Understanding the IT Needs of Video Surveillance

sourceSecurity.com
making the world a safer place

Alcatel·Lucent Enterprise

About the author

An experienced journalist and longtime presence in the U.S. technology marketplace, Larry Anderson is the Editor of leading digital publications SecurityInformed.com and SourceSecurity.com. Mr. Anderson is the websites' eyes and ears in the fast-changing security sector, attending industry and corporate events, interviewing leaders and contributing original editorial content to the two sites. He leads a team of dedicated editorial and content professionals, guiding the editorial roadmap to ensure that SecurityInformed.com and SourceSecurity.com provide the most relevant content for industry professionals. From 1996 to 2008, Mr. Anderson was editor of Access Control & Security Systems magazine and its affiliated websites. He has written numerous articles for and about some of the largest companies in the security industry and has received numerous awards for editorial excellence. He earned a Bachelor of Arts in journalism from Georgia State University with a minor in marketing.

9 Critical IT Concerns When Designing an IP Video System

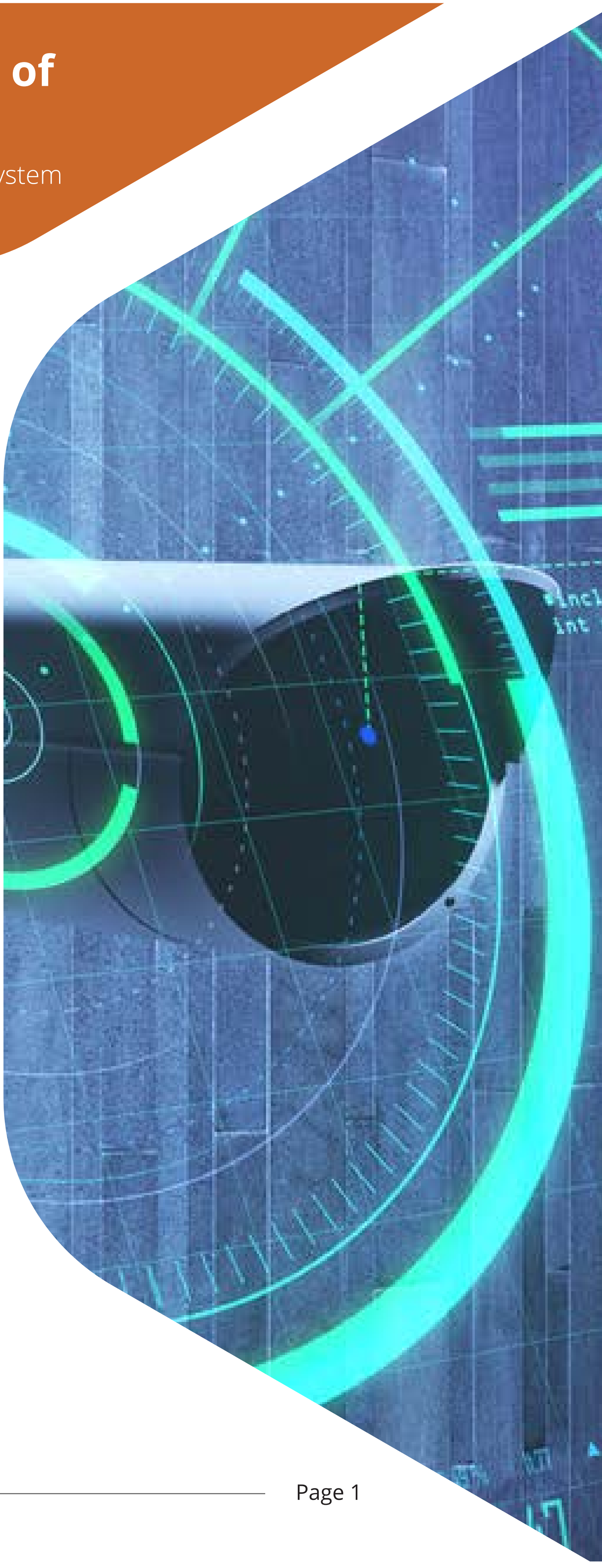
	Page
The Role of IT Expertise in Video Systems	**2**
Rightsizing Equipment to Meet Video Surveillance Needs	**4**
The Critical Role of Networking	**7**
Emphasizing Value Over Price	**10**
Cybersecurity Threats and Fixes	**11**
Limitations of an "Air Gapped" Approach	**13**
Ensuring No Lost Video Data	**14**
Managing Lifecycles in IP Surveillance Systems	**16**
The IT Ecosystem in Video Systems	**17**

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

Understanding the IT Needs of Video Surveillance

9 Critical IT Concerns When Designing an IP Video System

By Larry Anderson



A video surveillance system has specialized 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.

