

Recognizing Security Principles in the Access Control Point Design & Construction Process

This white paper examines the role security principles play in achieving a performance-based, 'systemic' view of the engineering, design and construction of Access Control Points (ACP). The goal of this paper is to shed light on the application of security principles and how these may serve as the 'glue' that connects many separate ACP concepts and stakeholders.

Introduction

There has been exponential growth in the US industrial security marketplace and specifically in the perimeter security sector in recent years. This new attention has resulted in a number of exciting advances in design/engineering guidance, technology and the number of industry participants. Yet, as with all growth and advancement, there remain many opportunities for improvement.

First, clarify the term 'Access Control Point' (ACP). For the purposes of this document the US Army term has been borrowed. The ACP is the entry/exit corridor at the perimeter of a facility. There are a number of complimentary terms including Entry Control Facilities (ECF), gates, checkpoints, building entrances and others. Irrespective of the term used, these corridors define the ingress/egress point through a facility's/building's perimeter security systems. It is broadly recognized that the perimeter security system (including the ACP), whether simple or complex in design, is the first and best place to defend against a perceived threat.

Following the advent of 9/11 the demand for physical security initiatives at the ACP increased dramatically. With increase in demand came new security directives, guidelines, design guides, technologies and channel participants (architects, engineers, general contractors, subcontractors).

There is a common tendency to look at new technologies as the quick fix to security problems (e.g. the latest vehicle barrier or detection sensor technology). While many stakeholders will acknowledge that a 'systems-based' approach is best, this often doesn't happen because it is felt that all of the factors cannot be controlled. This is compounded by the fact that the construction industry is still very stove-piped; the segmentation of disciplines into responsibilities, project phases and core competencies doesn't equate into a team-based approach and systemic view of security.

Why is a ‘Systems Perspective’ Important?

Jacques Chirac said “Terrorism has become the *systematic* weapon of a war that knows no borders or seldom has a face“. The emphasis here is on the word ‘systematic’. The enemy is meticulous, patient and has demonstrated the ability to think from a ‘systems perspective’. The response must be equally thoughtful. Therefore, systemic thinking must be applied to the ACP.

The process of engineering and constructing Access Control Points has evolved over the last few years. Yet, for all of the advancements, the approach is often hampered by a silo-based mindset that is common in the construction environment. Policy and directives lead to engineering and design which in turn leads to construction. While there are benefits to levels of separation, it can be counterproductive when a ‘systems-based’ approach is required. Also, there are a number of stakeholders involved in the process including engineers, architects, security and law enforcement professionals, equipment manufacturers, contractors and specialty subcontractors. Each stakeholder plays a vital role in insuring that the finished product safely allows the right people into a facility while effectively stopping the threat.

An interesting challenge to be faced is that all stakeholders do not speak the same language. One of the basic drawbacks relative to the ACP has and remains the challenge of fostering teams that think from a systems perspective. Different stakeholders speak distinct languages that are common to their disciplines. Each views solutions through a unique set of lenses. These languages include engineering, architecture, security, law enforcement, technology and more. There is, however, a common language. It is the language of ‘systems’. These are not independent systems like electronic security, vehicle barriers or traffic flow but the collective ACP system and its dual function of allowing access to friends and denying enemies. The ‘System’ is the entire ACP and how it works as a seamless entity designed to meet its intended functions.

A Security Practitioner’s Perspective

Security requires much more than getting the right technology. It’s about creating *systems* that balance the fundamental building blocks of security; People, Procedures and Equipment; operating as one, so the function of the whole accomplishes its intended purpose.

As security practitioners, it is recognized that a rudimentary understanding of security principles can serve as a common language that supports ACP design and construction. While there are a number of design guidelines (e.g. the Unified Facilities Criteria, UFGS, SDDC-TEA 55-15 and the Army Access Control Points Standard Definitive Design, etc) many stakeholders are not familiar with the security principles that serve as the *foundation* for ACP design. A broader understanding of these principles can serve to equip all stakeholders to work as a ‘Team’ to achieve a successful project.

