HFW3241M-AS-I2-1200B; IPC-HFW3241M-AS-I2-0600B; IPC-HFW3241M-AS-I2-0360B; IPC-HFW3241M-AS-I2-0800-B; IPC-HFW3241M-AS-I2-1200-B; IPC-HFW3241M-AS-I2-0600-B; IPC-HFW3241M-AS-I2-0360-B; IPC-HDW3241TM-AS-0600B; IPC-HDW3241TM-AS-0280B; IPC-HDW3241TM-AS-0360B; IPC-HDW3241T-ZAS-27135; IPC-HDBW3241F-AS-M-0360B; IPC-HDBW3241F-AS-M-0600B; IPC-HDBW3241F-AS-M-0280B

Application note: There are only three cases for the uniform matching character (*) in the model: none, P, N.

1.4.1.3 IPC 3 Series (2) devices

IPC 3 Series (2) includes the following devices:

DH-IPC-HFW3541TP-ZAS as the reference model, and

DH-IPC-HFW3441M*-AS-SFC-I2; DH-IPC-HDBW3441E*-S; DH-IPC-HDBW3441E*-AS; DH-IPC-HDBW3441R*-ZS; DH-IPC-HDBW3441R*-ZAS; DH-IPC-HFW3441T*-ZS; DH-IPC-HFW3441T*-ZAS; DH-IPC-HFW3441E*-SA; DH-IPC-HFW3441E*-AS; DH-IPC-HFW3441M*-AS-I2; DH-IPC-HDW3441TM*-AS; DH-IPC-HDW3441T*-ZAS; DH-IPC-HDBW3441F*-AS-M; DH-IPC-HDBW3541E*-S; DH-IPC-HDBW3541E*-AS; DH-IPC-HDBW3541R*-ZS; DH-IPC-HDBW3541R*-ZAS; DH-IPC-HFW3541T*-ZS; DH-IPC-HFW3541T*-ZAS; DH-IPC-HFW3541E*-SA; DH-IPC-HFW3541E*-AS; DH-IPC-HDW3541TM*-AS; DH-IPC-HDW3541T*-ZAS; DH-IPC-HDBW3541F*-AS-M; DH-IPC-HFW3549E*-AS-LED; DH-IPC-HFW3449E*-AS-NI; DH-IPC-HFW3449E*-AS-LED; DH-IPC-HFW3249E*-AS-NI; DH-IPC-HFW3249E*-AS-LED; DH-IPC-HDW3549TM*-AS-LED; DH-IPC-HDW3449TM*-AS-NI; DH-IPC-HDW3449TM*-AS-LED; DH-IPC-HDW3249TM*-AS-NI; DH-IPC-HDW3249TM*-AS-LED; DH-IPC-HDBW3449E*-AS-NI; DH-IPC-HDBW3249E*-AS-NI; IPC-HFW3441M-AS-SFC-I2-0800B; IPC-HFW3441M-AS-SFC-I2-0600B; IPC-HFW3441M-AS-SFC-I2-0360B; IPC-HDBW3441E-S-0280B; IPC-HDBW3441E-S-0360B; IPC-HDBW3441E-S-0600B; IPC-HDBW3441E-AS-0280B; IPC-HDBW3441E-AS-0360B; IPC-HDBW3441E-AS-0600B; IPC-HDBW3441R-ZS-27135; IPC-HDBW3441R-ZAS-27135; IPC-HFW3441T-ZS-27135; IPC-HFW3441T-ZAS-27135; IPC-HFW3441E-SA-0280B; IPC-HFW3441E-SA-0360B; IPC-HFW3441E-SA-0600B; IPC-HFW3441E-AS-0280B; IPC-HFW3441E-AS-0360B; IPC-HFW3441E-AS-0600B; IPC-HFW3441M-AS-I2-0360B; IPC-HFW3441M-AS-I2-0600B; IPC-HFW3441M-AS-I2-0800B; IPC-HFW3441M-AS-I2-1200B; IPC-HFW3441M-AS-I2-0600-B; IPC-HFW3441M-AS-I2-0360-B; IPC-HDW3441TM-AS-0280B; IPC-HDW3441TM-AS-0360B; IPC-HDW3441TM-AS-0600B; IPC-HDW3441T-ZAS-27135; IPC-HDBW3441F-AS-M-0600B; IPC-HDBW3441F-AS-M-0360B; IPC-HDBW3441F-AS-M-0280B; IPC-HDBW3541E-S-0280B; IPC-HDBW3541E-S-0360B; IPC-HDBW3541E-S-0600B; IPC-HDBW3541E-AS-0280B; IPC-HDBW3541E-AS-0360B; IPC-HDBW3541E-AS-0600B; IPC-HDBW3541R-ZS-27135; IPC-HDBW3541R-ZAS-27135; IPC-HFW3541T-ZS-27135; IPC-HFW3541T-ZAS-27135; IPC-HFW3541E-SA-0280B; IPC-HFW3541E-SA-0360B; IPC-HFW3541E-SA-0600B; IPC-HFW3541E-AS-0280B; IPC-HFW3541E-AS-0360B; IPC-HFW3541E-AS-0600B; IPC-HDW3541TM-AS-0280B; IPC-HDW3541TM-AS-0360B; IPC-HDW3541TM-AS-0600B; IPC-HDW3541T-ZAS-27135; IPC-HFW3549E-AS-LED-0280B; IPC-HFW3549E-AS-LED-0360B; IPC-HFW3449E-AS-NI-0280B; IPC-HFW3449E-AS-NI-0360B; IPC-HFW3449E-AS-LED-0280B; IPC-HFW3449E-AS-LED-0360B; IPC-HDW3549TM-AS-LED-0360B; IPC-HDW3549TM-AS-LED-0280B; IPC-HDW3449TM-AS-NI-0280B; IPC-HDW3449TM-AS-NI-0360B; IPC-HDW3449TM-AS-LED-0280B; IPC-HDW3449TM-AS-LED-0360B; IPC-HDBW3449E-AS-NI-0280B; IPC-HDBW3449E-AS-NI-0360B

Application note: There are only three cases for the uniform matching character (*) in the model: none, P, N.

