AXPRO Wireless Intrusion Alarm System

White Paper

V1.0.0

Chapter 1 Introduction 2
1.1 Overview 2
1.2 Function 2
Chapter 1 Wireless Technology Superiority 3
1.1 Background 3
1.2 Wireless Technology Point 3
1.2.1 Relay Network 3
1.2.2 TDMA Technology 4
1.2.3 FHSS Technology 4
1.2.4 Image Transferring Technology 5
1.2.5 Down-Link Communication in Low Consumption 5
Chapter 2 Detection Technology 7
2.1 Technology point 1. 3D Optical Lens Technology 7
2.2 Technology 2. IFT Signal Processing Technology 8
2.3 Technoligy 3. Digital Temperature Compensation Technology 9
2.4 3.4 Technology 4 Broadband Soundwave Detection 9
Chapter 3 IVaaS 10
3.1 Introduction 10
3.1.1 System Composition 10
3.1.2 Basic Principle 11
3.1.3 Key Design Points 11
3.2 Core Technology of IVaaS 11
3.2.1 Alarm & Video Correlation 11
3.2.2 Data Stream Transmission 12
3.2.3 Small Bandwidth Transmission 12
3.2.4 Video Stream Cache 13
3.2.5 Platform Compatibility 14
Chapter 5 Summary 15

Chapter 1 Chapter 1 Introduction

1.1 Overview

AXPRO series is a wireless intrusion alarm product published by Hikvision. It is targeted at Residential and SMB markets. It mainly provides alarm security system solutions for house, villa, apartment, shop and small office scenes. This series mainly includes security control panel, front-end wireless detector, alarm system control device, alarm output response device and supporting software products.

In this alarm system, hardware devices realize information interaction between security control panel and peripheral products through 868/433 MHz wireless transmission. Hikvision wireless technology can ensure timeliness, stability and long distance transmission of product communication. Security control panel can access Hik-connect and Hik-ProConnect through LAN/WiFi/GPRS/4G network. It provides software solutions for terminal users, installers and ARC (Alarm Receiving Center) to configure and manage intruder alarm system.

1.2 Function

This wireless alarm system mainly includes the following functions:

- Alarm detection: Different detectors and IPC can detect intruder, cars, door open and close, vibration, glass broken, smoke, water leak, temperature, etc. It can cover indoor and outdoor scenes.
- Control system: As the main control center, security control panel can analyze and process various alarm events. And it can complete corresponding actions such as sounder alarm linkage, relay switch linkage, etc.
- System operation: The keyfob, keypad, tag reader and indoor station can control the whole alarm system, such as arming, disarming and alarm clearing.
- Alarm report: By analyzing and processing the site situation, security control panel can push the report to APP or platform management software on time and provide it for center managers to answer alarm. It can also prompt alarm by calling or sending messages to user phones through 4G or GPRS.

Chapter 2 Wireless Technology Superiority

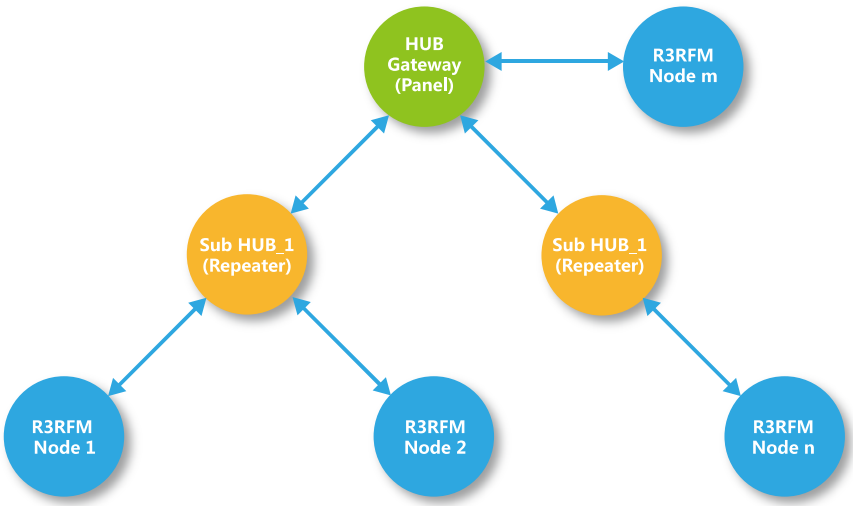
2.1 Background

With the rapid development of antenna and RF technology, the application of wireless technology has increased sharply and an increasing number of users prefer to choose wireless alarm system for the convenience of installation and maintenance, especially in the domestic aftermarket. As the wireless alarm system in Hikvision develops and iterates over generations, it shifts from one-way transmission to two-way communication, and then evolves into the third-generation wireless communication Tri-X and Cam-X with the cutting-edge functions of frequency hopping spread spectrum (FHSS), time division multiple access (TDMA), dynamic AES two-way encryption (black box encryption), high-speed picture transmission and video recombination and remote maintenance, which greatly improves stability, safety and reliability of the transmission system, aligns with industry benchmarking and guarantees the core competitiveness of products.

2.2 Wireless Technology Point

AES fully encrypted low-power private wireless protocol, which supports the tree network of first-level relay, has TDMA, 230 wireless node capacity, 40 channel pseudo-random sequence frequency hopping. It has strong data transmission ability, can resist external interference and realize bidirectional symmetrical interaction. The control panel can wake up and transmit data to low-power dormant detector peripherals in real time to meet the requirements of two-way real-time communication capability of low-power detector peripherals. It also supports wireless remote upgrade OTZ. The gateway HUB can initiate upgrading firmware for wireless node RFM, and support wireless transmission of image or video stream with large data volume. Wireless protocol meets relevant EN standards.

