Maximizing security and performance

The full lifecycle of video surveillance

securityinformed.com
Making The World A Safer Place

Alcatel·Lucent
Enterprise

Table of Contents

Introduction 3

Stage 1: Planning and design 4

Stage 2: Deployment 6

Stage 3: Operational management 8

Stage 4: Troubleshooting and maintenance 10

Stage 5: Upgrade and optimization 12

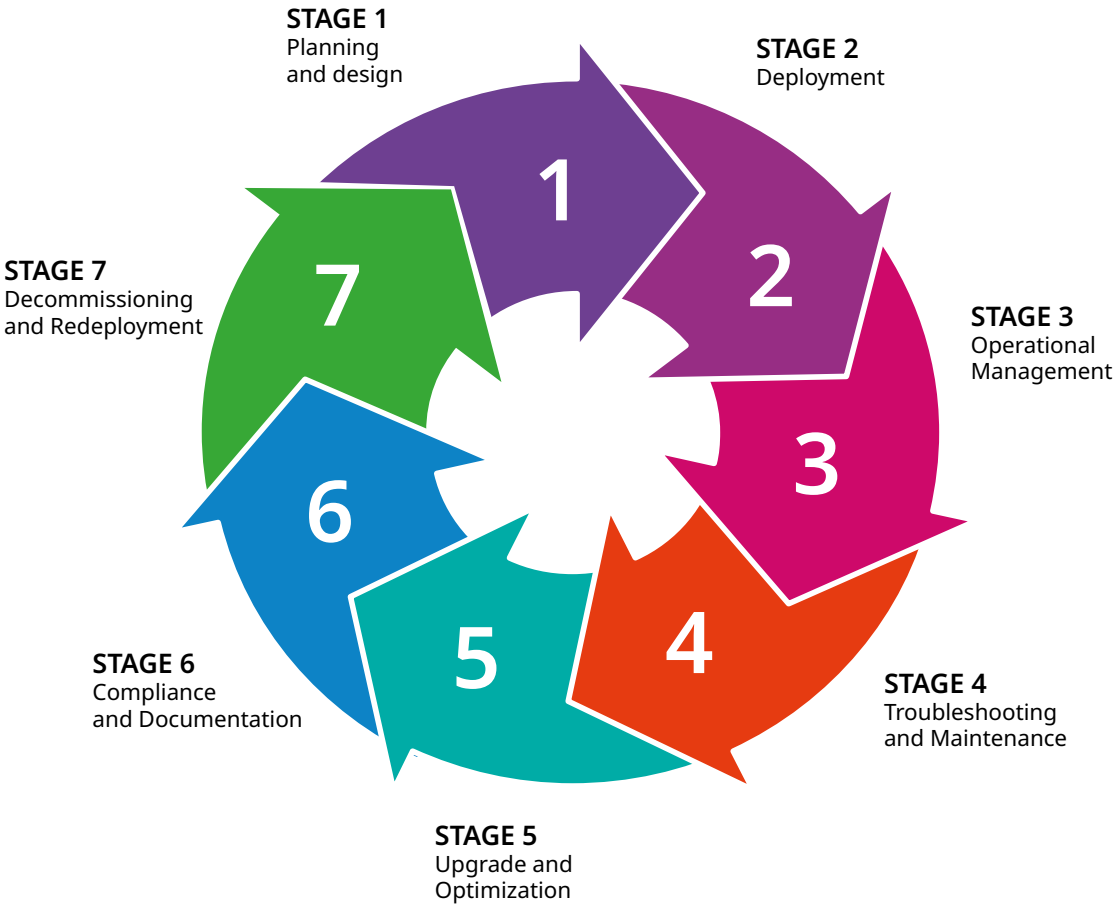
Stage 6: Compliance and documentation 13