1.4.1.4 IPC 3 Series (3) devices

IPC 3 Series (3) includes the following devices:

DH-IPC-HFW3841TP-ZAS as the reference model, and

DH-IPC-HDBW3841E*-S; DH-IPC-HDBW3841E*-AS; DH-IPC-HDBW3841R*-ZAS; DH-IPC-HDBW3841R*-ZS; DH-IPC-HFW3841E*-AS; DH-IPC-HFW3841E*-SA; DH-IPC-HFW3841T*-ZAS; DH-IPC-HFW3841T*-ZS; DH-IPC-HFW3849T1*-AS-PV; DH-IPC-HDW3841EM*-AS; DH-IPC-HDW3841TM*-AS; DH-IPC-HDW3841T*-ZAS; DH-IPC-HDW3849H*-AS-PV; IPC-HDBW3841E-S-0280B; IPC-HDBW3841E-S-0600B; IPC-HDBW3841E-S-0360B; IPC-HDBW3841E-AS-0280B; IPC-HDBW3841E-AS-0600B; IPC-HDBW3841E-AS-0360B; IPC-HDBW3841R-ZAS-27135; IPC-HDBW3841R-ZS-27135; IPC-HFW3841E-AS-0280B; IPC-HFW3841E-AS-0360B; IPC-HFW3841E-AS-0600B; IPC-HFW3841E-SA-0280B; IPC-HFW3841E-SA-0360B; IPC-HFW3841E-SA-0600B; IPC-HFW3841T-ZAS-27135; IPC-HFW3841T-ZS-27135; IPC-HFW3849T1-AS-PV-0280B; IPC-HFW3849T1-AS-PV-0360B; IPC-HDW3841EM-AS-0280B; IPC-HDW3841EM-AS-0360B; IPC-HDW3841EM-AS-0600B; IPC-HDW3841TM-AS-0280B; IPC-HDW3841TM-AS-0360B; IPC-HDW3841TM-AS-0600B; IPC-HDW3841T-ZAS-27135; IPC-HDW3849H-AS-PV-0280B; IPC-HDW3849H-AS-PV-0360B

Application note: There are only three cases for the uniform matching character (*) in the model: none, P, N.

1.4.1.5 Dome SD5A Series devices

SD5A Series includes the following devices:

SD5A445XA-HNR as the reference model, and

DH-SD65F233XA-HNR; DH-SD49225XA-HNR; DH-SD49425XB-HNR; DH-SD6CE445XA-HNR; DH-SD1A404XB-GNR; DH-SD5A445XA-HNR; DH-SD1A404XB-GNR-W; SD1A404XB-GNR; SD49425XBN-HNR; DH-SD6CE445XAN-HNR; SD49225XAN-HNR; SD49225XA-HNR; SD1A404XBN-GNR; DH-SD59232XA-HNR; DH-SD65F233XAN-HNR; DH-SD6AE233XA-HNR; DH-SD6AL445XA-HNR-IR; DH-SD65F233XA-HNR; DH-SD49425XB-HNR-G; DH-SD49225XAN-HNR; SD49425XB-HNR; DH-SD1A404XBN-GNR; DH-SD6AL233XA-HNR; DH-SD1A404XBN-GNR-W; DH-SD6AL233XA-HNR-IR; DH-SD49425XBN-HNR; DH-SD5A425XA-HNR; SD1A404XB-GNR-W; DH-SD6AL445XA-HNR; DH-SD49425XBN-HNR-G; DH-SD6AL233XAN-HNR-IR; DH-SD59232XAN-HNR; DH-SD6AL233XAN-HNR; DH-SD5A445XAN-HNR; SD6CE445XA-HNR; SD5A445XAN-HNR; SD6AE233XA-HNR; SD59232XA-HNR; SD6AL445XA-HNR; SD49425XBN-HNR-G; SD5A445XA-HNR; SD65F233XA-HNR; 5A445XANR; DH-SD5A225XA-HNR; SD6CE445XAN-HNR; SD5A425XAN-HNR; DH-PTZ1A225-HNR-XA; SD5A425XA-HNR; DH-SD6AE233XAN-HNR; DH-SD5A425XAN-HNR; SD49425XB-HNR-G; DH-SD6AE433XA-HNR; SD1A404XBN-GNR-W; SD6AE233XAN-HNR; DH-SD6AE433XAN-HNR; SD6AE433XA-HNR; SD6AE433XAN-HNR; SD6AL233XA-HNR-IR; SD6AL233XAN-HNR-IR; SD6AL233XA-HNR; SD6AL233XAN-HNR; SD65F233XAN-HNR; SD59232XAN-HNR; SD6AL445XA-HNR-IR; DH-SD6AL445XAN-HNR; DH-SD6AL445XAN-HNR-IR; SD6AL445XAN-HNR-IR; SD6AL445XAN-HNR; DH-SD5A225XAN-HNR; SD5A225XA-HNR; SD5A225XAN-HNR; DH-SD5A232XA-HNR; DH-SD5A432XA-HNR; DH-SD50232XA-HNR; DH-SD50432XA-HNR; DH-SD52C232XA-HNR; DH-SD52C432XA-HNR; DH-ECA7A1425-HNR-XA-F; DH-ECA7A1425N-HNR-XA-F; DH-SD6AL433XA-HNR; DH-SD6AL433XAN-HNR; SD6AL433XA-HNR; SD6AL433XAN-HNR; DH-PTZ1A225N-HNR-XA; PTZ1A225-HNR-XA; PTZ1A225N-HNR-XA; DH-SD5A232XAN-HNR; DH-SD5A432XAN-HNR; DH-SD50232XAN-HNR; DH-SD50432XAN-HNR; DH-

SD52C232XAN-HNR; DH-SD52C432XAN-HNR; SD5A232XA-HNR; SD5A432XA-HNR; SD5A232XAN-HNR; SD5A432XAN-HNR; SD50232XA-HNR; SD50432XA-HNR; SD50232XAN-HNR; SD50432XAN-HNR; SD52C232XA-HNR; SD52C432XA-HNR; SD52C232XAN-HNR; SD52C432XAN-HNR; DH-SD8A3440XA-HNR; 1A404XBNR; 49425XBNR; 6AL445XANR; SD8A440XA-HNR-YK; DH-SD5A225XA-HNR-SL; SD5A225XA-HNR-SL; DH-SD5A225XAN-HNR-SL; SD5A225XAN-HNR-SL; DH-SD5A245XA-HNR; DH-SD5A245XAN-HNR; SD5A245XA-HNR; SD5A245XAN-HNR; DH-SD8A440XA-HNR-F; DH-SD6AL245XA-HNR; DH-SD6AL245XAN-HNR; SD6AL245XA-HNR; SD6AL245XAN-HNR; DH-ECA3A1404-HNR-XB; DH-ECA3A1404-HNR-XB-F; SD6CE245XAN-HNR; DH-SD6CE245XAN-HNR; SD6CE245XA-HNR; DH-SD6CE245XA-HNR; DH-ECA3A1404N-HNR-XB-F; DH-ECA3A1404N-HNR-XB; DH-SD49425XB-HNR; SD49425XB-HNR; DH-SD49425XBN-HNR; SD49425XBN-HNR; DH-SD49225XA-HNR; SD49225XA-HNR; DH-SD5A432XB-HNR-AC; SD5A432XB-HNR-AC; DH-SD5A232XB-HNR-AC; SD5A232XB-HNR-AC; SD5A225XA-HNR-AC; DH-SD5A225XA-HNR-AC; DH-SD5A432XB-HNR; SD5A432XB-HNR; DH-SD5A232XB-HNR; SD5A232XB-HNR

