# Future-Ready Network Design for Physical Security Systems

## Avoid under-designing and overspending on physical security system networking

Version 1.7 – November 2024

**By Ray Bernard**
Independent Security Consultant
and Industry Analyst

© 2024 RBCS.

# Table of Contents


Introduction ..... 3

Traditional LANs ..... 3

Physical Security System Adoption of IT ..... 3

The Impacts of Artificial Intelligence ..... 4

Networking Terminology ..... 5

Types of Networks ..... 5

Internetworking ..... 6

Evolution of Network Design ..... 6

Hierarchical Network Design ..... 8

Hierarchical Network Design Concepts ..... 8

Hierarchical Network Layer Functionality ..... 9

Hierarchical Network Success ..... 11

Top-Down Network Design ..... 12

Critical Top-Down Design Misunderstanding ..... 13

A Common Design Shortcut ..... 15

General Purpose vs. Purpose-Built LANs ..... 15

Network Models and Security System Size ..... 18

Network Model Usage ..... 18

From Traditional LAN to a Modern Security System LAN ..... 19

The Modern LAN ..... 20

The Six Modern LAN Principles ..... 21

Modern LAN Network Design Roles ..... 24

Example Modern LAN Deployments ..... 26

Example 1: Large Government Agency 10,000 Camera Deployment ..... 26

Example 2: Maximum Security Prison ..... 27

Example 3: Leading Global Jewelry Chain ..... 28

Example 4: Spanish Retail Giant Massive Security Upgrade ..... 28

Example 5: Large Cruise Line Security Camera Deployment ..... 29

Acting on Modern LAN Contribution Opportunities ..... 29

Initial Steps ..... 30

Vendor Evaluation ..... 30

**Appendices** ..... **32**
Appendix A – Product and Manufacturer Mentions ..... 33
Appendix B – Cable Reuse Opportunities ..... 35
Appendix C – What Today's Architects Want to Know ..... 37
Appendix D – Wireless Networking ..... 43
Appendix E – Cloud VMS Modern LAN Example ..... 44
Appendix F – Secure and Manageable Physical Security Systems ..... 50
Appendix G – What Is a Future-Ready Network? ..... 60
Appendix H – Acknowledgements ..... 63
**About Ray Bernard** ..... **65**

# Introduction

At earlier points in time, physical security system capabilities – and thus their value – were always constrained by the technology limits of the time. Fortunately, that era has ended. We are now embarking on a time when, due to increasingly rapid technological advancement, our own knowledge and design thinking have become the main limitations.

The rate of this technological progression is staggering. To put it in perspective, 40 years ago, ten 18-wheeler trucks could not carry enough computer equipment to rival the radio-enabled multi-purpose computer platforms we now casually slip into our pockets and call "phones."

*So, in light of such rapid technology growth, why are we still building physical security system communication infrastructures using 40-year-old network designs? And what's more important, what should we be doing now?*

# Traditional LANs

## Physical Security System Adoption of IT

At this point in information technology advancement, it is crucial to examine how the physical security industry finds itself using office LAN architectures that make many security system network deployments overly complicated and too costly.

IT adoption in the physical security industry began in the late 1980s and early 1990s with the introduction of front-end computer software for user interaction. This software was essential to manage the increasing number of security devices and to respond effectively to information regarding access events (intrusion and access control) and activity in surveilled areas (video). At that time, PCs were linked to controllers using twisted-pair wires, typical in industrial systems. Similarly, the connections between access and intrusion controllers and their field devices also used this wiring. Video cameras were connected to monitors and recorders via coaxial cable (more commonly called "coax cable").

Later, the business world embraced multi-user client-server software, setting a new standard. This change led to a different approach in connecting security workstations and servers - they started using wired Ethernet. This method either mirrored or tapped into the existing business network infrastructure. As this network grew and the integration of physical security with IT advanced, access controllers adapted to become IP-enabled. This development allowed for a more practical use of the structured cabling found in office and industrial buildings. Now, security server computers could connect to security system

controllers through an Ethernet LAN in the same way they connect with printers, scanners and other computers.

The security system landscape changed even more in 1996 when Axis Communications introduced the IP camera. Network bandwidth expanded from 10 Mbps to 100 Mbps and eventually to 1 Gbps – needed by some network video recorders (NVRs) or video servers, but much more than any single camera would need. These advancements facilitated the transition from digital video recorders (DVRs) having coax cable camera connectors to NVRs with Ethernet ports. Subsequently, video servers began to replace NVRs. These changes accelerated the security industry trend to IP-enabled devices.

## The Impacts of Artificial Intelligence

Artificial intelligence (AI) software is transforming numerous industries, including physical security. Here, AI is utilized for advanced video content analysis, including video analytics, facial/license plate recognition, and behavioral pattern recognition. Historically, the focus in camera technology has been on continuously increasing image resolution. However, this approach has begun yield diminishing returns in terms of its security benefits. AI advancements in video content analysis, on the other hand, enable the management of large-scale security operations with fewer staff members, although this approach necessitates a higher initial investment in camera technology. This shift towards AI-enabled devices is resulting in a significant rise in the deployment of networked security devices.

AI brings an unparalleled level of precision to device capabilities. It excels in recognizing people and objects, as well as in system-level identification of emerging risk situations and assessing events in real-time. AI can collect, integrate, and analyze real-time data streams at volumes and speeds beyond human capability. This greatly enhances human situational awareness and enables automated, instantaneous responses to events and situations on multiple levels.

Consequently, there is an increasing trend towards implementing a variety of intelligent building and outdoor sensors. In some large facilities, this trend has resulted in a doubling of camera counts. This increase is due to the substantial security, safety, and business operations value of the data. As the number of sensors and intelligent devices grows, the scale of the network infrastructure correspondingly expands, mostly with devices that have low bandwidth requirements.

Given the security industry's strong shift to IP-enabled field devices and the utilization of IP-enabled sensor devices and systems, it is important to understand how the current IT approach to network design came about and why it doesn't make sense now.

## Networking Terminology

One objective for this eBook is to minimize the use of network terminology that will ordinarily not be familiar to non-network-savvy readers. However, because the use of some technical terms is necessary, we're starting of  off the discussion of networking with a small set of definitions. These will provide a common frame of reference regarding issues that do involve specific aspects of network design. Also, across the huge landscape of network design documentation and guidance, some networking terms have been given different and even conflicting meanings, and some terms are used interchangeably when they don't actually mean the same thing. That's another reason for providing definitions before entering into the discussion of networking.

> **Network:**
>
> **(1) Operational Definition.** From the end-user perspective, a network is a collection of electronic devices, like server and workstation computers, laptops, tablets, printers, scanners, and so on, that are connected together using wired and/or wireless data transmission. This connection enables their users to share information, access data files, and use shared resources like printers and Internet access. In simpler terms, it's like a community of electronic devices working together to make tasks like sending emails, creating and printing documents, viewing streaming video services otherwise accessing the Internet easier and more efficient for the user.
>
> **(2) Technical Definition.** In simple summary, a network is just the wired and wireless connections, and the equipment that makes the connections possible. This infrastructure includes routers, switches, modems, cabling systems, wireless access points, and network protocols that act as the unseen but essential backbone of the network. Unlike the computers and other devices used directly by end-users, this technical infrastructure operates largely in the background, ensuring that data flows smoothly and securely from one point to another within the network. The term "network" can refer to a single small network or a set of several connected networks.

*In this eBook, "network" refers to the technical definition above.*

### Types of Networks

Initially, networks were small, and connected equipment was in close proximity. As networking technology advanced, small networks were labelled Local Area Networks (LANs) and similar labels were established to characterize larger networks of various types and sizes. A few such labels as used in this eBook are:

- **Backbone network:** A high-speed high-capacity network used to connect a number of LANs or other networks together.
- **Building Network:** Multiple LANs within a building, usually connected by a building-backbone network.
- **Campus network:** Multiple building networks within a local geographical area (typically within a few miles), usually connected by a campus-backbone network.
- **Enterprise network:** A large and diverse network, consisting of buildings and/or campuses, remote access services, and one or more Wide Area Networks to connect the building or campus networks together.
- **Wide Area Network (WAN):** A large backbone network connecting networks across wide geographical areas such as cities, states, or even countries.

### Internetworking

Originally a network meant an individual LAN or a backbone network that connected LANs. The term internetwork referred to one or more networks connected together, typically by a backbone network. The overall field of network design was called “internetworking.” However, that term was too big a mouthful to keep repeating often, and so it in practical usage it was shortened to “Networking”, which was meant to refer to working with one or more networks of any size or type.

The Internet, of course, is the world’s largest internetwork and has over 5.3 billion users. Its name is a shortened version of “internetwork” and is sometimes less formally referred to as “the Net.” The Internet has now become a very common means of connecting widely geographically dispersed networks. *With the continuing growth of cloud computing, the Internet is quickly becoming a major element of physical security system networks.*

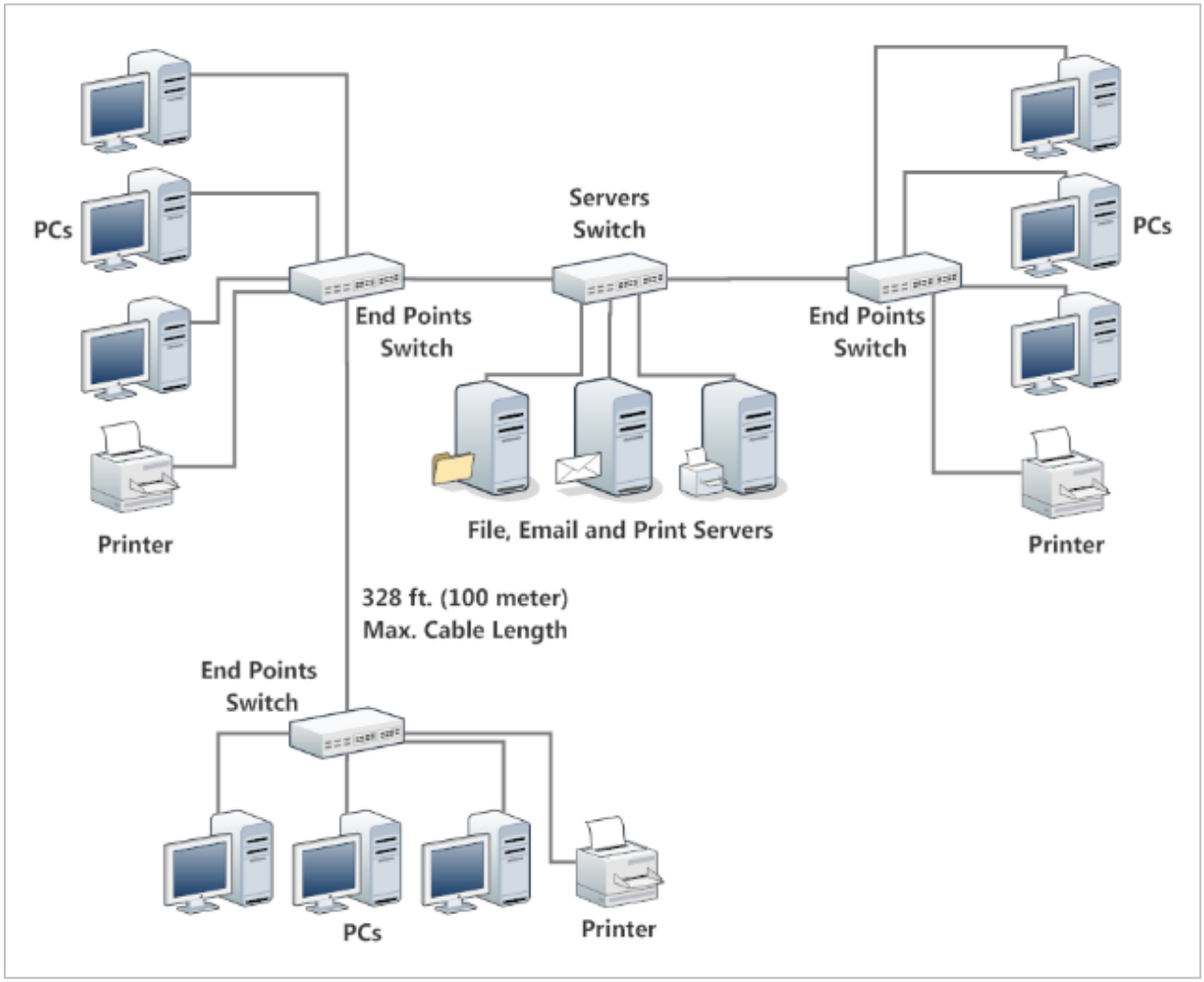
## Evolution of Network Design

The earliest business networks featured what we now call a 'flat' design, which was effective for the small scale of early networks. This approach is still used in very small networks today, as it remains suitable for their limited size. Refer to Figure 1 on the following page titled, “Flat Network Topology.”

In this configuration, PCs and printers share the same bandwidth. However, servers that require higher network bandwidth can be connected to their own switch capable of providing greater bandwidth. Thus, in a flat network, it's common to encounter two levels of bandwidth: one for servers and another for all the endpoints like PCs and printers. A flat network can work well for small physical security systems.

In this flat network example, note that even though printers do not require as much bandwidth as PCs, it is more cost-effective to connect printers to the same switches used by PCs. This is because the PC switches often have unused ports, effectively making the additional bandwidth for printers free. This approach is more economical than purchasing separate, lower-bandwidth switches for each printer. *It is characteristic of most office networks that the bulk of endpoint devices share the same bandwidth requirements. This is an important point that we'll refer back to later.*

***Figure 1. Flat Network Topology***




Over time, problems emerged as flat networks expanded significantly in size. A small flat network could grow through the addition of hubs and switches, evolving into a larger network. Yet, as the size increased, it became difficult to filter out unwanted traffic and control network traffic flow. This led to network congestion, slower response times, and deteriorating network performance. Additionally, troubleshooting became difficult because it often required inspecting the entire network, since no part of the network was

segregated from any other part. Business information system networks and large security system networks share the same challenges.

## Hierarchical Network Design

Eventually, as business networks continued to grow in size, the need for a new network design became evident. First mentioned as a "Hierarchical model" in a Cisco white paper in 1998[1], and broadly announced as *Hierarchical network design* by Cisco in 2002, has since been adopted as an industry-wide best practice. This concept is renowned for its ability to develop networks that are not only reliable and scalable but also cost-effective. Currently, this design concept is a standard part of the curriculum in colleges, universities, and technical schools. It's a straightforward concept that is particularly well-suited to office networking environments.

> Understanding the simple concepts behind hierarchical network design, will enable physical security technologists to how see it has been unintentionally misapplied to the design of large scale physical security system networks.

The most common hierarchical network design has three layers (described below), whose basic concepts are understandable even to non-technical readers. First, we'll examine a typical business office networking scenario, and then we'll contrast that with a physical security system scenario.

