The Advanced Analytics of Security Entrances

BOON EDAM

your entry experts

Security entrances actually have access to **extremely important security and operational data** that can **add significant value** above and beyond what most access control systems can provide.

Executive Summary

Controlling physical access to sensitive areas is the primary purpose of any physical security system. To achieve this physical control, every security system must include, at a minimum, three primary system elements:

1. A physical barrier or perimeter that defines the controlled area

2. An access control system to trigger the admittance of authorized people

3. Security entrances to provide access

It would be easy to think that all of the intelligence, data, and analytics associated with the physical security system is collected and used by the access controller, but that would not be correct. On the contrary, security entrances actually have access to extremely important security and operational data that can add significant value above and beyond what most access control systems can provide.

Collecting and making use of the analytic data available from modern security entrances can help improve both security and operations at many facilities.

Part I. The Current State of Access Control Analytics

Security management teams at many organizations, and perhaps even parts of the larger security industry, are still coming to terms with the existing weaknesses in their current security systems. One indicator of the current state is the lack of meaningful security and operational analytics that are collected and reported by these systems. In this section, we cover the current state of access control analytics, and highlight the available data and analytics that are not being used by today's systems.

Access Control: More Than a Controller

Here at the outset, it is important to note that within the security industry, the term "access control" is often used to refer to the control system that manages the list of authorized people and their credentials. The system triggers access when the authorized credentials are presented at authorized places and times. In truth, the control system is only one of the elements required to implement effective access control.

In general, access control requires three primary elements to be effective. Each of these elements may be made up of a variety of sub-systems:

1. **Physical barrier or perimeter.** This element may be made up of perimeter fences and walls, the walls of a building, its windows, and even interior walls and fences. The function of this element is to define the controlled area and prevent any entry except at the controlled entrances.

2. **The control system.** This element includes the controller itself, along with the credential reader function, the memory or communication function to check the presented credentials against the authorized credential list, and the linkage to the controlled locks or other access mechanisms. The function of this element is to determine the legitimacy of the credentials, generate and retain the required records, and trigger the unlocking or opening of the entrances.

3. **Security entrances.** This element includes the actual entrances that provide access to the controlled area when triggered by the access controller, along with any controlled locks or mechanisms required for operation. Some security entrances include their own controller that supervises their operation or the inputs of related sensors to provide additional functionality. Security entrances come in a variety of styles to meet a range of required security levels and throughput needs.

For the purposes of this paper, we will use the term "access control" in the broad sense that includes all three primary system elements, not just the controller. We will use the term "access controller" to refer to the credential management and authorization control system, and "entrance controller" to refer to any control functionality built into the security entrances.

Analytics and Security Weaknesses of Current Access Control

Despite the substantial attention and investments in security over the last 10 or 15 years, many current physical security systems have significant weaknesses inherent in their design and/or implementation. These weaknesses lead directly to lower actual levels of security than intended, as well as to a deficit of operational data and meaningful analytics that could be useful for making security and operational improvements.

Here is, perhaps, the biggest weakness in access control today:

> Most access controllers available today were developed in a world of swinging doors, and many facilities still use swinging doors as part of their security and access control systems.

Security entrances provide access to the controlled area **when triggered** by the access controller.

Swinging doors can only provide extremely **limited information**, such as "I'm open" or "I'm closed," which is **insufficient** to support any **meaningful analytics**.

Inherent Weaknesses of Swinging Doors

Why are swinging doors such a security issue? The short answer is that swinging doors have inherent weaknesses that cannot be overcome except by implementing a redundant security system such as security guard staffing or video monitoring. Here are some of the issues inherent in swinging doors:

1. When closed, swinging doors provide complete control of an entrance. When open, however, they transition to providing no control. When open, any number of people can pass in an uncontrolled fashion, in either direction, without presenting any credentials.

2. Even when used with an access controller to trigger unlocking, swinging doors generally cannot confirm that the specific authorized individuals, after presenting their credentials, actually passed through. In fact, these doors often cannot detect whether anyone actually passed through.

3. Even when used with an access controller, swinging doors offer no restrictions to the removal of an unlimited quantity of materials or goods of any size that will pass through the doorway.

4. While many, or most, access controllers have anti-passback functionality, swinging doors generally render this function ineffective. That is, most controllers will recognize that credentials presented for entry should not be used again for entry unless the person has already 'badged out'. Without this function, a card could be used repeatedly to trigger unlocking, then "passed back" to associates to be used again later. When used with swinging doors, however, the system cannot be sure that anyone actually entered when authorized, generating so many nuisance errors that the function is normally turned off.