Let's look at how the specialized needs of a video surveillance system impact which IT technologies are deployed and how they are used. This Technology Report was produced with the help of Alcatel-Lucent Enterprise, a provider of communications, networking, and cloud solutions. Additional commentary is provided by Stone Security, an integrator that specializes in physical security systems for professional and enterprise class customers.

1 The Role of IT Expertise in Video Systems

Designing and creating a video surveillance system based on Internet Protocol (IP) requires a high level of information technology (IT) expertise in the integrator community. Some integrators have sufficient skills to expertly launch an IP video system, while others may struggle.

Extra training and certifications, such as those familiar to anyone 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.

> *"We pick the best technologies the industry has to offer, and every employee is an expert in those products."*
>
> **Aaron H. Simpson,**
> President & CTO,
> Stone Security

"Our goal is to grow the knowledge of everyone who is coming up," says Aaron H. Simpson, President & CTO, Stone Security. "They must be able to talk knowledgeably to customers and their IT teams. There is more respect and confidence when we sit down with the end users to have conversations about IP ranges, domain name systems (DNS), and similar subjects."

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. "We pick the best technologies the industry has to offer, and every employee is an expert in those products," says Simpson. "That allows us to deliver a higher-grade product to our 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 that they have accumulated over a history of serving those markets. “Manufacturers who are serious about a specific vertical market will employ industry experts to ensure support specific to each customer’s needs”, says David King, ALE's Industry Specialist on Smart Buildings, Safety and Security IoT. Their guidance can help integrators succeed in new markets and/or streamline best practices for the markets they are in.

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 hone in on 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, too, such as frame count, image quality requirements, storage needs, day/night applications, use of video analytics – the list goes on.

A key skill when specifying an IP security system is to translate the equipment and functionality needs of the system into how much data will be needed to deliver on those needs. For an on premises system, that equates to a need to specify a computer server that maximizes system performance while lowering costs. Issues such as virtualization and cloud systems both complicate the equation and provide new flexibility.

Another variable related to system design is the use of cameras that can provide recording 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.

“You have to have a thorough view of the overall system, what will be connected, frame rates, resolution, and video codecs of the cameras,” says Simpson. “You have to calculate the network requirements, the power to run the system, server requirements, disk capacity, memory, storage, whether to use cloud or on premises systems. We at Stone Security have 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.

“There is a lot to consider when creating the footprint for a customer,” says Simpson. “We are very specific when considering what the layouts look like, server designs, warranties on the servers, and so forth.” Calculations should meet or exceed expectations and allow for future growth.

Implementation of cloud systems is another variable when it comes to design of video surveillance systems. The clear trend is toward use of more cloud systems for video surveillance, but 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 a choice of systems and not 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 and 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.

```
clude "win32n.inc"
ern MessageBoxA
port MessageBoxA user32.dll
tern ExitProcess
port ExitProcess kernel32.dll
        use32 class=code
```

```
  push UINT MB_OK
  push LPCTSTR window_title
  push LPCTSTR banner
  push HWND NULL
  call [MessageBoxA]

  push UINT NULL
  call [ExitProcess]
SECTION data use32 class=data
  banner: db "Hello, world!", 0xD, 0xA, 0
  window_title: db "Hello", 0
```

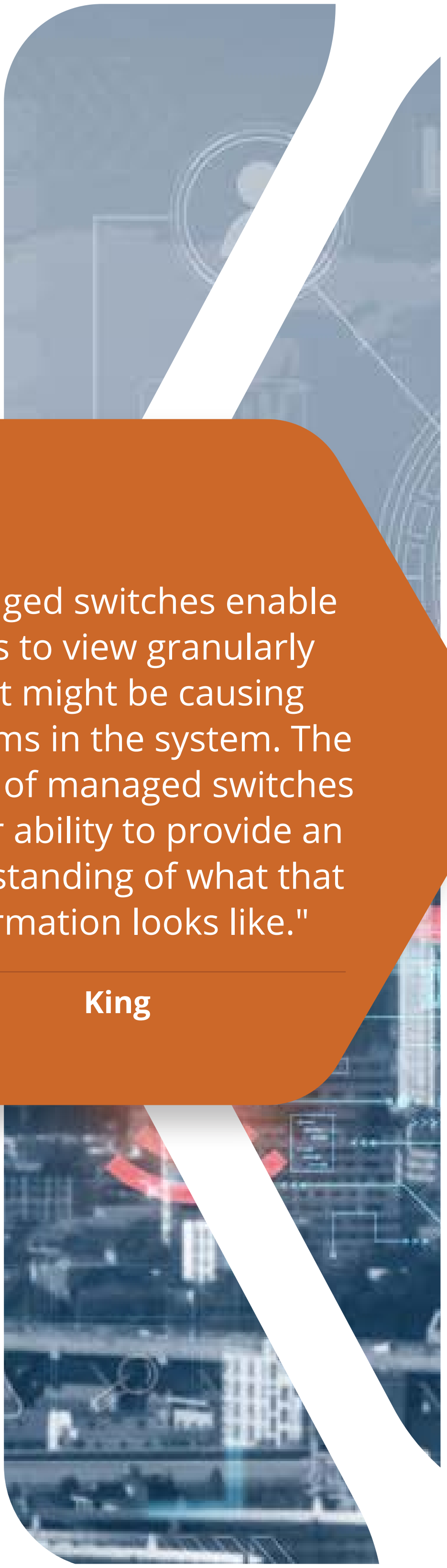
3 The Critical Role of Networking

A video system is only as strong as its weakest link. As the most visible components of a system, much depends on the selection of the best cameras and VMSs, among other equipment, etc. for a system. However, the less visible components of a system are also critical, especially network switches.