### Hierarchical Network Design Concepts

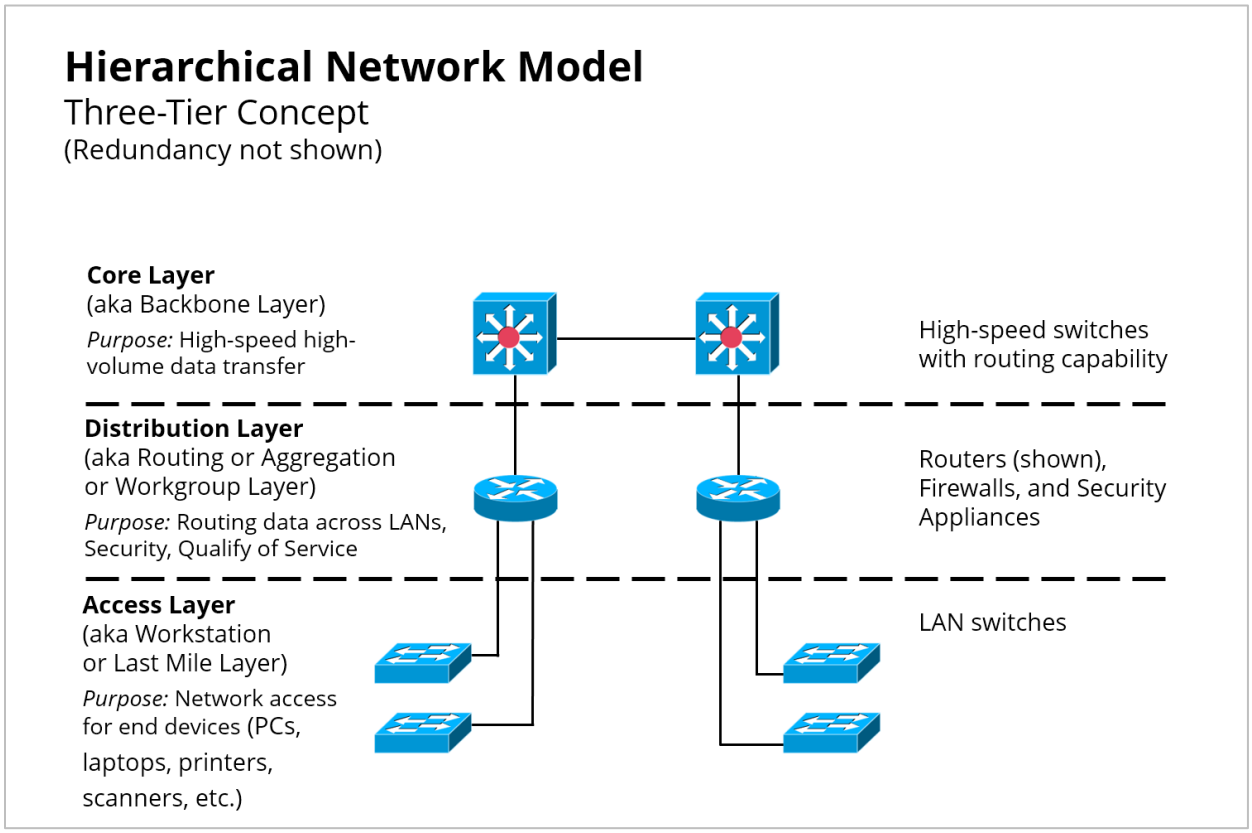
A hierarchical design separates a network into distinct layers, where each layer has specific functions that define its role in the network. Network designers can then choose the optimal hardware, software, and technical capabilities required for each layer's specific role. In large organizations most hierarchical network designs utilize three layers: core, distribution, and access.

The diagram in Figure 2 below is how hierarchical networks are typically presented visually, except that instead of using typical network diagram symbols alone, text explanations are to convey the purpose and functionality of each layer. To keep the depiction simple, we are

[1] Haviland, Geoff. "Designing High-Performance Campus Intranets with Multilayer Switching." Cisco Systems. Archived from the original (White Paper) on 2000-11-09. Retrieved January 17, 2024. https://web.archive.org/web/20001109064100/http://www.cisco.com/warp/public/cc/so/cuso/epso/entdes/highd_wp.htm

not showing the typically redundant elements, which double the core and distribution layer equipment and cross connect all the equipment to eliminate single points of failure.

*Figure 2. Hierarchical Network Concept*




## Hierarchical Network Layer Functionality

Each layer has important functional characteristics, which are described below.

1. **Core Layer (also known as the Backbone Layer):**

   The core layer is the central part of the network, responsible for providing fast, high-capacity transmission. It connects different parts of the network, such as various buildings or areas in a large campus or enterprise network. The core layer incorporates a collection of devices that maintain high performance by each performing only a single function. Example such single-function devices are firewalls, DHCP servers, routers, and equipment for connections to Internet Service Providers (ISPs).

   This approach ensures that the core is capable of transporting large amounts of traffic quickly and reliably. The core layer is designed with a high level of redundancy and aims to minimize downtime. While typically featuring a small set of functionalities, the devices in this layer are among the most powerful in the network, focusing primarily on the speed of traffic flow. The core layer avoids

network device CPU-intensive packet manipulation, which is caused by processes such as security inspection, quality of service (QoS) classification, or other similar tasks.

The core layer's scalability is typically achieved by using faster equipment, rather than more equipment, to maintain the network's high performance.

2. **Distribution Layer (also known as the Routing Layer or Aggregation Layer or Workgroup Layer):**

The distribution layer offers policy-based connectivity and regulates the boundary between the core layer and the access layer. Policies include access control (to permit or deny traffic based on specific criteria such as IP addresses, MAC addresses, protocols, or port numbers), quality of service for prioritizing critical and low-latency traffic over other traffic, and firewalls. This helps to prevent unauthorized access and mitigate potential security threats. It's where routing and data filtering takes place. Distribution layers aggregate (group) the traffic from access layers and distribute it into the rest of the network. Distribution layers can implement redundant connections to the core layer and to access layer switches. This redundancy ensures high availability and reliability, as traffic can be rerouted in case of a link or device failure.

There are two ways that the distribution layer may need to be scaled up. First, to expand connectivity, such as by adding more switches or/or replacing switches to increase in the number of connection ports available to the other two layers. Second, to increase its capabilities, such as for managing quality of service (QoS) or handling new types of network traffic such as virtual LAN (VLAN) traffic routing, increase security functionality or enhance network monitoring and management capabilities.

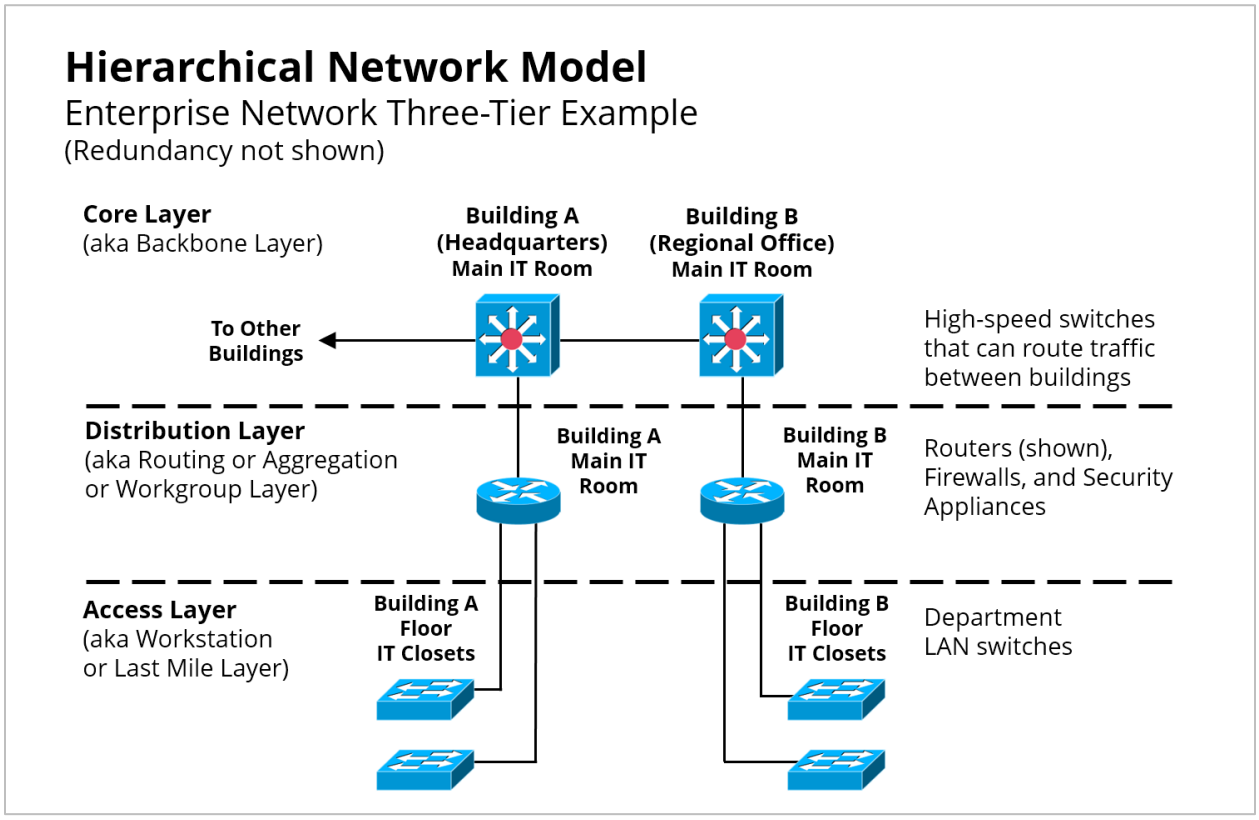
3. **Access Layer (also known as the Workstation Layer or Last Mile):**

The access layer is where endpoints such as PCs, laptops, smartphones, printers, scanners, and local servers are connected to the network through wired Ethernet and WiFi. The access layer provides users with network access via their devices. It's typically where network access control is performed and policies are enforced, such as port security and address assignment. Due to the number of end-user devices connecting to the network, there tend to be more switches on the access layer than the other layers in a typical hierarchical network design. This layer provides Power over Ethernet (PoE).

The access layer scales out (more device capacity) by adding more switches to accommodate more connected devices, for example, if more employees are given

company laptops. It scales up (higher connection speeds) by replacing existing switches with faster switches, if the intention is to increase the connection speed to some or all devices. This commonly happens when an organization refreshes all its laptops by replacing them with machines that can connect at a higher speed.

*Figure 3. Enterprise Network Example of Hierarchical Design*




## Hierarchical Network Success

The hierarchical network approach is highly valued for its scalability, reliability, and manageability, making it suitable for a variety of networks, including those in corporate, government, healthcare, retail, and educational institutions. *For decades, the primary challenge in network design has been to increase bandwidth to PCs from server rooms, data centers, and more recently, the Internet. This is especially true now due to the widespread use of video streaming such as for marketing purposes and Zoom-style video conferencing.* However, in a medium or large business physical security system there are many more devices to connect to the Access Layer than there are end user computers.

When there are hundreds of cameras or thousands of security devices to support, the important objectives in physical security system network design, for both cost and performance reasons, are different from office networks and require closer attention. It is crucial to accurately characterize device network traffic requirements so that devices with

similar networking requirements can be given their own right-sized LANs, avoiding excessive bandwidth cost and simplifying security and troubleshooting.

## Top-Down Network Design

The application of the hierarchical network model required a more comprehensive approach to network design than had been taken in the past by network designers. Cisco developed such an approach and called it *top-down network design*. It is documented very well in the book *Top-Down Network Design*, by Priscilla Oppenheimer and published by Cisco.[2] It is now in its third edition.

The top-down network design approach comprises four steps:

1. Analyze the End User and Technical Network Requirements
2. Develop the Logical Network Design
3. Develop the Physical Network Design
4. Test, Optimize, and Document the Network Design

As Oppenheimer states in her book, "Top-down network design is a methodology for designing networks that begins at the upper layers of the OSI reference model before moving to the lower layers."[3]

**IMPORTANT NOTE:** OSI stands for *open systems interconnection* (OSI) model. A very understandable and also technically accurate description is the illustrated explanation provided by Cloudflare on it's *What is the OSI Model?* page. *Go to that page and read the explanation presented, then come back here and continue with the Top-Down Network Design discussion.*

As Cloudflare states on that page, "The OSI provides a standard for different computer systems to be able to communicate with each other. The OSI Model can be seen as a universal language for computer networking. It is based on the concept of splitting up a communication system into seven abstract layers, each one stacked upon the last."

In a nutshell, it starts at the top layer with the human-computer interaction, and proceeds down from there with how the data (be it text in some format, pictures, voice or video) goes from the human-understandable format down into a *zeros and ones* binary format that can be securely and reliably communicated as electronic signals across a wire, and then goes back up again to arrive in the original human-usable form.

It is the most understandable yet technically accurate description that this author has seen. *If you are already a techie who fully understands the OSI model, read the Cloudflare page*

[2] Oppenheimer, Priscilla. *Top-Down Network Design, Third Edition* (Indianapolis: Cisco Press, 2011).
[3] Oppenheimer, 4.

*anyway as it will change the way you think and communicate about networks to non-technical people, some of whom are important stakeholders to your network projects.*

The OSI model layers are presented below for simple future reference.

***Figure 4. Open System Interconnection (OSI) Reference Model***

| Layer | Name |
|---|---|
| Layer 7 | Application |
| Layer 6 | Presentation |
| Layer 5 | Session |
| Layer 4 | Transport |
| Layer 3 | Network |
| Layer 2 | Data Link |
| Layer 1 | Physical |

## Critical Top-Down Design Misunderstanding

The Top-Down design approach for networks is often discussed in the context of hierarchical network design. Typical hierarchical design diagrams look like those in Figure 2 and Figure 3, which show the three typical layers: core, distribution and access. This has led many people to believe that top-down design means starting with the core layer first, then designing the distribution layer, and finally the access layer. Often the design process then begins with a logical outline of the network, followed by physical network design of the core, distribution and access layers.

As Oppenheimer says in her *Top-Down Design* book, "In the fast-paced presales environment of many systems engineers, it often is difficult to slow down and insist on a top-down, structured systems analysis approach. Wherever possible, this book includes shortcuts and assumptions that can be made to speed up the network design process."[4] One of those shortcuts is very relevant to physical security system network design, as mentioned on the following page.

The structured systems analysis approach in Oppenheimer's book consists of the four steps listed on the previous page. A critically important point is that the top-down design steps are intended to be applied to the design of *each layer within the hierarchy.* In fact, Oppenheimer makes the following explicit statements regarding the design approach for large networks, which are presented here with italic emphasis added for this eBook:

> "With large network design projects, *modularity is essential*. The design should be split functionally to make the project more manageable. For example, the

[4] *Oppenheimer, xxiii.*

> functions carried out in campus LANs can be analyzed separately from the functions carried out in remote-access networks, virtual private networks (VPN), and WANs."[5]
>
> "Cisco recommends *a modular approach* with its three-layer hierarchical model. This model divides networks into core, distribution, and access layers."[5]
>
> "With a structured approach to network design, *each module is designed separately*, yet in relation to other modules. *All the modules are designed using a top-down approach* that focuses on requirements, applications, and a logical structure *before the selection of physical devices and products to implement the design*." [5]
>
> "Finally, one other guideline for hierarchical network design is that *you should design the access layer first, followed by the distribution layer, and then finally the core layer*. By starting with the access layer, you can more accurately perform capacity planning for the distribution and core layers. You can also recognize the optimization techniques you will need for the distribution and core layers."[6]
>
> "You should design each layer using modular and hierarchical techniques *and then plan the interconnections between layers based on your analysis of traffic load, flow, and behavior*."[6]
>
> "As you select technologies for each layer . . . you might need to go back and tweak the design for other layers. *Remember that network design is an iterative process*." [6]

Unfortunately, most of the IT network designers involved in physical security system network design follow their very strong but incorrect belief that proper design starts with the core layer, proceeds to the distribution layer, and ends with the access layer. That can work in office and campus network design because there are few end user device types and they basically all have the same network traffic profiles. There is not much homework to be done there and they have basically already done it on earlier projects.

Those assumptions do not fit the critically different access layer requirements of physical security systems, and violates the top-down design approach of beginning with the user and technical requirements, with are derived from the access layer's needs.

*It is the failure to accurately capture both the user and technical requirements (i.e., the access layer requirements) that has led to the under-designing of and over-spending on medium and large size electronic physical security system networks.*

[5] Oppenheimer, 5.
[6] Oppenheimer, 130.

### A Common Design Shortcut

A common, useful and usually-valid design shortcut is to utilize aspects of an earlier network design project on a later project. When commonalities in network requirements across two different network design projects makes this feasible, is it a smart idea that avoids needlessly redoing design analysis work. This practice is one reason why the rigorous analysis steps of top-down design do not get applied to physical security system network design.

> It is the failure to accurately capture both the user *and technical requirements* that has led to the under-designing of and over-spending on medium and large size electronic physical security system networks.

