Anixter Complete Technology Solutions

PHYSICAL SECURITY SYSTEMS

INTEGRATED PHYSICAL SECURITY FRAMEWORK

It is often assumed that physical security systems work together seamlessly. The reality is that integration is complex and requires upfront planning. As physical security systems develop over time, each technology migrates at its own pace, leaving the capacity to integrate at varying levels. The ideal model is a physical security system that requires minimal customization and supports all technologies without sacrificing functionality.

COMPONENTS OF AN INTEGRATED PHYSICAL SECURITY FRAMEWORK

Proprietary	Legacy video, access control and intrusion systems with limited or nonexistent third-party integration, which often result in multiple disparate systems operating in silos. Proprietary systems provide systems integration from a single manufacturer. Third-party integrations, system options and features depend on proprietary manufacturer's roadmap and timeline.
Hybrid	Analog and digital technology mixed within the same system or appliance. Allows a proprietary and open interface technology to coexist within a single system or device. This is a transition in the conversion process and delayed investment of integration. Often the first step in migrating to an open interface and standard cabling infrastructure.
Open Interface	An integrated approach that allows for interoperability of systems through the use of APIs (application protocol interfaces) and SDKs (software development kits).
True Open Architecture	Standards-based, industry-supported, plug-and-play solution that allows multiple systems over a common infrastructure to be managed through a single user interface. Standards-based, open-architecture physical security systems incorporating intrusion and fire have yet to be introduced, while access control is under development.

WE ADD VALUE BY ENABLING:

Technology Selection	Systems Interoperability	Project Deployment

"Protected properly, the IoT will bring more efficient processing and analysis of data, so security stakeholders can take advantage of a huge resource of intelligence to detect risks proactively, respond to situations in real time and increase the efficiency of safety and security measures."

Source: SIA Megatrends Report

COMMON CHALLENGES

Adopting **EMERGING TECHNOLOGIES**

Realizing strategic **VALUE OF INVESTMENTS**

Addressing system **VULNERABILITIES**

Expanding **TECHNOLOGY CAPABILITIES**

Leveraging **DISRUPTIVE TECHNOLOGIES**

TECHNOLOGY SOLUTIONS

Adopting emerging technologies

Implementing emerging technologies with enhanced capabilities can improve operational and systems efficiencies. Understanding where technology is heading and evaluating performance is critical for successful implementation.

Realizing strategic value of investment

Intelligent devices are capturing more information, creating opportunities to utilize them for business intelligence. Advanced features can provide an avenue for cost savings and improved profitability. Collaborating to leverage business partner experience and demonstrate applications can help organizations to justify new technology investments.

Addressing system vulnerabilities

System vulnerabilities can increase if a system is not regularly maintained and updated. Adopting IT and security best practices, including a patch management schedule, following manufacturer hardening guides and policies can help protect security systems. Forgoing the investment in ongoing maintenance and security upgrades means sacrificing system performance, leaving the system open to cyber and physical attacks and limiting the opportunities for advanced integration between systems.

Expanding system capabilities

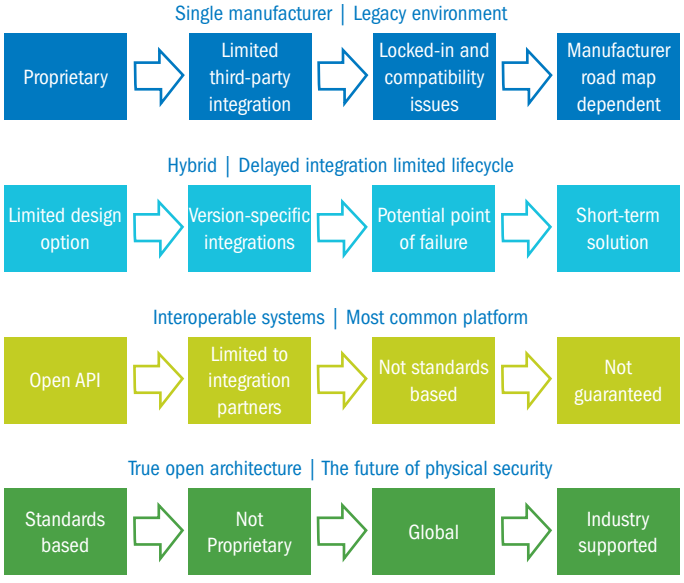
Integration of physical security systems can enable further physical and logical security collaboration. Incorporating analytics and video management solutions with advanced learning turns collected data into actionable, validated intelligence that can transform a reactive system into a predictive one for quicker response.

Leveraging disruptive technologies

Cloud and advanced analytics are disruptive technologies that can provide new insights that allow customers to extrapolate meaningful and actionable information from physical security systems. Collaborating with manufacturers, technical experts and a network of specialized integrators is key to accomplishing the goals for implementing these technologies in the future.

PATH TO TRUE OPEN ARCHITECTURE

Integrated and open systems are being driven by the need to eliminate redundancies, to improve efficiencies and to manage physical security through a single user interface. Best products can be selected for applications without encountering compatibility limitations. Developing standards like ONVIF provide a baseline that allows IP-based devices to operate together. As technologies converge, it remains critical to work with a qualified security integrator to design an integrated physical security framework.



FOR MORE INFORMATION VISIT **ANIXTER.COM/SECURITY** OR CONTACT YOUR LOCAL ANIXTER REPRESENTATIVE.

At Anixter, we help build, connect, power, and protect valuable assets and critical infrastructures. From enterprise networks to industrial MRO supply to video surveillance applications to electric power distribution, we offer full-line solutions—and intelligence—that create reliable, resilient systems that can sustain your business and community. Through our unmatched global distribution network, supply chain management expertise and technical know-how, we drive efficiency and effectiveness to benefit your bottom line.