

Important Considerations When Selecting..... Video

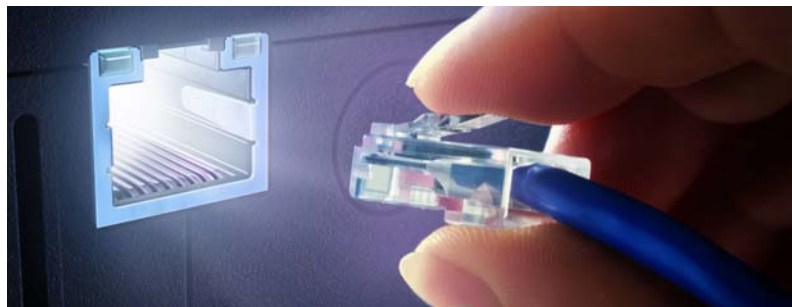
A **Video Surveillance** system is designed to monitor and record activity at a facility using cameras to transmit images back to a centralized recording device. Below is some common security terminology used when referring to video surveillance systems. If you are considering purchasing this type of security solution for your facility, we encourage you to review this information prior to making your decision.

Resolution – Picture quality is determined by resolution, and the primary measurement for resolution is pixels per foot (PPF). As a rule of thumb, the minimum pixel measurement needed to recognize a face is 40 by 40 or 1600 pixels. To read a license plate, a minimum of 80 by 80 or 6400 pixels is required. The higher the PPF of the camera, the more detailed the image will be. However, the settings on your recording device can influence resolution as well.

System Performance – Not all servers are created equal. Ten 5MP (megapixel) cameras will require more processing power than ten 1MP cameras. If you are considering expanding your system in the future, your server should be designed on the planned final system size and performance.

Frame Rate – This term refers to the total number of images recorded per second on your recording device. The higher the frame rate settings are, the more storage space is required for the data. Most cameras can record at 30 fps (frames per second). Motion pictures that you see at the movie theater are recorded at 24 fps, however the human eye will often perceive no difference in video recorded at 15 fps. The security industry standard ranges from 7.5 to 8 fps, which balances quality video playback with cost effective data storage.

Data Storage – System configuration affects how long recorded video can be stored. Considerations include number of cameras, continuous/event-based recording, number of hours per day camera(s) will be recording, frames per second, video compression type, and scenery (image complexity and lighting conditions). Your integrator can work with you to determine the appropriate configuration to achieve your data storage needs.



Scalability – When purchasing a security solution, consider potential expansion needs in the future. At this point you may wish to monitor only a portion of your facility, but perhaps a renovation or an increase in funding will give you the opportunity to add to your system in upcoming years. Planning for these needs will allow your integrator to provide you with the most cost-effective and flexible security solution.

Software Licensing – Many industry standard IP Video and Access Control security platforms often require annual software licensing subscriptions in order to provide access to manufacturer updates and technical support. These are valuable services that help to ensure the future viability and scalability of your system. Make sure you are aware of manufacturer software licensing requirements prior to selecting a security solution.

Wide Dynamic Range – In an environment with extremely bright and dark areas or in backlight situations where a person is in front of a bright window, a typical camera will produce an image where objects in the dark areas will hardly be visible. A wide dynamic range feature on a camera enables objects in both bright and dark areas to be visible.



Day/Night – A camera type designed to be used in outdoor installations or in indoor environments with poor lighting. A day/night, color camera delivers color images during the day. As light diminishes below a certain level, the camera can automatically switch to night mode to make use of near infrared (IR) light to deliver high-quality, black and white images. It is also important to note that high megapixel cameras do not perform well in night time or low light conditions.

Network Utilization - For larger video surveillance systems it is recommended that the system is established on a dedicated network to avoid any potential bandwidth consumption issues. The factors affecting bandwidth usage can include the number of cameras, the image resolution used, the compression type and ratio, frame rates and scene complexity.

Connectivity – Consider how you want to interface with your security solution. Do you want to be able to access it from a computer in a control room or on your laptop at home? Perhaps you want to log into the system through a smart phone such as Android or iPhone? A variety of connectivity options are available for security applications, although features such as multiple workstation client and web client/browser based software options may incur additional costs. Also, some security solutions will not offer all connectivity options for certain operating systems, so it is important to discuss the operating system your facility is currently using (Windows, MAC, Linux) with your integrator.

Standardization – In the past, security equipment manufacturers have designed proprietary communication protocol for their IP-based systems. This made it difficult to design functional systems with components from multiple manufacturers. Standards have recently been developed to help ensure interoperability between IP-based products regardless of manufacturer. ONVIF (Open Network Video Interface Forum) or PSIA (Physical Security Interoperability Alliance) are the two leading standards in the industry, with ONVIF currently being the most prevalent. Verify that the system you are purchasing complies with one of these formats to ensure the flexibility and future viability of the solution.