Systemic Thinking – Principles vs. Methods

“...As to methods there may be a million and then some, but principles are few. The man who grasps principles can successfully select his own methods. The man, who tries methods, ignoring principles, is sure to have trouble.” - Ralph Waldo Emerson

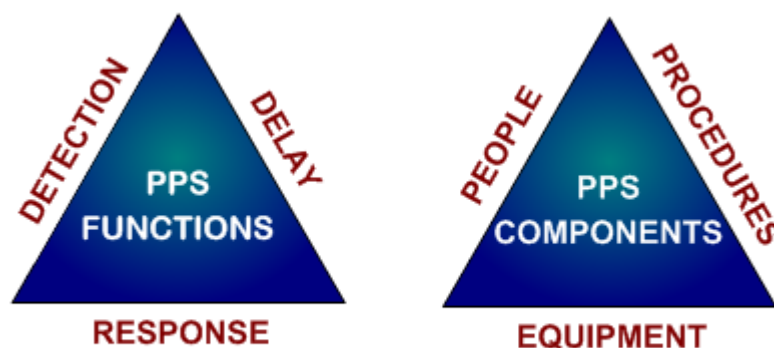
There are many methods for designing, engineering and/or constructing an ACP that are fine as long as the underlying principles that make each site unique are understood. From a security perspective, thinking systemically about the design and construction of an ACP requires the successful application of both principles and methods. Yet, there is a distinct difference between the two. Webster defines them as follows;

Principle: a comprehensive and fundamental law, doctrine, or assumption

Method: A procedure or process for attaining an object: as a way, technique, or process of or for doing something (2): a body of skills or techniques

On the topic of ‘Principles’ versus ‘Methods’, the security practitioner looks first at principles as the underlying backbone on which individual methods can be applied to create a successful project.

From this perspective, an Access Control Point (ACP) is a Physical Protection *System* (PPS) designed to integrate People, Procedures, and Equipment for the protection of assets or facilities against an attack. The security functions of the ACP include Detection, Delay and Response. From both the design and construction perspectives, the ACP as a Physical Protection *System* (PPS) Balances Design, Performance and Costs



Introductory Security Principles for ACP Design

Now that the role of principles in a systemic approach is recognized, the five useful security principles that a practitioner applies when looking at an ACP will be explored.

Security Principle #1: Delay without detection is not delay

Example: Consider the dead-bolt on the front door of a home. This is a classic delay barrier. Presuming one is purchased with the recommended one inch throw bolt, it will take some period of time for an intruder to penetrate the door. For instance, it may take a burglar, armed with rudimentary tools, five minutes to break through the door. It would seem reasonable then that the time value of the lock as a delay barrier is 5 minutes. However, on most household alarm systems the burglar isn't detected until the door is opened. Now it is seen that the time value of the lock as a physical barrier is actually zero. If the homeowner isn't home it wouldn't make any difference whether it took the burglar 5 minutes or 5 hours to get through the lock because **delay without detection is not delay**. This is why physical barriers, while very important, should be placed behind or in conjunction with detection sensors. For instance, using our home example, if there was a pressure sensitive mat in front of the door that detected the presence of the burglar, the time value of the lock is now valued at 5 minutes.

This principle also applies to the ACP. The final denial barriers are placed at the end of the 'Response Zone' and the entire ACP should be designed so that the passive and active barriers create an envelope of protection with equal ratings.

A common but limiting design approach is to be too product-centric; focusing primarily on the (active) final denial barrier with minimal attention to the detection elements within the ACP. Instead, take a systems perspective and look at how the detection elements of the ACP (over speed detection, CCTV, etc.) work in conjunction with the delay barriers.

Security Principle #2: Detection without assessment is not detection

Example: Using the home example again, let's now assume that the burglar has gotten through the front door and has been detected. Several things are assumed; (a) the alarm system has done its job and there is indeed a burglar present, (b) no one is home, (c) there isn't any onsite remote visual verification (e.g. CCTV) and (d) the alarm has been sent to a remote monitoring station. Presuming the monitoring station is on-the-ball and immediately dispatches the police to the house, it is still not known if the alarm is valid until the police arrive. It isn't until the police arrive at your house and assess the alarm do we know whether the detection is valid or not. In short, there must be a human interface with the system to confirm the validity of the detection, assess it and bring that phase of the alarm process to a close. **Without assessment we don't have detection.**

The application of this principle to the ACP is similar to the burglar alarm in the home intrusion example. First, detection takes place. This may occur, for instance, from the over-speed or wrong-way detection sensors. Presuming the detectors were installed correctly and are working, the detection process isn't complete until assessment takes place. The security forces on site assess the detection, determine whether there is a bona fide threat and close out the detection phase.