1.4.1.6 Dome SDT5X Series devices

SDT5X Series includes the following devices:
SDT5X425-4Z4-WA-2812 as the reference model, and
DH-SDT5X425-4Z4-WA-2812; DH-SDT5X425-4Z4-WA-0832; DH-SDT5X425N-4Z4-WA-2812; DH-SDT5X425N-4Z4-WA-0832; SDT5X425-4Z4-WA-2812; SDT5X425-4Z4-WA-0832; SDT5X425N-4Z4-WA-2812; SDT5X425N-4Z4-WA-0832

The delivery of the TOE to the customer is performed by an authorized courier service.
The TOE firmware will be pre-installed at factory but it can be updated from the Dahua's web site

The TOE deliverable includes the camera itself, the firmware already installed and the following items:

Item	Name	Version
Operational User Guidance	Dahua Network Camera Series AGD_OPE	V1.0
Preparative User Guidance	Dahua Network Camera Series AGD_PRE	V1.3
Security Hardening Guide	Dahua Product Security Hardening Guide	V2.0.3
User Manual	Dahua Network Camera Web 3.0_Operation Manual	V2.1.1
	Dahua Dual-PTZ Camera Web 3.0 User's Manual	V1.1.1
	Network Speed Dome & PTZ Camera Web 3.0 User's Manual	V3.0.1

Table 5 TOE deliverables

These deliverables can be downloaded in PDF format by the customer from Dahua's web site

1.4.2 Logical Scope

This section outlines the logical boundaries of the security functionality of the TOE.

1.4.2.1 Security Management

TOE provides security management of the device including:

1. User management;
2. Access Control management based on user roles;
3. Trusted channel management;
4. User authentication management;

5. Firmware update.

1.4.2.2 Identification and Authentication

The TOE management can be done either using a computer with a web browser supporting HTTPS or by a software platform implementing the NetSDK. In both cases the access to the TOE is protected by a user/password authentication. Access to the TOE is protected by a user/password authentication. The access to the management functions implements security controls to detect unsuccessful authentication attempts. When the user fails to log in 5 times (the default setting), TOE will prevent the user from using the login method to connect from the IP address, and the lock time is 300s. The TOE also requires a minimum complexity and length for user passwords.

1.4.2.3 Protection of the TSF

The TOE provides reliable time stamps.

1.4.2.4 Trusted Path/Channels

The following secure channels are enforced by the TOE:

- A trusted path implemented with HTTPS communication shall be established before accessing the TOE management functionality.
- When the non-TOE device connects to the TOE device through a private protocol to pull video stream, TOE has the ability to configure video stream encryption

1.4.2.5 Audit Logs

The TOE has the capability to generate audit records. TOE administrators have the ability to read the logs after establishing the trusted path and successfully log in.

1.4.2.6 Trusted Firmware Updates

The trusted firmware upgrade function is implemented and executed by using signature verification on the uploaded firmware. TOE only allows firmware that has been successfully verified to be updated.

1.4.2.7 TOE Access

The TOE provides the capability to restrict the maximum number of concurrent session for all users through the management interface. The user session will terminate after a certain idle time. Once a session has been terminated the TOE requires users to re-authenticate to establish a new session.

1.4.2.8 Cryptographic Support

The TOE provides cryptographic support for specific functionality:

- Configuration Encrypted Import and Export
- Configuration Encrypted Store
- Certificate private key encrypt Store
- Firmware encryption release
- HTTPS Certificate Generation and Import
- Verification of Firmware Upgrade Authenticity
- Verification of Run Time Software Authenticity
- Video Encryption Transmission

Application note: When the non-TOE device connects to the TOE device through a private protocol to pull video stream, TOE has the ability to configure video stream encryption.

1.4.2.9 Excluded Functionality

The following services and functions are not included in the evaluation scope, so they must to be disabled in the TOE configuration.

Services	Rationale
NTP	Services and functionalities disabled in the certified TOE configuration
HTTP	
RS-232/RS-485	
PPPoE	
DDNS	
SMTP	
UPnP	
SNMP(v1,v2 and v3)	
FTP	
NAS	
Platform access	
SSH	

Table 6 Disabled services and functionality

2 Conformance Claim

This security target claims conformance to CC Version 3.1 revision 5 [CCP1], [CCP2] and [CCP3].
This Security Target conforms to CC Part 2 extended and Part 3 conformant, with a claimed Evaluation Assurance Level of EAL 2, augmented by ALC FLR.2.
This Security Target does not claim conformance with any protection profile.

3 Security Problem Definition

This chapter identifies the Threats, Organisational Security Policies and Assumptions of the TOE.

3.1 Threats

The following table lists the threats addressed by TOE and its environment. The following threats are defined based on relevant information assets, attackers and specific bad behaviour. In the threats description below, the “threat agent” and “attacker” shall be both understood, indistinctly, as any individual entity, either human or machine, performing an adverse action on any TOE asset.

Threat	**Description**
T.UNAUTHORISED_ACCESS	Threat agents may try to gain access to TOE functionality without having the required permission. This threat includes： • Bypassing user authentication • Man in the middle attack • Operation replay Attackers may take advantage of poorly implemented security measures like authentication, session management, design of the communications, etc. By attacking this functionality it could be possible to execute malicious operations without having the proper privileges.
T.WEAK_CRYPTOGRAPHY	Threat agents may use weak encryption algorithms or brute force crack weak passwords. Improper use of encryption algorithms, modes, and key sizes can be exploited by attackers. Attackers can destroy algorithms or try keys brute force to gain unauthorized access.
T.VIDEO_DISCLOSURE	Threat agents may use poorly designed protocols or imperfect key management to perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will steal code stream information, leading to the disclosure of key information. Please note that this threat only applies to Dahua Private Protocol.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access and change the security functions of network devices without the administrator's knowledge. This may cause the attacker to find ways to damage the device (for example, configuration errors, product defects), and the administrator will not know that the device has been damaged.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide firmware that disrupts the security functions of the device. Unauthenticated updates or non-secure firmware are more likely to be used by attackers to destroy firmware.

Threat	Description
T.UNAUTHORISED_SOFTWARE	Threat agents may use some methods to implant unauthorized software (such as malicious programs, malicious kernel modules) on TOE devices, and run the unauthorized software on TOE to achieve some special purposes, such as digital currency mining, DDoS attacks, etc.

Table 7 Threats

3.2 Organizational Security Policies

There are no Organizational Security Policies identified for this TOE.

3.3 Assumptions

The following table identifies the assumptions of TOE device and its environment.

