



IT considerations for designing an IP video system

Nine critical IT concerns when designing an IP video system

Table of Contents

Introduction	3
1. The role of IT expertise in video systems.....	4
2. Rightsizing equipment to meet video surveillance needs	5
3. The critical role of networking	6
4. Emphasising value over price	7
5. Cybersecurity threats and fixes	7
6. Limitations of an “air-gapped” approach	8
7. Ensuring no lost video data	9
8. Managing lifecycles in IP surveillance systems.....	10
9. The IT ecosystem in video systems	10

Alcatel-Lucent Enterprise commissioned SourceSecurity.com to produce this document.



Introduction

A video surveillance system has specialised needs when it comes to information technology (IT). While a digital video system may use the same technologies as other IT systems, they are configured differently and with the specific needs of video surveillance in mind.

Video is a more demanding environment and puts a heavier workload on every part of an IT system. Given the stress, and especially in the case of a larger enterprise system, things can begin to break. Choosing the right equipment for the job ensures greater dependability over time.

Alcatel-Lucent Enterprise worked with industry experts SourceSecurity.com and Stone Security to identify the nine critical IT concerns when designing an IP video system. In this White Paper, we explore how the specialised needs of a video surveillance system impact which IT technologies are deployed and how they are used.

White Paper

IT considerations for designing an IP video system



1. The role of IT expertise in video systems

Designing and creating a video surveillance system based on the Internet Protocol (IP) requires a high level of IT expertise in the integrator community.

Some integrators have sufficient skills to expertly launch an IP video system, while others may struggle.

The extra training and certifications familiar to most in the IT world can enable integrators to deliver the required high level of service. To start, installers must have the right aptitude and a basic understanding of networking and troubleshooting skills.

Integrators can ensure a knowledgeable workforce by limiting their range of technology choices and making sure every employee is well trained in the smaller number of technologies. Picking best-in-class solutions and ensuring employees are expert in those products allows an integrator to deliver a higher-grade system to customers.

Limiting the product mix also enables an integrator to better understand the breadth of features offered by any given product. Too often, a customer buys a system that offers a span of features and then only uses a limited number of those features in day-to-day operation, thus undermining the value of the system they paid for.

Integrators can help customers by educating them to unlock the full value from whichever system they buy.

Integrators may also depend on the pre-consulting services of equipment manufacturers to guide them. In some cases, equipment manufacturers have specific knowledge about various vertical markets, accumulated over a history of serving those markets.

Manufacturers who are serious about a specific vertical market will employ industry experts to ensure support that is specific to each customer's needs. Their guidance can help integrators succeed in new markets and/or streamline best practices for the markets in which they operate.

Manufacturers also provide training and certifications to ensure integrators are well equipped to install their systems. Efficient and substantive training should be presented in shorter sessions that respect the value of each attendee's time.

2. Rightsizing equipment to meet video surveillance needs

Issues such as bandwidth and Power over Ethernet (PoE) requirements are important variables in a video system. And the video server has a higher load, especially when it comes to video from a live feed. Every bit of data lands on the server, even data that is not being recorded.

Video is buffered, which ensures there are at least a couple of seconds of video that can be preserved in advance of an actual alarm-triggering video recording. Longer periods of buffering might be called for in the case of identifying an image approaching from a longer distance. All the inputs and outputs go through the server, even though a limited amount of data will be written to long-term storage.

There is a fundamental difference between how security system integrators view system size versus how IT professionals view it. Systems integrators are more likely to speak in terms of camera count, while IT professionals are more likely to speak in terms of managing data from the system. The two are intrinsically linked, of course, but the relationship is not linear. In general, a higher camera count equates to more data to be managed by the IT department. However, there are other factors involved that impact data needs, such as frame count, image quality requirements, storage needs, day/night applications and use of video analytics.