The ACP presents a unique case where the 'People' and 'Procedures' components of the PPS must be well articulated. This stems from the fact that security personnel have very little time to react against the most common threat; a moving vehicle. Depending on the design guidelines being used to lay out the ACP, the response time can be as short as seven or nine seconds from the point of detection. This is a very short period of time. Meeting these design standards is only possible with a clear systemic view of the ACP and all of the interrelationships between People, Procedures and Equipment.

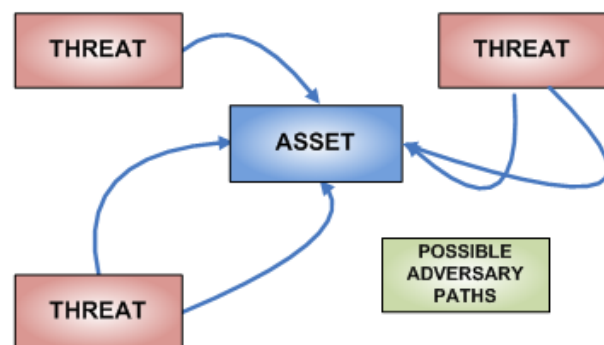
Security Principle #3: People make great assessors but poor detectors

Example: One of the classic examples of this principle was studied in prison security control rooms where the guards were monitoring multiple banks of Closed Circuit Television monitors. Studies have shown that after a very short period of time a guard will not see an intruder on a CCTV monitor. The guard, in essence, becomes immune to the presence of a threat. This is why most security systems are set up to annunciate on 'exceptions' to a normal state as opposed to relying on the guard to detect when that takes place. In short, **people make great assessors but poor detectors**.

This is a particularly important principle to remember as it relates to the ACP. A common mistake is to assume security personnel will be able to detect a threat in a sufficient amount of time to respond and deploy the final denial barriers. Required response times are simply too short and people don't make good assessors. The decision to rely solely on security personnel can stem from any number of reasons including costs or the assumption that security personnel will detect an ensuing threat. From a practical standpoint, security personnel should focus their attention on procedures that require direct human interaction including ID checks and overall ACP security management. It's the role of detection equipment to alert on a threat and allow security personnel to function in an assessment role.

Security Principle #4: Adversary path

Example: Go back to the home example. The **Adversary path** is the route that the burglar takes to accomplish the objective which in this case is to take valuables from your home or harm people. There are a number of paths the burglar can take through the home to accomplish the objective. For instance, they may go up



a staircase to the bedroom or take another path to some other room in the house. In more complex environments, there will be multiple Adversary Paths. The adversary (Threat) will, in theory, attempt to minimize detection probability until detected and then minimize path time until the event is carried out—this is the worst case scenario.

In the ACP security looks at multiple Adversary Paths. The more obvious ones are highlighted by the various threat scenarios listed in various design directives. For example, in the Army Access Control Points Standards Definitive Design Guide there are four Threat Scenarios;

1. Vehicle Threat Scenario #1. Threat vehicle enters the ACP in the inbound or outbound lane(s) at the maximum speed attainable at the ACP entrance and then immediately accelerates at its maximum acceleration rate through the ACP. Army policy sets the maximum acceleration rate of a threat vehicle at 11.3 f/s/s.
2. Vehicle Threat Scenario #2. Threat vehicle enters the ACP in the inbound or outbound lane(s) at or under the posted ACP Speed Limit and then, later at some point further in the Approach Zone, accelerates at its maximum acceleration rate through the rest of the ACP.
3. Vehicle Threat Scenario #3. Threat vehicle attempts to covertly enter the ACP, but is detected and denied entry by guards at the ID Check Area. Vehicle driver then defies guards and accelerates through the rest of the ACP at the vehicle's maximum acceleration rate.
4. Vehicle Threat Scenario #4. Similar to Threat Scenario 3 above, except the driver of the denied vehicle drives toward the Turn-around or Search Area at the ACP Speed Limit (25mph) as if complying with guard instructions, but then fails to turn and instead accelerates at its maximum acceleration rate through the rest of the ACP.