5. Finally, swinging doors have an inherent weakness in the provision of data and analytics. This is because they can only provide extremely limited information – basically, just "I'm open" or "I'm closed" – which is insufficient to support any meaningful analytics.

Inherent Controller Weaknesses

Access controllers are another source of security issues in perimeter protection. Because they were developed in a world of swinging doors, many access controllers have "designed in" weaknesses that reflect the inherent weaknesses of these doors. Here are a few examples:

1. Because swinging doors are unable to provide useful security or operational data back to the controllers, access controllers generally haven't been designed to capture this kind of data. In almost every case, they are only designed to capture the door status and the identity of the credentials presented.

2. As mentioned, when access controllers are implemented with swinging doors, they generally cannot distinguish between a "credential pass-back" and a "failed entry and retry", among other everyday, common complications.

3. No matter how complex their programming, logic, and functionality, access controllers implemented with swinging doors cannot prevent tailgating infiltrations.

4. And, without the capability to capture security and operational data, access controllers cannot collect and make use of any additional information that could be provided by the doors, nor generate meaningful analytics from door information.

The bottom line is that the inherent security weaknesses of swinging doors make them the weakest link in many physical security systems. And, this means that they are also the weakest link in many cybersecurity systems, since physical access to internal network assets can generally bypass many of the safeguards normally in place for electronic assets!

In terms of the focus of this paper – analytics – it is clear that because of the use of swinging doors, as well as the impact of a "swinging door" world on the design and development of access controllers, there are limited analytics being generated, collected, or understood in today's access control systems. This is an information gap, as the data could otherwise be used to understand and improve the facility's security posture, as well as to gain insight and make improvements to operations.

Today's security entrances not only provide enhanced security by reducing or eliminating tailgating and other security weaknesses, but they can also collect and provide valuable security and operational data that can support improvement programs. In the next section, we will examine these in more detail.

Part II. The Improved Security and Information of Security Entrances

Security entrances are completely different from traditional swinging doors. These differences support a wide range of security and operational improvements for security teams.

Security Entrance Advantages Over Swinging Doors

Security entrances do not have the inherent weaknesses of swinging doors – in fact, they have substantial advantages, as they were specifically designed to strengthen the security posture of a facility. Here are a few of the ways they can support this purpose:

Unlike swinging doors, many **security entrances** are capable of capturing and delivering **meaningful data** regarding security and operational factors.

Types of Security Entrances

Tripod Turnstiles

For applications where crowd control is the main security goal, tripod turnstiles are an ideal solution as they effectively direct users through specific, guarded entry points. Entertainment venues, transit stations, and public buildings, among many types of applications, choose tripod turnstiles for their ability to withstand a large volume of users.

Full Height Turnstiles

Rugged, low-maintenance solutions for the harshest outdoor conditions. They act as a deterrent against tailgating and unauthorized entry at your fence line. Building interiors can also benefit with transparent full-height turnstiles designed for this purpose. They are also well-suited as exit-only solutions for many applications.

Optical Turnstiles: Barrier-Free

Manage the movement of people in lobbies and building interiors with varying degrees of security clearance. Users around the globe are implementing optical turnstiles coupled with an access control or visitor management system. Barrier-free optical turnstiles effectively detect tailgating with minimal inconvenience to users and without forming an obtrusive barrier.

Optical Turnstiles: With Barrier

These optical turnstiles include a physical barrier to entry for enhanced security. Options include glass panels that swing, slide, or utilize retracting angel wings, plus a variety of heights. All act as a physical deterrent to entry while being aesthetically appealing.

Security Revolving Doors

An unmanned solution that is ideal when you need both high security and high traffic flow. Security revolving doors prevent tailgating by design, and can be upgraded to stop piggybacking attempts. Payback is possible in just one to two years.

Security Portals

Unmanned entry solutions that reliably and predictably prevent tailgating and piggybacking into sensitive buildings or interior areas. They operate with any type of access control technology and can accommodate two- or three-factor authentication to offer the highest-level of security available in a physical entrance.

Security entrances, making use of an entrance controller, can **capture analytics** about user behaviors and **tie that information** directly to **threat and risk assessments**.

1. Security entrances come in a range of types and security levels to meet a wide range of application needs. (See the sidebar on entrance types). At the lowest security level, they can regulate the movements of a large crowd for safety and swift throughput. At the highest levels, they can completely eliminate unauthorized intrusions, tailgating, and piggybacking without requiring any supervision by guard staff.

2. At every security level, security entrances are designed to ensure that only authorized people enter or exit.

3. Unlike swinging doors, many security entrances are capable of capturing and delivering meaningful data regarding security and operational factors. For example, failed entrance attempts, tailgating and piggybacking attempts/alarms, and similar data can all be easily captured by the entrance controllers for review and use.