Network designers unfamiliar with differences between office networking and physical security system networking can, for example, mistakenly assume that because the same makes and models of network equipment used in an earlier project are being used on a security system project, that aspects of the network design from the earlier project can be applied also. It happens almost as an unconscious action, which can be due to unfamiliarity with security system networking requirements or exposure to inappropriately designed physical security system networks.

Sometimes, property owners, managers, and facility engineers are led astray by an incorrect assumption. They sometimes believe that since office computers, building control system computers, and security system computers and controllers all use the same category of network cable (typically between Cat 5 and Cat7a), a single network design will suffice for all systems.

There are fundamental differences between office networking designs for general purpose computers and networks for electronic security system equipment. Let's examine some key differences.

## General Purpose vs. Purpose-Built LANs

*Office LANs are general purpose networks.* In a general purpose network, performance (bandwidth) must be deployed even where it won't always be used. For example, a conventional WiFi network will provide gigabit speeds to all wireless access points, even if there are few or no clients connected to the access points. As mentioned earlier, office

LANs provide gigabit speeds to printers and other devices that don't need it, because there aren't enough of that kind of device to warrant creating a separate LAN for them.

*Office LANs are general purpose networks. In contrast, security system LANs are purpose-built networks.*

Additionally, general purpose LANs must support all kinds of network traffic going back-and-forth anywhere on the network. Business needs change from year to year, and the network designers have only a general idea of what specific kinds of traffic will go where, and how much of it there will be. End user devices, especially smartphones, are replaced by end users when higher-performing devices become available. So, network design often focuses primarily on speed out to each endpoint as the primary way to ensure user satisfaction.

*In contrast, security system LANs are purpose-built networks.* The nature of security system LANs is different from office LANs in several important ways.

1. **Endpoint Device Product Life.** Unlike PCs, laptops, and smartphones, most security system devices have a useful product life of 10 to 15 years. The devices don't change, so their network requirements remain the same throughout their product life. Security system LANs can be designed around the requirements of the specific devices. Low-bandwidth devices, like access card readers, intrusion detection sensors, and other IoT sensor systems (such as for occupancy detection and lone-worker activity sensing) are well-served by low-bandwidth networking, whose equipment has a lower cost than high-bandwidth equipment. When there are hundreds or thousands of such devices, the cost savings definitely add up.
2. **Right-Sized LAN Performance.** Security system LAN switch configurations must be fine-tuned for exactly the kind of traffic they will handle. Video data packets from security surveillance high-megapixel cameras are typically large and utilize different network protocols than card readers, sensors, and intercoms. Quality of Service (QoS) requirements are different for each category of devices. There are enough of each device type to create LANs for different device types. It is simpler to design a high-performance LAN when it's purpose-built for a specific type of device.
3. **Simple Network Paths.** Security systems have much simpler network paths than general purpose networks. Let's compare a state university's video pathing to that of a large security system.

   ***State University Video Scenario.*** In state university with 18,000 students living on-campus, imagine the network requirements for Internet-based video streaming. If only 10% of the students are watching educational or entertainment videos at a single time, the network's Internet connection must manage all those video streams,

with the potential for multiple different video streams to flow to any one of the campus WiFi access points. Over a thousand different end user devices will be receiving incoming video. There will be one source of video streams entering the network, the Internet connection. There will be thousands of potential endpoint devices (laptops, tablets, smartphones, and TVs) receiving video traffic located all over campus. There is no way to physically segregate video traffic from other traffic going to a user's device. The general purpose network must support all traffic types across all endpoint connections. The network's distribution and core layers are very busy not just with video traffic, but with many types of user activity, including email, web browsing, and gaming. It's a complex picture.

***Security System Video Scenario.*** A large security system's networking scenario is reversed when it comes to video. The video traffic comes in not from one source, but from a thousand endpoint devices (cameras). The video traffic has one destination: the video recording servers. A dedicated LAN that is physically separate from the other security system LANs can be used to handle the video traffic. In fact, the camera LANs can be separate from the recording server LAN. Dedicated high-bandwidth network paths can connect to each camera LAN. The camera LANs themselves can be 100 Mbps LANs, while the recording server LANs can be very small 1 or 10 gigabit LANs. The video network traffic cannot interfere with other network traffic because it is physically isolated from it.

4. **LAN Capacity Planning.** As explained above in Simple Network Paths, up until now 80% or more of the physical security system traffic has remained within the overall security system network, because the traffic is both generated and stored within the network. However, this picture is changing due to the increasing adoption of cloud-based security system applications. Video data is the part of the traffic pattern that is changing, due to the transfer of video to cloud storage, where cloud-based video analytic applications may process it. However, in some cases, on-premises video analytic inferences engines (the part of AI that analyzes and draws conclusions from the video data) generate metadata for cloud storage and further processing in the cloud. The video data may or may not be stored in the cloud. It's a complex and evolving picture that increases the need for adaptability and scalability in various elements of security system edge computing and networking design.
5. **Cybersecurity.** It is easy to establish firewall protections between device LANs, because security device LANs deal with a specific traffic category of network traffic from specifically identified sources (devices, servers, and controllers) that don't change. Devices can authenticate each other using digital certificates. Firewalls can block all unauthorized and unexpected traffic. It's not feasible to do this kind of physical network segregation and cyber security protection with a general purpose

network. Cybersecurity for a large general purpose network is typically much more complicated than for well-designed a large security system network.

*Determining the endpoint requirements of a security system network requires a different kind of analysis than for a general purpose network . . .*

Determining the endpoint requirements of a security system network requires a different kind of analysis than a general purpose network like that of a college campus network. This is why, when the top-down approach of hierarchical network design is applied to security system design, the network designers – typically lacking expertise in security system endpoint devices and constrained by the 328 ft. (100 meter) distance limitation of office LAN Ethernet cabling – frequently end up with a network design that is costly and yet does not result in a high-performing, trouble-free security system network.

## Network Models and Security System Size

As we saw in the State University vs. Security Video network comparison above, most video traffic in a campus network has the potential to travel anywhere within the network. In contrast, in a physical security system network, there is typically only one primary destination point for the video. In security systems, most endpoint device traffic is directed to specific controllers and servers, with minimal traffic traversing the entire network. Most of the action happens in the endpoint (access layer) portion of the overall network.

For this reason, many physical security systems are more practically served by a two-tier hierarchical design. This is known as the Collapsed Core design, where the core and distribution layers are merged into a single layer. The access layer gets a purpose-built design for each security system, and the nature and volume of its device LAN traffic sets the requirements for the combined core and distribution layer. Sometimes, there is no need for the core layer at all, such as for a single-building security system.

## Network Model Usage

As a general guideline rather than a firm rule, it can be helpful to categorize physical security system networks based on the number of security devices. Table 1 below shows common size categories and the network models typically applicable to them as recommended by Cisco.[7]

[7] Cisco Networking Academy, Connecting Networks Companion Guide (Indianapolis: Cisco Press, 2014), Online Sample Chapter available at: https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4. Retrieved January 17, 2024.

*Table 1. Network Size Categories*

| Category | Number of Devices | Typical Network Model |
|---|---|---|
| Small Network | 200 | Flat Model |
| Medium-Size Network | 200 to 1,000 | Collapsed Core Hierarchical Model |
| Large Network | 1,000+ devices | Three-Tier Hierarchical Model |

## From Traditional LAN to a Modern Security System LAN

Office LAN technology was not originally designed to support networked device deployments like those found in security systems. A key limitation of office LANs is the Ethernet cable length constraint: the cable between a device and its network switch cannot exceed 328 ft. (100 meters). As a result, network switch wiring closets (or Intermediate Distribution Frames, IDFs) must be strategically located throughout buildings to bring the switches within a viable distance of the networked devices.

When the top-down approach for hierarchical network design not correctly applied to security system design, network designers face challenges. Lacking expertise in security system endpoint devices and constrained by the 328 ft. distance limitation of office LAN Ethernet cabling, they frequently end up with network designs that are costly and fail to result in high-performing, trouble-free networks.

This Ethernet cable length constraint is well-known to professionals working with security system networks, who often resort to one-off solutions to circumvent the distance limitation. However, as the size of security system deployments continued to grow, these ad hoc, unmanaged workaround solutions proved inadequate, particularly for Internet of Things (IoT) device networks. In 2018, the global analyst firm Frost & Sullivan identified several important factors regarding the contemporary networking for IoT systems.

**Standards Advancement.** The industrial sector, through the Institute of Electrical and Electronics Engineers (IEEE), had evolved Ethernet standards beyond office LAN technology. Since 1980, when the first Ethernet standard was released, the IEEE 802.3 working group released over 80 LAN standards. Some have been used to meet industrial network needs, which often require network connections three or four times longer than office LANs.

**New PoE Capabilities.** IEEE 802.3 developed standards providing Power over Ethernet (PoE) capabilities over various cables, including CAT3, CAT5, CAT5e, CAT6, CAT6A, single twisted pair telephone cabling, and coax cable. IT network architects, generally unfamiliar with these advanced Ethernet standards used in Industrial IoT operations, often don't consider them for security system network design.

**Potentials for Cable Reuse.** Over the past 75 years, advancements in voice and data communications technologies have left many facilities with a significant amount of now-

unused cabling. This cabling can be repurposed for security system networking, significantly reducing the cost of new security systems and existing security system upgrades. This is especially true for video surveillance camera deployments and IoT sensor systems. Cable reuse represents a significant labor and materials cost-saving factor. See Appendix B titled, "Cable Reuse Opportunities."

**Environmental Considerations.** Networks based on traditional LAN design require a wide array of uninterruptible power supply (UPS) units spread throughout the facility. These units are expensive, hard to maintain, and environmentally unfriendly. An approach using modern networking technologies can optimize UPS deployment to devices that need it, thus providing a more sustainable approach to battery usage. These factors are very important to facility architects and engineers, as well as to facility owners.

**Need for New Network Design Practices.** The network design practices and assumptions for office LANs are not suitable for designing high IoT device-count networks, especially those requiring PoE network connections to extend well beyond 328 ft.

# The Modern LAN

These significant findings prompted Frost & Sullivan analysts to reassess the Internet of Things (IoT) landscape. Mirroring Cisco's realization in 2002 that large-scale networks required a new approach to network design, Frost & Sullivan recognized the need for a completely new design approach in a world increasingly shaped by digital transformation and an expanding array of IoT devices and systems. In response, Frost & Sullivan developed the Modern LAN design principles tailored to meet the specific requirements of security and other IoT networks.

*The Modern LAN principles have simplified the design of security system networks and significantly reduced deployment costs, by 40% to 80%, for medium- and large-scale implementations.*

Central to these principles is the adoption of Long-Range Ethernet (LRE) and Long-Range Power over Ethernet (LRPoE) technologies.[8] *The Modern LAN principles have simplified the*

[8] The term "Long Reach Ethernet", also abbreviated "LRE", was the name of a proprietary networking protocol marketed by Cisco Systems, intended to support 5 to 15 Mbit/s performance over telephone-grade unshielded twisted pair wiring over distances up to 5,000 feet (1.5 km). The full product name was "LRE/VDSL (Long-Reach Ethernet/Very-high-data-rate DSL)". It was introduced in 2001 and discontinued in 2006. Since then, both "long reach Ethernet" and "long range Ethernet" have been used by various to describe Ethernet extender products. *Except when quoting directly from third-party documents, this eBook uses the terms "Long Range Ethernet (LRE)" and "Long Range Power over Ethernet (LRPoE)", as generic references to Ethernet extender technologies, regardless of whether the individual products names include "Long Range" or "Long Reach."*

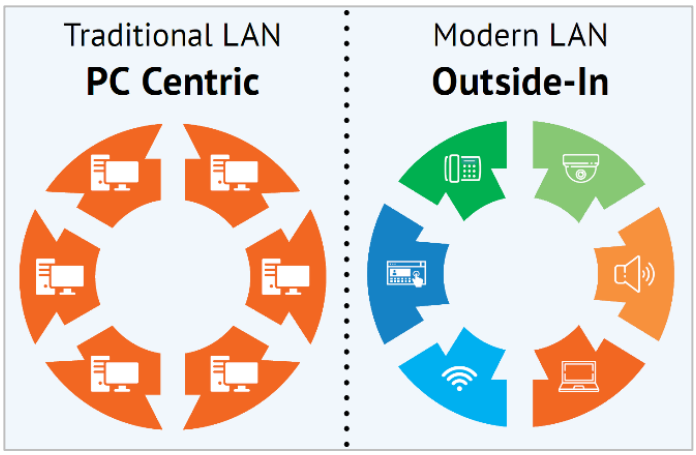
*design of security system networks and significantly reduced deployment costs, by 40% to 80%, for medium- and large-scale implementations.* The Modern LAN principles are fully consistent the network design principles and guidance presented in Oppenheimer's *Top-Down Design* book.

## The Six Modern LAN Principles

The Modern LAN paper was developed for all network designers who, these days, must deal with a myriad of IoT devices. For this eBook, the wording of these principles has been fine-tuned for applicability to physical security systems, and in some cases expounded on in more detail using an appendix.

**Principle 1: Take the Outside-In Approach.** Adopt an "outside-in" approach to local area network design and planning. In new system designs and when adding devices to existing systems, identify the power, bandwidth, and application requirements of each unique physical device to determine the best network topology and infrastructure to support it. See Figure 5, *Traditional LAN vs. Modern LAN Design Approach*.

*Figure 5. Traditional LAN vs. Modern LAN*



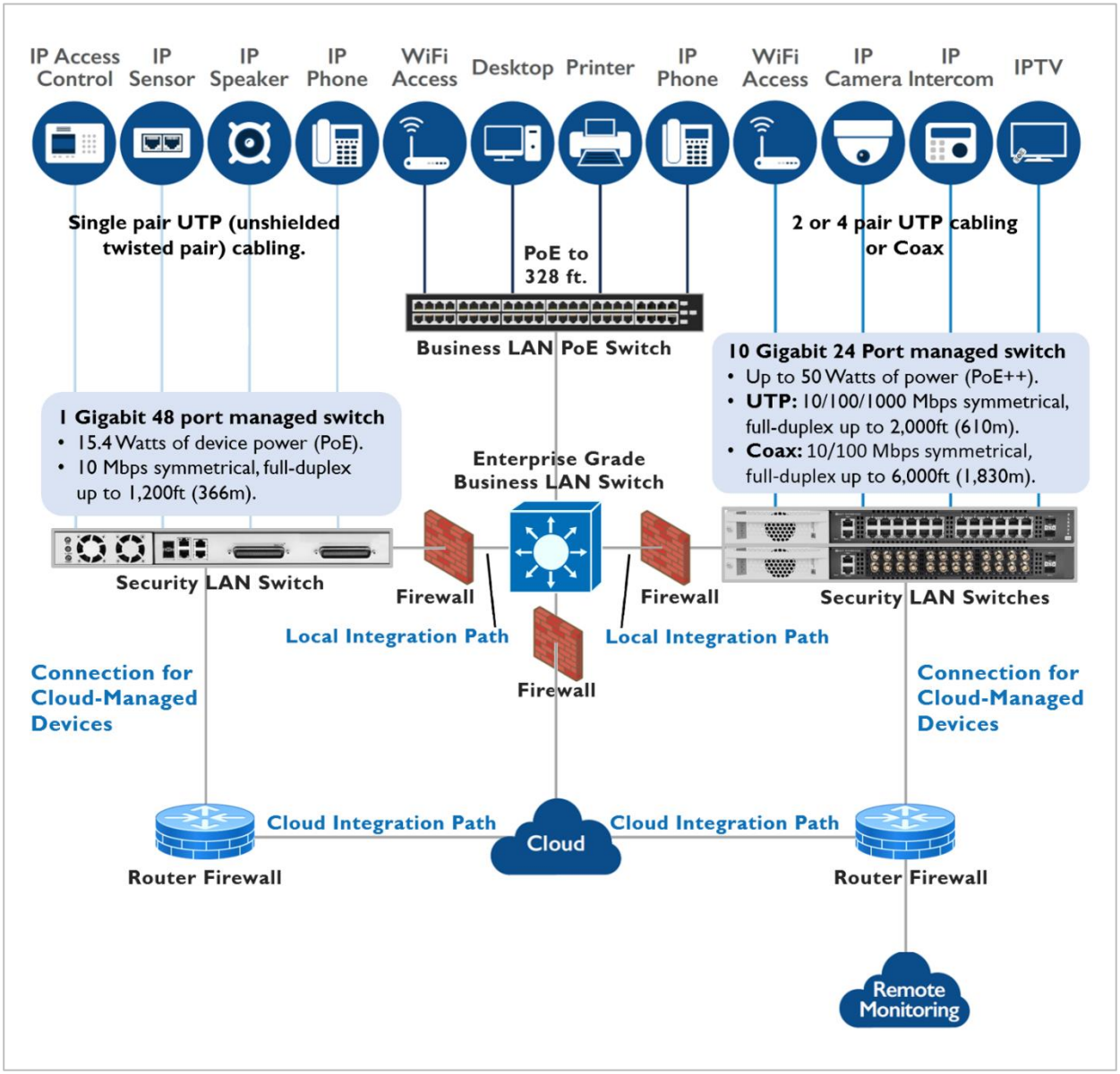

Consider the impacts of all additional endpoints and applications on the network to ensure overall reliability, security, and ease of management today and into the future.