Assumption	Definition
A.PHYSICAL_PROTECTION	It is assumed that TOE is physically protected in its operational environment and will not be a subject of physical attacks that compromise security or interfere with the physical operation of the device.
A.TRUSTED_ADMINS	The administrator of the TOE is a trusted individual which must correctly configure and install the TOE in its operational environment by following the guidance documentation. The Administrators of the TOE are considered trusted individuals which will not carry out any malicious action trying to compromise the availability of the TOE.
A.NETWORK_ SEGREGATION	It is assumed that the TOE LAN is segregated from any other network and, if not physically isolated, it includes the necessary firewall / gateway / physical isolation devices to provide an effective logical isolation and protection against attacks coming from any external network. The TOE LAN is controlled in the sense that only the devices defined as part of the TOE environment in the TOE introduction section of this document can be connected to the TOE LAN.
A.CAMERA_AVAILABLE	It assumed that the TOE environment will prevent attempts to attack TOE from internet or external networks with flooding, malformed packages or other means intended to subvert the TOE TSF or cause a loss of availability of the TOE, such as losing of control or device restarting.

Table 8 Assumptions

4 Security Objectives

This chapter identifies the security objectives for the TOE and for the operational environment of the TOE.

4.1 Security Objectives for the TOE

The following table identifies the security objectives for the TOE.

Objective	Description
O.USER_MANAGEMENT	The TOE provides management capabilities to the Administrator role for adding/removing users into the system (Operator and User roles) and to configure the access permissions to the TOE functionalities
O.USER_AUTHORISATION	The TOE manages different access control to operations for different user roles, by means of a unique account and password.
O.USER_AUTHENTICATION	The TOE provides authentication mechanisms for users. When logging in the TOE, must verify the validity of its identity.
O.SECURITY_MANAGE	TOE provides tools or methods to allow authorized administrators to manage their security functions.
O.AUDIT_LOGS	TOE supports the recording function of events and alarms.
O.VIDEO_CONFIDENTIALITY	TOE supports the function of encrypting and transmitting video in private encryption mode, using strong cryptographic algorithms.
O.TRUSTED_PATH	TOE provides the ability to establish a trusted channel before accessing to the TOE management functionality, using strong cryptographic algorithms.
O.FIRMWARE_UPDATE_INTEGRITY	TOE will verify the integrity and validity of the firmware upgrade package during the firmware upgrade process, and ensures that only valid firmware is accepted for upgrade. Additionally, the upgrade is allowed only when the security version of the firmware is greater than or equal to the current TOE security version.
O.TRUSTED_SOFTWARE	The TOE will verify the integrity and authenticity of the any software elements prior to be launched.

Table 9 Security Objectives for the TOE

4.2 Security Objectives for the Operational Environment

The following table identifies the security objectives for the operational environment.

Objective	Description
OE.TRUSTED_ADMINS	The administrator of the TOE is a trusted individual which will correctly configure and install the TOE in its operational environment by following the guidance documentation. The administrators of the TOE are trusted individuals that will not perform any malicious action trying to compromise the availability of the TOE.
OE.TRUSTED_NETWORK	Attackers have no chance to connect any malicious devices into the local network of the TOE.
OE:SEGREGATED_NETWORK	The TOE LAN is segregated, either by a physical isolation or the presence of logical isolation devices preventing unauthorized access from outside of the TOE LAN.
OE.PHYSICAL_SECURITY	The physical security of TOE and the data it contains is ensured in the physical operating environment.

Table 10 Security Objectives for the Operational Environment

4.3 Security Objectives Rationale

The following table maps the threats of the security problem established to the security objectives of the TOE and the security objectives of the operational environment.

Threat	Security Objectives
T.UNAUTHORISED_ACCESS	The **O.USER_MANAGEMENT** objective determines the user's identity role and manages the users who are allowed to log in to TOE. The **O.USER_AUTHORISATION** objective determines that only authorized administrators with appropriate permissions can access TOE management functions. The **O.USER_AUTHENTICATION** objective requires users to authorize and authenticate when managing TOE functions or obtaining TOE services. The **O.SECURITY_MANAGE** objective requires that TOE can manage the above functions to administrators only.
T.WEAK_CRYPTOGRAPHY	The **O.VIDEO_CONFIDENTIALITY** objective requires using secure cryptographic functions. The **O.TRUSTED_PATH** objective requires using secure cryptographic functions.

Threat	Security Objectives
T.VIDEO_DISCLOSURE	The **O.VIDEO_CONFIDENTIALITY** objective requires that when communicating with TOE through NetSDK, TOE can encrypt the code stream to prevent video disclosure. The **O.TRUSTED_PATH** objective requires that TOE can transmit code stream data through a common secure channel.
T.UNDETECTED_ACTIVITY	The **O.SECURITY_MANAGE** objective requires TOE to manage the audit function. The **O.AUDIT_LOGS** objective requires TOE to generate audit records that will inform about events and alarms detected on the TOE.
T.UPDATE_COMPROMISE	The **O.FIRMWARE_UPDATE_INTEGRITY** objective prevents upgrading the TOE firmware with software from untrusted sources.
T.UNAUTHORISED_SOFTWARE	**OE.PHYSICAL_SECURITY, OE.SEGREGATED_NETWORK,** and **OE.TRUSTED_NETWORK** prevent attackers from accessing the TOE. **OE.TRUSTED_ADMINS** ensures that administrators having access to the TOE will not install malicious software elements. **O.TRUSTED_SOFTWARE** ensures that unauthorized software elements will not be executed.
Assumption	**Security Objectives for the Environment**
A.PHYSICAL_PROTECTION	**OE.PHYSICAL_SECURITY** ensures that attackers will by no means have physical access to the TOE.
A.TRUSTED_ADMINS	**OE.TRUSTED_ADMINS** makes sure that the administrators with access to the TOE are trusted and that they will correctly configure and install the TOE in its operational environment by following the guidance documentation. The administrators of the TOE will not perform any malicious action trying to compromise the availably of the TOE.
A.NETWORK_ SEGREGATION	**OE.SEGREGATED_NETWORK** ensures that the TOE LAN is segregated and that attacks from external networks are prevented. **OE.TRUSTED_NETWORK** ensures that attacker have no chance to connect malicious devices to the TOE LAN.
A.CAMERA_AVAILABLE	**OE.SEGREGATED_NETWORK** ensures attacks from Internet or external networks are prevented.

