SANDIA REPORT
SAND2005-7177
Unlimited Release
Printed November 2005

Comparison of Two Methods to Quantify Cyber and Physical Security Effectiveness

Kristl A. Gordon and Gregory D. Wyss

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

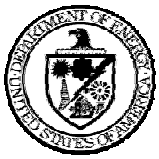
Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online



SAND2005-7177
Unlimited Release
Printed November 2005

Comparison of Two Methods to Quantify Cyber and Physical Security Effectiveness

Kristl A. Gordon and Gregory D. Wyss
Security Systems Analysis Department
Sandia National Laboratories
Albuquerque, NM 87185

Abstract

With the increasing reliance on cyber technology to operate and control physical security system components, there is a need for methods to assess and model the interactions between the cyber system and the physical security system to understand the effects of cyber technology on overall security system effectiveness. This paper evaluates two methodologies for their applicability to the combined cyber and physical security problem. The comparison metrics include probabilities of detection (P_D), interruption (P_I), and neutralization (P_N), which contribute to calculating the probability of system effectiveness (P_E), the probability that the system can thwart an adversary attack. P_E is well understood in practical applications of physical security but when the cyber security component is added, system behavior becomes more complex and difficult to model. This paper examines two approaches (Bounding Analysis Approach (BAA) and Expected Value Approach (EVA)) to determine their applicability to the combined physical and cyber security issue. These methods were assessed for a variety of security system characteristics to determine whether reasonable security decisions could be made based on their results. The assessments provided insight on an adversary's behavior depending on what part of the physical security system is cyber-controlled. Analysis showed that the BAA is more suited to facility analyses than the EVA because it has the ability to identify and model an adversary's most desirable attack path.

Acronyms

B	Beginning
BAA	Bounding Analysis Approach
C_1	Cyber Network 1
C_2	Cyber Network 2
C_1+Phys	Cyber Network 1 plus Physical Attack
C_2+Phys	Cyber Network 2 plus Physical Attack
C_1+C_2+Phys	Cyber Network 1 and 2 plus Physical Attack
E	End
EASI	Estimate of Adversary Sequence Interruption
EVA	Expected Value Approach
M	Middle
P_D	Probability of Detection
P_E	Probability of Total System Effectiveness
P_{EC}	Probability of Cyber System Effectiveness
P_{EC1}	Probability of Cyber Network 1 Effectiveness
P_{EC1-2}	Probability of Cyber Network 1 and 2 Effectiveness
P_{EC2}	Probability of Cyber Network 2 Effectiveness
P_{EP}	Probability of Physical Protection System Effectiveness
Phys	Physical Attack Path
P_I	Probability of Interruption
P_N	Probability of Neutralization
PPS	Physical Protection System
RF	Response Force
SD	Standard Deviation
T	Adversary Task Time

Contents

Figures

Tables

Acknowledgments

The work described in this report was performed under a project sponsored by the Laboratory Directed Research and Development (LDRD) Program at Sandia National Laboratories for the purpose of developing a method that integrates physical security and cyber security vulnerability analysis techniques under a common framework. Kristl Gordon performed this work and wrote this report during her time at Sandia under the Student Internship Program, with Gregory Wyss acting as her technical advisor. The authors thank the LDRD Program and the Student Internship Program for their support. The authors also extend thanks for the support given by the project staff, as led by Jennifer Depoy and James Phelan. Finally, the authors thank Diane Ross for her work as the editor of this report.

1. Introduction

Increasing reliance on cyber technology to control a physical protection system (PPS) creates a problem for system assessment because the facility now becomes more vulnerable to a cyber attack instead of just a physical attack. In the past, methodologies were developed to assess cyber and physical security systems separately and did not model attacks that involved an adversary attacking both physical protection and cyber protection system elements (e.g., hackers disabling a sensor prior to a physical attack). A need exists to create a new methodology or expand an existing one in order to accurately model the cyber and physical security interaction.