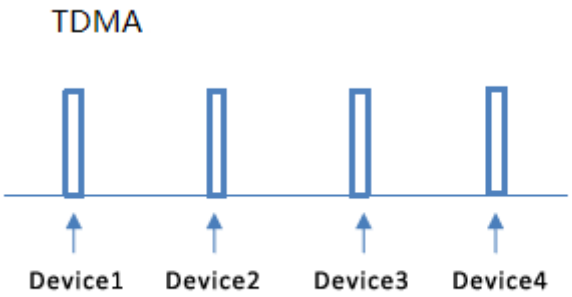
2.2.1Relay Network



The initial topology of wireless system is star type structure, which supports the formation of simple tree topology by connecting to the first-level relay and forwarding device, and improves the coverage of wireless network.

2.2.2 TDMA Technology

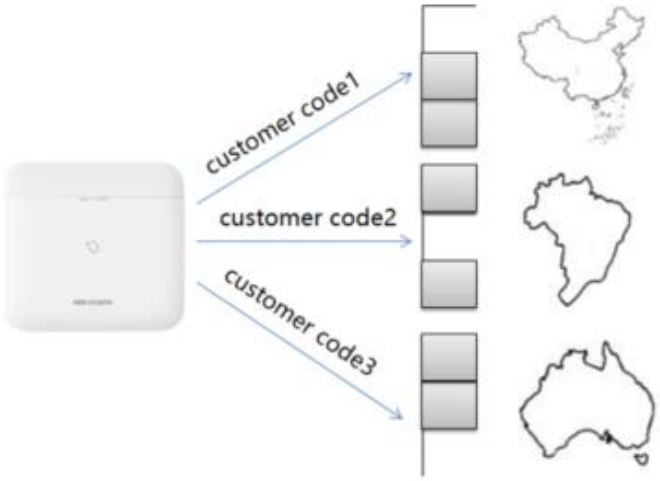
Wireless system has strict requirements on the working time and wake-up time of peripherals. The wake-up time of different devices is determined according to the node number at the time of registration. The internal timer of the device is always in working state. After each interaction with the control panel, the control panel will synchronize the next time interval allowed to report to the peripheral. The peripheral will alarm only in the time node allowed to report. This mechanism can ensure the time synchronization of all devices to report information only in their own working time nodes, which can minimize the internal interference of the system.



2.2.3 FHSS Technology

The wireless alarm system operating on the 433/868 MHz frequency band for wireless communication runs the risk of encountering interference in environments, where devices from various departments and wireless personal communication devices are in use. These devices operate on the same unlicensed 433/868 MHz frequency band, which is available for free in the client area. Integrated with frequency hopping technique, Hikvision wireless system is much less prone to interferences from the external system signals.

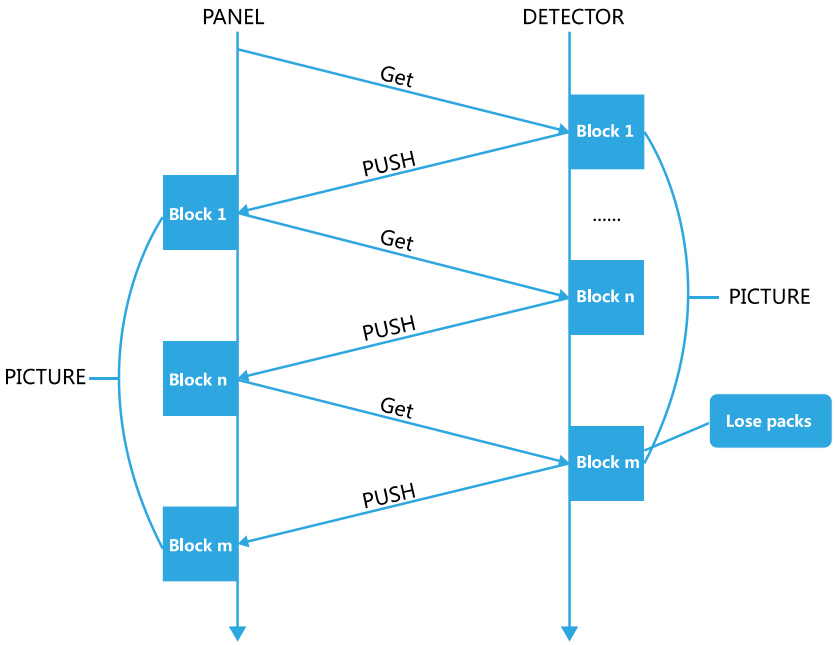
The Hikvision wireless protocol supports up to 50 wireless frequency hopping channels. With built-in customer codes, Hikvision wireless system presets different channel numbers according to customer codes and can hop across these channels in a random fashion in compliance with local laws and regulations. For example, in the European Union, the wireless system operates on the frequency band ranging from 868.0 MHz to 868.7 MHz. Select 7 channels from 0 to 6 for frequency hopping receiving. The system randomly distributes 7 channel numbers in 50 frequency hopping channel slots. When the system is working, according to time division multiple access and time synchronization, devices can calculate the operating channel of other devices and change channels to communicate with them.