As explained in the *Top-Down Design* book, by starting with the access layer you can more accurately perform capacity planning for the distribution and core layers and recognize the optimizations needed for them.

**Principle 2: Design for Security and Management.** Create secure and robust local area networks that are easy to configure, deploy, manage, and troubleshoot. Ensure systems integration flexibility by allowing for separate, on-premise, or Cloud-based integration; simplifying LAN management, and minimizing core network breach risk. See Figure 6 below, "Modern LAN Network Architecture Applied to Physical Security Network Design." Also see Appendix F titled, "Secure and Manageable Physical Security Systems."

**Principle 3: Maximize Efficiencies and Reduce Complexity.** Maximize efficiencies by leveraging all technological advancements, including the latest long-reach Power over Ethernet (LRPoE) switch innovations. This approach helps reduce network complexity and

*Figure 6. Modern LAN Principles Applied to Physical Security Systems Networking*




minimize implementation costs. Actively seek opportunities to repurpose existing cabling

infrastructure. Doing so can reduce disruptions during security system upgrades and significantly lower implementation costs. Additionally, it speeds up the deployment of emerging technologies and accelerates the advancement of security systems. Evaluate and certify network switches and infrastructure solutions that offer long-range power over Whenever possible, reuse and repurpose existing endpoint cabling infrastructure, reduce IDF closet requirements, and adopt energy-efficient PoE switches and endpoints wherever possible. Align with your organization's environmental responsibility framework, such as LEED (Leadership in Energy and Environmental Design) and BREEAM (Building Research Establishment Environmental Assessment Method) sustainability standards. See Appendix C titled, "What Today's Architects Want to Know About Facility Network Designs."

**Principle 4: Deliver Environmentally Superior Solutions.** Include not only bandwidth and power requirements, but also environmental impacts in LAN design and deployment. Whenever possible, reuse and repurpose existing endpoint cabling infrastructure, reduce IDF closet requirements, and adopt energy-efficient PoE switches and endpoints wherever possible. Align with your organization's environmental responsibility framework, such as LEED (Leadership in Energy and Environmental Design) and BREEAM (Building Research Establishment Environmental Assessment Method) sustainability standards. See Appendix C titled, "What Today's Architects Want to Know About Facility Network Designs."

**Principle 5: Physically Separate, Functionally Integrate.** Construct physically separate but functionally integrated IP network paths for different and dedicated applications, ensuring physical security systems are future-proofed and not impacted by disruptions from other business networks. This is also a key principle of hierarchical network design. Utilize network segregation to isolate cloud-managed endpoints and minimize security or network-breach exposure. Develop network designs that account for multiple applications and platforms, including on-premises server-based applications, cloud-based platforms, and hybrid solutions.

**Principle 6: Reallocate Resources to Maximize ROI.** Expand sustainable ROI by reallocating resources gained from repurposing existing endpoint cabling infrastructure and reducing IDF closet requirements and using them to further physical security system deployment or other business initiatives.

### Modern LAN Design and Physical Security

Another key difference between office LAN endpoint devices and security system devices lies in their product lifespans. Most security devices have a long lifespan, typically 10 to 15 years, whereas office LAN endpoint devices are replaced more frequently. In office LAN networks, network switches are regularly upgraded to enhance bandwidth capabilities for endpoint devices. This is not usually the case with security system networks.

Given the Modern LAN design principle of adopting an outside-in approach, starting with endpoint requirements, IT domain network designers face significant challenges when designing physical security system networks. This is primarily due to their unfamiliarity with the complexities and characteristics that affect the network bandwidth needs of physical security devices, especially cameras. These needs can vary depending on the intended use of the devices. For instance, general activity surveillance cameras might require lower resolution, such as Full HD, unless they are tasked with covering large outdoor areas, where a 12-megapixel resolution may be necessary.

Therefore, in the early stages of network design, IT domain network designers are heavily dependent on security system designers to provide detailed device network requirements. These requirements are not just based on make and model, but also on the intended use of each camera throughout its lifecycle.

For example, a camera in a reception area lobby will likely maintain a fixed resolution, as its field of view and purpose are unlikely to change, nor are its resolution and frame rate. Conversely, a high-resolution camera on a food manufacturing product line might have its frame rate adjusted from 30 fps to 60 fps if its role is expanded to capture product labels on a high-speed manufacturing line. Additionally, if the manufacturing lines are reconfigured every few years, the camera's network requirements may change at regular intervals.

## Modern LAN Network Design Roles

*Physical Security and IT now have complementary roles in network design, acceptance inspections and testing, and cybersecurity.*

Understanding the need to first determine endpoint requirements (as per Modern LAN principle #1), Physical Security and IT personnel (including internal IT staff and/or external IT service providers) now have complementary roles in network design, acceptance inspections and testing, and cybersecurity.

These roles include:

- **Physical Security Roles**
  - **Requirements:** Specializing in endpoint requirements for network access layer design. This includes identifying where 10 Mbps network segments will suffice for equipment with long lifespans whose network bandwidth requirements will not exceed 1 or 2 Mbps. For example, this includes many IP cameras and all IP-enabled access card readers.

  - **Acceptance Inspections:** Collaborating in network cable installation inspections, including cable labeling.
  - **Acceptance Testing:** Contributing to the design of security system network acceptance test procedures, such as creating realistic high-bandwidth usage scenarios. Evaluating the impact of network testing (like redundant network path failover and recovery) on security system performance and conducting necessary operational steps for network testing.
  - **Cybersecurity:** Providing IT with guides on security system application and device hardening, and product cybersecurity information. Collaborating in establishing cybersecurity hygiene practices and evaluating tools for firmware updates, digital certificate management, and password management. Jointly documenting and validating computer and network security.
  - **Data Privacy Compliance:** Collaborating in validating data privacy measures.
  - **Network Optimization:** When the number or configuration of devices on the network changes, determining the changes to the nature of network traffic and collaborating with IT on whether or not they require revised configuration or expansion of the networking equipment.
- **IT Roles**
  - **Requirements:** Designing the network access layer, considering the security system's size, potential expansion, and core and distribution layer requirements.
  - **Acceptance Inspections:** Collaborating in cable installation inspections, including network cable labeling and certification.
  - **Acceptance Testing:** Collaborating in the design of security system network acceptance test procedures, executing, and documenting network test steps.
  - **Cybersecurity:** Evaluating product cybersecurity information, applying device hardening guidance, collaborating in establishing cybersecurity hygiene practices, and evaluating tools for firmware updates, digital certificate management, and password management. Jointly documenting and validating computer and network security.
  - **Data Privacy Compliance:** Collaborating in validating data privacy measures.
  - **Network Optimization:** When the number or configuration of devices on the network changes, evaluating the changes to the nature of network traffic and collaborating with physical security on whether or not they require revised configuration or expansion of the networking equipment.

Purposeful collaboration between physical security and IT in network design and deployment is essential for achieving resilient, high-performing physical security systems.

# Example Modern LAN Deployments

There are both economic and business reasons to utilize modern Long Range PoE technology. Typically, the larger the deployment, the greater the savings, and the bigger the business value of eliminating business disruptions. The first example is not a physical security system but a telephone system upgrade. There are still many analog phone systems in use whose organizations want to switch to VoIP phone systems but haven't yet, due to the high cost and disruptions involved in deploying an organization-wide low-latency Ethernet network using traditional LAN equipment.

## Example 1: Large Government Agency 10,000 Camera Deployment

**Objective:** A government agency sought to modernize its outdated analog surveillance system by replacing 10,000 analog cameras with intelligent IP cameras across 360 customs offices and border crossings. This upgrade aimed to make extensive use of video analytics to enhance risk identification and decrease response times to threats. Additionally, the agency sought to boost efficiency by automating the processing of imports and exports at critical points, reduce paperwork, minimize personnel interactions, and shorten wait times at customs.

**Situation:** The enormous size of the project introduced major challenges:

High costs were associated with ripping-and-replacing the existing Coax-based infrastructure, and obtaining the physical space required to build and equip new IDF closets to support IP cameras beyond the 330ft Ethernet cable length limitation of standard PoE switches.

- Need to shut down border crossings to trench for installation of network fiber optic cable.
- Estimated time of four years for new surveillance system deployment across 360 locations.
- Concerns over high risks and network complexity in establishing a network platform to support IP camera video surveillance.
- Concerns over loss of revenue caused by disruption to government import and export operations on a massive scale across the country.
- Safety concerns caused by insufficiency of pre-upgrade video coverage.

**Solution:** Leverage the agency's existing coax-based infrastructure to create the new IP camera network. Deploy enterprise-grade 10-gigabit Ethernet Over Coax PoE switches to transformed the existing and reliable Coax infrastructure into a power-providing IP/PoE backbone, that can support the planned IP cameras with cable distance requirement of up to 6,000ft (1,830m) –18 times greater than that of standard Ethernet switches.

**Result:** All 10,000 cameras were installed in just 10 months, rather than four years originally estimated. The agency experienced:

- Over $3 million saved in infrastructure costs by avoiding the traditional rip-and-replace upgrade model. The long range Ethernet Over Coax PoE switch capabilities enabled the deployment of IP cameras in all areas without installing new IDF closets.
- Zero disruption during the modernization to IP; ensuring the country's import and export operations were not affected.
- An 80% reduction in planned deployment time.
- A robust and simplified network platform that is flexible and easy-to-manage, as the deployment maintained a physically separate and cyber-secure point-to-point network topology.
- An environmentally responsible upgrade by repurposing the existing coax-based infrastructure and eliminating costly IDF closet requirements, which prevented over 60 tons of cable e-waste (electronic waste).

Along with increasing security at the locations, the agency was able to leverage new business intelligence and technology to implement a new automated customs process. The addition of QR readers in the import and export locations has enabled the agency to:

- Reduce by 50% an individual's average time spent at a border crossing location.
- Minimize the amount of paperwork required in the import/export process.
- Eliminate personnel interaction; further increasing safety and labor cost savings.

## Example 2: Maximum Security Prison

**Objective:** Replace the prison's 50 analog security cameras with IP cameras, to improve camera image quality and take advantage of video analytics.

**Situation:** The cost to run new network cable and install new computer equipment in this specially constructed maximum security facility for the criminally insane, was concluded to be over $250,000 for 50 cameras. The construction project would have involved moving a portion of the prisoners to alternate prison facilities, and constantly be relocating prisoners to create safe unoccupied areas as the construction project work moved through the facility. The cost and logistics involved made the project infeasible.

**Solution:** Leverage the existing analog camera coax cable. With no construction project needed, in a single day replace each analog camera with an Ethernet over coax adapter and an IP camera. At each camera location, the area around the camera was cordoned off to isolate it. Each analog camera was unplugged and replaced by an adapter and an IP camera.

**Result:** The new surveillance system was up and running in a single day.

- The cost to upgrade the network infrastructure was about $25,000.
- No prisoners had to be transferred to another facility or moved to another cell.
- Elimination of communications cable e-waste.

## Example 3: Leading Global Jewelry Chain

**Objective:** Across all facilities, perform a phased upgrade of analog low-resolution cameras to IP high-resolution cameras.

**Situation:** Due to the high cost of installing the network infrastructure meant that budget constraints would restrict the pace of facility upgrades to an unacceptably slow pace from a business risk perspective.

**Solution:** Significantly reduce the video network infrastructure video costs by repurposing existing analog camera coax cable.

**Result:** More critical locations were able to be upgraded quicker than possible using the original traditional LAN planned approach.

- The initial 30 locations were upgraded for $195,000 – less than half the originally planned $500,000 cost.
- A larger number of critical locations, such as stores and vaults, were upgraded in the initial phase.
- There was no communications cable e-waste to send to a landfill.

## Example 4: Spanish Retail Giant Massive Security Upgrade

**Objective:** Modernize retail locations by upgrading from analog CCTV to IP-based surveillance, and increase camera counts, to deter theft and establish better recognition capabilities.

**Situation:** One of Europe's largest department store groups needed to upgrade to IP cameras and increase their current camera count to over 90,000 cameras. However, there was no Ethernet network infrastructure in place for such an upgrade. Key concerns were:

- The very high costs and lengthy calendar time requirements to retrofit hundreds of locations with new cable and equipment
- The renovation business disruption could create revenue loss and degrade the customer experience
- The number of IDF closets required to support network connections to the specific IP camera locations needed would reduce valuable retail floor space

**Solution:** Reuse the existing analog camera coax cable to greatly reduce the video upgrade costs. This would establish a physically separate network path for the security devices and applications, ensuring the performance of both the security and overall business networks.

## Example 5: Large Cruise Line Security Camera Deployment

**Objective:** Modernize to an IP-based security and surveillance system to gain high-resolution viewing and recording capabilities, improved monitoring and better application management.

**Situation:** The existing analog cameras were supported by a coax-based infrastructure that ran throughout the ships. The cruise line was considering removing the existing coax cable and installing Ethernet cable to support the deployment of new IP cameras. As the casino planned the modernization, they became concerned with:

- The extremely high costs to remove the coax cables and install new Ethernet throughout the ship
- Loss of revenue caused by time in dock needed to complete the network overhaul
- How to support the new IP cameras throughout the entire ship; given the 330ft distance limitation of standard Ethernet switches
- The environmental impact and waste produced from re-cabling the ships

**Solution:** Repurpose the existing analog camera coax cable to greatly reduce the video upgrade costs.

**Result:** The Cruise Line was able to:

- Across eight cruise ships, install over 4,000 IP cameras using the existing coax-based infrastructure during each ship's normally scheduled 2 weeks of dry-dock repairs and maintenance.
- Using an adapter supporting up to four IP cameras over a single coax cable, increase the number of IP cameras in all public areas
- Reduce network infrastructure costs by more than $4 million while simplifying and reducing the deployment project time frame to improve return on investment
- Support IP cameras exactly where they were needed thanks to the Long Range PoE capabilities
- Prevent over 120 tons of communications cabling e-waste from entering a landfill
- Simplify the overall network requirements

## Acting on Modern LAN Contribution Opportunities

The Modern LAN principles provide a very rare opportunity to contribute positively to a facility's sustainability picture in a way that provides cost savings instead of requiring an

investment. Two factors make this possible. First, the traditional LAN approach to security system networking – especially for security IP cameras – is energy wasteful due to the short distance constraint of 328 ft. on traditional LAN Ethernet cable, requiring powered and HVAC conditioned IDF closets at close intervals. Second, the availability of significant UTP and coax cabling infrastructure that, in its reuse, will prevent e-waste by eliminating rip-and-replace of communications cable infrastructure.