Stage 7: Decommissioning and redeployment 13

Lifecycles depend on customer's needs 14

The value of a lifecycle approach for video surveillance networks 14

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



Introduction

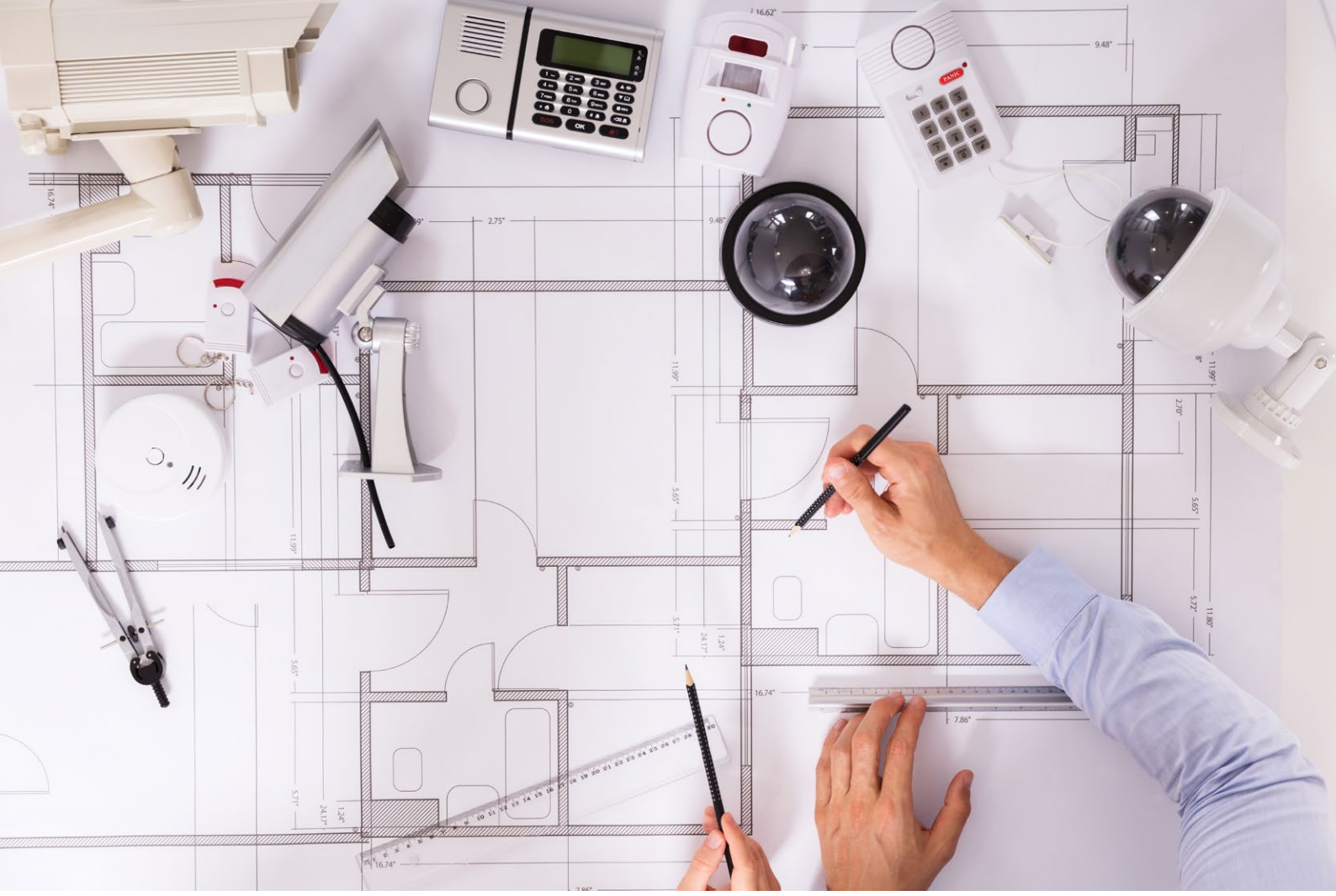
In today's security-conscious world, video surveillance networks are indispensable for safeguarding people, assets and infrastructure.