Security Entrances Provide Additional Data

Valuable security and operational data is available for the taking, and it can support analytics that can be used for guiding improvements, in terms of security and also in training, operational planning, and other business purposes.

For example, current access controllers can capture and log such data as entry attempts, accepted and denied credentials, and the times and locations of each event. These data points are submitted to the controller from the readers at the entry locations. While we are accustomed to this level of security data, with a little thought it becomes clear that this level is fairly superficial. It cannot address deeper questions such as how often intruders tried to tailgate an authorized person – or how often they were successful.

In contrast, security entrances, making use of an entrance controller, can provide more complete information about what has occurred. They can capture analytics about user behaviors, and tie that information directly to threat and risk assessments.

Consider the operation of a security revolving door and the information that can be captured for every entry attempt. In this case, a typical access controller would know if and when credentials were presented, accepted, and door access was triggered, just as it does with swinging doors today. It would also log the identity of the credentials.

In sharp contrast, the security revolving door and its entrance controller knows much more, including how many times:

- entry was authorized *and the person successfully entered*
- entry was authorized *and the person didn't enter*
- entry was authorized, the person entered, *and a second person tried to enter* with them in the same compartment (piggybacking)
- entry was authorized, the person entered, *and a second person tried to enter* in the following compartment (tailgating)
- entry was authorized, the person entered, *and a second person tried to exit* in the opposite compartment (unauthorized exit/entry)

The sophisticated design of the **StereoVision 2®** system lets managers select the desired **balance between security risk and user convenience** by making use of a **predictive probability metric**.

Clearly, this more complete information would be of high interest to security and facility management because it affects both security and operational issues. Today, unfortunately, many access controllers generally do not have the capacity to collect or make use of this level of information. However, Boon Edam is working with select leaders in the field to improve these capabilities going forward.

Predictive Metrics

When it comes to certain security entrance models or designs, it may be possible to go even further. This is true, for example, of a Boon Edam entrance called the Circlelock Solo security mantrap portal that is equipped with two curved sliding doors. The outer door opens based on a presentation of credentials and authorization from the access controller. Once the user has entered the portal, the outer door closes and a unique presence detection system (called StereoVision 2®) confirms that the user is alone, preventing piggybacking. At this point, an optional, interior biometric identification system can be used to confirm the identity of the user. When a clear signal is given, the second door opens and the user can enter the secured area. In this way, the Circlelock portal and its entrance controller ensures that only the right person is admitted.

Because of the design of the Circlelock portal and the unique sensor system used to confirm that only a single person is in the portal chamber, there are some settings that can be used to fine tune the operation of the unit, along with the desired level of security. For example, at high sensitivity levels, the system can detect and reject every piggybacking attempt, but at the expense of an increased likelihood of a "false positive" – that is, that a single authorized individual would be wrongly rejected for wearing a backpack, for example. By lowering the system sensitivity, security management can reduce the number of these false rejections, but by doing so they increase the risk of a potential piggybacking breach. The sophisticated design of the StereoVision 2® system lets managers select the desired balance between security risk and user convenience by making use of a predictive probability metric. Predictive probability metrics cannot be provided by other types of controlled entrances, or even by security guards stationed at entrances. (See the sidebar for more information on predictive metrics.)

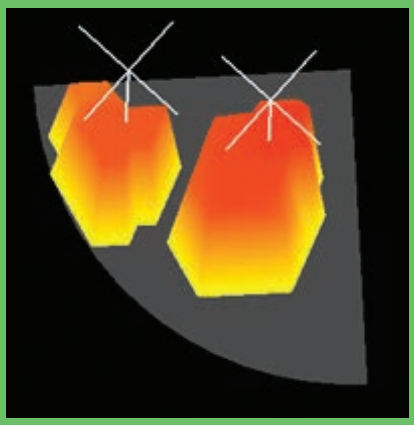
Security Entrance Sensors and Predictive Metrics

A critical element of a high security entrance is the ability to use interior sensors to confirm that only one person is attempting passage. When such an entrance is used, whether it is a security revolving door or a mantrap portal, there is a point where the person attempting passage is temporarily "trapped" inside a compartment. It is at this point that the sensor technology confirms that only one person is in the compartment.

In the past, sensitive floor mats were used to detect more than two feet pressing on the floor of the chamber, but people quickly found that if one person literally was "riding piggyback" on the other, this test would be defeated. Setting a weight range could exclude some piggybacking attempts, but that approach raised other complications. Weight mats are not in common use any more.