Subject to calculation and hardware errors, the calculated time may deviate. To reduce errors, the host hardware system features high-precision active crystal. With the software design, the host computer will also quickly scan the previous channel and standby channel while receiving the signal in the current channel to ensure that the host terminal receive the signal even when the signal in the transmitting end is interfered.

LBT mechanism (listen before transmit) enables the device to monitor the interference of the current channel before sending a signal. If the interference exceeds the threshold, the system will re-select the transmission channel to maximize alarm information upload.

2.2.4 Image Transferring Technology



The device applies sub package and chunked transferring of image data, and re-transferring of packet loss to ensure a stable and reliable image data transferring.

2.2.5 Down-Link Communication in Low Consumption

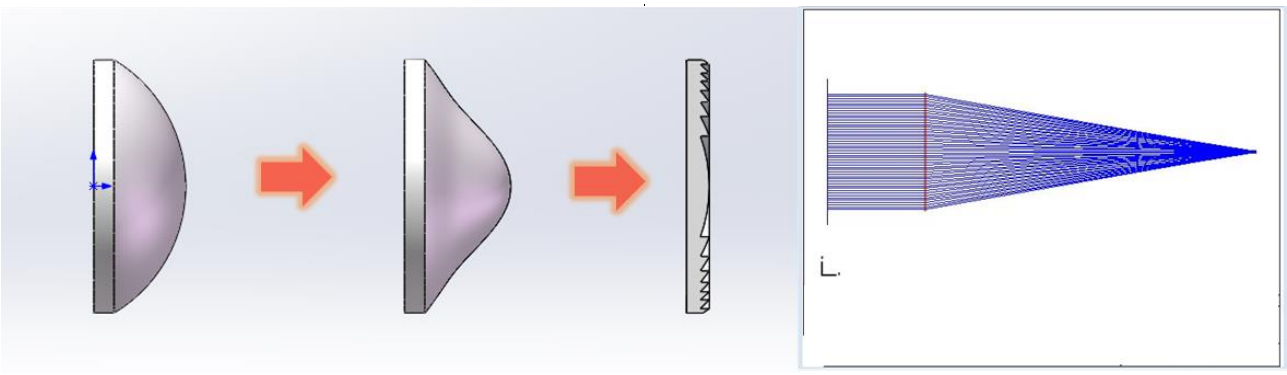
Most of the time, the low consumption wireless node is in the sleep mode (super low consumption). In order to satisfy the real-time down-link data transmission from the wireless gateway HUB to wireless node RFM module, based on all wireless nodes and gateways are at the same time, you can wake up the wireless peripherals in the broadcast window in schedule, detect the wireless data that might be applied, receive controlling and configuration information that applied by gateway in real time.

Chapter 3 Detection Technology

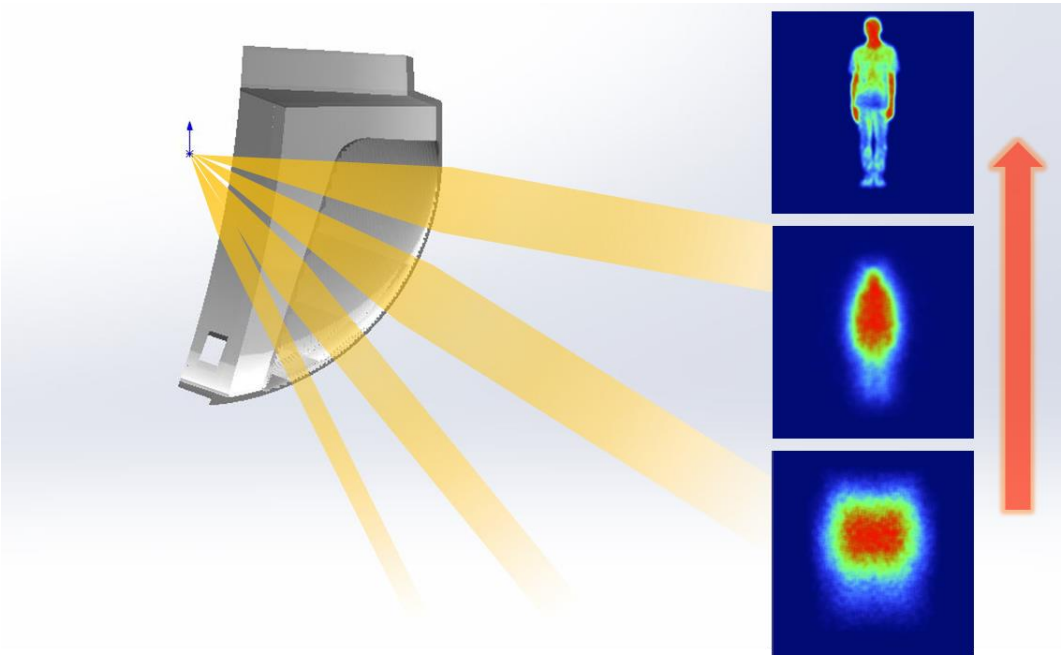
3.1 Technology point 1. 3D Optical Lens Technology

3D optical lens technology optimizes lens performance globally, including line design, lens array, sector distribution and material optimization.