Table 11 Security Objectives Rationale

Threats and assumptions / Objectives	T.UNAUTHORISED_ACCESS	T.WEAK_CRYPTOGRAPHY	T.VIDEO_DISCLOSURE	T.UNDETECTED_ACTIVITY	T.UPDATE_COMPROMISE	T.UNAUTHORISED_SOFTWARE	A.CAMERA_AVAILABLE	A.PHYSICAL_PROTECTION	A.TRUSTED_ADMINS	A.NETWORK_ SEGREGATION
O.USER_MANAGEMENT	X									
O.USER_AUTHORISATION	X									
O.USER_AUTHENTICATION	X									
O.SECURITY_MANAGE	X			X						
O.AUDIT_LOGS				X						
O.VIDEO_CONFIDENTIALITY		X	X							
O.TRUSTED_PATH		X	X							
O.FIRMWARE_UPDATE_INTEGRITY					X					
O.TRUSTED_SOFTWARE						X				
OE.TRUSTED_ADMINS						X			X	
OE.TRUSTED_NETWORK						X				X
OE:SEGREGATED_NETWORK						X	X			X
OE.PHYSICAL_SECURITY						X		X		

Table 12 Threats and Assumptions to Security Objectives Mapping

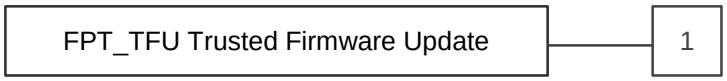
5 Extended Components Definition

5.1 Definition of the Family FPT_TFU – Trusted Firmware Update

Family Behaviour

Components in this family address the requirements for the verification of the integrity and authenticity of the TOE firmware before updating.

Component levelling



Management: FPT_TFU.1
There are no management activities foreseen.

Audit: FPT_TFU.1
There are no actions defined to be auditable.

FPT_TFU.1 Trusted Firmware Updates.

Hierarchical to: No other components.

Dependencies: None

FPT_TFU.1.1 The TSF shall provide [***assignment: authorised users***] the ability to query the currently executing version of the TOE firmware.

FPT_TFU.1.2 The TSF shall provide [***assignment: authorised users***] the ability to manually initiate updates to the TOE firmware and ***[selection: [assignment: list an update mechanism], no other update mechanism***].

FPT_TFU.1.3 The TSF shall provide means to authenticate firmware updates to the TOE using a [***assignment: digital signature mechanism, published hash, other mechanisms***] prior to accepting and installing those updates.

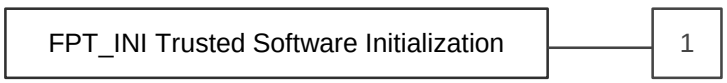
FPT_TFU.1.4 The TSF shall provide means to verify the integrity of firmware images to the TOE using a [***assignment: hashing algorithm, other mechanisms***] prior to accepting and installing those updates.

5.2 Definition of the Family FPT_INI – Trusted Software Initialization

Family Behaviour

Components in this family address the requirements for the verification of the integrity and authenticity of the TOE software before launching.

Component levelling



Management: FPT_INI.1
There are no management activities foreseen.

Audit: FPT_INI.1
There are no actions defined to be auditable.

FPT_INI.1 Trusted Software Initialization.

Hierarchical to: No other components.

Dependencies: None

FPT_INI.1.1 The TSF shall maintain a Root of Trust in the form of **[*selection: public key, symmetric key*]** of length **[*assignment: length of the key*]** and algorithm **[*selection: RSA, EC, AES,* [*assignment: other algorithm*]]**.

FPT_INI.1.2 The TSF shall maintain a Root of Trust that **[*selection: cannot be modified or deleted, can only be modified by:* [*assignment: list of authorized users or subjects*]]**

FPT_INI.1.3 The TSF shall verify the integrity and authenticity of any software component, using the hierarchy root of trust chain, prior to be launched.

FPT_INI.1.4 The TSF shall not execute any software component which integrity and authenticity verification has failed, and ***[selection: none, log this event,*** [***assignment: list of other actions***]]***.***

6 Security Requirements

6.1 Security Functional Requirements

The operations on the SFRs have been identified using the following typographical distinctions:

- Iteration: name of the SFR followed by "/" and iteration identifier
- Refinement: **Refinement**
- Selection: *selection*
- Assignment: *assignment*

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the *not specified* level of audit; and
c) *Login/logout of user;*
d) *Firmware update operations*

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and;
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *none*.

Application note: Since technically unsuccessful login events are not logged. But when the defined number of unsuccessful authentication attempts has been surpassed (FIA_AFL.1.2), this event will be logged to log file.

6.1.1.2 FAU_GEN.2 User Identity Association

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.3 FAU_SAR.1 Audit Review

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide *authorized users* with the capability to read *all the auditable events as defined in FAU_GEN.1* from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information

6.1.1.4 FAU_SAR.2 Restricted Audit Review

Hierarchical to: No other components

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.1.2 Identification and Authentication (FIA)

6.1.2.1 FIA_AFL.1 Authentication Failure Handling

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when *an administrator configurable positive integer within 5* unsuccessful authentication attempts occur related to *user authentication through all the interfaces*.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *surpassed*, the TSF shall *terminate the session of the user trying to authenticate and block the user account from the connecting IP address using the same login type for 5 minutes*.

Application note: the interfaces include only the NetSDK interface implementing the protocols HTTPS and RTSP. If the TOE is powered off and back on, the blocking of the IP address is reverted; however, for an attacker to exploit this scenario he would need to have physical access to the TOE, which is assumed not possible.

6.1.2.2 FIA_SOS.1 Verification of Secrets

Hierarchical to: No other components

Dependencies: No dependencies

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet *the Following:*

a) Passwords have a minimum length of 8 characters;

b) Passwords have a maximum length of 32 characters;

c) Passwords strength rating, required above the Medium

- *Score >=70, strong;*
- *Score<70 and >=50, medium;*
- *Score<50, weak.*

d) The scoring rules are as follows：

- *Length: 5 score – length less than or equal to 4 symbol; 10 score – length between 5 symbol to 7 symbol; 25 score – length greater than or equal to 8 symbol;*
- *Letters: 0 score-no letters; 10 scores --all uppercase (lower) characters; 20 scores -case mixed string;*
- *Numbers: 0 score -no number; 10 scores -1 number; 20 scores - more than 1 number;*
- *Symbols: 0 score -no symbol; 10 scores -1 symbol; 25 scores - more than 1 symbol;*
- *Rewards: 2 scores -letter and number mix; 3 scores -letter, number and symbol mix; 5 scores -uppercase and lowercase letters, numbers and symbols mix.*

6.1.2.3 *FIA_UAU.1 Timing of Authentication*

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UAU.1.1 The TSF shall allow *the connection of the trusted path as defined in FTP_TRP.1* on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.2.4 FIA_UID.1 Timing of Identification

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UID.1.1 The TSF shall allow *the connection of the trusted path as defined in FTP_TRP.1* on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.3 Security Management (FMT)

6.1.3.1 FMT_MOF.1 Management of Security Functions Behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to *modify the Behaviour of* the functions *defined in FMT_SMF.1* to *Administrator**.***

6.1.3.2 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components

Dependencies: No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

1. *Creation/deletion of Users*
2. *Access permissions of existing Users*
3. *Trusted path/channel certificate management*
4. *Configuration of unsuccessful authentication attempts*
5. *Configuration of the limitation on multiple concurrent sessions*
6. *Operation of firmware update.*

6.1.3.3 FMT_SMR.1 Security Roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles *Administrator and User**.***

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.4 Protection of the TSF (FPT)

6.1.4.1 FPT_STM.1 Reliable Time Stamps

Hierarchical to: No other components

Dependencies: No dependencies

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.1.4.2 FPT_TFU.1 Trusted Firmware Update

Hierarchical to: No other components.

