# IoT Security Control System

## Overview

With the backdrop of rapid development of Internet of Things (IoT) and IP-based infrastructure communication system, it is an inevitable trend that a huge number of devices become interconnected through the Internet. Evidenced by the large number of front-end devices, including IP cameras, capturing devices and RFID units, that are widely used in every corner of the city serving the public security, transportation, power and other industries, it is without doubt that the world has gradually entered the era of IoT. IoT is characterized by a huge number of front-end devices and a wider range of physical deployments compared with the traditional Internet, and includes a lot of interconnected devices in addition to human-machine interconnection. How to ensure a fully controllable and available IoT at all times has become a brand new challenge to the Industry. Given the large number of front-end IoT devices deployed in unattended environment, it is a difficult task to perform in-person supervision. This vulnerability is easy to be exploited by hackers, who may penetrate into the entire network, resulting in failure of core business systems and a great amount of confidential information being stolen. Therefore, building a perfect management and control mechanism for access assets and devices and applications is of paramount significance for the construction of a secure IoT system.

Focused on the R&D of IoT terminal access control, L2 to L7 whitelist, and other key techniques, DPtech has developed a set of IoT security control system, or Device Application Controller (DAC). The system is capable of performing accurate management of front-end IP devices and transmitted traffic over the IoT. Only authenticated devices are allowed to access, and only traffic from legitimate applications is allowed to be transmitted over the Internet. In this way, illegal private connection, counterfeiting devices, unauthorized scanning and DDoS attacks can be effectively prevented.

Designed specifically for the IoT scenarios, DACs can be widely applied in "building a safe city" projects, Intelligent Transportation, power, energy, medical, production automation and other industries. In particular, DACs address the problem of access authentication and security management of a massive volume of IP cameras and other front-end IP devices in the video surveillance application scenario, making IoT secure and fully controllable for users.

## Product Features

- **Unified Management of Heterogeneous Assets**

  Compatible with monitoring systems from mainstream manufacturers, DACs capture asset information of access devices in the video networks by active scanning, passive monitoring and

manual settings. Access devices include cameras, PC and NVR. Information captured involves device IP, type of device, online status, access link status, vendors, geo-location, etc. Through classified statistics, a unified asset database can be established to provide a sound solution to the difficulty in unified supervision in the context of multiple security product manufacturers.

- **Trusted Identity and Controllable Behaviors**

  By implementing access control on connecting devices through MAC addresses, IP addresses, device fingerprints and other authentication methods, DACs grant access to authenticated devices only to prevent illegal access from front-end devices.

  Moreover, based on the detection of protocol feature, DACs apply application-level control on transmitted data, grant access permissions only to legal application data, and block all illegal data, they can effectively eliminate any illegal scanning and DDoS attacks. Combined with device authentication, accurate control on access devices and transmitted traffic on the entire network is made possible, enabling a dedicated private network.

- **Real-time Blocking of Illegal Access**

  DACs perform real-time and comprehensive detection of source IP, destination IP and application layer protocol. Illegal traffic can thus be cut off in real time upon discovery. By pinpointing the IP address, MAC address, access port, geo-location, intrusion behaviors and other information concerning the intrusion, DACs enable users to provide quick response to security incidents.

- **Convenient IP Resource Management**

  The usage of IP resources can be given in a graphical manner on DACs, including IP addresses used and unused as well as the type of terminals at each IP address. This will help administrators work out an overall plan for the usage of IP resources in video networks, assign IP resources quickly, and realize recycling registration management.

- **Visualized Security and Predictable Risks**

  DPtech provides a visual monitoring platform for access assets and security situation in video networks. Through monitoring statistics of online terminals, online utilization rate, distribution of camera vendors, and the number of assets, it help administrators gain an overall grasp of operations performed in the video networks. Meanwhile, the platform will trigger real-time alerts to assist administrators in handling newly connected devices, disconnected devices, and illegal terminal access in the video networks.

- **Seamless Integration with Business Systems**

  DACs can be deployed online or side-by-side, allowing seamless integration with user's network. Online deployment is preferred for new networks, in which access devices and transmitted data can be monitored and controlled in real-time. As for existing networks, side-by-side deployment is recommended to enable control and monitoring through traffic control and mirroring.

  Built on the industry-leading APP-X high-performance hardware platform, DACs feature a processing delay of less than 20us, outperforming the industry standard of 50ms. Upon deployment, zero impact will be made on live services in existing networks.

In conjunction with devices from mainstream security product manufacturers, DACs can achieve deep coupling between network and services.