A key skill when specifying an IP security system is to translate the system's equipment and functionality requirements into the data necessary to deliver those needs. For an on premises system, that equates to a need to specify a computer server that maximises system performance while lowering costs. Issues such as virtualisation and cloud systems can both complicate the equation and provide new flexibility.

Another variable related to system design is the use of cameras at the edge of the network to record video using SD cards. There are even systems today that are “serverless”; for example, all recording takes place at the edge. Such an approach, in effect, offloads the computational burden from the server to the edge, with a resulting decreased need for server capacity. Today's cameras provide data beyond the video stream, such as metadata and audio, which also impact system design.

IT professionals should have a thorough view of the overall system, such as what will be connected, frame rates, resolution and video codecs of the cameras. With this information, they can calculate the requirements around the network, power, servers, disk capacity, memory, storage and whether to use cloud or on premises systems. This ensures a thorough and thoughtful approach to design and deployment.

Manufacturers provide software “calculators” to help integrators design systems by translating system requirements into specific equipment specifications. Keep in mind that calculations should meet or exceed expectations and allow for future growth.

Implementation of cloud systems is another variable when it comes to the design of video surveillance systems. The clear trend is toward the use of more cloud systems for video surveillance. However, choosing the cloud versus on premises solutions should be made on a case-by-case basis. Systems designers and end users should resist the seeming inevitability of the cloud, and rather make decisions based on the needs of the customer.

Many manufacturers are under pressure to transition their systems to the cloud but ideally should provide their customers with customers with a choice of systems and not a one-size-fits-all solution.

Manufacturers are in a good position to advise customers on the desirability of a cloud configuration versus an on premises design. Integrators should also be well-versed in the advantages of either approach or facilitate a customer decision either way. The market should not be pushing applications to the cloud unless that is the optimum approach for each individual customer.

3. The critical role of networking

A video system is only as strong as its weakest link. The network switches may not be as visible as the cameras and VMSs, but they are no less critical.

What tends to happen though is that customers take the operation of a network for granted, paying little attention to how it works or to how to maximise its utility. In fact, some customers want to install a video system using an existing network infrastructure. This is possible, but the ability to optimise the network piece of a video system can be limited.

Ideally, the customer will opt for the best switches for video surveillance, which will ensure a system that operates dependably and effectively.

Each video system is different, so giving special attention to its individualised requirements ensures it achieves its unique mission. When commissioning a system, the network should not be seen as an afterthought. Rather, it should be carefully assembled using the best components to both enable and enhance operations system-wide.

Switches that work at “wire speed,” meaning they have enough processing power to handle full Ethernet speed at minimum packet sizes, are now standard in the industry. A new point of differentiation among switches is the ability to understand and manage their traffic.

Unmanaged switches are available in the market but are not typically used for commercial and/or enterprise applications. They are designed for use in small networks with basic needs; there are no settings to configure.

Conversely, managed switches enable the detection and diagnosis of performance problems and ensure dependable performance of video surveillance systems. They enable users to granularly view what might be causing problems in the system and provide an understanding of what that information looks like.

The value of managed switches, which are fully configurable, customisable and provide a range of data about performance, will be obvious over the course of system life, providing important insights into system operation and permitting easier troubleshooting to identify problems.

Switches should be designed to address the needs of IP video systems. An example, in the case of a 16-port switch, is a sufficient power budget to operate all the video cameras connected to the switch. Today's PoE cameras draw more power than previous generations. Integrators need to know that a switch provides sufficient power to handle the camera count and future growth.

“When we are making our hardware selection, we want every switch to have the bandwidth capabilities, the power budget and to be a managed switch that saves us massive amounts of time when troubleshooting. They save us money and they save the customer money. It's more investment up front, but it will pay for itself in the long run by creating a more serviceable system.”

**Aaron H. Simpson,
President & CTO, Stone
Security**

4. Emphasising value over price

Reliability is critical in video surveillance, and it starts with equipment choices.