### Initial Steps

IT departments can contribute to their company's sustainability strategy by:

- Inventorying no-longer-used UTP and coax communications cable.
- Identifying the potential opportunities for cable reuse via future upgrades or additions to building systems.
- For the next security or communications system upgrade planned, qualify a Long Range PoE vendor (applying the guidance below) who can provide all of the Modern LAN technology needed, not just pieces of it, and collaboratively execute the project.
- Document the cost savings and sustainability contributions and get the information to the right people in your organization.
- Update the organization's sustainability strategy to account for the Modern LAN contribution opportunities.

### Vendor Evaluation

Several network innovations are consistent with Modern LAN principles, including those from NVT Phybridge, Vigitron, Comnet, Altronix, Planet, Veracity, and more. Before choosing a provider, it is crucial to understand that Power over Ethernet (PoE) innovations vary significantly in capabilities and use cases, so thorough research is essential.

When evaluating Long Range PoE solutions, consider the following key factors:

1. **Company Commitment and Offering:** Determine if Long Range PoE is a core or complementary offering for the provider and assess the range of solutions they offer, from simple unmanaged units to complex managed systems.
2. **Solution Breadth:** Avoid needless complexity by ensuring that the vendor's offerings can accommodate the customer's current and anticipated LRPoE needs.
3. **Features & Capabilities:** Evaluate the feature set, particularly the power strategy, such as redundancy and hot-swappable power supplies, which are crucial for minimizing downtime. NVT Phybridge, for example, offers robust power and connectivity with innovative power-sharing and redundancy features. Ensure the solution's features align with your customer needs.

4. **Core Technology:** The underlying technology, like HomePlug, MOCA, VDSL, ADSL, or straight Ethernet, significantly influences performance. Consider the bandwidth (symmetrical or asymmetrical) and whether the technology suits the deployment environment and endpoint requirements.
5. **Technology and Performance:**
    - **Bandwidth:** Understand the implications of duplex (full or half) and bandwidth type (symmetrical vs. asymmetrical) on network performance and reliability.
    - **Latency:** Consider latency's impact, especially for real-time applications like voice or video, where low latency is crucial.
    - **Noise/Crosstalk:** Be aware of noise production, particularly in large deployments, as it can lead to interference, slowing devices, and packet loss.
6. **Quality and Speed of Technical Support Teams:**
    - **Quality:** Be sure that the vendor's technical support personnel are more than simply feature-aware. They must have deployment experience and be familiar with the LRPoE  deployment situations that pose challenges or require special attention that the networking service provider may not be familiar with.
    - **Speed:** Make sure that the vendor's speed and availability of technical support will fit the needs of the deployment project.
7. **TAA & NDAA Compliance:**
    - For U.S. federal government projects, non-compliance can result in disqualification from contracts, financial penalties, and damage to reputation.

# Appendices

**Appendix A** – Product and Manufacturer Mentions ..... 33

**Appendix B** – Cable Reuse Opportunities ..... 35

**Appendix C** – What Today's Architects Want to Know About Facility Network Designs..... 37

**Appendix D** – Wireless Networking ..... 43

**Appendix E** – Cloud VMS Modern LAN Example ..... 44

**Appendix F** – Secure and Manageable Physical Security Systems ..... 50

**Appendix G** – What Does Future-Ready Mean? Does Future-Ready Mean? ..... 57

**Appendix H** – Acknowledgements..... 63

## Appendix A – Product and Manufacturer Mentions

Back to Appendix List

This eBook focuses on the present and future states of Ethernet networking in electronic physical security systems. It explains the need for improving security system network design, the importance of careful selection of networking products, and the adoption of modern deployment practices. The goal to create high-performing networks that are both manageable and scalable, to enable keeping pace with the rapid advancements in computing and networking technologies. This ensures that we meet the evolving needs of clients and customers in the electronic physical security sector.

Deploying electronic physical security systems both responsibly and cost-effectively hinges on a thorough comprehension and careful application of Modern LAN principles, alongside established best practices in enterprise network design and deployment.

Electronic physical security systems cannot be responsibly or cost-effectively deployed if the Modern LAN principles are not well-understood and thoughtfully applied, and if proven best-practice enterprise network design and deployment practices are not used.

Over the last two years, I've engaged with numerous professionals in physical security system design and service provision. Unexpectedly, none were acquainted with Modern LAN principles or the latest in IoT and IIoT Ethernet networking technology. My own introduction to Modern LAN principles came with the release of the seminal Frost & Sullivan paper five years ago, and my understanding of current IoT and IIoT networking technologies was broadened through insights from NVT Phybridge about two years back.

In my research, I identified two additional companies within the physical security sector whose product offerings align with Modern LAN principles: Eagle Eye Networks and Viakoo. A common factor among these companies is that their founders and technical teams hail from the from the ICT realm (Information and Communications Technology).

Another common factor is that they all have been consulting clients of mine at various times over the past 15 years. Collaborating on their product documentation work provided me with a deep understanding of their technologies, leading to my recognition of Modern LAN principles in their products.

I was taken aback when I initially realized that their various product innovations that align with Modern LAN principles *predate Frost & Sullivan's Modern LAN work by three to ten years or more*. This is a testimony to their in-depth understanding of networking and communications technologies and of the requirements of large-scale intelligent device

deployments. It should be no surprise that they hold positions as technology pioneers in a security industry often characterized by less advanced offerings.

NVT Phybridge partially funded the research and analysis work that led me to write this eBook. They also provided many details from their numerous customer deployments beyond the examples included herein. All three companies contributed insights and valuable perspectives on large-scale customer deployments and the value of Modern LAN principles.

Ray Bernard
January 2024

# Appendix B – Cable Reuse Opportunities

Back to Appendix List

There are two types of cable reuse opportunities. The first is cable abandoned in place after a previous update of an analog network, phone or intercom upgrade to current day Ethernet network. The second is cable infrastructure currently in use by an outdated system about to be upgraded.

## Cable Abandoned in Place

For buildings constructed before the 1990s, multiple types of no-longer-used wiring from older phone and intercom systems, such as Key, Centrex, or PBX telephone systems, may still be present. In office and industrial buildings, phone and intercom systems commonly utilized unshielded twisted pair (UTP) wiring, including CAT3 cable. As of 2003, it was estimated that around 20 million Centrex lines were installed worldwide by 20 telephone companies, with the majority in the United States (15 million).

It's not uncommon for upgrades to VOIP systems to leave behind unused CAT3 cable. The vast majority of this cable remains functional. Sometimes, wire terminations may need simple redoing on a very small percentage of the cable.

Unused coax cable can also be found in many types of buildings. Older Ethernet networks, early public address (PA) systems, background music systems, and hospital TV systems used coax cables. Additionally, coax cable formerly used for analog CCTV camera systems can be found in buildings that have upgraded to IP cameras.

Due to advancements in enterprise/industrial grade Ethernet LAN networking technology developed for IoT devices and systems, all these cable types can be repurposed for security system devices. Furthermore, recent breakthroughs in enterprise-grade technology based on IEEE Ethernet standards have overcome the traditional 328 ft. distance limitation of office LANs.

Standards-based long-range power-over-Ethernet technologies can extend Ethernet cable runs up to 1,000 ft., 2,000 ft., and even 6,000 ft., depending on the type of cable (UTP) and the required bandwidth. Table 2 and Table 3 on the following page detail the maximum speed and cable length for full-duplex operation of each cable type, along with the PoE rating. Note that Tables 2 and 3 represent the technology capabilities of the leading global long range PoE equipment vendor and are not representative of the industry at large.

## Analog to IP Camera Upgrades

There are still many analog camera systems that haven't been upgraded to IP cameras solely because the network infrastructure cost to upgrade from coax cable to an Ethernet LAN with IDF rooms every 328 ft. is cost prohibitive. Now, long range PoE coax provides affordable 100 Mbps Ethernet connections through the reuse of the analog camera coax cable for cable runs of 1,500 ft. to 2,000 ft. to 3,000 ft., depending on the cable type. See Table 3 below for cable type and maximum length of cable.

Additionally, some LRPoE switches can utilize adapters that enable four cameras to utilize a single cable as long as 3,000 ft.

Also see the details of these Modern LAN Deployments: Example 3: Maximum Security Prison and Example 5: Spanish Retail Giant Massive Security Upgrade for the impressive cost savings and reduced deployment times for these analog to IP camera conversion projects.

***Table 2. Long Range PoE UTP Maximum Cable Lengths and Speeds.***

| UTP Cable Type | Data Rate | Maximum Cable Length |
|---|---|---|
| Single UTP and individual pairs of CAT3 and CAT5 cable* | 10 Mbps | 1,200 ft. (365m) |
| CAT5e 4-pairs and CAT6 4-pairs | 100 Mbps | 2,000 ft. (610m) |
| CAT5e 2-pairs and CAT6 2-pairs | 10 Mbps | 2,000 ft. (610m) |
| | 100 Mbps | 1,000 ft. (305m) |

*CAT3 cable may have 2, 3 or 4 copper wire pairs. For CAT3 and CAT5 cable, there are no 2-pair or 4-pair options. Each pair in a CAT3 or CAT5 cable constitutes its own single Ethernet connection.

***Table 3. Long Range PoE Coax Cable Maximum Lengths and Speeds.***

| Coax Cable Type | Data Rate | Maximum Length |
|---|---|---|
| RG59 | 100Mbps | 1,500 ft. (457m) |
| | 10Mbps | 4,000 ft. (1,220m) |
| RG6 | 100Mbps | 2,000 ft. (610m) |
| | 10Mbps | 6,000 ft. (1,830m) |
| RG11 | 100Mbps | 3,000 ft. (915m) |
| | 10Mbps | 6,000 ft. (1,830m) |

# Appendix C – What Today's Architects Want to Know About Facility Network Designs

Back to Appendix List

Building Information Modeling (BIM), Building Energy Modeling (BEM), and Digital Twins have revolutionized the construction industry by transforming the approach to design and construction processes. Consequently, detailed information about a facility's building control systems, including security systems and their networking, is now required a phase earlier in the building design process.

This information is crucial not only for building project financing decisions but also for individuals and businesses considering investments in the owning company and in prospective major building tenants. Furthermore, it plays a significant role in public relations, influencing external support for or opposition to the community involvement efforts of these organizations. The environmental impact and sustainability practices of an organization are board-level concerns with wide-ranging implications. This underscores the importance of Modern LAN Principle #4, which advocates for "Delivering Environmentally Superior Solutions."

For instance, the influence of a Modern LAN design on space allocation for equipment and IDF rooms can be substantial, necessitating consideration even before the Schematic Design phase, where it is typically addressed. The size, location, and number of IDF rooms directly affect the building's overall energy use and efficiency. For example, strategically placed IDF rooms can optimize cooling requirements and reduce energy consumption. If the Modern LAN approach significantly reduces IDF room requirements, it may be beneficial to include a descriptive paragraph or two about this impact prior to the Schematic Design phase.

In the context of the roles of architects and engineers, the term "sustainability" refers to a holistic approach to building design, construction, and operation. This approach aims to minimize environmental impact while enhancing health, wellbeing, and resource efficiency. Both LEED (Leadership in Energy and Environmental Design) and BREEAM (Building Research Establishment Environmental Assessment Method) certifications define sustainability through specific criteria and benchmarks across various dimensions.

### LEED's Definition of Sustainability:

1. **Energy Efficiency:** Designing and operating buildings in a way that reduces energy consumption and greenhouse gas emissions.

2. **Water Efficiency:** Implementing strategies to reduce water consumption and waste.
3. **Sustainable Site Development:** Minimizing the impact on ecosystems and water resources, promoting sustainable site selection, and encouraging alternative transportation.
4. **Materials and Resources:** Using sustainable building materials and reducing waste through recycling and reuse.
5. **Indoor Environmental Quality:** Ensuring healthy indoor air, access to natural light, and occupant comfort.
6. **Innovation:** Encouraging innovative approaches to sustainability and environmental stewardship.
7. **Regional Priority:** Addressing specific environmental priorities and challenges of the project's geographic location.

Of these LEED sustainability elements, Energy Efficiency, Materials and Resources, Innovation, and Regional Priority are relevant to building control systems.

**BREEAM's Definition of Sustainability:**

1. **Management:** Promoting sustainable management practices throughout the building's lifecycle.
2. **Health and Wellbeing:** Ensuring the wellbeing of occupants through quality indoor environments, lighting, and acoustic performance.
3. **Energy:** Reducing energy use and carbon emissions through efficient design and renewable energy sources.
4. **Transport:** Encouraging sustainable transport options for building users.
5. **Water:** Efficient use and management of water resources.
6. **Materials:** Using sustainable construction materials and minimizing waste.
7. **Waste:** Reducing waste production and promoting recycling during and after construction.
8. **Land Use and Ecology:** Protecting and enhancing the ecological value of the site and minimizing the building's impact on its surroundings.
9. **Pollution:** Reducing pollution and ensuring minimal environmental impact from building operations.

Of these BREEAM sustainability elements, Energy, Materials, and Waste are relevant to building projects.

LEED and BREEAM view sustainability as a comprehensive and multi-faceted concept that encompasses not just environmental aspects, but also the health, comfort, and wellbeing

of building occupants, as well as broader considerations like resource efficiency and ecological impact. These certifications provide frameworks and guidelines for achieving sustainability goals in built environments. LEED and BREEAM certifications are designed to encourage sustainable practices in various types of building projects, including new constructions, renovations, and retrofits.

### Architecture and Engineering Considerations

You will see mention of cabling reuse and e-waste prevention in many of the Example Modern LAN Deployments that start on page 26. In many projects, applying Modern LAN principles will contribute to the building project's sustainability, and for some projects will the sustainability contributions will be very important.

### LEED Certification:

- **Energy Efficiency:** For new construction, energy efficiency involves designing and building structures that minimize energy consumption through efficient HVAC systems, high-quality insulation, energy-efficient lighting, and potentially the use of renewable energy sources. In remodeling projects, energy efficiency can be addressed by upgrading existing systems to more efficient ones, improving the building envelope (like windows and insulation), and implementing energy-efficient lighting and appliances. The goal is to reduce the energy demand and improve the overall performance of the existing building.
- **Innovation Credit:** Innovative strategies that significantly reduce environmental impact can contribute to earning points under the 'Innovation' credit in LEED.
- **Materials and Resources Credit:** LEED has specific credits for waste reduction and resource reuse. By preventing e-waste, the project can earn points under this category. This is particularly relevant under the 'Construction and Demolition Waste Management' credit, where reducing waste contributes to achieving higher certification levels.
- **Regional Priority:** Regional Priority credits are designed to address environmental priorities specific to the project's geographic location. These credits provide an incentive for achieving certain credits that are particularly important for the ecology and environmental concerns of the project's region. For both new constructions and remodels, these credits encourage builders and designers to focus on local environmental issues, whether it's water conservation in arid regions, stormwater management in areas prone to heavy rainfall, or habitat restoration in ecologically sensitive areas.

### BREEAM Certification:

- **Sustainable Purchasing:** If a new building or remodel upgrade includes purchasing new equipment that is more energy-efficient or environmentally friendly, this could contribute to LEED points under the Sustainable Purchasing category.
- **Waste Management:** BREEAM awards credits for effective management of waste. By preventing e-waste, the project can demonstrate efficient resource management and waste minimization, which are key aspects of BREEAM's assessment.
- **Materials Credit:** Similar to LEED, BREEAM also evaluates the environmental impact of materials used in a project. Reusing existing infrastructure instead of procuring new materials can contribute to this credit.
- **Innovation Credits:** BREEAM also recognizes and rewards innovative practices. The significant reduction of e-waste can be considered an innovative approach to environmental stewardship and resource efficiency.

For any specific building project, the design phase during which information is required, the timeline for providing this information, and the necessary level of detail will vary. These aspects are project-specific and depend partly on the extent to which BIM, BEM, and Digital Twins (further described below) are utilized in the project.