## Function Descriptions

### Hardware Parameters of Board DACs

| Product Model | DAC-Blade-S | DAC-Blade-XS | DAC-Blade-AI | DAC-Blade-XA |
|---|---|---|---|---|
| Processing Capabilities for Video Surveillance Scenarios | IP cameras of 800-channel 4M bit-stream, scalable to a maximum of 8,000 channels as a whole unit | IP cameras of 800-channel 4M bit-stream, scalable to a maximum of 8,000 channels as a whole unit | IP cameras of 1600-channel 4M bit-stream, scalable to a maximum of 16000 channels as a whole unit | IP cameras of 1600-channel 4M bit-stream, scalable to a maximum of 16000 channels as a whole unit |
| Scalability | Support cloud-based board technology to achieve aggregated performance of multiple service boards | | | |
| Maximum Slots of Hosts | 10 slots | | | |
| Maximum Ports | Scalable to 480 Gigabit interfaces, 320 10-Gigabit interfaces, 40 40G optical interfaces | | | |
| Hardware Redundancy | Dual-master redundancy; Key hardware redundancy of power supplies and fans | | | |
| Operating Temperature | 0~45℃ | | | |

### Hardware Parameters of Cassette DACs

| Product Model | DAC-A | DAC-S |
|---|---|---|
| Processing Capabilities for Video Surveillance Scenarios | IP cameras of 600-channel 4M bit-stream | IP cameras of 250-channel 4M bit-stream |

| | | |
|---|---|---|
| fixed interfaces | 8 Gigabit optical interfaces + 8 Gigabit electrical interfaces + 40 Gigabit optical interfaces | 16 Gigabit optical interfaces + 8 Gigabit combo interfaces |
| Expansion Slots | 2 expansion slots, scalable to 10-Gigabit optical interface, Gigabit optical interface, Gigabit electrical interface | 2 expansion slots, scalable to 10-Gigabit optical interface |
| Hardware Redundancy | Key hardware redundancy of power supplies and fans | |
| Operating Temperature | 0~45℃ | |

## Software Features for Video Surveillance Scenarios

| Product Model | DAC-S | DAC-A | DAC-Blade-S | DAC-Blade-XS | DAC-Blade-AI | DAC-Blade-XA |
|---|---|---|---|---|---|---|
| Security Access of Devices | Support access mechanisms based on MAC address, IP address, and device fingerprints | | | | | |
| Data Application Control | Support the whitelisting mechanism for application control based on protocol features, allowing only authorized services to be transmitted in the network; can detect control signaling and transmission protocols including SIP, RTSP, RTP/RTCP, HTTP, FTP and NTP; Support content-based deep service detection | | | | | |
| Asset Detection and Management | Capture asset information in the video networks by active scanning, passive monitoring and manual settings, and establish a unified asset database; Conduct regular scanning of devices in the video networks, and compare scanning results with asset database in order to discover abnormal devices and trigger alarms in time. | | | | | |
| Visualized Security Situation and Status Monitoring | Enable alarm logs and real-time display of behaviors such as newly connected devices, disconnected devices, and illegal terminal access in the video networks. Information captured involves device IP, type of device, geo-location, time, type of logs, etc. Provide statistics of online terminals, including the number of online terminals such as cameras, PCs and NVRs;Provide statistics of online utilization rate and online profile, including the number of online and offline units and the online utilization rate; Display the exact number of cameras from each vendor; Support regional terminal statistics at the provincial/city level and the city/district/county level or the district/county/township level, providing information on terminal quantity at all levels; | | | | | |

| | |
|---|---|
| Outreach Breach Detection | Enable terminal with illegal internet access in real time and perform cutoff as needed. |
| Compatibility | Compliance with requirements set forth in national standards, including GB 35114-2017 and GB/T28181-2016; Identify the business of mainstream security product manufacturers; A signature library upgrade is provided, which can be updated to enable detection of unconventional services |
| Three-layer Features | IPv4: Static routing, RIP v1/2, OSPF, BGP, policy-go-together, etc. IPv6: IPv6 static routing, RIPng, OSPFv3, BGP4+, transition tunnel technology from IPv4 to IPv6, etc. |
| Deployment Modes | Support Online and Bypass Deployments |
| NAT Function | Support NAT modes such as one-to-one and address pool |
| Management and Maintenance | Support RMON real-time temperature detection and alarm Support SNMP, CLI, system adminnistration, and Unified Management Center (UMC) Support local and remote output of system logs, operation logs, commissioning and debugging information, etc. |

## Product Series

**LSW1000-8T-IW**

**LSW1000-8T2GP-IW**

**LSW1000-8GT2GP-IW**

Hangzhou DPtech Technologies Co., Ltd.
Address: 6th Floor, Zhongcai Building, No. 68 Tonghe Road, Binjiang District, Hangzhou City, Zhejiang Province
Postcode: 310051
Official Website: www.dptech.com
Service Hotline: 400-6100-598