However, these systems are far from "install-and-forget" solutions. Instead, they require a systematic lifecycle management approach to adapt to evolving technological, operational and security needs.

Network lifecycle management (NLM) offers a structured framework that covers every aspect of an IP video surveillance system's lifespan—from planning and design through to decommissioning. This lifecycle approach not only ensures that systems remain robust and compliant but also minimizes costs and boosts performance over time.

A lifecycle approach to networked systems is a well-worn strategy of the information technology (IT) world. However, the arena of video surveillance is just now embracing the approach, led by larger systems integrators. Discussing video systems in the context of lifecycle management paves the way for integrators and end users to embrace higher quality technologies with an eye toward maximizing their value over time rather than focusing on lower-priced equipment.

This white paper explains how considering the various stages of the video surveillance lifecycle can direct the selection of the best hardware and software systems. Continuous monitoring of the network is part of the lifecycle approach, and networking technologies are evolving to enable more effective monitoring of the network infrastructure and faster response if there is a problem.



STAGE 1

Planning and design

Setting the foundation for longevity

The planning and design stage is when integrators define the system's long-term objectives and design a network architecture tailored to security, scalability and regulatory needs. A comprehensive design plan should outline the network's key components, bandwidth requirements and storage solutions while accounting for future technology upgrades and operational scalability.

Integrator challenges include defining the right path for the video stream (live or recorded); e.g., coming from the camera to the recording server and then storage. IP video networks have specialized requirements compared to other IT networks. They need more bandwidth, for example, and require that video streaming be captured and stored 24/7. Video networks are critical for security, and they are typically managed by non-IT people. They also have specialized power needs, notably Internet of Things (IoT) devices with higher Power over Ethernet (PoE) requirements.

The requirements of an IP video surveillance system can be summed up by the "Five Ss." That is, Software, Surveillance IoT (cameras), Servers/Storage, Switches and Services/Support. Considerations of each element must be the focus at the planning and design phase and throughout the lifecycle.

Networking technologies are available to serve any size facility, from a small single site to a large, multi-tiered facility or even a critical infrastructure installation. A manufacturer's vendor team, trained and dedicated to physical security integrators, can direct the optimum selection of technologies for the customer's needs.

In the design phase, clear objectives are essential. For instance, does the system need high-resolution feeds or low latency for real-time monitoring? Requirements should also address compliance with cybersecurity and data privacy regulations.

The design architecture must ensure adequate network bandwidth to handle video data traffic, especially with high-resolution or 24/7 video streams. As network demand grows, systems that lack proper capacity planning can experience slowdowns, data loss, or require costly retrofits.

Designing the network involves calculating the required loads on switches and other components, while factoring in variables related to routing, switching and networking to ensure an optimized overall solution.

The solution should also incorporate lifecycle thinking to plan for future growth, even during the design phase. By approaching design with future stages in mind, integrators can create flexible, future-ready networks that support growth without costly adjustments.

High-quality components are fundamental when designing systems that can handle current capacity and future growth. For example, entry-level network switches are inadequate for the latest artificial intelligence (AI) systems.

- **Five 'S's Framework:** Key elements — Software, Surveillance IoT, Servers/Storage, Switches, and Services/Support — are critical for system planning and design.
- **Bandwidth and scalability:** Adequate planning ensures the system can handle high-resolution, 24/7 video streams and support future growth without costly retrofits.
- **High-quality components:** Essential for current and future needs, including AI readiness and operational scalability.
- **Role of integrators:** Integral in planning, monitoring and maintaining the system to meet evolving operational demands and regulatory compliance.
- **Customer relationships:** Emphasis on long-term partnerships for managing and upgrading systems throughout their lifecycle.
- **Monitoring technologies:** Evolving tools allow for effective network infrastructure monitoring and faster issue resolution.

STAGE 2

Deployment

Ensuring successful implementation

Once a clear plan is in place, the next phase involves procurement, configuration, testing and deployment of hardware and software components. Deployment is where systems often face initial issues, particularly around bandwidth requirements and device integration. Calculating the bandwidth requirements based on the video path ensures stable live streaming and playback. Surveillance networks need robust solutions to handle video feeds and the data loads they generate.