Dependencies: None

FPT_TFU.1.1 The TSF shall provide *authorised users with "System Info" permission* the ability to query the currently executing version of the TOE firmware.

FPT_TFU.1.2 The TSF shall provide *authorised users with "Maintenance" permission* the ability to manually initiate updates to the TOE firmware and *no other update mechanism*.

FPT_TFU.1.3 The TSF shall provide means to authenticate firmware updates to the TOE using a *digital signature mechanism* prior to accepting and installing those updates.

FPT_TFU.1.4 The TSF shall provide means to verify the integrity of firmware images to the TOE using a *hashing algorithm* prior to accepting and installing those updates.

6.1.4.3 FPT_INI.1 Trusted Software Initialization

Hierarchical to: No other components.

Dependencies: None

FPT_INI.1.1 The TSF shall maintain a Root of Trust in the form of *public key* of length *2048* and algorithm *RSA***.**

FPT_INI.1.2 The TSF shall maintain a Root of Trust that *cannot be modified or deleted.*

FPT_INI.1.3 The TSF shall verify the integrity and authenticity of any software component, using the hierarchy root of trust chain, prior to be launched.

FPT_INI.1.4 The TSF shall not execute any software component which integrity and authenticity verification has failed, and *none*.

6.1.4.4 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: None

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: *Attempt to rollback the firmware to an older version.*

Application note: While performing a Firmware Update operation, the TOE shall compare the ~~security version~~ of the already installed firmware and compare it with the new firmware, and reject the firmware update if its version is older than the existing version.

6.1.5 TOE Access (FTA)

6.1.5.1 FTA_MCS.1 Basic Limitation on Multiple Concurrent Sessions

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to **all users**.

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of *10* sessions ~~per user~~ **for all users globally.**.

Application note: the limit of sessions is the total number of connections to the TOE, for all users globally.

6.1.5.2 FTA_SSL.3 TSF-initiated Termination

Hierarchical to: No other components

Dependencies: No dependencies

FTA_SSL.3.1 The TSF shall terminate an interactive session after *30 minutes.*

6.1.5.3 FTA_SSL.4 User-initiated Termination

Hierarchical to: No other components

Dependencies: No dependencies

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

6.1.6 Trusted Path/Channels (FTP)

6.1.6.1 FTP_TRP.1 Trusted Path

Hierarchical to: No other components

Dependencies: No dependencies

FTP_TRP.1.1 The TSF shall provide a communication path between itself and *remote* users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *modification, disclosure*.

FTP_TRP.1.2 The TSF shall permit *remote users* to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for *initial user authentication and all subsequent operations performed on those interfaces after the user has been authenticated.*

Application note:

This SFR requires the implementation of TLS 1.2, according to RFC5246. The implementation of these secure channels requires the implementation of the following algorithms:

- **AES, according FIPS PUB**
- **RSA, according FIPS PUB 186-4**
- **SHA1, SHA2 according FIPS PUB -4**
- **HMAC, according FIPS PUB 198-1**
- **ECC, according RFC4492**
- **ECDH, according RFC4492**
- **GCM, according NIST SP 800-38D**

6.1.7 Cryptographic support (FCS)

6.1.7.1 FCS_COP.1/AES Cryptographic operation (AES Data Encryption/Decryption)
Hierarchical to: No other components.
Dependencies: FCS_CKM.1/AES Cryptographic key generation
FCS_CKM.4/AES Cryptographic key destruction

FCS_COP.1.1/AES The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *AES in CBC mode or AES in OFB mode* and cryptographic key sizes *256 bits* that meet the following:*[FIPS197].*

6.1.7.2 FCS_CKM.1/AES Cryptographic key generation
Hierarchical to: No other components.
Dependencies: FCS_CKM.4/AES Cryptographic key destruction
FCS_COP.1/AES Cryptographic operation

FCS_CKM.1.1/AES The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *KDF or random number Generation* and specified cryptographic key sizes *256 bits* that meet the following: *none*.

Application note: AES keys for configuration import/export and storage are derived using KDF. AES keys for video encryption are randomly created.

6.1.7.3 FCS_CKM.4/AES Cryptographic key destruction
Hierarchical to: No other components.
Dependencies: FCS_CKM.1/AES Cryptographic key generation

FCS_CKM.4.1/AES The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *overwriting the key value with zeros* that meets the following: *none*.

6.1.7.4 FCS_COP.1/Sign Cryptographic operation (Signature Generation and Verification)
Hierarchical to: No other components.
Dependencies: FCS_CKM.1/Sign Cryptographic key generation
FCS_CKM.4/Sign Cryptographic key destruction

FCS_COP.1.1/Sign The TSF shall perform *digital signature generation and verification* in accordance with a specified cryptographic algorithm *RSA with SHA1, RSA with SHA-256, RSA with SHA-384, RSA with SHA-512* and cryptographic key sizes *1024 and 2048* bits that meet the following: *[FIPS PUB 186-4*].

6.1.7.5 FCS_CKM.1/Sign Cryptographic key generation
Hierarchical to: No other components.
Dependencies: FCS_CKM.4/Sign Cryptographic key destruction
FCS_COP.1/Sign Cryptographic operation

FCS_CKM.1.1/Sign The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *RSA key generation* and specified cryptographic key sizes *2048 bits* that meet the following: [*FIPS PUB 186-4*].

6.1.7.6 FCS_CKM.4/Sign Cryptographic key destruction
Hierarchical to: No other components.
Dependencies: FCS_CKM.1/Sign Cryptographic key generation

FCS_CKM.4.1/Sign The TSF shall destroy cryptographic keys in accordance with a specified

cryptographic key destruction method *overwriting the key value with zeros* that meets the following: *none*.

6.1.7.7 FCS_COP.1/Hash Cryptographic operation (Hash Algorithm)
Hierarchical to: No other components.
Dependencies: FCS_CKM.1/Hash Cryptographic key generation
FCS_CKM.4/Hash Cryptographic key destruction.