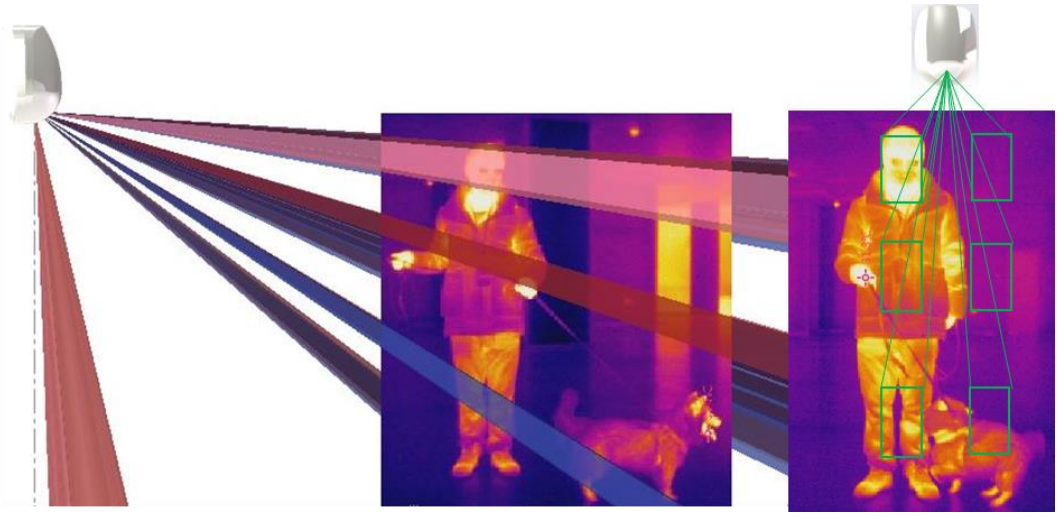
Adopting technologically advanced aspheric Fresnel lens design to suppress aberrations, so that the lens still has excellent focusing performance when the lens is large F#, and can pick up external energy to the greatest extent.



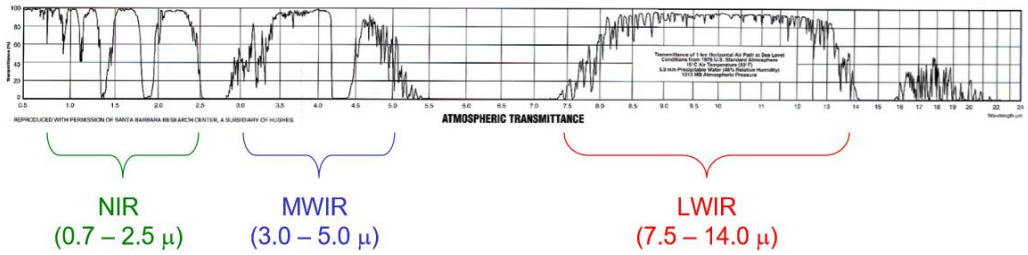
The design of the all-focus arc surface array lens group enables the lens in all directions to have the same excellent focusing performance, which ensures the energy balance of the detector within its protecting angle, which is better than the focus performance of ordinary cylindrical lenses.



The use of optical aliasing integral design optical lens group ensures that the product has a relatively excellent pet immune performance from the optical design level.



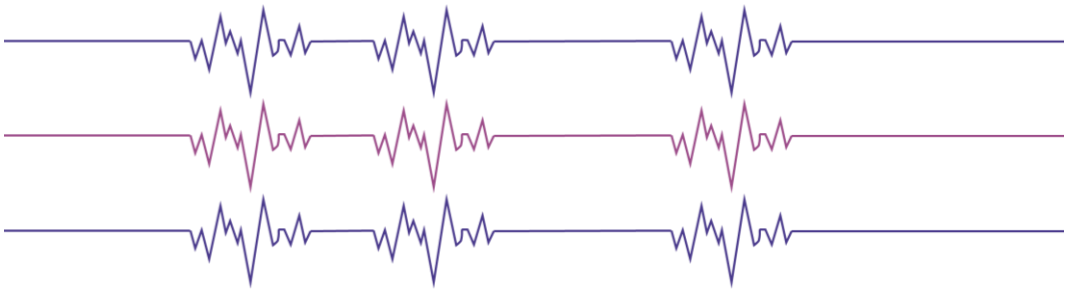
Using a customized high-performance HDPE formula, it achieves high transmittance in the human body radiation band, suppression of visible light band, band pass of near-infrared band, and excellent anti-aging effect from the material.



3.2 **Technology 2. IFT Signal Processing Technology**

IFT (Independent Floating Thresholds) signal processing technology enables the detector to automatically adjust trigger thresholds according to background noise, ensuring stable properties.

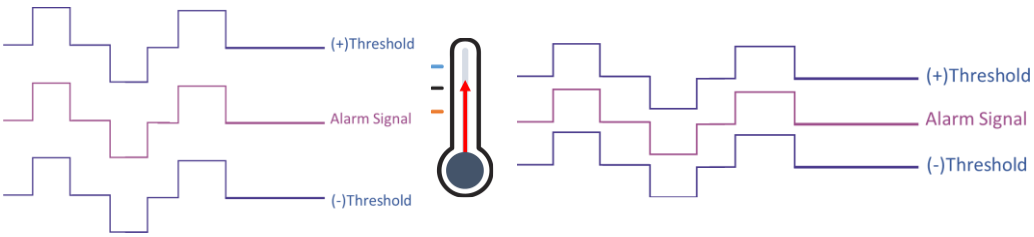
The detector can actively get and judge the current amplitude of background signal on a regular basis, and automatically superimpose it on the +/- trigger thresholds conditions, which is similar with active noise reduction and thus weakens many contingency electromagnetic interferences in the real life and fixes the problem of signal attenuation because of long term use.



