RISE
RESOURCE

# A Guide to Network Video Surveillance Systems for Security Professionals

*By JonPablo Ramirez & Michael Harty*

**So, you've been tasked with designing and installing a surveillance system.** There are many moving parts to ensure that a system will add a measurable increase in security. You may be familiar with cameras and a recorder, but there's much more to it than that. What cameras do you need for which locations? How much storage is needed? Will the site need physical access controls? How about the ability to automatically read license plates, or send an alert to security personnel when a person enters a restricted area?

In this guide, we will delve into the different types of cameras, explain video management software, and identify infrastructure requirements. We'll help you understand the capabilities and benefits of edge processing, and outline cybersecurity best practices essential for any installation. Once we've established these foundational pillars, we'll provide some practical tips on designing a system and exploring unique implementations.

### Let's start by looking at what camera types are available:

**Dome cameras** are aptly named, and their design helps them more naturally blend into their environment. They have the added benefit of being difficult to tamper with. A smoked dome can hide the direction of the camera, making it very popular in both office and retail environments. Many models have both indoor and outdoor variants.

**Panoramic cameras** capture a wide view, up to 360 degrees. Some are multi-sensor, while single-sensor cameras give a fisheye overview that can be dewarped into usable views of a large area. An added benefit of panoramic cameras is reduced project costs as fewer cameras would be needed to cover a particular area.

**PTZ (pan, tilt, and zoom) cameras** (my favorite kind of camera) has mechanisms that control the pan, tilt, and zoom of the camera allowing for remote adjustment. These cameras give the user total control over what is being monitored in real-time. PTZ cameras are ideal for monitoring large areas where a more detailed image may be needed for security incidents. A stadium, for example, is a great place for PTZ cameras' flexible viewing capabilities and the addition of an automated tour between preset positions can offer a high level of detail between points of interest.

**Box cameras** are characterized by their rectangular "boxy" shape. They are often more customizable than other camera types, offering many different view areas and compatibility with a variety of lenses. The advantages of box cameras are both their customizability and - a point that can't be understated - that they give the classic security camera look which acts as a good form of inherent deterrence.

**Bullet cameras** are typically longer in length and shaped like a cylinder, with some models boasting an impressive range. These units are often used with license plate recognition analytics and excel in situations such as monitoring long and narrow areas like corridors or along fence lines.

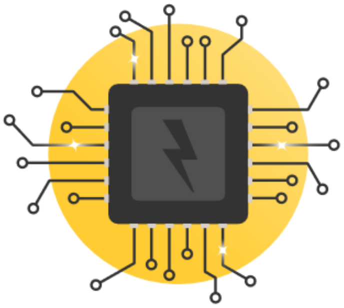
**Thermal cameras** are unique as their lenses are not made of the typical glass, but of an expensive metalloid called germanium. This germanium lens is the key to thermal cameras as it allows them to see the temperature of the scene, making them effective in any light conditions. Thermal cameras are reliable in any kind of weather conditions, whether there is haze, smoke, or it's just a dark moonless night, this camera will still deliver a usable image.

**Explosion-protected cameras** have a common misconception that they are designed to survive an explosion, which is incorrect. The purpose of these cameras is to not cause an explosion using their certified enclosures. Explosion-protected cameras are essential for any hazardous environment where a spark may lead to fires or explosions. Example use cases include firework factories, chemical plants, or oil refineries.

## What is the "edge"?

The terms "edge" and "edge-processing" refer to the computational capability of cameras themselves, with many being equipped with onboard CPUs to extract data from a scene. In this context, data refers to metadata, which is information that describes visual data. Modern cameras can count the number of people or vehicles in an area and determine how long they have been there. They can read license plates and identify which plates were seen, and when. They can even identify what color a person's clothes are.

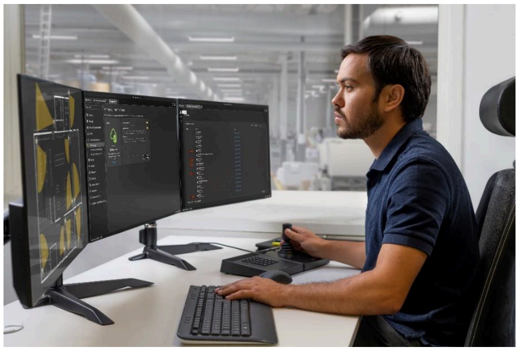
Processing at the edge takes an enormous computational load off a central server, saving money on costly hardware and electricity usage.



The camera sends this information as metadata for use as search criteria later. For example, you might need to look for an individual between 3:00PM and 3:30PM, wearing a red shirt and blue jeans. Using metadata, this person can be found in seconds by inputting those search parameters.

What if your security team received an alert if a gunshot was fired? Consider audio analytics. With these capabilities, it's possible to determine if there are gunshots, glass breaking, or loud noises in the camera's area. Alerts can be sent in real time to security personnel for a quick response.