### Building Information Modeling

Building Information Modeling (BIM) in the construction industry refers to a digital (i.e., software-based) process that provides a collaborative and comprehensive way of working throughout the entire lifecycle of a construction project. BIM involves creating and using an intelligent 3D model to facilitate the planning, design, construction, and management of buildings and infrastructure. Key aspects of BIM include:

- **3D Modeling:** Unlike traditional 2D design methods (like blueprints and drawings), BIM involves creating detailed three-dimensional digital models of the building. These models provide a realistic representation of the physical and functional characteristics of the project.
- **Information-Rich Models:** BIM models are not just graphical representations; they embed crucial data about each component of the building, from structural elements to materials, spatial relationships, and more. This data can include specifications, manufacturers, costs, maintenance schedules, and environmental impact.
- **Collaboration Across Disciplines:** BIM facilitates collaboration among all stakeholders involved in the construction process, including architects, engineers, contractors, and owners. This collaborative approach helps coordinate efforts, reduce conflicts and changes during construction, and ensure that all parties are working from a single, shared model.

- **Lifecycle Management:** BIM supports the entire lifecycle of a building, from initial concept and design, through construction, to its operational life and eventual demolition. It allows for better project management and more efficient maintenance and operation of the building post-construction. While Building Information Modeling (BIM) is heavily utilized during the design and construction phases, its benefits can indeed extend into the entire lifecycle of a building, including its operation and maintenance. Although lifecycle management extends beyond the timeframe and scope of work typically associated with architects and engineers, lifecycle information is valuable to property owners and operators.
- **Improved Efficiency and Accuracy:** By using BIM, construction projects can achieve greater efficiency and accuracy. It helps in detecting potential issues early in the design phase, improves cost estimation, and reduces the time and resources spent on resolving issues during construction.
- **Simulation and Analysis:** BIM models can be used for simulations and analyses, such as sunlight studies, energy performance analysis, and logistics planning, helping in making more informed decisions.

### Building Energy Modeling

Building Energy Modeling (BEM) is the practice of using computer-based simulation software to perform a detailed analysis of a building's energy use and energy-using systems. Architects use BEM to design energy-efficient buildings, specifically to inform quantitative trade-offs between up-front construction costs and operational energy costs. In many cases, BEM can reduce both energy costs and up-front construction costs.

Building Energy Modeling (BEM) analyses play a crucial role in achieving LEED (Leadership in Energy and Environmental Design) and BREEAM (Building Research Establishment Environmental Assessment Method) certifications. BEM provides detailed insights into a building's energy performance, which is a key component of both these sustainability standards.

### Digital Twins

As the name clearly suggests, a Digital Twin is a digital copy of real-world spaces. Using these 3d models, you can interact virtually with the physical property during the early planning and designing stages. While BIM provides the static model and initial data, Digital Twins integrate BIM's initial data with real-time operational data, offering a dynamic, living model of the building. Digital Twins allow for continuous monitoring and optimization of building performance, which is beyond the traditional scope of BIM but can be seen as an extension of it in the context of lifecycle management.

## Summary

Building Information Modeling (BIM), Building Energy Modeling (BEM), and Digital Twins have significantly transformed the construction industry. These technologies necessitate earlier access to detailed information about a facility's building control systems, including security systems and networking, during the design process. This information can be crucial for project financing, investment decisions, public relations, and aligning with sustainability practices, emphasizing the importance of Modern LAN Principle #4's "Delivering Environmentally Superior Solutions."

The impact of Modern LAN design on space allocation, particularly for equipment and IDF rooms, is significant and should be considered even before the Schematic Design phase. This approach can substantially affect a building's energy use and efficiency, highlighting the need for a holistic approach to sustainability in building design, construction, and operation.

Security system designers, whether part of an A&E firm's in-house staff or an external design resource, should proactively consider the requirements and impacts of traditional versus Modern LAN designs in new and remodeled building projects. Early estimations, even if approximate, of the differences between these two approaches can be valuable. Such preliminary assessments can serve as a productive starting point for further discussions about a project's information needs and their timing in relation to the building design process.

# Appendix D – Wireless Networking

## WiFi Access Points and Private 4G LTE and 5G Base Stations

Back to Appendix List

Wireless device communication is essential for Smart City networking, especially Private 4G LTE and 5G communications. Smart City deployments have a wide variety of venues and buildings to cover with surveillance cameras, such as for traffic management, safety and security for event venues, parks, public parking lots, and of course city buildings. Many of those cameras are in outdoor locations where electrical power is available or easily can be to power IP cameras, but extending wired network connections to all cameras would be prohibitively costly and involve lengthy time frames. However, today affordable wireless connectivity is very feasible.

Mexico City began it's smart city Mi Calle (My Street) deployment project for 58,000 cameras in 2020. The city installed the first 13,000 cameras in just four months using 4G/LTE connectivity, reducing the infrastructure costs by 80% compared to the original wired connectivity plan. For a closer look at the multiple network architectures involved download the Eagle Eye Network's Smart Cities white paper.

Such projects can now save even more by strategic use of LRPoE.  Getting network connectivity and power to WiFi access points and Private cellular base stations can be a significant part of the cost of a city security video surveillance system if only traditional office LAN networking technology is being used, especially in locations where power outlets are not readily available or where running power lines would be impractical or expensive.

Utilizing long range PoE has reduced the cost of network and power infrastructure by over 50% in large warehouse facilities, and even more for mining operations, oil & gas fields and pipelines, and seaport piers. LRPoE deployments can include redundant PoE for power for Wireless routers and private cellular base stations, enhancing wireless reliability while reducing power and communications infrastructure costs.

Deploying network infrastructure in large or complex environments can be challenging. LRPoE simplifies this process by reducing the number of components and connections required. This not only lowers initial deployment costs but also simplifies ongoing maintenance and potential future expansions.

The extended range of LRPoE provides greater flexibility in the placement of WiFi access points and 4G LTE and 5G base stations. This is particularly beneficial in large warehouses or outdoor industrial environments where optimal placement is key to ensuring adequate coverage and network performance.

# Appendix E – Cloud VMS Modern LAN Example

## Modern LAN Principles In a Cloud Video Management System

Back to Appendix List

Breakthrough technologies in the physical security industry typically emerge from external sectors. Notable examples include:

- **Lenel Systems International – Industry-first access control software company.** Initially a multimedia software firm, Lenel entered the security sector in 1995, disrupting a market then dominated by large, traditional companies. As the pioneer of software-based access control and standalone security software sales, Lenel transformed the role of software in the physical security industry.
- **Axis Communications – Globally-first IP camera and industry-first network surveillance camera.** Originating as an IT company focused on network solutions, Axis revolutionized the industry by introducing the IP camera. It rapidly became a leader in camera technology, cybersecurity, and product range, later expanding into access control, audio systems, intercoms, and IoT sensors.
- **Milestone Systems – Industry-first enterprise class video management software, first VMS with system-internal hot redundant backup servers and redundant video data storage.** With roots in financial software, Milestone's founders applied their expertise in data transfer to the security video domain. They developed a robust, open on-site client-server software platform for video management, encouraging third-party innovations through add-on applications.
- **Brivo Systems – Industry-first cloud-based physical access control system, first with secure device to cloud data connections, first with digital certificate-based device authentication, first security industry member of the Cloud Security Alliance STAR registry.** Brivo's co-founder, president and CEO served in a variety of senior management roles in high-technology companies and software development spanning web development, healthcare and satellite communications prior to establishing Brivo Systems. In contrast to most of the access control system industry segment, Brivo started out with a strong system-security mindset and a clear customer-experience focus.
- **Eagle Eye Networks – Industry-first true cloud-based video management system, first cloud-based VMS platform to include on-premises video buffering and recording and network appliances that themselves create highly-secure camera LANs, second security industry member of the Cloud Security Alliance**

**STAR registry.** Dean Drako, founder of Barracuda Networks, launched Eagle Eye Networks in 2012 after encountering challenges at Barracuda trying to remotely utilize existing video surveillance systems. The aim of Eagle Eye Networks was to enhance remote video surveillance management, leveraging Drako's innovative network appliance experience at Barracuda to pioneer true cloud-based remotely manageable VMS. This appendix is about how Eagle Eye Networks applied Modern LAN principles to its cloud-based video management system, being the only cloud VMS solution provider to take responsibility for the on-premises camera LANs as well as the cloud-based software platform, in order to ensure the optimal performance of video data management as well as assuring the cybersecurity entirety of the on-premises network deployment.

## The First True Cloud Video Management System

Dean Drako and his development team at Eagle Eye Networks, with their extensive expertise in network security appliance innovation, were uniquely positioned to launch a pioneering cloud-native Video Management System platform in the physical security industry that would be the first to provide both cloud and on-premise recording. The Eagle Eye Cloud VMS stands out as the first and only cloud-based Video Management System (VMS) that segments and secures the LANs of connected cameras through its cloud-managed on-site appliances, which also ensure the integrity of video transmissions to the cloud, all while conserving the bandwidth of shared business Internet connections.

## Modern LAN Principles and Cloud VMS Camera LANs

There are two Modern LAN principles (#2 and #5) that are critically important to apply to security video camera LANs. The Eagle-Eye Cloud VMS applied them to its Cloud VMS platform at least four years before Frost & Sullivan's "The Modern LAN" paper called attention to them. The Cloud VMS platform facilitates the inclusion of two additional Modern LAN principles (#3 and #4) in surveillance system network design. These Modern LAN principal are repeated below to allow additional annotations relevant to the Eagle Eye Cloud VMS, and are italicized and enclosed in braces (*[like this]*).

**Principle 2: Design for Security and Management.** Create secure and robust local area networks that are easy to configure, deploy, manage, and troubleshoot. *[By default, each Cloud VMS Bridge and Recorder appliance creates a highly secure camera LAN, and isolates one Camera LAN from any other, as explained on the following pages.]* Ensure systems integration flexibility by allowing for separate, on-premise, or Cloud-based integration; simplifying LAN management, and minimizing core network breach risk. *[The Cloud VMS platform's open API provides advanced cloud-based integration at any scale, comprehensive enough to enable smart city video functionality for Mexico*

*City's 58,000-camera deployment that includes the incorporation of video streamed from cab driver and passenger cell phones, as well as video related to a duress call via the City's citizen mobile app.]*

**Principle 3: Maximize Efficiencies and Reduce Complexity.** Maximize efficiencies by leveraging all technological advancements, including the latest long-reach Power over Ethernet (LRPoE) switch innovations. This approach helps reduce network complexity and minimize implementation costs. Actively seek opportunities to repurpose existing cabling infrastructure. Doing so can reduce disruptions during security system upgrades and significantly lower implementation costs. *[Multiple LRPoE technology options for cable reuse including coax, no longer used telephone system twisted pair wiring are available as described following pages.]* Additionally, it speeds up the deployment of emerging technologies and accelerates the advancement of security systems. Evaluate and certify network switches and infrastructure solutions that offer long-range power over Whenever possible, reuse and repurpose existing endpoint cabling infrastructure, reduce IDF closet requirements, and adopt energy-efficient PoE switches and endpoints wherever possible. Align with your organization's environmental responsibility framework, such as LEED (Leadership in Energy and Environmental Design) and BREEAM (Building Research Establishment Environmental Assessment Method) sustainability standards. See Appendix C titled, "What Today's Architects Want to Know About Facility Network Designs."

**Principle 4: Deliver Environmentally Superior Solutions.** Include not only bandwidth and power requirements, but also environmental impacts in LAN design and deployment. Whenever possible, reuse and repurpose existing endpoint cabling infrastructure, reduce IDF closet requirements, and adopt energy-efficient PoE switches and endpoints wherever possible. *[See following pages.]* Align with your organization's environmental responsibility framework, such as LEED (Leadership in Energy and Environmental Design) and BREEAM (Building Research Establishment Environmental Assessment Method) sustainability standards. See Appendix B titled, "What Today's Architects Want to Know About Facility Network Designs."

**Principle 5: Physically Separate, Functionally Integrate.** Construct physically separate but functionally integrated IP network paths for different and dedicated applications, ensuring physical security systems are future-proofed and not impacted by disruptions from other business networks. This is also a key principle of hierarchical network design. Utilize network segregation to isolate cloud-managed

endpoints and minimize security or network-breach exposure. *[See Figure E-2 that follows.]*

### Secure Camera LAN Network Appliances

There are two types of on-site network video appliances. *Bridges* buffer and intelligently transmit video to an Eagle Eye Cloud VMS data center based on schedules and/or a configurable percentage of available Internet connection bandwidth. *Cloud Managed Video Recorders (CMVRs)* that include all Bridge functionality but additionally record video. Both Bridges and CMVRs are purpose-built network appliances that include router, firewall and DHCP server functionality as well as video management capabilities. The devices analyze video for motion, compress it, and encrypt it for safe storage. The cybersecurity features of the Eagle Eye VMS appliances protect other cameras and other networks from any pre-infected cameras that already exist on the camera LAN or are added later.

See Figures E-1 and E-2 (provided by Eagle Eye Networks) on the following page that contrast the camera LAN cybersecurity profile of many common analog camera Digital Video Recorders (DRVs) and IP camera Network Video Recorders (NVRs) with that of an Eagle Eye Cloud VMS platform. The camera LANs of many client-server VMS recording servers are similarly exposed.

The Eagle Eye appliances automatically detect connected video cameras and configure the network appropriately. It takes one click to add a camera. The devices are cloud-managed, including automatic firmware updates and digital certificate management that requires no action on the part of the end-user customer or installing/maintaining security service provider. Basically, the Eagle Eye platform provides self-managing secure camera LANs, aligned with and going every further than Modern LAN Principle #2.