3.3 **Technoligy 3. Digital Temperature Compensation Technology**

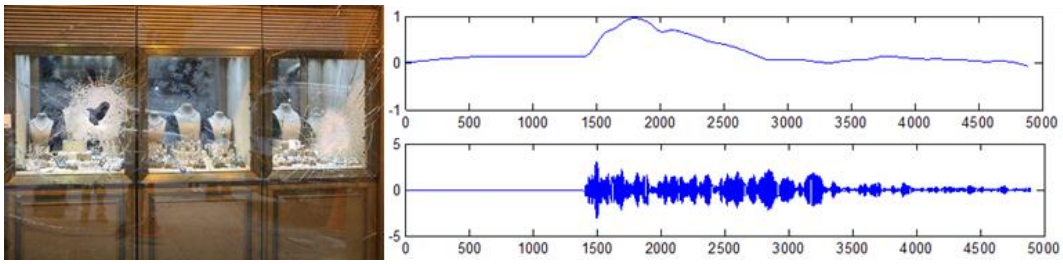
Environmental temperature has great influence on the detector due to the heat sensitive of pyroelectric sensor. The detector can read the real-time temperature of installation environment by digital temperature compensation technology, and based on that, automatically adjust the trigger thresholds to ensure good weather resistant and detection.

When the room temperature rises, while the body can keep temperature constant, therefore, the temperature difference value between the detected unit and the background dramatically decreases, which leads to a reduction in the perceived energy of sensor. Then the detector will automatically close the difference of trigger thresholds to improve the sensitivity at high temperature and ensure detection consistency, and vice versa.



3.4 **Technology 4 Broadband Soundwave Detection**

For a glass break detector, error report or failing to report is difficult to balance. In order to avoid the impact of various sounds in real life on the detector, we have developed and adopted a customized broadband receiver to receive the sound of glass breaking in the full frequency range without loss. By sampling and analysis of the sound, we extract two inevitable characteristic audios: one is close to infrasound and the other is close to ultrasound. We use the smart algorithm to analyze these two frequencies and accurately determine whether they are triggered truly, and filter out most of the accidental noises on the false trigger of the detector and ensure the accuracy and reliability of detection.



Chapter 4 IVaaS Technology

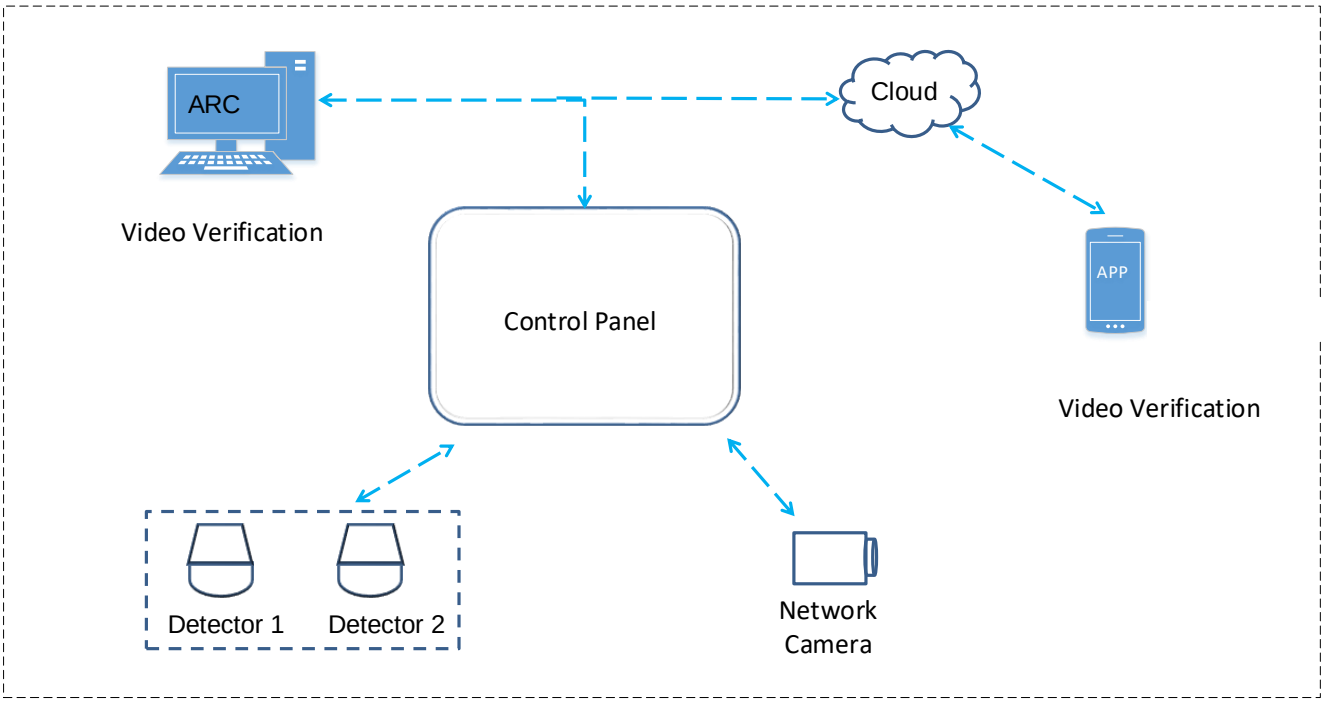
4.1 Introduction

IVaaS (Intruder Verification as a Service) is a key technology of a fully integrated intruder alarm solutions that fuse video surveillance and alarm systems. This technology has been widely used in the security systems of sectors that have huge impacts on people's everyday life, including the financial sector, the cultural, educational, and healthcare systems, power plants and water conservancy projects; public security monitoring in shopping malls, factories, warehouses, office buildings and other public places as well as personal security protection in apartments and villas.