Sandia developed two approaches:

- The **Bounding Analysis Approach** (BAA) considers the probability of effectiveness of physical protection (P_{EP}) and the probability of effectiveness of cyber protection (P_{EC}) separately. P_{EP} is the probability that the PPS elements will prevent an adversary from accomplishing his goal and P_{EC} is the probability that the cyber protection system will deter or be strong enough to keep an adversary from hacking in and gaining access to the PPS. This methodology then combines P_{EP} and P_{EC} to determine a total probability of system effectiveness (P_E), which is the probability that the system is able to thwart an adversary attack.
- The **Expected Value Approach** (EVA) uses the P_{EC} in the P_{EP} calculations arrive at the P_E.

The purpose of this study was to assess these two methodologies to determine if they accurately represented the cyber and physical security interaction. The methodologies were tested with numerous sample values to gather data and analyze trends.

2. Physical Security Modeling

Generally, a PPS is modeled as one or more layers of protection surrounding a target, with each layer comprising one or more PPS elements (e.g., fences, locks, alarm systems, etc.). Physical security deals with the different PPS elements and their metrics. Each PPS element has a defined probability of detection (P_D) and an adversary task time (T). For detection of an intruder to occur, three things must happen: 1) the sensor must work properly (P_S), 2) the intrusion must be communicated to the Central Alarm Station (P_C), and 3) the response force must assess the alarm (P_A). If any of those conditions fail to be met (i.e., the security officer ignores the alarm), detection does not occur. P_D is the probability that an adversary will be detected at that PPS element and T is the amount of time (in minutes) required by the adversary to complete the task at that element (e.g., jump over a fence, pick a lock, etc.).

Assessments of a PPS also factor in the response force time, which is the time that it takes for the response force to interrupt the adversary after detection has occurred. The PPS's detection and delay technology must allow enough time for the response force to travel to and intercept the adversary. If the response force cannot arrive in time to prevent the adversary from completing his task, the PPS is ineffective.

When assessing the P_E for a PPS, two variables were examined:

- The *probability of interruption* (P_I) is the probability that the response force can interrupt an attack before the adversary completes his attack sequence.
- The *probability of neutralization* (P_N) is the probability that the response force can stop the adversary from succeeding.

Equation 1 illustrates the relationship between P_E, P_I and P_N.

$$P_E = P_I * P_N \quad (1)$$

For these assessments, response force effectiveness was not included as a parameter; therefore, P_N was automatically assigned the value 1, which means that complete neutralization would occur. With P_N equal to 1, the equation simplifies to $P_E = P_I$ and is referred to simply as P_E.

3. Cyber and Physical Security Modeling

3.1 Assumptions

The following assumptions were made for these assessments:

- If an adversary is going to use both a cyber and physical attack, it was assumed that the cyber attack occurred first.
- The adversary knows if the cyber attack was successful before starting a physical attack.
- A cyber attack gives an adversary the ability to totally defeat physical security elements that are cyber-controlled.
- For these assessments, there may be two separate cyber networks.

3.2 Possible Adversary Attack Paths

With two networks, there are four possible adversary attack paths:

- Path 1 is a physical-only path (Phys) in which the adversary does not manipulate any PPS elements before attempting a forced entry into a facility.
- Path 2 is cyber network 1 (C_1) plus the Phys path (C_1+Phys) that has been manipulated through C_1.
- Path 3 is cyber network 2 (C_2) plus the Phys path (C_2+Phys) that has been manipulated through C_2. When an adversary attacks through Path 2 or 3 they have manipulated those PPS elements that are controlled by that system and then proceeded with the forced entry.
- Path 4 is a combination of C_1 and C_2 plus the Phys path (C_1+C_2+Phys). An adversary using Path 4 has hacked into both cyber networks and so has manipulated the physical elements controlled by both networks and then has proceeded with the forced entry physical attack.

Path 1 is described as a physical-only attack and Paths 2, 3 and 4 are cyber-enabled physical attacks.

For these assessments each cyber network was assumed to be progressively more difficult to hack. C_1 has a lower P_{EC} than C_2 and C_2 has a lower P_{EC} than C_1+C_2. It would be more difficult

for the adversary to hack into the more advanced networks and so it is assumed that it would require more skills and be more difficult to access both cyber networks than it would be to access any one of them alone.

