

SDM

NEW DIRECTIONS FOR SECURITY SYSTEMS & INTEGRATION

HOW TO BUY SINGLE-DOOR ACCESS SYSTEMS

Single-door, standalone access control devices are actually far less complicated than the elaborate industry parlance describing them would imply. All such systems have two characteristics in common. They are mechanically or battery-operated and autonomous. What could be simpler than that?

"There are two stratum of standalone products currently available in the marketplace," explains Chris Nieshalla, marketing manager for IR Security and Safety, Carmel, Ind. "The first is represented by the pure and basic type of system often deployed on storeroom doors and other low-level security portals.

"Most systems of this type are anything but fancy," he notes. "Non-computerized and key or membrane pad-based, they provide protection when a lock and key is not enough but more heavy-duty security measures are not mandated."

Level two systems are computerized, Nieshalla continues, but still battery-powered and not networked. Nevertheless, they are "intelligent" systems. Programmable via PC, Palm Pilot or iPAC, level two standalones can be scheduled to lock, unlock and relock at times of day redesignated by programmers.

They also can be cued to accept or reject electronic credentials, such as magnetic stripe cards, proximity cards (which work on radio frequency identification or RFID), and iButton devices (which are microchips housed in small metallic cylinders attached in most cases to a key chain).

Straight standalone keypads are just entering the commodity phase, Nieshalla adds. More common now are ID-based, locking systems in which access control and locking are merged into a single product. In the security marketplace, such systems are referred to as "single-door" or "self-contained access control products." This is because the two are virtually synonymous concepts.

STANDALONE SHORTCOMINGS

"The mechanical standalone offers a convenient way to control access between public and private

Not restricted just to keypads and cards, standalone systems are being operated with smart cards, biometrics and iButton devices.

By D. Douglas Graham

areas," declares Jo Brown, advertising coordinator, KABA Access Control, Winston-Salem, N.C. "There are no keys or cards to manage, no computers to program, no batteries to replace and combinations can be changed in seconds without removing the lock.

"Those are the high sides of the technology," she asserts. "Its major disadvantage is the fact that you have no audit trail allowing you to review who's come in and out of your protected space. For that you need a software program."

Although standalones in general fall more or less into the category of affordable security (prices range from the low hundreds to \$10,000 or less), they come with several downsides. Principal among these may be the fact that their functionality is completely dependent on the information that has been programmed into them.

"Typically an online system would allow for more users than a standalone," points out Mark Dearing, product manager, Stanley Security Systems Inc., Indianapolis. "While online systems are programmed with an internal database population, they also allow you to expand that database from without.

"You might have an internally-programmed population of 1,000 users and another 5,000 online you can route to the door," he theorizes. "An online system, in other words, can be adjusted. This is not the case with standalones."

Standalone systems also are extremely high maintenance, maintains Peter Boriskin, chief technology manager for Fire & Security Access

SDM

Control and Video Systems, part of Tyco International Ltd. (Software House, Boca Raton, Fla., is a subsidiary of this company).

Because each system is autonomous, two doors require twice the administrative effort, four doors four times the work and so on, Boriskin insists. Moreover, every time a new individual is added to the roster of personnel authorized to enter a secured space, his or her name must be hand-keyed into the system.

"Traditional standalone, single-door access systems have a very limited scope," Boriskin stresses. "They can also turn into a huge headache when many new people are added to the list of authorized personnel."

BIOMETRICS

Currently, there are only three possible methods of authentication, Boriskin explains – something you have (a card for example), something you know (typically a PIN number) or something you "are." Biometric access control devices cue-in on the last of these.

The technology grants authorization based on physical characteristics, such as fingerprints, voice printing or hand geometrics, and identifying signatures read in retinal, iris and full-facial scans.

"The lowest-priced standalones are the simple keypad systems, the highest the biometrics," declares John Smith, product marketing manager, Honeywell Access Systems, Syosset, N.Y. "There are standard keypunch systems available right now for less than \$200.

"From there, you move up a peg to the magnetic stripe readers, which will usually cost an end-user between \$300 and \$400," he notes. "Next are radio frequency proximity cards. These are good for outdoor applications because there's no physical contact involved. A typical price for a proximity system is \$400 to \$500.

"Finally, you have the biometrics," Smith adds. "These can run as low as \$1,000 for fingerprint readers all the way up to \$10,000 for facial recognition."

Biometric scanning systems scan for highly specific anatomical characteristics. Fingerprint readers look for from 15 to 30 minutia points on the fingerprint of the person seeking entry.

The system collects the points and converts them via an algorithm into a numerical representation of the fingerprint. Access is granted when the representation matches the one already programmed into the system.

Hand geometric systems read the bones of the

hand, whose length and spatial arrangement are highly individualized from person to person.

Retinal readers no longer are widely used because they have acquired a reputation for being personally invasive technology. Iris-reading is much friendlier because it is really nothing more than capturing a photographic image.

Voice is an emerging, ultrasound technology, and facial recognition is an even more futuristic access control method in which an entire countenance is scanned for identifying characteristics.

NEW DEVELOPMENTS

"Dealers are looking for more diverse product," maintains Thomas Moro, access systems product manager for Amano Cincinnati Inc., Roseland, N.J. "We're seeing products now that ask not only for identification but justification.

"After the person presents his tag, he's asked to key in a 'reason' code based on what he sees on the legend next to the reader," Moro relates. "Not only does he have to tell the system who he is, he has to provide it with a good reason for letting him in."

Recent years have brought significant improvement to standalone systems. Not only have they been enhanced functionally, they also have been modified for use outside. Membrane keypads, weather shield and stainless steel keypads all now are commonplace inside and outdoors.

The systems also have been cosmetically improved though changes in size, color and other aesthetics that help them blend better with the environment in which they are deployed. However, according to industry experts, the biggest improvement has not been in functionality, weather-resistance or cosmetics, but intelligence.

"Smart cards are so named because they are programmed with memory," Boriskin explains. "With process and memory, the cards not only send information to the reader but pick up data from the reader.

"Things like user transactional history, access rights and privileges can be transmitted to the reader and collected as well," he adds. "Until smart cards, this sort of thing was not possible without some form of computer intervention. Now you can do with a card what you once had to do with a laptop, iPAC or Palm Pilot.

"Smart cards are a hugely important development with the potential to revolutionize the standalone reader market," Boriskin maintains. "The market won't be the same after smart card technology becomes pervasive in our industry. Smart cards will change everything." ■