Acquiring and setting up hardware such as servers, cameras, switches and storage solutions is fundamental. In this phase, selecting equipment that aligns with lifecycle needs—from initial deployment to eventual decommissioning—ensures system longevity.

Testing each component can verify functionality, compatibility and performance under realistic conditions. Deploying enterprise-level networking solutions with simplified configurations can transform the process.

Edge devices are part of the network and should be brought into the “best practice” lifecycle management infrastructure. The cameras attached to an IP video network, for example, are now part of the network and should be considered in the context of the lifecycle approach.

Today, IP video networks are mostly connected and no longer depend on “air gaps” to prevent unauthorized access. An air-gapped system is a network security measure that physically isolates one or more computers from other networks. In today’s video surveillance systems, use of air-gapped systems has decreased due to the increasing reliance on network connectivity to provide benefits such as data analytics and AI.

A feature of Alcatel-Lucent Enterprise’s network devices is Universal Network Profiling (UNP), which allows for dynamic and granular control over network access and traffic based on user, device, application and other factors, in effect, creating “profiles” for each device or user to automatically adjust network behavior depending on needs and security requirements. Features like device fingerprinting and user authentication identify devices and users on the network, assigning them appropriate profiles based on their identity and role.

There is a simple, automated process for onboarding of IoT devices, dynamically recognizing devices and supplying the correct network resources for an IoT system while ensuring against cyberattack and data loss.

Advanced monitoring and configuration tools ensure that all components operate smoothly within their network environment, optimizing both performance and stability.

The Alcatel-Lucent Enterprise OmniSwitch® Lightning Config tool provides simplified, out-of-the-box deployment for customers, business partners and service integrators. The tool reduces setup times and empowers installers to perform routine updates and troubleshoot issues in minutes rather than hours.

Benefits include enhanced security and flexibility to configure the switch according to specific needs.

Easier-to-install systems make it possible to employ entry-level technicians without sacrificing value and performance. With Lightning Config, an installer with 50 minutes of training can install a network device within five minutes.

The planning and implementation phases are critical to long-term success of a video surveillance system. A customer’s requirements and needs must be matched with the right architecture. Employing highly experienced engineers deploying the best networking equipment provides the right solution at the right price.

STAGE 3

Operational management

Proactive monitoring for network health

Post-deployment, video surveillance networks enter the operational management phase. This phase includes continuous monitoring of the system for performance, uptime and security, as well as regular updates to ensure optimal performance and regulatory compliance

Network monitoring tools are increasingly useful to end users to ensure smooth operation of a system. Monitoring provides more awareness of what's going on in the network environment, how power supplies are operating, how switches are performing, etc. Is there a spike in PoE or packets being lost? Monitoring provides early notice of a possible system failure, and helps explain any observed problem, whether it is a camera that is rebooting or a pixelated image.

Systems must be designed with a long-term view to infrastructure up-time. In video systems, lost video cannot be tolerated. The ALE Network Management portfolio features multi-tenant management, backup/restore, health checks and monitoring for large, on-premises organizations. Smaller end users or large distributed sites can use a cloud system.

ALCATEL-LUCENT ENTERPRISE'S NETWORK MANAGEMENT SOLUTIONS

OmniVista Enterprise
Dedicated on-premises management for large organizations

OmniVista Cirrus:
Subscription-based, cloud management for small end users and large distributed sites

Milestone Plugin
Integrates switch information directly with VMS for better visibility and control

* Source: https://resources.idg.com/download/cio-pandemic-business-impact-study

Monitoring tools are essential to keep track of network health, storage, and device performance. These tools help detect and mitigate issues before they lead to significant disruptions or security breaches. ALE's network management offerings include integrated templates for large end users in the on-premises, dedicated Alcatel-Lucent OmniVista® Enterprise system. For small end users and large distributed sites, the OmniVista Cirrus is a cloud-based, subscription-based network management service.