FCS_COP.1.1/Hash The TSF shall perform *cryptographic hashing* in accordance with a specified cryptographic algorithm *SHA1, SHA-256, SHA-384,SHA-512, MD5* and cryptographic key sizes *none* that meet the following: [*FIPS 180-4], [RFC1321]*.

6.2 SFRs Rationale

Objective	Rationale
O.USER_MANAGEMENT	This SOT is met by FMT_MOF.1, FMT_SMF.1 and FMT_SMR.1 which ensures the required management functionalities and user roles structure to the administrators
O.USER_AUTHORISATION	This SOT is met by FMT_MOF.1, FMT_SMF.1 and FMT_SMR.1 which ensures the required management functionalities and user roles structure to the administrators. Furthermore, FIA_AFL.1, FIA_SOS.1, FIA_UAU.1 and FIA_UID.1 ensures that users are properly identified before authorization is granted.
O.USER_AUTHENTICATION	This SOT is met by FIA_AFL.1, FIA_SOS.1, FIA_UAU.1 and FIA_UID.1 which ensures that users are properly identified. Furthermore, FTA_MCS.1, FTA_SSL.3 and FTA_SSL.4 ensures a proper session management.
O.SECURITY_MANAGE	This SOT is met by FIA_AFL.1, FIA_SOS.1, FIA_UAU.1 and FIA_UID.1 which ensures that administrators are properly identified. Furthermore, FMT_MOF.1, FMT_SMF.1, FMT_SMR.1, FAU_SAR.1 and FAU_SAR.2 ensures that the required management functionalities and user roles structure are made available to the administrators
O.AUDIT_LOGS	This objective is met by FAU_GEN.1, FAU_GEN.2 and FPT_STM.1.
O.VIDEO_CONFIDENTIALITY	This objective is met by FTP_TRP.1, FCS_COP.1/AES, FCS_CKM.1/AES, FCS_CKM.4/AES
O.TRUSTED_PATH	This objective is met by FTP_TRP.1. The establishment of the trusted path requires the availability of certificates that is ensured by FCS_COP.1/Sign, FCS_CKM.1/Sign, FCS_CKM.4/Sign, FCS_COP.1/HASH.
O.FIRMWARE_UPDATE_INTEGRITY	This SOT is met by FPT_TFU.1, which ensures the integrity and authenticity of new firm wares and FPT_FLS.1 which prevents rolling back the firmware to previous versions. The necessary cryptographic support is ensured by FCS_COP.1/Sign, FCS_COP.1/HASH.
O.TRUSTED_SOFTWARE	This SOT is met by FPT_INI.1 which ensures that any software component is verified prior to be executed, according the Root of Trust chain. The necessary cryptographic support is ensured by FCS_COP.1/Sign, FCS_COP.1/HASH.

TOE Objectives / SFRs	O.USER_MANAGEMENT	O.USER_AUTHORISATION	O.USER_AUTHENTICATION	O.SECURITY_MANAGE	O.AUDIT_LOGS	O.VIDEO_CONFIDENTIALITY	O.TRUSTED_PATH	O.FIRMWARE_UPDATE_INTEGRITY	O.TRUSTED_SOFTWARE
FAU_GEN.1					X				
FAU_GEN.2					X				
FAU_SAR.1				X					
FAU_SAR.2				X					
FIA_AFL.1		X	X	X					
FIA_SOS.1		X	X	X					
FIA_UAU.1		X	X	X					
FIA_UID.1		X	X	X					
FMT_MOF.1	X	X		X					
FMT_SMF.1	X	X		X					
FMT_SMR.1	X	X		X					
FPT_STM.1					X				
FPT_TFU.1								X	
FPT_INI.1									X
FPT_FLS.1								X	
FTA_MCS.1			X						
FTA_SSL.3			X						
FTA_SSL.4			X						
FTP_TRP.1						X	X		
FCS_COP.1/AES						X			
FCS_CKM.1/AES						X			
FCS_CKM.4/AES						X			
FCS_COP.1/Sign							X	X	X
FCS_CKM.1/Sign							X		
FCS_CKM.4/Sign							X		
FCS_COP.1/HASH							X	X	X

Table 13 SFRs to SOT mapping

6.3 SFR Dependencies

Requirement	Dependency (CC part 2)	Rationale
FAU_GEN.1	FPT_STM.1	Included
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	Included
FAU_SAR.1	FAU_GEN.1	Included
FAU_SAR.2	FAU_SAR.1	Included
FIA_AFL.1	FIA_UAU.1	Included
FIA_SOS.1	None	NA
FIA_UAU.1	FIA_UID.1	Included
FIA_UID.1	None	NA
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	Included
FMT_SMF.1	None	NA
FMT_SMR.1	FIA_UID.1	Included
FPT_STM.1	None	NA
FPT_TFU.1	None	NA
FPT_INI.1	None	NA
FPT_FLS.1	None	NA
FTA_MCS.1	None	NA
FTA_SSL.3	None	NA
FTA_SSL.4	None	NA
FTP_TRP.1	None	NA
FCS_COP.1/AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/AES, FCS_CKM.4 /AES included
FCS_CKM.1/AES	[FCS_COP.1 or FCS_CKM.2], FCS_CKM.4	FCS_COP.1/AES, FCS_CKM.4/AES included
FCS_CKM.4/AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1/AES included
FCS_COP.1/Sign	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1/Sign, FCS_CKM.4/Sign included
FCS_CKM.1/Sign	[FCS_COP.1 or FCS_CKM.2], FCS_CKM.4	FCS_COP.1/Sign, FCS_CKM.4/Sign included
FCS_CKM.4/Sign	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1/Sign included
FCS_COP.1/Hash	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4	FCS_CKM.1, FCS_CKM.4 not included because the Hash algorithm does not involve usage of any key.

6.4 Security Assurance Requirements

This Security Target claims conformance to EAL2, augmented with ALC_FLR.2.

The EAL2 package has been chosen because these type of products, in the same market niche, provides resistance against attackers with a Basic attack potential (AVA_VAN.2).

The ALC_FLR.2 augmentation has been chosen in order to provide a good response in front of security flaws detected by TOE users or the developer itself.

Assurance Class	Component	Component Title
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Functional specification
	ADV_TDS.1	Basic design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC_ Life-cycle support	ALC_CMC.2	CM capabilities
	ALC_CMS.2	CM scope
	ALC_DEL.1	Delivery
	ALC_FLR.2	Flaw reporting procedures
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE: Tests	ATE_COV.1	Coverage
	ATE_FUN.1	Functional tests
	ATE_IND.2	Independent testing
AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

7 TOE Summary Specification

7.1 Security Audit

FAU_GEN.1: The TOE generates an audit record that is stored internally within the TOE whenever an audited event occurs. The audit logs cover all the audit events as listed in this SFR, and includes details of time, user triggering the event and type of event.