Specifying lesser quality components may seem like an economic necessity at the time. In the long run, however, system operation will suffer. The cost of choosing a less-than-optimum operation may not be obvious when designing a system but will become abundantly clear over time.

On the other hand, choosing better equipment – even if it is more expensive – will pay off.

It is critical to weigh the costs (such as the price of better equipment) against the risks of system inadequacy or failure. Taking a total cost of ownership (TCO) approach when evaluating costs and risks is the best strategy. Another long-term cost element to consider is the value of open systems, which can ensure flexibility when expanding or changing a system in the future.

It is always best to work with a supplier who offers product they have confidence in and which they can support over a long period of time.

5. Cybersecurity threats and fixes

Historically, an irony in the physical security industry has been a lack of attention to the cybersecurity of IP systems.

Fortunately, physical security stakeholders are now paying more attention to cybersecurity concerns at every level and throughout the physical security supply chain. In fact, cybersecurity has become one of the key pillars of the decision-making process for larger video security systems.

A minimum step toward guarding against cyberthreats and restricting access to a system is to avoid the use of default passwords. These are less secure and can be guessed more easily by a hacker or bot. In fact, default passwords have been outlawed in California.

Cybersecurity risks begin in the supply chain, where attacks can compromise a product before it is even delivered. Analysing a product for possible “backdoor” or “buffer overflow” attacks prior to delivery can mitigate the threat. Customers may also opt to virtually install “good code” after hardware products are delivered, thus ensuring cybersecurity and overwriting any malicious code that might have been installed during shipping.

There is also a range of cybersecurity measures to be addressed during installation and at various stages of system implementation. For example, “learned port security” ensures that a port is accessed only by an authorised device. If an unauthorised device tries to connect to the system — for instance, to connect a new camera — an alert triggers and access to the port is denied until authorised by a human.

Shortest Path Bridging (SPB) technology can prevent malicious activities leapfrogging from one system to another. Rules are set up so that a camera can only stream to the recorder, and other powerful segmenting technology is deployed on multi-IoT networks.

Systems should disable insecure protocols such as FTP and Telnet, which facilitate communication across a network, but can provide additional opportunities for hackers. These capabilities should be “secure by default” so as not to allow a connection to the network unless it is intentional.

Effective cybersecurity also requires restricting physical access to a system. If a switch is deployed in a janitor's closet where physical access is open to all, then it is not well protected. Allowing physical access to a system makes it easy for anyone — including an employee posing an insider threat — to plug in a laptop and access the whole system.

Cameras should record access to network equipment as a “defence in depth” approach.



6. Limitations of an “air-gapped” approach

When it comes to protecting video systems from cybersecurity attacks through the internet, a common approach historically has been to create air-gapped systems.

An air-gapped system involves isolating a computer or network and preventing it from establishing an external connection. Because an air-gapped computer is physically segregated and incapable of connecting wirelessly or physically with other computers or network devices, the approach is seen as a panacea to ensure video system cybersecurity.

However, it is a risky proposition to depend on an air gap as the only cybersecurity protection. There is a variety of situations in which an air-gapped system might be exposed to the internet, even for a short period. When that happens, the system depends on any other cybersecurity measures — if they exist — to protect it from disaster.

Assuming a system will be air gapped forever is not a solution for cybersecurity. It is instead a disaster waiting to happen.

Air-gapped systems are also not able to take advantage of artificial intelligence (AI) and other features that depend on accessing many users and analysing shared experiences. Data from a single customer is not as useful as data from hundreds of customers, available in the cloud. Air-gapped systems do not allow customers to leverage the additional value of smarter analytics. Giving up some data (which comes with privacy considerations) is a price customers pay to leverage greater value.

Given today's customer requirements to connect and have continual access to their systems, the use case for air-gapped systems is becoming more and more limited.

Organisations also tend to push back at the prospect of creating a totally separate network infrastructure for video surveillance. There is no such thing as a “separate, secure” network.