A service assurance solution from ALE enables remote troubleshooting for common camera issues directly from video management systems (VMSs) such as Milestone. For example, information about ALE's managed switches is available through integration with the Milestone XProtect VMS system using a plug-in. The OmniSwitch Milestone Plugin provides an additional level of control and visibility for the video network. If an end user is looking at a particular camera and there are quality issues, information about the associated switch is provided in the environment of the VMS.

ALE's native, open and easy-to-implement switch application programming interfaces (APIs) support a growing list of IoT device monitoring tools being used by integrators. ALE's Spacewalkers Developer Center gathers all available APIs or plugins. The R&D team provides clients, partners and any developers a single, central location for all ALE network solution APIs in order to streamline access to services and improve the user experience.

APIs open the door to using a variety of platforms to monitor network devices, so users and integrators can see the health of the cameras, the switches, the servers, etc. Providing insights into network operation in the context of a VMS system, for example, avoids operators having to look at multiple screens.

Effective fault management helps avoid downtime by identifying issues early. At the same time, proactive cybersecurity management, such as patching vulnerabilities, is necessary to prevent unauthorized access and data theft. The concept of "set it and forget it" does not apply.

Operational management is essential in avoiding network vulnerabilities and minimizing risks.

Integrators should consider cybersecurity insurance and compliance as part of this stage to safeguard both the network and the end user from financial liabilities.

STAGE 4

Troubleshooting and maintenance

Minimizing downtime and costs

As the network operates, routine troubleshooting and maintenance are necessary to ensure system uptime. Maintenance activities typically include firmware updates, system patches and hardware inspections, all designed to extend the lifespan of the network.

Scheduled maintenance, such as firmware upgrades and security patches, can significantly enhance network reliability.

In mission-critical applications, uptime is paramount. Integrators can boost system resilience through redundancy setups, where multiple systems back each other up to avoid data loss or system failures during maintenance.

Video systems must be operating all the time, and systems cannot be taken down even for firmware upgrades, for example. Designing redundancy into the system enables managing system upgrades with no downtime: firmware can be installed while a redundant system is carrying the video load.

Helping to keep systems running are ALE's Limited Lifetime Warranty and available Enterprise Support Agreements – one year for deployment assurance and five years for service assurance.

ALE's Software Toolkits, designed for the integrator, reduce troubleshooting from 48 hours to minutes, including PoE management and a simplified management and health check before the technician leaves the site. The PoE wizard verifies every PoE device on a switch and diagnoses and resolves common PoE problems with one click. The "Auto Ticket" capability enables low-level debugging, automatically resets ports, and collects required technical information until human Tech Support can respond. A "Traffic Analysis" module checks the network for common problems and saves the analysis results for expert review (or provides an intelligent data feed for AI).

Software provides an overview of a network's switches to anticipate potential failures even before they happen. Troubleshooting and monitoring of a network ensures that cameras are online and operating correctly versus only finding out a camera is malfunctioning when there is missing video.

Integrators can access their customer's networks remotely to ensure they are operating as intended. An integrator can offer remote monitoring of a system on a subscription basis to generate additional recurring revenue.

STAGE 5

Upgrade and optimization

Adapting to technological advances

Over time, as technology progresses, security networks must be upgraded to handle increased data loads, higher-resolution cameras, and enhanced analytics capabilities. This Optimization phase is an opportunity to integrate new tools and improve network efficiency.

Upgrades to storage, servers and networking hardware keep the network capable of handling increasing data demands. Advanced video analytics and AI applications, for example, require higher storage and processing capacity. By upgrading equipment in phases, integrators can manage costs while staying technologically current.

Emerging AI tools can provide valuable insights into network health, user behavior, and security trends. Integrators can implement these tools to anticipate and resolve potential issues before they become serious, thus optimizing network performance.

