

WHAT IS IT?

Open architecture is a software architecture that is designed to make adding, upgrading and replacing components simple. The security industry has no set definition for open architecture which allows some manufacturers to state their products are “open” by simply making their products available for integration with others. To support a true open architecture, manufacturers must be compliant with a set of industry accepted standards or specifications, or have a publicly published protocol that anyone can use.

WHY IS IT IMPORTANT?

End users are driving the industry away from closed proprietary system to open architecture for many reasons.

- Interoperability enables the seamless connection of multiple components and system software platforms without integration.
- A single user interface simplifies the management of platforms and speeds the sharing of data from multiple devices for faster and proactive responses to security threats.
- Choice of best-of-breed components and software in order to design a system that matches the needs of the end user.
- Lifecycle management, to replace or upgrade components as needs change or as technology changes.
- Lower costs, both from a deployment and integration standpoint as well as more simplified management of the security system allowing for lower personnel costs.

STANDARDS AND SPECIFICATIONS

Standard	Name	Notes
ONVIF Profile C & A	Open Network Video Interface Forum	While still in development, there are a few companies that are producing door controllers that are compliant with this specification.
OSDP	Open Supervised Device Protocol	The communication from the reader to the control panel is bidirectional and encrypted, allowing for supervision of the reader and the secure transmission of data.
ODBC	Open Database Connectivity	Is an API for accessing database management systems and is important if you want the HR system to share information with your access control system.
Open API	Application Programming Interface	A publicly published protocol detailing how to integrate to hardware or software components that anyone can use. Some manufacturers may share their “open” API selectively – in these cases, that is not considered open.

SYSTEM CONSIDERATIONS

End users expect a basic level of interoperability between access control systems and video management systems (VMS). The access control system pushes events and controls to the VMS, where they are logged, so alarms can be viewed alongside video.

Additional design considerations include:

- Interoperability with both perimeter and building intrusion detection systems, as well as the VMS and access control systems, to address incidents and events faster.
- Greater flexibility through access control software that works with multiple door and intrusion controllers simultaneously.
- VMS capability to accept information from multiple access control systems, display events and alarms, and control basic operations, e.g. locking or unlocking doors.
- Access control interoperability with wireless intelligent door hardware including IEEE 802.11 2.4GHz Wi-Fi, Assa Abloy Aperio™, IEEE 802.15.4 ZigBee, and 900MHz wireless.

For standards requirements, access control hardware and software should support:

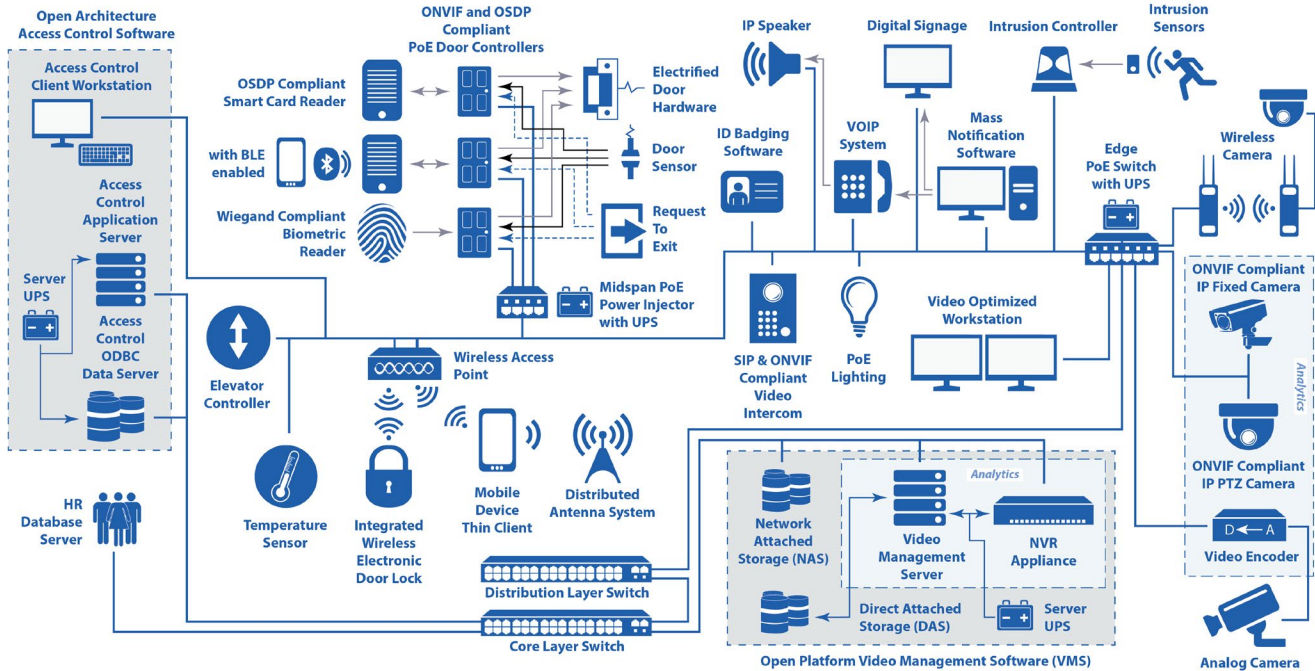
- ONVIF Profile C (door controller)
- OSDP version 2 (door controllers and card readers)
- ODBC (software)

TECHNOLOGY APPLICATION GUIDE

Open Architecture Access Control



OPEN ARCHITECTURE SECURITY SOLUTION



SUMMARY

Open architecture - while new to the security industry - is growing with end users. Anixter can provide options for open architecture systems that can be deployed for any size business or environment.

WHY ANIXTER?

- Over 1,600 sales specialists and more than 90 technology support service experts devoted to cabling and security solutions
- The broadest infrastructure offerings to fit your current and future industrial communication and control, network cabling, security application, data center and enterprise cabling needs
- Our footprint supports customers' and suppliers' operations around the globe



Technology Alliance PartnersSM



Anixter's Technology Alliance Partners provide solutions designed to connect the world's most important systems. Our partners help organizations operate more efficiently and securely, while maximizing value.

About Anixter: anixter.com/aboutus
Legal Statement: anixter.com/legalstatement

Anixter Inc. World Headquarters
2301 Patriot Boulevard
Glenview, Illinois 60026
224.521.8000

16G7139GL © 2017 Anixter Inc.

1.800.ANIXTER | anixter.com



Products. Technology. Services. Delivered Globally.