*Figure E-1. Traditional DVR and NVR recorder camera LAN.*

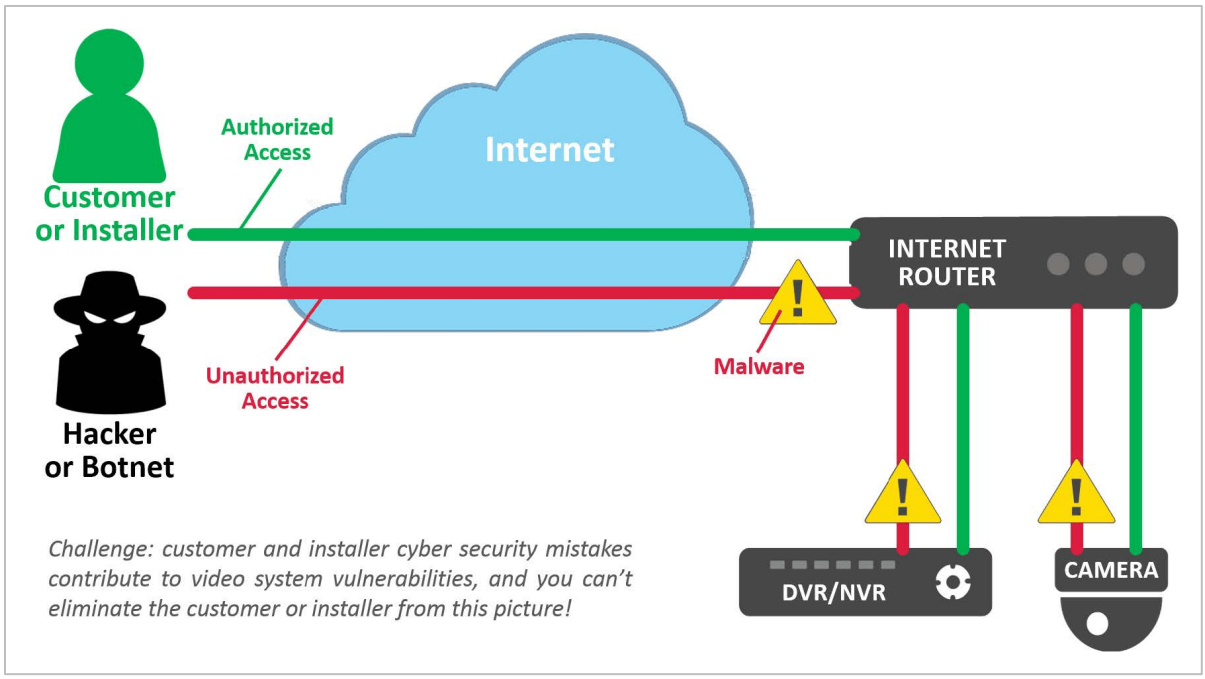
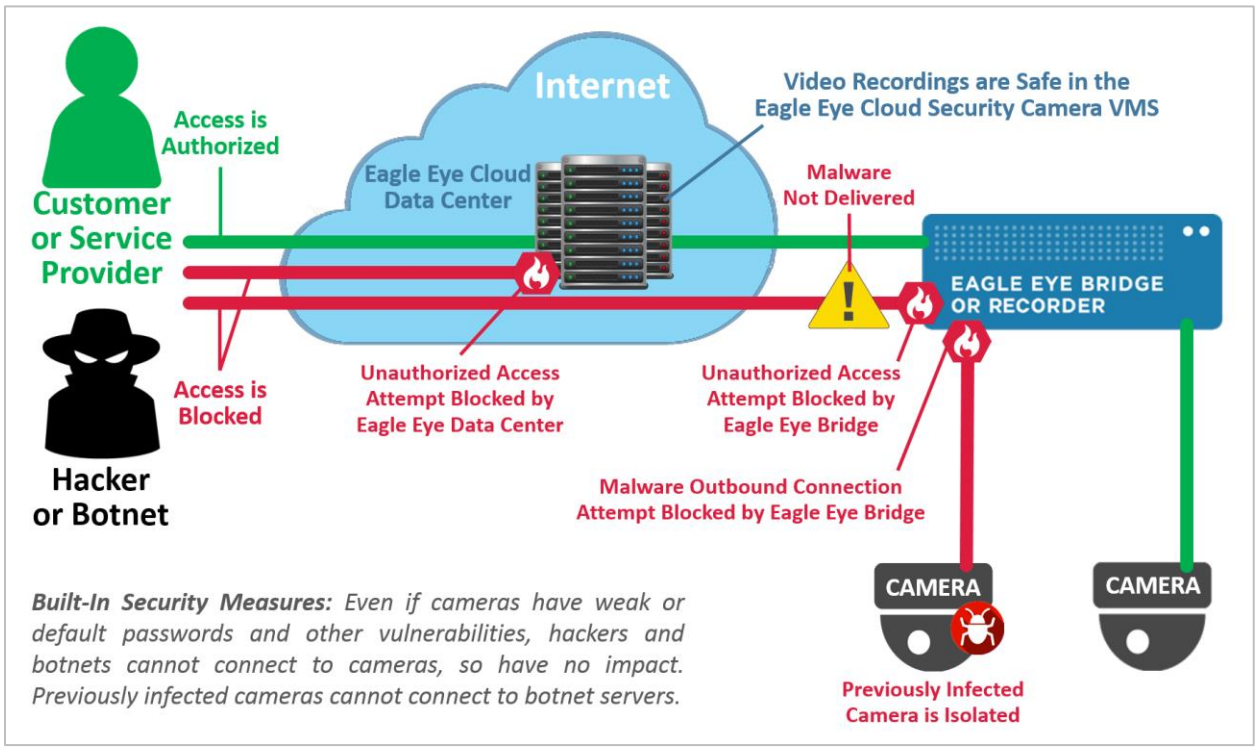



*Figure E-2. Eagle Eye Cloud VMS platform cloud-managed camera LAN.*



## Secure, Simple and Manageable Camera LANS with LRPoE

There are multiple options to enable long range PoE connections for Eagle Eye Bridges and Recorders to extend with Ethernet camera connections runs to up to 2,000 ft, using new or reusing existing twisted pair and coax cable. Here are a few examples from NVT Phybridge technology:

- **Network cable (including 30-Watt and 50-Watt options):**
  - *CAT5e and Cat6 4-pairs:* 100 Mbps to 2,000 ft.
  - *Cat5e and Cat6 2-pairs:* 10 Mbps to 2,000 ft.; 100 Mbps to 1,000 ft.
- **Coax cable (including 30-Watt and 50-Watt options):**
  - RG59: 10Mbps to 4,000 ft., 100Mbps to 1,500 ft.
  - RG 6: 10Mbps to 6,000 ft., 100Mbps to 2,000 ft.
  - RG 11: 10Mbps to 6,000 ft., 100Mbps to 3,000 ft.

The above examples are provided to show how combining existing technologies that align with Modern LAN principles is a sound approach to achieving a high-performing secure and manageable camera LAN deployments.

## Long Product Lifecycles vs. Rapid Technology Advancement

Historically in the physical security industry, the working life of a product far outlasted its warranty period. Additionally, a product may be working as originally intended but, due to new product feature advancement, its replacement may be desirable. This is a previously unaddressed industry challenge to achieving future-ready deployments. A product or system's status with regard to the two Modern LAN principles mentioned earlier, including the "future-proof" objective, may be compromised by technology advancement and/or cyber-threat advancement.

The Eagle Eye Rapid Replacement program addresses these concerns by providing an extended warranty period (20 years) with rapid replacement for all Eagle Eye hardware (including Eagle Eye cameras), plus the ability to obtain hardware upgrades upon request every 6 years.

# Appendix F – Secure and Manageable Physical Security Systems

Back to Appendix List

Historically, the manageability and cybersecurity of large-scale electronic physical security systems have been inadequate, partly because general-purpose LAN technology and network design approaches, suitable for office environments, do not meet the unique needs of physical security systems. Today, modern network technologies and Modern LAN design can enhance the security and performance of these systems while significantly reducing costs.

However, achieving manageable and cyber-secure large-scale physical security systems extends beyond network architecture. It's crucial to ensure that security applications and devices themselves are manageable and secure at scale. Relying solely on physically separate camera LANs connected to other networks or the Internet via a firewall, as shown in Figure 6 on page 22, "Modern LAN Principles Applied to Physical Security Systems Networking", is insufficient.

## Information Systems Peak Performance and High Uptime

In the last two decades, networked information systems have become the backbone of business, and 24/7 systems uptime is an absolute business necessity. IT developed ways to achieve *99.999% uptime* (commonly called *five nines*) across a mix of multi-vendor application suites, computing platforms, and network infrastructure.

In order to keep its applications and computer infrastructure running around the clock, *IT needs deep visibility into the faults, events, capacities, performance profiles, and configurations across its networks and systems.* IT has to be proactive, preemptive and predictive to keep the organization's information systems running. IT must do so in the face of growing cyber threats against their systems. *Thus, the mission of IT is to keep information flowing and applications running at peak performance while assuring the confidentiality, integrity and availability (CIA) of its information systems.*

## Bringing Physical Security Systems Up To IT Management Standards

Physical security systems in terms of compute, storage, networking, and cyber vulnerabilities are functionally very similar to what exists in a data center. In order to manage and secure them to an IT standard, such as five nines of reliability, there are similar foundational elements needed:

1. **Asset and application discovery**: Detailed inventory records, including what devices are tied to which applications and on what ports.
2. **Service assurance:** Immediate identification of failures and generation of corrective action plans.
3. **Automated lifecycle management:** Being alerted as to when devices go out of service, out of warrantee, have new firmware, or have newly discovered vulnerabilities present.
4. **Fleet-wide firmware, password, and certificate management (that is application-aware):** Unlike IT systems, many device-level firmware and password operations must be done in coordination with the application managing the devices, such as between a camera device and a VMS.
5. **Historical record of operations (for compliance and audit):** Whether it is to pass internal or external audits, for cyber insurance applications, or for identifying areas of concern within the operation, having logs and records is critical.

### Increasingly, Hackers Attack Physical Security Systems

Today, while businesses are using advanced analytics to get end-to-end insight across their entire information systems infrastructure, security directors and managers are still assigning security officers the task of scrolling through video camera displays to make sure that all cameras are online and recording. It's not effective, because officers can't watch all cameras all the time, and can't really tell if cameras are recording as they are supposed to be. Recording or retention failures are often not caught for days or weeks or ever.

The self-test health check functions of video management systems can detect when video is not being received from a camera. However, it cannot provide any diagnostics information, and it cannot tell if a still-transmitting camera is under a cyberattack or has been infected with malware.

Many corporate security departments apply manufacturers' hardening guide information for their application servers, but still rely on manual diagnostics and manual management of passwords and firmware in cameras and other IP-enabled devices. Why?

Many security practitioners underplay the existing vulnerabilities of their security systems and devices because they are under the impression that a cyber-attack or insider misconduct is not very likely.

But starting about four years ago the number of cyber vulnerabilities impacting IoT devices (including networked security video cameras) started exceeding those aimed at IT systems, a trend that continues today. Palo Alto Networks Unit 42 in 2021 reported that the least secure devices in an organization were the IP cameras (33% of security issues).

Starting in early March of 2022, the hacker group Anonymous began hacking into hundreds of IP cameras in Russia, including inside the Kremlin, and has used that access to distribute messages to the Russian people, gain military reconnaissance, and move laterally on the network to gain access to other systems. In January of 2023, Russia has been hacking camera systems inside residential complexes in Ukraine in order to surveil the movement of people and traffic on the streets.

In November 2022 Mandiant analyzed Russian cyber-attack patterns and determined that Russia had shifted its focus to edge devices (routers, cameras, firewalls, etc.) as they are easier to hack into, and perhaps most importantly, are often forgotten in remediation efforts and thus leaving a foothold for threat actors to leverage in the future.

Non-military hackers follow these kinds of hacking successes and target the kinds of systems that have been found to be vulnerable. Security practitioners think that "insider threat" refers to people with malicious intent. They typically trust their employees and vetted vendors not to abuse the access they are given to security systems and their networks, not realizing that accidental human error is a common source of system and network vulnerabilities. Based on a 2022 study by IBM, human error contributes to 95% of cyber security breaches.

### Unmanageable Security System Passwords and Firmware

No one in IT or corporate management would think it okay to put hundreds or even just dozens of server computers around a building campus and network them together, placing some in lobbies, meeting rooms, and even outside the buildings, and not keep their firmware updated or closely manage their passwords. Yet, this is common practice with network security cameras. In 2016, camera and recorder cybersecurity vulnerabilities allowed 1.5 million connected cameras and recorders (DVRs, NVRs, and recording servers) to be hijacked to create the world's largest Mirai botnet. The malware took full control of the devices' underlying Linux operating systems.

> Network security alone doesn't provide enough protection for security system devices.

Connecting the cameras via a protected network is insufficient because it establishes only a single layer of defense with many attack points. If just one attack point is compromised, vulnerable cameras can be exposed to a myriad of automated and manual attacks. A single compromised camera can then spread the malware infection to other devices on the network, not just to other cameras. For example, malware on cameras could spread to servers and workstations. It could lock out all users from business applications by attacking the business's Active Directory system. The business disruption would last from a few hours to a few days,

depending upon the recovery measures in place for business IT systems. But there would likely be a significant negative impact to the business.

## The Key Vulnerabilities

The key vulnerabilities of video cameras and other intelligent IoT devices fall into two categories: Password vulnerabilities and Firmware vulnerabilities. Addressing these two categories of vulnerabilities will stop most attacks from being successful, especially automated malware attacks.

### *Addressing Password Vulnerabilities*

Most cyber-attacks work by gaining access via user login credentials and exploiting device and system vulnerabilities to obtain a high level of access that gives attackers full control. Most automated and manual cyber-attacks succeed through the existence of factory-default passwords, easily-guessed passwords, passwords discovered because they were transmitted in plain text, and weaknesses that allow device and system access privileges to be escalated.

Intelligent security device password management can be complicated. They are typically part of a system with hundreds or thousands of connected devices. Security system devices are typically in constant use by other devices, systems, and software. Changing a password on a single device may also involve updating the password information on a connecting device or system.

### *Poor Password Practices*

The approach to password management in many organizations often prioritizes simplicity and convenience, which unfortunately creates significant vulnerabilities. A common practice is to assign the same set of passwords to all security system devices. This typically includes a master password, a system or device password, and a service technician password. The risk here is substantial: if the password for one device is compromised, it effectively compromises all devices.

This risk is further exacerbated when password management is outsourced to service contractors. Considering that most industrial systems have lifecycles spanning several years, the turnover of service personnel—who might leave the organization disgruntled—poses a significant security risk. Knowledge of passwords becomes a liability when it's in the hands of many, including those whose relationship with the organization may change over time.

Moreover, the situation becomes even more complex when service technicians use their own preferred passwords across multiple clients' devices. This practice means that the security of one client's system could inadvertently compromise another's. For instance, if a

technician services two different organizations using similar security devices, the password knowledge from one could potentially be used to access the other's system.

The danger escalates if a technician typically leaves default passwords unchanged, as this makes all their clients' devices vulnerable to a wide range of potential cyberattacks. Any successful hack or malware infection in one system could then provide attackers with access to all other systems serviced by the same technician.

### Management at Scale Has Been Impossible

Effectively managing passwords for a small security system with only a few devices is relatively straightforward. However, the challenge magnifies exponentially when dealing with systems that encompass hundreds or thousands of intelligent security devices. In such cases, automated password management tools become a necessity.

These tools are required not only to change passwords within the devices themselves but also to update the stored passwords in the connected devices and software. Unfortunately, such tools have been largely absent in the security industry, particularly for large-scale deployments like those involving thousands of security cameras. This lack of adequate tools represents a significant shortcoming in the industry. Fortunately, tools are starting to emerge for managing device passwords at scale.

Fortunately, tools are starting to emerge for managing device passwords at scale.

Automated tools are essential for ensuring that default or easily-guessed passwords are not used. They can facilitate secure (e.g., HTTPS) network connections to prevent passwords from being transmitted in plain text. Moreover, these tools can regularly update passwords to reflect changes in service personnel, maintaining a high level of security. Importantly, they allow device owners to retain control over password management and provide auditable records of adherence to password management policies.

It's crucial to note that managing a device’s password by storing it in an application that uses the device (such as a DVR or VMS) can hinder the establishment of a centralized point of password management across all software applications and devices. It can also constitute another avenue for password compromise, because passwords are loosely controlled and not centrally managed with strong access control protection.

### Addressing Firmware Vulnerabilities

Cybersecurity is not the only reason to update IoT device firmware. Maintaining devices at their most recently-released versions of firmware is typically required by manufacturers for their provision of factory technical support. Additionally, modern technologies are continually updated for bug fixes as well as feature and performance improvements.

Intelligent IoT devices can be expected to receive several feature and performance updates per year, and likely at least one or two security updates. Many current-technology cable TV set-top boxes are updated nightly by their service providers. However, this is driven by consumer market feature competition as well as bug fixes and security updates. Industrial IoT devices should not require daily updates.

### Firmware Update Realities

There is only one way to deal with discovered firmware vulnerabilities: install new firmware that has its known vulnerabilities fixed. This is often not a simple picture for intelligent IoT devices, and network video cameras are a good example of how complex it can get.

Managing firmware can be complicated due to version-dependencies of other devices or system firmware or software. This is very true for networked video cameras. Version compatibility must be maintained with video management software's server applications, video analytics applications running on the camera, and video analytics software running on an analytics appliance or server. There are typically two or three such dependencies involved per make and model of the camera. Because cameras, as well as the applications and systems that use them, are all evolving technologies these dependencies will remain for the foreseeable future.

Often, the Video Management System (VMS) software version must be upgraded first, as well as server-based or camera-based analytics software, prior to the camera firmware upgrade. Thus, industrial IoT device uptime should be defined as the time that the device is available for full use by the system, not just the time that the device is powered up and network-connected. This is especially applicable to security video cameras and is why firmware/software version dependencies are important.

Security device uptime should be defined as the time that the device is available for full use by the system, not just the time that the device is powered up and network-connected.

#### *Testing Firmware Compatibility*

It is not enough that the various vendors of video software and camera analytics have lab-tested camera firmware for compatibility with their own products. These are bench-tests performed with test configurations that don't match the configurations used by end-user customers.

The firmware of third-party products must be tested with the exact same product configurations that the camera owners are using to ensure full compatibility. Product vendor limited resources don't permit testing that is that extensive.

