WHITE PAPER

How Industrial PoE Switches Facilitate Reliable Outdoor IP Surveillance Networks

Jackey Hsueh
Product Manager

MOXA®

Abstract

Outdoor IP surveillance networks can reap substantial benefits from PoE technologies. Although PoE solutions save considerable deployment costs and effort by transmitting data and power over the same cable, system integrators need to consider power consumption, network bandwidth, fault recovery, and cybersecurity requirements in order to ensure high reliability and availability for outdoor IP surveillance networks.

Introduction

Along with the overall trend towards smart city development, demand for IP surveillance applications has also grown rapidly over the past few years because governments and property owners need to monitor the real-time status of critical infrastructure to enhance operational efficiency and protect critical assets. To construct flexible and cost-effective IP surveillance systems, security managers and system integrators (SIs) often take advantage of Power over Ethernet (PoE) technology. PoE utilizes a single cable to transmit data and supply power, which not only increases flexibility for IP camera installation in remote locations, but also reduces wiring costs and installation time during deployment. Undoubtedly, PoE switches have become popular and their adoption is increasing for IP surveillance applications.

Especially for outdoor IP surveillance systems, PoE is widely used to reduce installation costs and effort. It also ensures high reliability by providing an isolated power source that is centralized, making it easy to set up a backup power supply for the system and all connected devices. Mission-critical applications that use outdoor IP surveillance include highway traffic control and monitoring, oil field and pipeline monitoring, power generation and distribution monitoring, water and wastewater station monitoring, and more. In these applications, asset owners care most about the reliability and availability of their surveillance systems, and require constant video streaming because IP surveillance is needed to guard human safety and protect critical facilities, in addition to enhancing operational efficiency. Furthermore, in order for security managers to clearly monitor site conditions and take the actions needed to respond to emerging events, HD PTZ cameras—which require higher power consumption and higher bandwidth communication—are often deployed to cover wide range monitoring and provide uninterrupted high-resolution video. However, the challenge lies in ensuring that PoE switches can provide high power output and sufficient network bandwidth while remaining highly available and reliable, even when operating in conditions with extreme temperatures, harsh environments, high environmental noise, and potential cybersecurity risks.

Released on March 9, 2018

Moxa is a leading provider of edge connectivity, industrial networking, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things. With over 30 years of industry experience, Moxa has connected more than 50 million devices worldwide and has a distribution and service network that reaches customers in more than 70 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for industrial communications infrastructures. Information about Moxa's solutions is available at www.moxa.com.

How to contact Moxa
Tel: 1-714-528-6777
Fax: 1-714-528-6778

MOXA®
Reliable Networks ▲ Sincere Service

To overcome these challenges, there are four considerations that system integrators should consider when integrating industrial PoE solutions into their outdoor IP surveillance systems. First, outdoor PTZ cameras consume more power than regular IP cameras. Consequently, high power consumption and sufficient PoE budgets need to be considered during the design phase. Second, the PoE network must reserve sufficient bandwidth to ensure the smooth transmission of high-resolution video. Third, to construct a highly reliable and available video system, it is important to implement failure recovery mechanisms for both network infrastructure and IP cameras. Lastly, to protect against cyberattacks or ill intent that may jeopardize human safety or critical facilities, cybersecurity should be implemented on network systems and devices. This white paper discusses these considerations in greater detail to help system integrators effectively utilize industrial PoE solutions to create highly reliable outdoor IP surveillance networks.

1) Providing High-Power PoE to Modern Surveillance Devices

During normal operations, a surveillance camera often requires around 10 to 20 W to perform basic surveillance functions. If cameras that operate around the clock need to use IR illuminators during periods of low light, this may increase the amount of power the camera requires to 30 W. Nowadays, there are a number of industrial PoE switches available that provide up to 30 W to connected devices, and do not require an additional power supply. However, as surveillance cameras support a growing number of functions to fulfill customer requirements while performing in harsh environments, industrial PoE switches that can only provide up to 30 W per port often no longer suffice. One type of deployment that often experiences problems is using PTZ surveillance cameras to patrol a large outdoor area during periods of low light. Turning on additional functions such as a heater or blower in harsh weather conditions can require more power than usual. For project deployments that include multiple HD PTZ cameras surveilling large areas with a lot of activity taking place, it is important to have a PoE injector or switch that is capable of supplying 60 W, as well as a power budget and power supply that can sufficiently support any other connected devices.