Customers tend to take the operation of a network for granted. There is an expectation that it will work, but little attention is paid to how it works or to maximizing its utility. In effect, the network is an “invisible” part of the system. However, it becomes very visible really fast if it fails!

Unfortunately, the ability to optimize the network piece of a video system can be limited if the customer wants to install a system using an existing network infrastructure.

Selecting the best switches for video surveillance ensures a system that operates dependably and effectively. Every system is different, so giving special attention to the individualized requirements of a system ensures it achieves its unique mission. When commissioning a system, the network should not be seen as an afterthought, but rather should be carefully assembled using the best components to both enable and enhance operation of the more visible components.



Switches that work at "wire speed," that is, 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. The use of fully managed switches today provides information to detect and diagnose any switching problems.

Use of managed switches enables diagnosis of performance problems and ensures dependable performance of video surveillance systems. 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. “The value of managed switches, which are fully configurable, customizable 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,” says King.

“Managed switches enable users to view granularly what might be causing problems in the system. The beauty of managed switches is their ability to provide an understanding of what that information looks like."

King

“Managed switches enable users to view granularly what might be causing problems in the system. The beauty of managed switches is their ability to provide an understanding of what that information looks like," adds King.

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," says Simpson. "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."

4 Emphasizing Value Over Price

Reliability comes at a cost. Choosing better equipment, even if it is more expensive, will pay off. Specifying lesser quality components, including network switches, may seem like an economic necessity. However, in the long run, system operation will suffer. Less-than-optimum operation has a high cost, too, which may not be as obvious when designing a system but will become abundantly clear over time.

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.

Stone Security only offer top-tier products they have confidence in and that they can support over a long period of time. "For customers to have the experience they want and expect, we need to be installing and configuring products that deliver," says Simpson.

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. How can an industry whose business is security take a slipshod approach when it comes to protecting its own systems from cybersecurity threats?

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 to ensure cybersecurity and restrict access to a system is to avoid the use of default passwords, which are less secure and can be guessed more easily by a hacker or a bot. In fact, default passwords have been outlawed in California. Cybersecurity risks begin in the supply chain even before a system is delivered. Cybersecurity attacks targeting the supply chain can compromise the cybersecurity of a product before it is even delivered. Analyzing a product for possible “backdoor” or “buffer overflow” attacks before it is delivered can mitigate the threat. Customers may also opt to install “good code” virtually 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 authorized device. If an unauthorized 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 authorized by a human.

“Shortest path bridging” is one technology that can prevent malicious activities from 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 anyone has physical access to a janitor’s closet where a switch is deployed, 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 “defense 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 cybersecurity of video systems.

However, depending on an "air gap" as the only cybersecurity protection is a risky proposition. In a variety of situations, 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 forever "air gapped" is not a solution for cybersecurity but rather 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 analyzing 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 to and have continual access to their systems, the use case for air gapped systems is becoming more and more limited.
Organizations 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. How is data lost in a video system, and how can a system address any data loss problems before they undermine a system's performance? 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. Use of managed switches can enable system administrators to quickly diagnose and address any data loss problem. Managed switches 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 fiber transmission to copper and Ethernet. Electrical transceivers are used to translate data from fiber 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 that is, in effect, lost forever. There is no way to restore video images that are lost during downtime outages. In the case of a casino application, for example, a failed video system means there is no coverage of a gaming table, and revenue is lost.

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 designing such a system comes with costs because the system does not perform as intended.

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 provides data to several recipients. Many video surveillance applications operate in unicast mode – a camera is being 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 seeks to transition 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, and *vice versa.* Proper configuration on this point throughout the system is crucial.

Smart “network advisor” capabilities enable an end user to understand what’s “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 still video cameras performing in the field that are decades old. 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 after that. 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 operation of a system.

Open standards ensure maximum flexibility for customers in the present and in the future. Simplified offerings are also useful. For example, Alcatel-Lucent Enterprise have a single operating system that functions with every Ethernet switch they sell.

When creating its “ecosystem,” Stone Security only embraces products that “play well” in their environment and with other products in the ecosystem. “We provide only best-in-breed systems that play nice in our ecosystem,” says Simpson.

A successful IT ecosystem doesn’t 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, and 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.