Interestingly, there can be a number of other Adversary Paths other than the roadways. This includes vehicular access at any point adjacent to the ACP. This is why design directives clearly cite that there should be balanced protection across the entire perimeter of the ACP. Ironically, this is often one of the first cost concessions from a design standpoint.



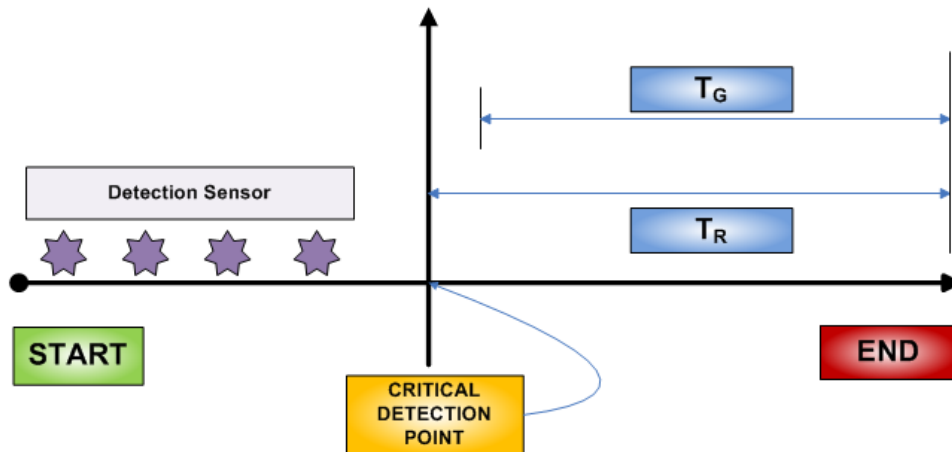
Security Principle #5: Critical Detection Point

The final security principle we address here is the **Critical Detection Point**. This is a culminating principle that borrows from the first four. Once the most likely Adversary Paths are determined, each possible path must be analyzed by measuring the time it takes the adversary (Design Basis Threat) to reach the asset and the associated probability of detection. The adversary will, in theory, attempt to minimize detection probability until detected and then minimize path time until the event is carried out—this is the worst case scenario. In the case of the ACP, the more common threat scenarios are defined in the design guidance documents (see above). From a security engineering perspective several calculations are performed including;

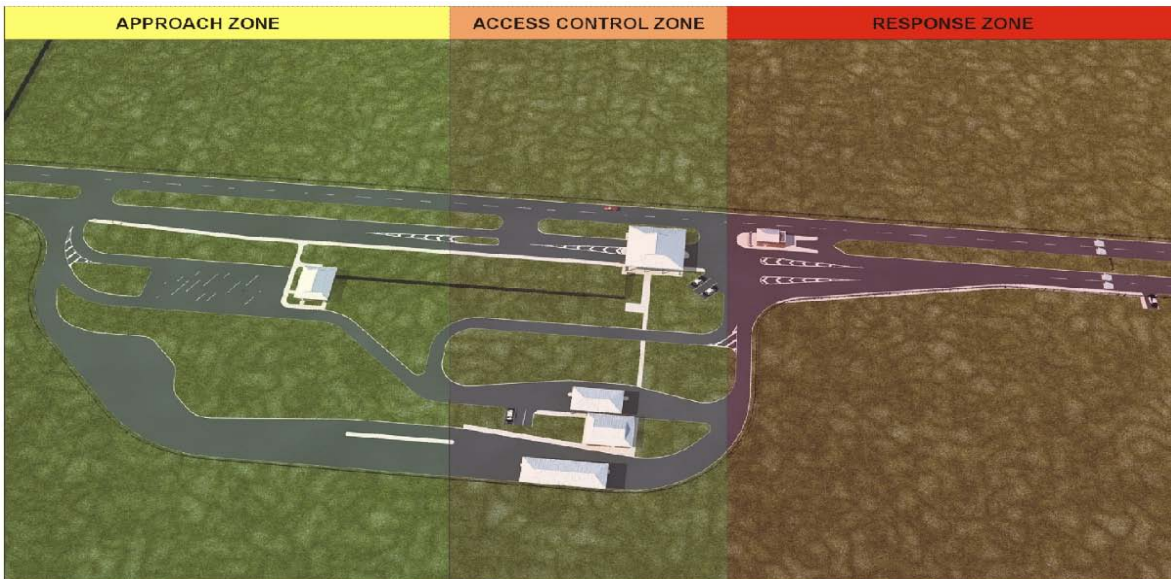
1. Define the: **Probability of Detection** (P_D) – This relates to the detection sensors (over-speed detectors, etc.) It is the product of sensing, assessment and transmittal probabilities for the sensors along the adversary path ($P_D = P_S * P_A * P_T$)
2. Define the: **Guard Response Time** (T_G) – This is the time required for the threat to be interrupted by a sufficient number of response force arriving at the appropriate location to stop the adversary's progress. Simply put, in the ACP the security force must be able to assess the threat in a sufficient amount of time to deploy the final denial barriers and take other steps necessary to stop the adversary. This includes the communication time and deployment time.
3. Define the: **Time Remaining after Detection** (T_R) – This is the maximum amount of allowable time after the detection sensors enunciate that the security force has to respond
4. Define the: **Probability of Interruption** (P_I) – This is the probability that the security force can achieve its mission citing these other factors