To deal with this need for power, system integrators usually purchase HD PTZ cameras that include a 60 W PoE injector. However, there are limitations to these injectors as outdoor IP surveillance applications often have many technical requirements that need to be met, such as a wide operating temperature range and electromagnetic compatibility (EMC). Bundled PoE injectors often do not meet these requirements, forcing the system integrator to find an alternative solution. A better option is to use industrial managed PoE switches, as they are built to perform in harsh environments and can connect directly to the cameras, eliminating the need for individual injectors for each camera. However, another problem presents itself; because the 802.3bt high-power PoE standard has yet to be ratified, cameras may use different proprietary 4-pair wiring designs in order to support 60 W PoE. Thus, it is important to select an industrial PoE switch that can be programmed to support the different types of proprietary 4-pair 60 W designs so that connected outdoor PTZ cameras can be connected and powered without hassle.

2) Creating a Network with Sufficient Network Bandwidth

When designing a network topology that will support multiple surveillance cameras in industrial applications, it is very important to reserve sufficient uplink bandwidth to ensure the transmission of high quality image packets under any condition without interruption.

The following example illustrates how to ensure that sufficient bandwidth has been deployed for an industrial network. For modern industrial surveillance networks, a high-resolution camera may require between 10 and 20 Mbps to support 1080P at 30 FPS using H.264 video compression. If an industrial Ethernet switch is deployed to connect 25 cameras, 500 Mbps of bandwidth should be available to provide 20 Mbps to each camera so that they can reliably perform their functions. For a deployment such as this, it is advised to reserve around 50 percent of this bandwidth because there are certain periods when extra bandwidth will be required. For example, when PTZ cameras are surveilling large areas or if there is a lot of activity taking place in front of multiple cameras at the same time, there will often be a surge in the amount of bandwidth required and the cameras must have sufficient bandwidth available in order to continue to supply high-quality video without any stuttering or video loss.

3) Providing Built-In Failure Recovery for a Surveillance Network

For outdoor IP surveillance applications, it is becoming increasingly popular for industrial PoE switches to support automatic failure recovery mechanisms that do not require a human technician to intervene should a network issue occur. The three main benefits of including built-in failure recovery are maximized system availability, convenience, and lower total cost of ownership, all of which will now be explored in more detail.

A situation that often happens on networks that host large numbers of IP cameras is that the cameras may freeze, stutter, or experience lag, which can result in image quality being reduced to the point of being unusable. For nearly all electronic devices that experience problems, the first stage in the troubleshooting process is to reboot the device. IP cameras are bandwidth-hungry devices that continuously process a lot of data, which often results in the cameras using up all of their temporary memory. If an industrial PoE switch that is deployed on the network supports device failure checking, and the camera does not respond to the switch for a defined period of time, the industrial PoE switch can stop supplying power to the camera, causing the camera to turn off. The switch can then start supplying power again so that the camera will reboot itself, clearing all of the temporary data that is causing the camera to freeze or experience lag. Most of the time, this simple action can allow the camera to function normally again as it now has enough storage available to perform its functions smoothly. As this type of problem frequently occurs on industrial networks, utilizing device failure checking to reboot a device, as opposed to dispatching an engineer to the site, can result in significant savings for maintenance and troubleshooting while also maximizing IP camera availability.

Network redundancy is also an important feature as this will almost eliminate the possibility of the network experiencing downtime and maximizes the availability of video streaming. In order to ensure smooth video communication in dynamic surveillance areas, the failure recovery time for network redundancy is recommended to be under 500ms throughout the entire network. This is because the monitoring screen will show highly fragmented images or a still image when image packets are lost for over 500ms. In addition to the inconvenience of the network going down and the possibility of losing vital surveillance footage, another problem is that downtime is expensive to fix, as an engineer may need to be deployed to the site to perform maintenance.