A new development is the Alcatel-Lucent OmniVista Network Advisor, which leverages AI to provide an intelligent and autonomous system including real-time network monitoring and alerts for potential risks and network remediation.

STAGE 6

Compliance and documentation

Meeting security standards and regulations

There is no physical security without cybersecurity. Any cybersecurity liability has a resulting physical security liability, such as if a camera watching a door is remotely disabled.

Maintaining up-to-date documentation for each component and network configuration ensures easy troubleshooting and smooth upgrades. Regular security audits are crucial to assess vulnerabilities and confirm compliance with regulatory requirements.

With growing regulatory demands and security standards, documentation and compliance management have become integral to the network lifecycle. Many organizations now require video surveillance systems to comply with cybersecurity standards for insurance purposes.

Cyber-insurance policies are essential, especially for industries with sensitive data. Integrators should ensure that the surveillance network complies with the requirements of cyber insurance policies to mitigate risk.

Compliance and thorough documentation help integrators respond to evolving regulatory needs, strengthening the network against both external threats and liability risks. ALE provides tools and guidance for integrators to meet cybersecurity and documentation requirements effectively. Our advanced support helps integrate compliance processes into the network lifecycle seamlessly.

STAGE 7

Decommissioning and redeployment

Concluding the lifecycle responsibility

The final phase of a video surveillance network's lifecycle is decommissioning, which involves securely phasing out outdated components and preparing for new installations. This stage is critical to ensuring that end-of-life components are handled responsibly, thus avoiding potential data security issues.

When decommissioning a system, data must be securely migrated to new hardware or archived according to regulatory standards. Any equipment containing sensitive information should be wiped and disposed of in line with data privacy laws.

Replacing old components with new, more advanced equipment allows for continuous improvement without interrupting service. Many organizations opt for a phased approach to upgrading, allowing them to integrate newer technologies gradually, such as AI-based analytics or next-generation cameras.

This phase ensures that security networks continue to meet evolving needs efficiently and responsibly.

Lifecycles depend on the customer's needs

In some cases, customers follow a standard three-to-five-year lifecycle, refreshing equipment within that time period. End users may be working around "rolling budgets" that replace servers, switches and other equipment every three to five, or even seven years. Other customers seek to stretch out the lifecycle and use equipment longer.

Some customers are aware of product and system lifecycles, while others have to be educated on how to manage systems over time.

Rapid technology development also impacts lifecycle considerations. For example, cameras may be replaced before end-of-life in favor of newer models offering features such as better resolution or AI analytics. Building a more robust network can help to anticipate the need to switch out cameras, in effect, future-proofing the network infrastructure.

In some cases, over-engineering elements of a system can prepare for future expansion and worst-case scenarios during a system's lifecycle.

A move toward managed security services, in which integrators commit to long-term maintenance of a system for a monthly fee, is also a growing trend.

End users increasingly are seeking to budget recurring operational expenses (OPEX) versus a one-time capital expenditure (CAPEX). If the integrator is responsible for ongoing maintenance costs, it behooves them to use the best equipment with the best warranty to ensure fewer expensive "truck rolls," and thus lower the cost of the service they have committed to provide.

The value of a lifecycle approach for video surveillance networks

Adopting a lifecycle approach to video surveillance networks benefits both security integrators and end-users by enhancing system reliability, security and cost-effectiveness. In a world where surveillance systems are increasingly complex and critical, a structured lifecycle approach is essential for maximizing the value of these investments.

Equipment that delivers value throughout the technology lifecycle paves the way for integrators to succeed as embedded service providers for their customers. Quality equipment makes it economical for an integrator to provide long-term service for a fixed fee, guiding the customer as they upgrade and tweak their design and promoting a partnership that enables integrators to retain customers longer.

As cybersecurity, AI and IoT continue to shape the future of video surveillance, network lifecycle management will play an even more critical role. For security professionals looking to maximize the utility and longevity of their surveillance systems, embracing the full network lifecycle is not just a recommendation—it's a necessity.

Alcatel·Lucent Enterprise