Instead, leading suppliers have improved other types of sensors to achieve this task. For example, Boon Edam employs a sophisticated overhead sensor technology called StereoVision 2® which scans the entire compartment using near-infrared scanners and "time of flight" technology. By measuring the time it takes for beams to bounce off objects in the chamber, it forms a 3D image of the contents of the compartment; by analyzing this image, the system can determine with a very high accuracy whether one or more than one person is in the compartment.

Managers can adjust several parameters in StereoVision® that will affect the sensitivity of the assessment to meet the needs of a facility; this exercise results in access to predictive analysis of the risk of a potential breach by piggybacking. As a manager adjusts the sensitivity higher, it is more likely that individuals will be rejected erroneously for wearing a lumpy backpack or fidgeting, for example. Lowering the sensitivity will decrease rejections (be more forgiving) but increase the risk of potential piggybacking breach. Calibration therefore involves finding the balance between convenience and risk. As the sensitivity is adjusted, StereoVision 2® displays the chance of a successful piggybacking breach as a percentage per 100 attempts using highly accurate sampling data. Considering that piggybacking attempts are rare to begin with, many managers have calibrated their doors to a risk of piggybacking to 5% or lower, while still keeping unintended false rejections at a reasonable level. This is an example of the predictive probability metric regarding potential breach that can be obtained for a given entrance, which is something that other types of security entrances or guards cannot provide.



Infrared detection of piggybacking attempt

Managers can also set every employee entrance to the same settings across many facilities, or tailor each door differently to meet unique needs. Once a manager determines a set of preferred settings, all the doors set the same way will work in the same way, regardless of where they are located, time of day, or any other variable. This way, management can have a clear understanding of the risk at these entrances and be certain that any infraction is not an accident.

For mantrap portals, there is one additional assurance that can be employed. To ensure that the person that presented the accepted credentials at the start of the process is the same person that is passing through the portal, a biometric sensor can be located in the transit compartment to confirm the identity of the person as they are passing through the portal. If they cannot confirm their identity with the biometric sensor, they are denied entry.

Operational Data

Security entrances can also collect and track analytic data in the entrance controller regarding the condition of the door, its current status, and its ability to function. Collecting and analyzing actual operational data can help security management gain a clear understanding of real usage patterns, empowering them to prioritize and implement improvement actions.

For example, actual operational data may highlight precursors to trouble, such as sensor malfunctions, or a greater number of user rejections than normal. Such indicators can trigger proactive maintenance, repair actions, or even a training activity – whichever is indicated, avoiding the disruption and high cost of emergency repairs or downtime.

In addition, real usage data can also point to operational improvements, potentially providing input into a wide range of items such as the timing of parking lot lighting, efficient work scheduling, and any other matters that may flow from the analysis of real worker arrival and departure data.

Future Potential

In the future, stronger security entrance integrations with other security systems could also lead to ongoing improvements. For example, a tailgating attempt might trigger the door to alert the video surveillance system, so that it could preserve and highlight the 10 seconds before and after the intrusion attempt for additional review and, if indicated, follow up action.

And, arming security management with a greater amount of real and accurate usage data supports a deeper understanding of actual security and operational conditions. For example, a deeper understanding of tailgating attempts makes it more possible to drill down to the root causes for these attempts, and to provide for appropriate countermeasures.

A **deeper understanding of tailgating** attempts makes it more possible to **drill down to the root causes** for these attempts, and to provide for **appropriate countermeasures**.

Boon Edam will continue to work aggressively with select security system manufacturers to **capture and report security entrance analytics** that can **support improvements** for both security and operational matters.

Conclusion: Access Control Analytics Can Bring Value

After reviewing the data that is made available by security entrances, the current situation clearly seems to represent a missed opportunity. The data is there for the taking, yet current access control systems, as well as other security systems, generally do not have any provision for capturing and reporting this data, and are not yet making use of the data. As a result, security management is also deprived of the potential insight and value that the data from security entrances could provide.

Fortunately, there are signs that the situation will change in the very near future. For example, Boon Edam will continue to work aggressively with select security system manufacturers to capture and report security entrance analytics that can support improvements for both security and operational matters, particularly when joined with the log information from access controllers. These improvements will directly address the current rising awareness of risks and risk management, along with addressing evolving guidelines coming from regulatory agencies.

Going forward, savvy security teams are starting to recognize the potential of system upgrades to go beyond improving facility security and safety, which they certainly do, to provide tangible operational and financial benefits. These benefits change the nature of security entrance upgrades from a cost item to an investment item, because they can make positive contributions to organizational ROI – a win/win scenario for both security and business management.