There are numerous reasons why most business owners want to avoid dispatching personnel to conduct site visits. First, as the sites are often in remote locations, it is very time consuming and expensive to dispatch personnel. In addition, surveillance cameras are often deployed in hard-to-reach places, such as on top of a tall pole. Placing cameras in these locations allows the cameras to provide better coverage and also prevents those with malicious intent from being able to tamper with the cameras. Unfortunately, it also makes maintenance more difficult. Even though industrial PoE switches that support failure recovery may have a higher initial cost, they can substantially reduce the costs and workload needed throughout the duration of a project. Networks that have a combination of device failure checking and network redundancy are much more likely to avoid both network downtime and the associated costs incurred when resolving an issue.

4) Protecting the Network with Cybersecurity

An unsecured or compromised IP surveillance system can be targeted by cyberattacks because IP surveillance systems are frequently used to guard human safety and protect critical facilities, such as in law enforcement and crime prevention applications, transportation safety and traffic monitoring, or industrial process oversight. Addressing cyber threats and network vulnerabilities are critical tasks that must be handled, especially by those managing networks that handle critical infrastructure.

However, for many years, cybersecurity was not a primary concern for system operators who thought their surveillance networks were well protected due to their isolation from other networks. Now that this is no longer the case, network operators must constantly update their security practices if they want to keep their networks secure and ensure the safety and security of on-site personnel and critical facilities. Typically, isolated parts of an industrial network and certain devices are secure from targeted threats. However, all that is required is to compromise the security of an entire network is the infiltration of one device or area of the network. As soon as someone with malicious intent has gained access to a single device on the network, it is very easy to corrupt and control other areas and devices on the network. Therefore, both device-level security and system-level security are highly recommended for industrial PoE switches used in mission-critical outdoor IP surveillance applications.

To mitigate cybersecurity risks, it is essential for industrial managed PoE switches to be equipped with device-level and system-level security features, such as strong passwords, account management, login password retry lockout, sticky MAC addresses, 802.1X authentication, and MAC bypass authentication to ensure that intruders cannot easily gain remote access to devices and alter settings in a way that puts devices or the network at risk. For example, by setting access control lists, industrial managed PoE switches can drop traffic from unauthorized IP addresses or MAC addresses. This technique prevents unauthorized devices from accessing switches, cameras, or other systems. In addition, sticky MAC addresses can bind specific switch ports to specific camera MAC addresses so that they are no longer available when someone tries to replace an original device with another device and connect to the network locally.

However, implementing a solid security policy is only the first step. It is equally important to review security settings constantly to ensure that the network remains secure for its entire deployment as outdoor surveillance networks continuously evolve. The more changes that happen on the network, the more chances there are for vulnerabilities to arise and for someone with malicious intent to gain access and corrupt the network. Network operators must pay attention to cybersecurity issues and do everything possible to prevent security breaches, ensure the safety and security of critical facilities, and maximize system uptime.

Conclusion

When deploying multiple IP surveillance cameras on industrial networks, there are several advantages to deploying PoE solutions as opposed to using separate power and Ethernet lines. Even though there are several options available for supplying power to multiple surveillance cameras, an industrial PoE switch is recognized as the most reliable and efficient solution. However, asset owners need to carefully consider specific features when selecting an industrial PoE switch in order to meet their requirements, such as a high-power PoE design, available bandwidth, fault recovery features, and last but not least, cybersecurity protection. Even though the starting price of deploying industrial PoE switches is relatively high, it pays dividends in the long term because the advanced features provided by industrial PoE switches can help reduce the total cost of ownership while satisfying key technical requirements to ensure that connected surveillance cameras provide excellent video quality and to maximize total system availability.

For further information, see https://www.moxa.com/product/industrial_poe_switch.htm.