7. Ensuring no lost video data

Lost data is a problem for any IT system, but much more so for IT systems that provide video surveillance. A video surveillance system is mission critical and must operate 24/7. There is no downtime to allow administrators to diagnose and solve any data loss problems; rather, the issues must be addressed perpetually and in real time.

This is where managed switches can help. Managed switches can enable system administrators to quickly diagnose and address any data loss problem. They can also easily identify the source(s) of data loss. There is no “finger-pointing” in terms of which system component is at fault.

Packets can be dropped because of data being converted from fibre transmission to copper and Ethernet. Electrical transceivers are used to translate data from fibre transmission to electrical transmission, and the devices can be a source of dropped data packets.

In video surveillance, a lost packet of data equates to compromising a video image — causing it to be, in effect, lost forever. There is no way to restore video images that are lost during downtime outages. Consider a casino application, for example, where the consequence of a failed video system is lost coverage of a gaming table which, in turn, can also mean lost revenue.

In the broad variety of video surveillance applications, redundancy is needed to ensure continuous operation 24/7.

The need for reliability must be weighed in the context of risk versus benefit. A system might be less expensive, less complex and/or less fault tolerant, but such a system might not perform as intended — which has its own costs.

Another variable that can cause performance issues in video systems revolves around the distinction between unicast and multicast, which are two methods for sending data over a network. Unicast provides a one-to-one communication model in which a single sender delivers data to a single receiver. In contrast, multicast is a one-to-many model in which a single sender delivers data to several recipients.

Many video surveillance applications operate in unicast mode. This means a camera is monitored in real-time by an individual — one video stream is involved.

However, some applications require multicast, in which a single video stream is viewed by multiple users. Problems arise when a system transitions from unicast to multicast. Making the transition involves more than just “flipping a switch,” and nuances and details of transitioning can cause problems in system performance. Problems arise if parts of a system are set for unicast when they should be multicast or the other way around. Proper configuration on this point throughout the system is crucial.

Smart network advisor capabilities enable an end user to understand what is normal in terms of network performance and then detect when something is abnormal, or out of bounds of usual expectations. Any deviations are reported automatically, and humans may intervene as needed to address the issues.



8. Managing lifecycles in IP surveillance systems

In the world of IT, product lifecycles may be three to 10 years depending on the industry and product. There are existing protocols to address issues such as meantime between failure (MTBF), firmware and security patches.

In the arena of video surveillance, product lifecycles have historically been longer — there are decades-old video cameras still performing in the field. Adapting IT management strategies to IP video systems can reveal a disconnect.

IT support provided by a manufacturer provides immense value to the integrator and the end user. Historically, longer lifecycles in physical security have resulted in systems that continue to operate beyond the expected period and in an unsupported environment.

There are inherent risks of continuing to use equipment that is not supported by the manufacturer. For example, failing to update firmware can open the door to cybersecurity threats.

Most equipment today has a five-year warranty and realistically could continue to operate for an additional five years. However, with the rapidly changing technology landscape, most customers will want to take advantage of the most current capabilities. In effect, technology acceleration equates to shorter lifecycles in security, just as it does in the broader IT and networking environment.

9. The IT ecosystem in video systems

A unified IT ecosystem is the best approach to ensure a successful IP video system. The success of any new technology relies on an IT ecosystem that supports it. Issues such as hardware and software interoperability ensure smooth system operation.

Open standards ensure maximum flexibility for customers in the present and in the future. Simplified offerings are also useful. For example, [Alcatel-Lucent Enterprise](#) has a single operating system that functions with every Ethernet switch the company sells.

Maintain a strategy of embracing products that “play well” in their environment and with other products in the ecosystem to ensure success.

A successful IT ecosystem does not just happen. Rather, it is nurtured by industry partners working together to ensure success. Principles such as openness and interoperability contribute to the IT ecosystem. Success boosts the performance of every component of a system and of the system as a whole.

[Learn more about Alcatel-Lucent Enterprise video surveillance solutions.](#)