IVaaS enables video verification of events by providing video clips of the scenes as forensic evidence in the event of an activation. Supervisors can receive alarm information via multiple platforms, remotely view the pre-alarm and post-alarm video clips to apprehend a suspected intruder and prioritize timely responses. Compared with the traditional on-site verification, IVaaS not only greatly reduces the probability of missed and false alarm, facilitates timely confirmation in the event of an alarm, recovers losses caused by on-site verification, but also guarantees that users can enjoy undisturbed security control service.

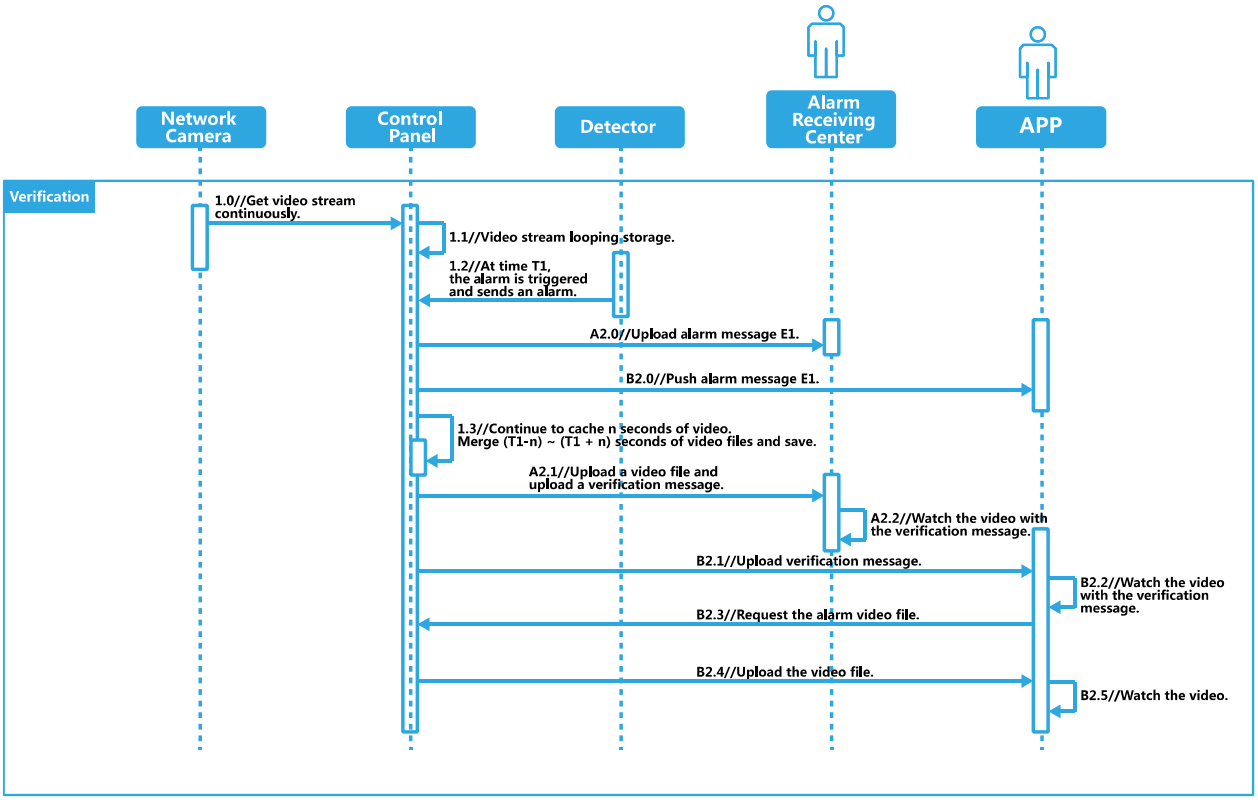
4.1.1 System Composition

The IVaaS system consists of detectors, control panels, network cameras, alarm receivers, and cloud service.



4.1.2 Basic Principle

While the alarm is triggered at a certain time (T), a signal will be sent to the control panel. The control panel records the alarm that will be then uploaded to the alarm receiver center and mobile client through the network. At the same time, the control panel intercepts the video of n seconds before and n seconds after T, and pushes the video to the alarm receiver center and mobile client where the supervisors can watch the uploaded alarm videos.



4.1.3 Key Design Points

- The system supports linking the zone with network cameras. The accessibility of the network camera is based on the device performance.
- The control panel continuously acquires data stream from the network cameras and adopts looping storage for each camera. The system preserves cache space according to the video size.
- The system will generate a video clip recording the event course and correlate the video with alarm information including zone No., time, etc.