FAU_GEN.2: The TOE shall ensure that each auditable event is associated with the user that triggered the event and as a result they are traceable to a specific user.

FAU_SAR.1: The TOE fulfils this requirement by providing log review authority, and admin user or the user with log review authority has the privilege to review the audit log.

FAU_SAR.2: Log audit has a separate permission type. TOE restricts only users with log audit authority to perform audit operations.

7.2 Identification and Authentication

FIA_AFL.1: The TOE fulfils this requirement by preventing login of user who has reached a defined threshold of unsuccessful authentication attempt. The TOE allows 5 failed authentication attempts for per user. When this number is reached, the IP address of the connecting user is blocked for a period of 5 minutes before being able to attempt any further login. If the TOE is powered off and back on, the blocking of the IP address is reverted; however, for an attacker to exploit this scenario he would need to have physical access to the TOE, which is assumed not possible.

FIA_SOS.1: The TOE meets this requirement by verifying the strength of the password. The password strength calculation method is as follows:

a) Passwords have a minimum length of 8 characters;
b) Passwords have a maximum length of 32 characters;
c) Passwords strength rating, required above the Medium
   - Score >=70, strong;
   - Score<70 and >=50, medium;
   - Score<50, weak.
d) The scoring rules are as follows：
   - Letters: 0 score-no letters; 10 scores --all uppercase (lower) characters; 20 scores -case mixed string;
   - Numbers: 0 score -no number; 10 scores -1 number; 20 scores - more than 1 number;
   - Symbols: 0 score -no symbol; 10 scores -1 symbol; 25 scores - more than 1 symbol;
   - Rewards: 2 scores -letter and number mix; 3 scores -letter, number and symbol mix; 5 scores -uppercase and lowercase letters, numbers and symbols mix.

FIA_UAU.1: Users must login into the camera before being able to perform any operation.

FIA_UID.1: Users must login into the camera before being able to perform any operation.

7.3 Security Management

The admin user creates all initial users uniformly. When creating users, the admin user can bind roles to the users and assign rights to the roles.

FMT_MOF.1: The Administrator have the ability to perform the management functions supported by the TOE (as defined in FMT_SMF.1).

FMT_SMF.1: The TOE supports the configuration of the following functions:

- Creation, modification and deletion of Users. There is only one admin user, which is created when the user initializes the TOE.
- Access permissions of existing Users
- Trusted path/channel certificate management
- Configuration of unsuccessful authentication attempts
- Configuration of the limitation on multiple concurrent sessions
- Operation of firmware update.

FMT_SMR.1: The TOE supports the user types Administrator–and User. TOE is divided into admin group and user group.

7.4 Protection of the TSF

FPT_STM.1: The TOE time setting can be configured by authorized users to provide a reliable time stamp.

FPT_TFU.1: The TOE provides the ability for authorized users to upgrade the firmware, and only trusted firmware can be upgraded.

FPT_INI.1: The TOE fulfils this requirement by verifying software's integrity and authenticity before running the software

FPT_FLS.1: The TOE fulfils this requirement by judging whether the firmware version meets the upgrade requirements. While performing a Firmware Update operation, the TOE shall compare the version of the already installed firmware and compare it with the new firmware, and reject the firmware update if its version is older than the existing version.

7.5 TOE Access

FTA_MCS.1: The TOE fulfils this requirement by restricting the maximum number of concurrent sessions of the all users. And the maximum number of defaults is 10, supported configurable.

FTA_SSL.3: After reaching the idle time limit, the session will be terminated. The user interface requires the user to re-authenticate the account login operation.

FTA_SSL.4: The TOE allows manual logout of users on all interfaces.

7.6 Trusted Path/Channels

FTP_TRP.1: The TOE fulfils this requirement by providing secure channels (via TLS) when a remote user communicates with the TOE. The TOE implements a TLS1.2 using OpenSSL v 1.0.2t.

7.7 Cryptographic Support

FCS_COP.1/AES: The TOE provides symmetric encryption and decryption capabilities using AES in CBC mode or AES in OFB Mode (256bits).

Function	Rationale
Configuration encrypted import and export	AES in CBC Mode (256bits)
Configuration encrypted Store	AES in CBC Mode (256bits)
Video encryption transmission	AES in OFB Mode (256bits)
Certificate private key encrypt Store	AES in CBC Mode (256bits)
Firmware encryption release	AES in CBC Mode (256bits)

FCS_CKM.1/AES: The TOE shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm.

Function	Rationale
Configuration encrypted import and export	the KDF algorithm (256bits)
Configuration encrypted Store	the KDF algorithm (256bits)
Video encryption transmission	a specified cryptographic key generation algorithm random number generation (256bits)
Certificate private key encrypt Store	the KDF algorithm (256bits)
Firmware encryption release	the KDF algorithm (256bits)

FCS_CKM.4/AES: The TOE shall destroy cryptographic keys by overwriting the flash with zero.

FCS_COP.1/Sign: TOE shall have RSA signature and verification capabilities.

Function	Rationale
HTTPS Certificate generation and import	Generation: RSA with SHA-256 (2048 bits) Perform verification during certificate import: RSA with SHA1, RSA with SHA-256, RSA with SHA-384, RSA with SHA-512 (1024 and 2048 bits)
Verification of Firmware upgrade authenticity	RSA with SHA1(1024 bits)
Verification of run time software authenticity	RSA with SHA-256 (2048 bits)

FCS_CKM.1/ Sign: The TOE shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm RSA2048. RSA is implemented in the following function: HTTPS Certificate generation.

FCS_CKM.4/Sign: The TOE shall destroy cryptographic keys by overwriting the flash with zero.

FCS_COP.1/Hash: The TOE provides a specified cryptographic algorithm SHA1, SHA-256, SHA-384, SHA-512, MD5 for digest.

Function	Rationale
HTTPS Certificate generation and import	Generation: SHA-256 Perform verification during certificate import: SHA1, SHA-256, SHA-384,SHA-512, MD5
Configuration encrypted import and export	SHA1
Verification of Firmware upgrade authenticity	SHA1
Verification of run time software authenticity	SHA-256

A Abbreviations and Glossary

CC	Common Criteria
EAL	Evaluation Assurance Level
IPC	IP Camera(Network Camera)
IT	Information Technology
KDF	Key Derivation Function
NetSDK	Network Software Development Kit
OSP	Organizational Security Policies
SOE	Security Objective for the Environment
SOT	Security Objective for the TOE
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TSS	TOE Summary Specification

B References

[CCP1]	Common Criteria for Information Technology Security Evaluation. Part 1: Introduction to General Model, Version 3.1, Revision 5, April 2017.
[CCP2]	Common Criteria for Information Technology Security Evaluation. Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
[CCP3]	Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance components, Version 3.1, Revision 5, April 2017.