This means that camera owners or their service providers must establish and maintain a capability to test device firmware before deploying it. Organizations with high-camera-count deployments typically maintain a lab environment with systems and devices whose configurations match their deployed counterparts. Smaller organizations typically test selected deployed devices one at a time, which can usually be done with security video systems.

For cameras deployed in 24-hour production environments where cameras are required for business reasons – such as a high-speed food or drug production line where video records of each item and its label are critical for quality assurance and compliance reasons – production-area cameras cannot be used for firmware compatibility testing.

Due to the large number of camera industry makes and models, video software manufacturers may not be able to test the firmware for all customer cameras in a time frame that is acceptable to customers. This is sometimes the case with infrared cameras or with cameras where the firmware update only relates to a feature that doesn't directly involve the software functionality, such as the camera's low-light capability.

Sometimes, configuring new firmware features requires a special video software development cycle for that feature. Testing of the camera firmware compatibility may be scheduled for after the software update is completed. Yet customers may want to perform an update sooner per their cybersecurity policy. This is another reason to be prepared for in-house camera firmware testing.

### *Device Firmware Profiles*

Due to the complexities of firmware updates for high device-count IoT device deployments, an evolving best practice among organizations with significant IoT device deployments is the use of product lifecycle management, which includes inventory and control of hardware and software assets. Such asset management has long been an IT best practice and is also a practice mandated by cybersecurity frameworks like the CIS Controls by the Center for Internet Security and the NIST Cybersecurity Framework.

Managing firmware for IoT devices with high device counts, like security cameras, is complex. Adopting product lifecycle management, including hardware and software asset management, is becoming a best practice, and is recommended by cybersecurity frameworks like CIS Controls and NIST Cybersecurity Framework.

Product lifecycle management involves creating firmware profiles for each device. These profiles detail the compatible versions of related software (such as the most recent version

of VMS software that supports the latest firmware upgrade for a particular make and model of camera) and are essential for planning firmware updates. It is critical to identify and document product firmware/software version dependencies.

Key data for each device includes:

- Camera ID, Make, Model
- Firmware Versions (Original and Current)
- Compatibility with other systems (VMS, Analytics, etc.)

How to best organize the data depends upon the type and amount of data to be collected. The update plan – which can be as simple as a one-page outline – should specify which products, if any, must be updated to which versions before the camera firmware updates can be performed.

### *Camera Firmware Update Procedure*

Updating firmware manually for large deployments is impractical. A typical update process involves:

1. Logging the update start.
2. Connecting to the camera via a web browser.
3. Verifying camera details and checking for error log items.
4. Stopping video streams in the VMS software.
5. Uploading and verifying the new firmware.
6. Restarting video streams and logging the update completion.

This process, taking 15 -20 minutes per camera, is efficient but can be challenging for large-scale systems.

### *Cybersecurity at Scale Requires Automation*

For large intelligent security device deployments, automation is key to managing cybersecurity effectively. Automated tools can:

- Eliminate repetitive task errors.
- Keep detailed records of cybersecurity actions.
- Ensure secure password practices and reduce cybersecure password management costs.
- Manage passwords efficiently and automatically for any number of devices, generating new device passwords per password profiles and changing them on-demand or per scheduled intervals in the devices themselves and as needed in related application software.
- Significantly cut down the time and labor involved in managing large-scale systems.

For some insight into this picture, let's examine the costs and staff time aspects of updating firmware for 2,000 cameras – well over a $1 million technology infrastructure investment. We'll use the best-case cost and performance figures in Table B-1below.

***Table B – 1. Cost and Staff Time to Manually Update Firmware for 2,000 Cameras***

| **Cost Factor** | **Value** |
|---|---|
| Number of Cameras | 2,000 |
| Task Hours Per Workday | 6.5 |
| Hourly Contractor Technician or Fully Burdened Employee Daily Labor Cost | $75 |
| Daily Contractor or Fully Burdened Employee Daily Labor Cost | $600 |
| Per-Camera Update Time | 10 minutes |
| Cameras Updated per Hour | 6 |
| Cameras Updated per Workday | 39 |
| **Labor Cost to Update Cameras Once** | **$30,780** |
| Per-Camera Labor Cost | $15.38 |
| **Staff-Days to Update Cameras Once** | **51.3 Workdays in 2-1/2 Calendar Months** |

Additionally, when considering the costs of supervision and the manual generation of audit reports from camera update work logs and inventory, it's important to note that this manual approach often leads to unverified audits. This is due to the absence of records on firmware update errors and the lack of validation of the device inventory. Furthermore, completing three update cycles and producing at least one audit report using manual methods would likely exceed $90,000 and take about eight calendar months.

In contrast, the use of an automated tool would not only be more cost-effective but also ensure 100% accuracy in audit reports. These reports would be based on electronically verified device states. Most significantly, the staff time required for each update cycle would be reduced to five workdays or less, a substantial decrease from the fifty or more days needed for manual updates. Automated processes and procedures, being electronically verified, are executed precisely as prescribed, ensuring full compliance with all established requirements.

### *Automated Password Management*

For large security systems, automated password management is essential. It allows for immediate password changes across hundreds or thousands of devices, a task impossible to perform manually. Automation ensures each device has a unique password, maintaining high security standards efficiently.

### *Compliance-Based Device Management*

Large organizations often adopt cybersecurity frameworks like NIST or CIS Controls, which mandate strong asset and password management. Maintaining comprehensive firmware profiles ensures these devices meet the organization's cybersecurity standards.

For details of how IT cybersecurity practices and frameworks such as the CIS Controls apply to intelligent security device deployment, as well as how purpose-built monitoring and service assurance tools for intelligent security devices and systems differ from standard IT tools, see the Viakoo online white paper titled, “Video System Cyber and Performance Assurance.”

### *Sustainable Cybersecurity for Intelligent Industrial IoT Devices*

Future-proofing security for intelligent devices means ensuring their firmware and password management can be automated. Secure configurations should be standard, and manufacturers must provide clear guidance for system hardening. This modern approach is crucial for the effective security of physical security system infrastructures.

## Modern Approach to Securing Physical Security System Infrastructure

Comparing traditional and modern management approaches:

- **Problem Detection:** Automation identifies all issues, unlike the hit-and-miss nature of manual checks.
- **Problem Assessment and Resolution:** Automated systems provide consistent, efficient solutions based on extensive data, unlike the limited scope of manual methods.
- **Communication and Network Description:** Automated alerts and self-discovery of devices offer a more efficient and accurate overview compared to manual methods.
- **Setup and Management:** Automated tools require no specialized programming or device knowledge, making setup quick and straightforward.

In summary, automation transforms the management of large-scale IoT systems, making them more efficient, secure, and compliant with organizational policies.

# Appendix G – What Is a Future-Ready Network?

Back to Appendix List

By 2018, security industry vendors had been using term "future-proof" for over a decade. This prompted me to explore its meaning in an article titled, "Future-Proof", considering the then-current context of managed services, continuous delivery, and rapid technological advancements. Research revealed that the term was being applied very loosely, apparently evolving over time – but not in keeping with the advancement of technology. So, In the article, I offered a new definition that reflected the pace of technological progress.

**2018 Definition of Future-Proof**

Based on technology trends it seemed that a product or system in the physical security industry could be deemed future-proof if it met the following criteria:

1. Its features, including cybersecurity capabilities, can be updated in real-time or near-real-time to align with the manufacturer's latest technological advancements.

2. It supports long-established and emerging standards for internet and local connectivity, ensuring interoperability, or can be updated to provide that support (in keeping with the previous definition).

3. It provides an open and secure API for integration with other systems, designed to preserve compatibility across updates, except when incompatible changes are necessary for cybersecurity enhancements.

4. The manufacturer demonstrates a commitment to continuous innovation, informed by feedback from users and the partner community.

I also wrote, "Today's emerging products are designed to be part of an evolvable technology infrastructure, and that requires the future-proof attributes defined above."

However, technological advancements – especially AI – are driving an significant expansion in the number of security devices deployed. Two examples are the use of mobile credentials and mobile apps to improve the building and campus experience, and the nearly doubling in size of security video camera deployments, based on improved capabilities and the business operations value now obtainable through computer vision.

Thus, an addition to the Future-Proof attributes is required:

5. The device or system is easily manageable and updateable at large scales of deployment.

### Why Future-Proof Considerations Aren't Enough

While the above concepts of "future-proof" above remain relevant for evaluating individual hardware and software products, there is a new situation that we face. It is the exponential advancement of technology, which in the previous decade rounded the corner of its slowly rising near-horizontal line and rounded its curve into sky-rocketing vertical technology advancement. This situation brings additional aspects that apply to evaluating physical security system deployments. *How do we design physical security systems, and their networks, to account for rapidly rising technology?*

It starts by realizing that a "physical security system" is actually a system of systems.

According to Sandia National Laboratories articler titled, System-of-Systems Modeling and Analysis, "The science of System-of-Systems (SoS) is still in its infancy and thus concurrence on a single definition has yet to occur." This is natural, because each technology domain and field of technology application has their own specific needs and specific types of systems, of which a physical security system is just one example. International Organization for Standardization (ISO) began developing standards relating to SOS in 2016 and in 2019 released three standards relating to SOS lifecycles and defining terminology relating to SOS. This is an aspect of security system design that we haven't paid enough attention to, one whose importance is increasing exponentially every day.

TechTarget provides a definition for an SOS that is applicable to physical security systems: "A system of systems (SoS) is the collection of multiple, independent systems in context as part of a larger, more complex system. A system is a group of interacting, interrelated and interdependent components that form a complex and unified whole." TechTarget also points out that, "Individual systems in an SoS work together to provide functionalities and performance that none of the independent systems, or constituent systems, could accomplish on their own."

Thus, it is crucial to consider, for example, the system architectures of each individual system comprising a physical security system, given that the architecture must provide functionality that supports the purposes and requirements of the overall system. Each system must be *evolvable* in a way that enhances itself and the overall system, without breaking or diminishing the functionality of the system as a whole or any of its other parts.

### Future-Ready Network Design

A "future-ready" network is a network whose overall architecture and detailed design accounts for the inevitable expansion of its physical security system including the addition of new sub-systems as well as the expansion of existing sub-systems and their integrations. The Modern LAN network design principles and the top-down design approach described in this eBook are fundamental to achieving a network whose high performance and ease of

operation and maintenance can be maintained, improved and expanded over time through ordinary efforts and without becoming troublesome and itself posing a risk to any part of the physical security system.

This is what security industry customers need from design consultants and technology service providers (both in IT and physical security), as well as from manufacturers. It is not only doable – it's our job.

# Appendix H – Acknowledgements

Back to Appendix List

## Individual Contributors

Thanks and appreciation go to the following individuals for providing survey responses and, in some cases, in-depth discussions regarding their experiences with and considerations about physical security system networking without having seen this paper's content.

| Name | Company Name | Job Title |
|---|---|---|
| Mark Bennet | MSB Security Consulting, Inc | President |
| Marc Beningson | WSP USA | National Practice Lead |
| Jim Black | Microsoft | Sr. Director, Security Architect |
| Tommy Burns | Burns & Associates, Inc | President |
| Lorna Chandler | Security By Design Inc | Principal |
| Bill Durso | The Durso Group, LLC | Founder & Principal Advisor |
| William Edaburn | ASML | Senior Security Specialist |
| Frank Ehrman | Security Thru Design LLC | Principal |
| Roe Gammon | Henderson Engineers | Security Consultant |
| Maria Gonzalez | Teecom | Principal, Security Consultant |
| Brian Gouin | Nationwide Security Corporation | Senior Security Consultant |
| Rob Hammond | Security Consulting and Design | Owner |
| Michael Johnson | Guidepost Solutions | Senior Consultant |
| Eugene Keller | Cyber Consulting, LLC | Principal Consultant |
| Raymond Kolodzieczak | Guidepost Solutions | Senior Project Manager |
| Ray Navarro | TEECOM | Principal Consultant |
| Werner Preining | Interpool Security Ltd | European Operations |
| Rene Rieder Jr | Burns Engineering | Security Practice Leader |
| Ben Scaglione | Cerami & associates | Associate Principal |
| Adam Shane | Burns Engineering | Systems Integration Manager |
| Breanna Sieferman | TEECOM | Associate Principal |
| Dave Skusek | Triad Consulting & System Design Group | Senior Systems Engineer |
| Jeff Smith | TEECOM | Principal/VP |
| Frank Soltero | AppliedTech Dynamics | Principal |
| Jarod Stockdale | Faith Group LLC | Sr. Project Manager |
| Maria Sumnicht | OT Governance | Founder and CEO |
| Ryan Taylor | Coupang | Technology & Design |
| Rodney Thayer | Smithee Solutions LLC | Convergence Engineer |
| Jim Townzen | SRMC, LLC | Staff Consultant |
| Mike Ulwelling | Triad Consulting & System Design Group | Managing Director |
| Bryan Warren | WarSec Security | President / Chief Consultant |
| Sean Wellford | Guidepost Solutions | Senior Consultant |
| Rick Withers | Trilogy Security Consulting & Design | Owner / Principal Consultant |

## Industry Technology Subject Matter Experts

Special thanks go to individuals from the named manufacturers for providing reality checks regarding traditional and current leading field practice for security system cybersecurity for large scale security, and network design for communications systems and physical security systems deployments based on Modern LAN principals.

| Name | Company Name | Job Title |
|---|---|---|
| Ken Francis | Eagle Eye Networks | President |
| John Gallagher | Viakoo | VP Viakoo Labs |
| Richard Kasslack | NVT Phybridge | Sr. VP of Sales and Corp. Development |
| Eddie Meltzer | Security Cloud & Mobile Partners | Principal |
| Nicolas Puello | NVT Phybridge | Team Lead – Sales Engineering |
| Maria Sumnicht | OT Governance | CEO |
| Rodney Thayer | Smithee Solutions | Convergence Engineer |

## Top-Down Design

Very special thanks go to Priscilla Oppenheimer, for sharing her encyclopedic knowledge of real world networking by authoring the classic book, *Top-Down Design*, from which I have extracted many quotations for this eBook. Although written for network designers, she never forgets the customer – the ultimate reason that we have networks in the first place. You can't go wrong by taking her advice to heart and doing the thorough job that will result in a future-ready network. Available online are the entire table of contents and the first 20 pages of Chapter 1 in an online sample at the Top-Down Design link above.

# About Ray Bernard

Ray Bernard is a security consultant and author who has provided pivotal direction and advice in the security industry and the security profession for over 30 years. Ray is President and Principal Consultant of Ray Bernard Consulting Services (www.go-rbcs.com), a group of highly expert corporate, physical and IT security consultants with outstanding track records in their fields of expertise. Ray has led many noteworthy security projects for international airports, nuclear disarmament facilities, sports stadiums, water districts, electric utilities, manufacturing plants and multiple-tower high-rise facilities.

Ray is also the founder and CEO of GSO Events, Inc., the producer of the Global Security Operations events, a regional event for 40 to 50 regional, national or global security practitioners. The event takes a 3- to 5-year look ahead at where physical security leadership and advancing physical security technology are going.

He is also the Convergence Editor for *Security Technology Executive* magazine, for which he writes the monthly Convergence Q&A column as well as a highly-regarded articles about the Convergence of Physical Security and IT. He is a regular contributor to *Security Business* magazine (formerly *Security Dealer & Integrator*). He also writes the Real Words or Buzzwords? article series for SecurityInfoWatch.com.

Ray was named as one of the IFSEC Top 50 Fire and Security Global Influencers for 2018, #12 in the Security Thought Leadership category. Ray was named one of security's Top 10 Movers and Shakers of 2006 by *Security Technology & Design* magazine.

Ray has authored the book, *Security Technology Convergence Insights*, published by Elsevier and available on Amazon and elsewhere. He is a contributing author to the *Encyclopedia of Security Management, Second Edition*, covering the topics "The Convergence of Physical Security and IT", "Access Control Levels", and "Authentication, Authorization and Cryptography."

Ray has been an active member of ASIS for 25 years and participates in its educational committees and activities.