4.2 **Core Technology of IVaaS**

4.2.1 Alarm & Video Correlation

The principle of correlating alarm messages and video files is as follows:

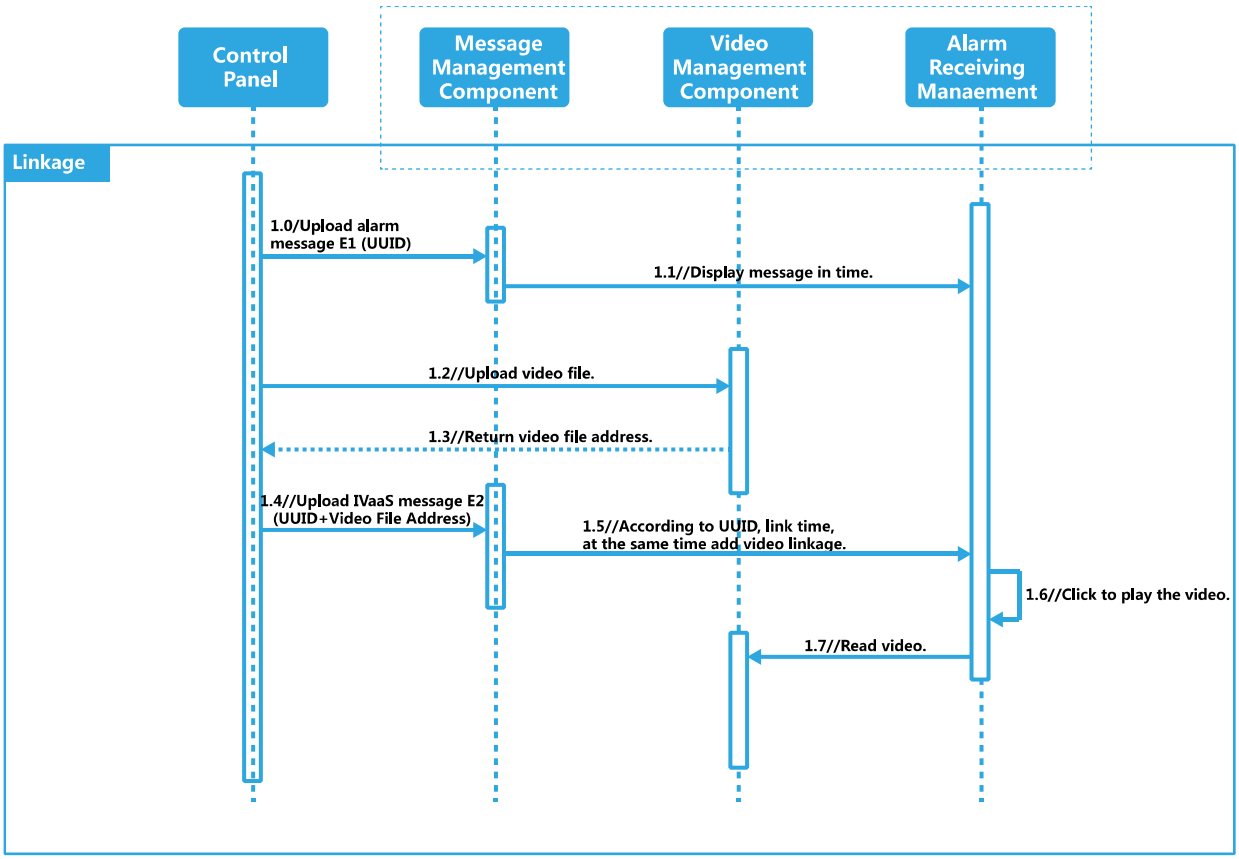
1. When an alarm is triggered, the control panel uploads an alarm message (with a unique identifier UUID) to the message server for instant notification.

2. When the video file is generated, the control panel uploads the video file to the video server.

3. The video server saves the file and returns the file address to the control panel.

4. The control panel uploads the UUID and video file address to the message server.

5. The message server correlates the UUID and file address, and generates a link for the video clip.



4.2.2 Data Stream Transmission

The digital video stream from the network camera is high compressing encoded by the H.264/H.265 standard, packed and sent through the RTP (Real-time Transport Protocol), and re-encapsulted to the PS (Program Stream) stream which can only be identified and decoded by Hik-Connect.

To satisfy the needs of watching video clips on multiple platforms, the packets will be re-encapsulted to MPEG-4 streams and be encoded to generate a video files.

The video can be played directly on multiple platforms with players, such as media player, through the mailbox, FTP, EHome or the third-party platform protocol.

