

WHEN A SECURITY SYSTEM OFFERS MORE THAN JUST SECURITY

As technology has advanced, security has branched out beyond simple surveillance and intruder deterrence. A security system can now be made up of multiple sensors that provide data about the environment. For example, a door position switch is a sensor that tells you whether a door is open or closed, a thermometer is a sensor that gives you temperature data, and water pressure and flow sensors provide data about your water sprinkler systems.

As systems have migrated to the use of Ethernet as a communication protocol and interfaces with other systems have been developed, the data that each system provides can now be more readily used in another system. Security is one of these systems that migrated to the use of Ethernet and we are just starting to see some of the possibilities that this is offering far beyond security purposes.

Imagine the following sequence of events:

1. You enter your company's parking lot. By either presenting your badge at a gate (access control) or a camera identifying your license plate (video surveillance with analytics), the system identifies you as being on the property.
2. You enter the building at your usual entry point (access control). If at an unusual entry point or at a different time of day, the system recognizes an anomaly and flags that data for observation by those concerned. Facial recognition verifies that it is you using the associated credential.
3. At the time of your entry, the temperature (HVAC) and lighting (building automation) adjust your work area to the level specified when occupied.
4. When you attempt to log in to your network device (network administration), it first checks to verify that you are on the property by interfacing with the access control system.
5. If you leave the property for lunch or the end of the day, facial recognition and access control at building ingress/egress note that you are exiting and send that data to network administration. The logical security system is locked for your network account. The HVAC and lighting adjust as appropriate.

This sequence may have been possible in the past, but it would have been done through many inputs and outputs on the various systems. Now that these systems can link via the Ethernet protocol, the software links provide network intelligence that can automate the events.

One of the challenges to creating these links is that each software is constantly being updated and improved by the manufacturer. We have not gotten to the single pane of glass for end users to see every system in their facility at the same time. They currently must jump from one system to the other for correlation of data. As that software system is developed, many standards will need to be developed to maintain those links.

Standards in building automation and communication are developing in each subsystem. IEEE provided us with 802.3 for wired Ethernet and 802.11 for wireless. Now each subsystem needs to develop a standard interface to a software that uses that protocol. That single-pane software will need to communicate with the interface that each subsystem provides as a standard. For example, video surveillance uses the ONVIF video and access control profiles to offer an interface, whereas lighting, HVAC, and other systems will be offering systems that use an open interface for integrating data to a single platform.

As new technology continues to enter the market, you can expect to see even more devices join the Internet of Things to bring building intelligence and automation to a whole new level.

Visit anixter.com/security to learn more about Anixter's security solutions.