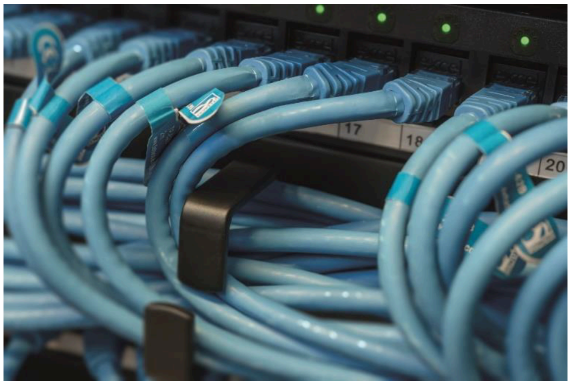
## Video Management Systems



A video management system (VMS) is software that serves as the central hub for managing network cameras, recordings, and operator access. Here, users can view live video feeds, review recorded footage, and adjust camera settings. Many VMS solutions can accommodate hundreds or even thousands of cameras making them scalable to the site's needs. You can run a VMS on-prem, in the cloud, or even implement a hybrid solution. There are many different vendors who provide VMS software. Understand the features you'll need, and make sure your software will be compatible with the cameras. For smaller installations, consider a network video recorder (NVR). This is a pre-built appliance that offers storage, administration, and in some cases integrated PoE for an all-in-one solution.

## Power Over Ethernet

A major key to network video escalating in popularity was the integration of Power over Ethernet or PoE. PoE allows network devices to receive power and data over a single cable connection, with a typical maximum range of 100 meters (about 328 feet) from the power source. Some models may offer additional AC or DC power input, if perhaps being used at a solar-powered site, or when using a fiber cable to connect the camera at an extended range. There are also PoE extenders that can push copper ethernet cable's range far past 100 meters.



PoE combines power and data transmission, but it's also crucial to have devices dedicated solely to transferring data from the camera to the VMS, local network, and, if needed, the wider internet. A data transfer setup requires switches and routers. Switches facilitate data transfer from one or multiple devices to the network and routers enable internet access and data transfer through the internet service provider's network.

## Physical Access Control System

Physical access controls are another aspect of a security solution that can integrate seamlessly with some video management systems. Access controls ensure that only authorized personnel are allowed entrance to a site, to a particular building, or even within certain areas of a building, and during which hours of the day an individual has access.

**Badge reader, PIN pad, or intercom:** These devices identify who a person is. Badges can be used in combination with a PIN if extra security is desired. If a badge or PIN is not used for automatic identification, an intercom with an included video camera can be used for visual verification by personnel at a security desk before granting access.

**Door controller:** A door controller is a powered device that locks or unlocks the door itself. This can be triggered automatically by one of the devices above or manually by security personnel.

**Zone:** A zone is self-explanatory. It can be customized to include a site, building, or areas of a building where personnel are allowed based on security requirements and access levels.

## Designing a System

Before getting started designing a system, consider any legal requirements restricting any monitoring solutions. Once those are established, the system design itself follows a distinct process:

- **Site survey:** What areas will be monitored? Are there restricted areas where physical access controls will be necessary?
- **Camera selection and placement:** Resolution at a particular distance, field of view, and lighting are the main items to consider. Keep in mind that not all cameras are capable of audio or analytics.
- **VMS software selection:** Understand what VMS software contains all the features needed for a site. Are you looking for an entirely on-premises solution or would you like the flexibility of a cloud solution? Not all VMSs integrate with physical access controls.

- **Storage sizing:** Storage must be sized correctly to accommodate the number of cameras and retention time. Surveillance-grade hard drives must be used. Regular consumer drives are less expensive, but the constant writing of video footage will drive them to premature failure.

**For some more specific design examples:**

Trigger a siren when a trespasser enters a restricted area: To secure an area with both video monitoring and active deterrence, you can use an edge application for object classification combined with an audible siren. When the camera detects a human in a restricted area, it triggers the siren, effectively deterring trespassers and alerting nearby staff or law enforcement.

A gate that opens as you drive up: Streamline access control for community residents by employing a camera with license plate recognition, eliminating the need for badges, codes, or manual authorization. This system automatically opens the gate when a recognized license plate is detected, enhancing efficiency and saving resources for the facility.

## Cybersecurity

When discussing network systems, cybersecurity should always be a top priority. This is especially crucial for IP surveillance systems, where lost or corrupted video can hinder an investigation. Here are some points to address that should be in place at a bare minimum:

- Update firmware for cameras and VMS software on a regular and frequent schedule. These updates contain cybersecurity patches for vulnerabilities, as well as stability and bug fixes
- Segment the camera's network physically or logically (using VLANs)
- Use encryption whenever possible, for example, HTTPS, so that unencrypted data and video are not sent over the network
- Avoid using port forwarding for remote access, more secure options for remote access include a remote access relay service or a VPN
- If internet access is required, install a firewall to mitigate risk from a remote malicious actor
- Use strong passwords for administrative accounts on a VMS, as well as the cameras themselves

Don't forget about the weakest link in any security solution – human beings:

- Training and awareness are paramount, as the human element represents the most significant vulnerability in security systems. Conducting regular training sessions is essential to educate staff on cybersecurity practices.

- Restricting physical access to the system is crucial to minimize the risk of unauthorized access. A malicious actor outside of the premises is much less of a threat than a malicious actor who has direct access to the ports, cabling, and other hardware of the system.

By focusing on these items, you can significantly enhance the security of your IP surveillance system, ensuring it remains a reliable tool for safeguarding assets and maintaining public safety. Ensuring a system is designed and integrated with the needs of a site is paramount in maximizing the benefit to security personnel and the safety of everyone. It's an important task, but now you have a better understanding of the essential tools that make up a video management system.

### Additional resources

*Intelligent Network Video: Understanding Modern Video Surveillance Systems*

https://books.google.com/books/about/Intelligent_Network_Video.html?id=jJOEPQAACAAJ

Written by security industry leader Fredrik Nilsson, this book covers everything in a modern surveillance system that can’t be summarized in an article. A highly valuable read for any security industry professional.