Note: These calculations take into account each of the three components of the PPS; Equipment (Over-speed detectors, barriers, etc.) People (security forces), and Procedures (protocols for assessing a detection and responding accordingly). It is the Critical Detection Point(s) that drives much of the ACP design – Designers and Engineers need to insure the ACP layout allows as much time as possible for the security force to respond to an approaching threat.

While these calculations may appear a bit technical their intent is rather straightforward. Using these numbers can determine the Critical Detection Point, and The CDP is the point where the Guard Force Response Time (T_G) just exceeds the Time (the security force has) Remaining after Detection (T_R). Basically, this is the point along the adversary path where the security force has one last chance to interrupt the adversary. If the adversary makes it past that point it's too late. The adversary that can avoid detection until after the CDP will be successful. The true measure of effectiveness of the security system, and in this case the Access Control Point, is the Probability of Interruption (P_I) at the CDP. Simply put, it can determine the CDP based on the Guard Response Time and then measure the combined Probability of Detection of all ACP sensors up to that point. The path with the lowest P_I is the Critical Path—the most vulnerable route to the asset. The principle of “balanced protection” then dictates that all paths should have approximately the same P_I .



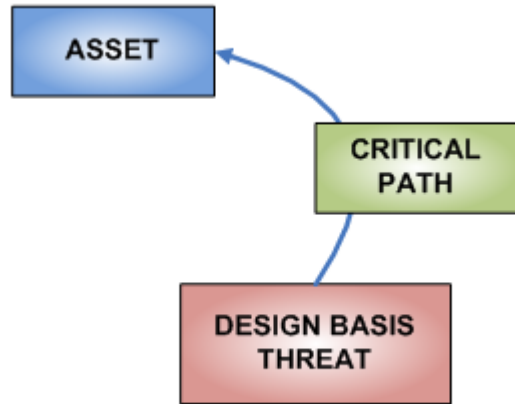
From an ACP design standpoint, the ACP is divided into 3 primary zones; 'Approach', 'Access Control' and 'Response'. There is a 4th zone around the ACP called the Safety Zone. Look at the 3 primary zones in the ACP corridor and it can begin to be understood how critical these security principles are relative to ACP layout and design. Generally speaking, the detection elements need to be placed either in the Approach or



Access Control zones in locations that will insure Guard Force Response Time for alarm, assessment, and response. Since all of these components take time, looking at calculated response times directly affect engineering and design. This also has a direct bearing on where the final denial barriers are placed. If they are placed too closely behind the Access Control Zone, the security force will not have a sufficient amount of time to respond to the threat.

Designing the ACP from a Security Standpoint

Based on the application of these security principles designers compare the effects of different delay, detection and response models to determine the required sub-systems (detection sensors, barriers, etc.) that provide the most cost effective vulnerability solution. In order to be successful, a 'Systems Approach' will always include a combination of personnel, equipment and procedures. There is no single equipment-based solution that can successfully take the place of this approach.



Concentric Security, LLC
7560 Main Street
Sykesville, MD 21784
410-552-9950 P
410-552-9939 F
Website: <http://www.concentricsecurity.com>
Email: sales@concentricsecurity.com

Recognizing Security Principles in the Access Control Point
Design & Construction Process

Authored by:

Mr. Mark Oakes, PSP – Chief Executive Officer
<http://twitter.com/MarkOOakes>