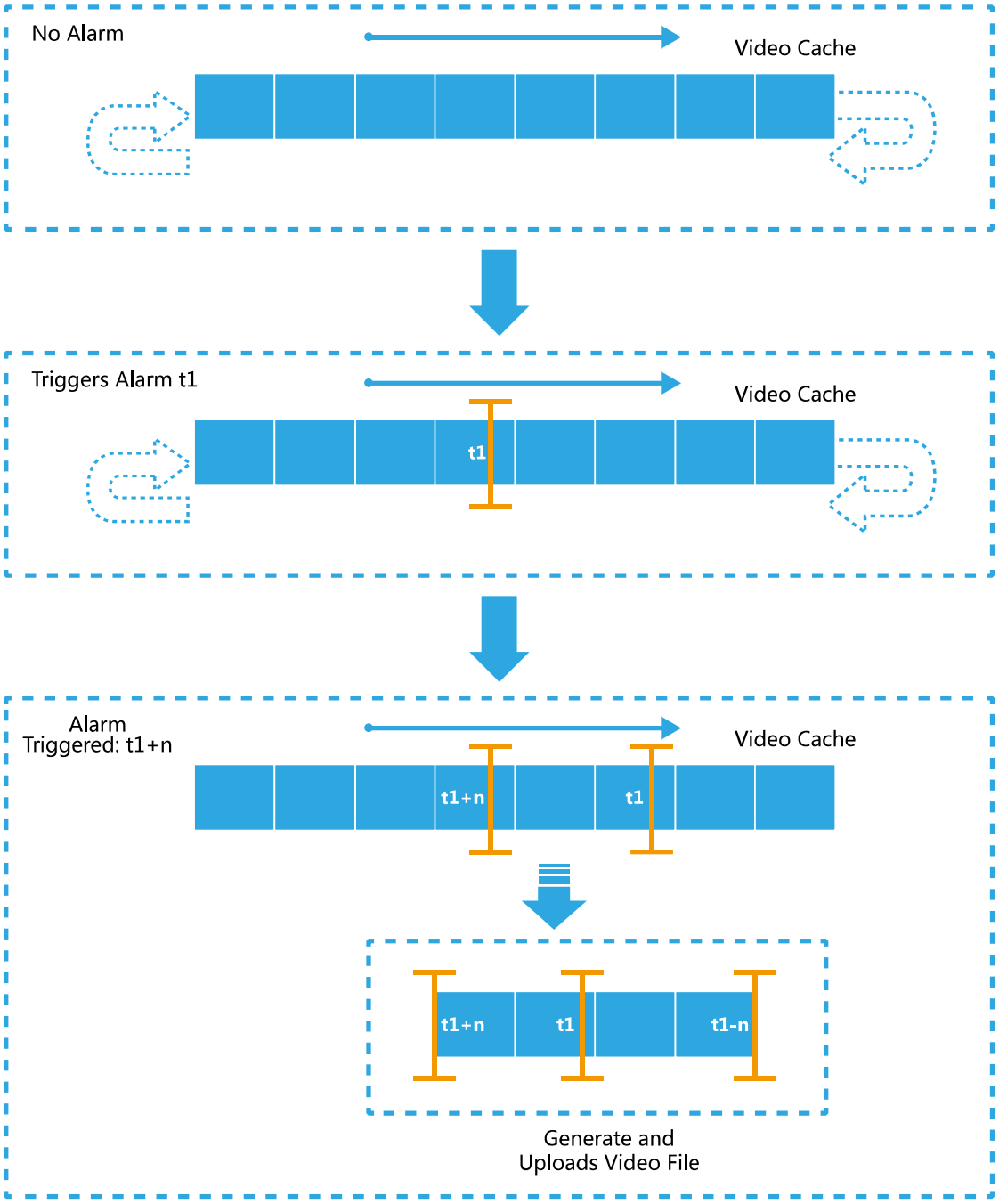
4.2.3 Small Bandwidth Transmission

For small size alarm message, the current 2G network is also the mainstream choice. However, data transmission through low-speed networks has a high probability of transmission exception or timeout. Especially for big chunk of information, the retransmission takes a long time. To ensure smooth transmission, big data is clipped into small segments to perform partial retransmission, which helps reduce the transmission time.

Considering the user experience, the size of the video clip has been restricted. The essence of the verification is whether an event is actually occurred at the time of the alarm or not. So the duration of the video clip is designed to be 7s (the video durations before and after the alarm are configurable) to ensure that the records of the event course is integrated. The use of sub-stream video reduces the file size and data flow costs, improves the video transmission efficiency, and ensures the video quality.

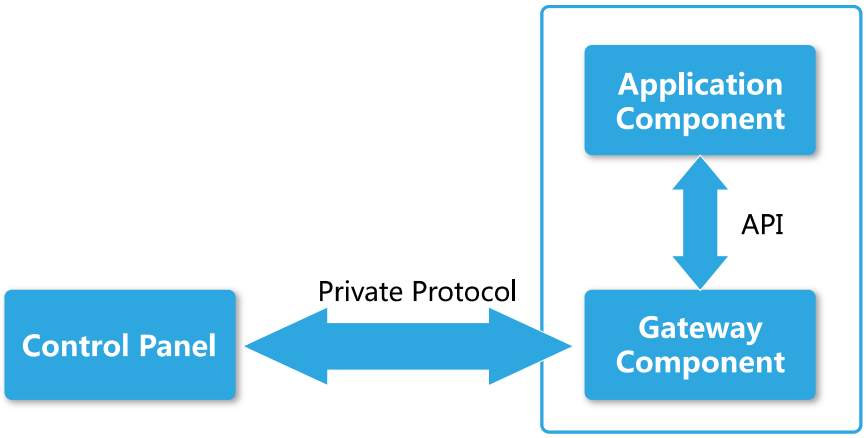
4.2.4 Video Stream Cache

The control panel continuously acquires the stream from network cameras and adopts looping storage for each camera. The system preserves cache space according to the video size. While an alarm is triggered, the stream of video recording the event course (7s, the video durations before and after the alarm are configurable) is clipped and transferred to multiple platforms, which allows users to watch the alarm video via mobile client, email, FTP, etc.



4.2.5 Platform Compatibility

With the continuous iteration of products and functions, the compatibility between platform and product becomes particularly critical. The gateway component scheme, which makes the upgrade of gateway component synchronously with the device, adopts private protocol to improve the safety of data transmission. Components and platform services develop a standard API (Application Program Interface) that is compatible with multiple platforms.



Chapter 5 Summary

AXPRO series products, greatly improve the stability and usability of the products through Hikvision cutting-edge software and hardware technologies and algorithms. It integrates video and non-video products, and complete an innovation in the traditional alarm industry. With the continuous enrichment of Hikvision alarm solutions, it brings more convenience to the installers and end users, and meets more practical use scenarios and services.


See Far, Go Further