The adversary objective for these assessments is to reach the asset (the target), such as a water valve. The adversary attack path is completed when the adversary completes all tasks required to reach the asset. This study did not consider the adversary exiting the facility or having another task once he reaches the asset. The consequence of concern is the adversary access to the asset through the cyber system and/or PPS.

4. Estimate of Adversary Sequence Interruption Software

To model both approaches, the team chose an Excel-based software package developed by Sandia National Laboratories called EASI (Estimate of Adversary Sequence Interruption). EASI is described as:

> "…a simple calculation tool that quantitatively illustrates the effect of changing physical protection parameters along a specific path. It uses detection, delay, response, and communication values to compute the P_I. But, since EASI is a path-level model, it can only analyze one adversary path or scenario at a time. Path level means that the model analyzes the protection system performance along only one possible adversary path or one adversary scenario (adversary goes over fence, through the portal and explodes through the vault door). Even so, it can be used to perform sensitivity analyses and analyze PPS interactions and time trade-offs along that path…The input for the model requires (1) detection and communication inputs as probabilities that the total function will be successful or P_D and (2) delay and response inputs as mean times and standard deviations for each element or T. The output will be P_I (P_E for these assessments)." [Garcia 2001]

To model the cyber and physical security systems together, cyber elements were added to some of the attack paths that EASI allows users to establish. EASI uses normal distributions for all delay and task times and calculates the probability that the "facility" wins based on convolution of these normal distributions.

The BAA used EASI to obtain a P_{EP} value and then calculated the P_E value. The EVA combined the P_{EC} with EASI metrics and then relied on EASI to yield a total P_E value.

The EASI setup for all assessments is the same. EASI allows for the detection location at each layer to be at the beginning (B) of the T, the middle (M) or the end (E) of the adversary T. All runs through EASI were done with the Layer 1 detection location at the beginning and Layer 2 and 3 detection location in the middle of the T.

The standard deviation (SD) for the response force time and the adversary T means are the values that the EASI program automatically assigns when you enter a layer T or response force time. The program assigns the SD to be approximately 30% of the mean entered.

EASI also allows the user to control two other variables that affect success: alarm communication and response force neutralization. This study assigned a "1" to both variables, assuming that the alarm was communicated and the response force could neutralize the adversary.

Figure 1 is an example of the EASI user interface with all of the values and parameters described above entered and the P_I value calculated.

Probability of Interruption:	**0.21513**

Estimate of Adversary Sequence Interruption	Probability of Alarm Communication	P_N	Response Force Time (in Minutes)	
			Mean	Standard Deviation
	1	1	30	9

Task	Description	P(Detection)	Location	Delays (in Minutes): Mean:	Standard Deviation
1	Fence	0.3	B	1	0.3
2	Portal	0.7	M	20	6
3	Vault	0.5	M	9	2.7
4					0
5					0

Figure 1. EASI Interface

5. Assessment Set-Up

The facility used for the assessments is a simple, three-layer facility (Figure 2). This facility has a fence, a portal, and a vault for Layers 1, 2, and 3, respectively.

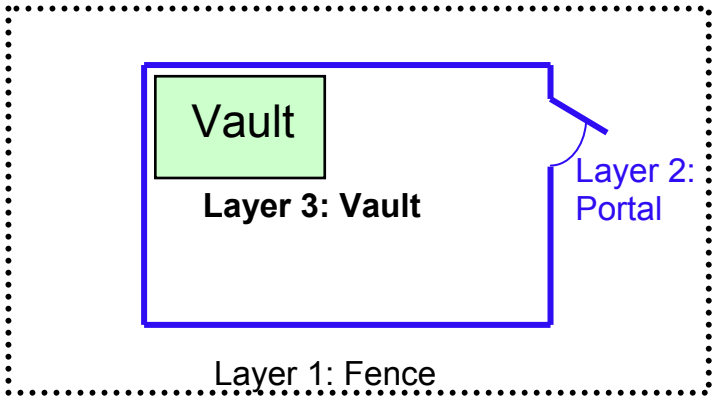


Figure 2. Three-Layer Facility

Table 1 is the assessment table. Column one shows the possible adversary attack paths. Columns two, three, and four are the layers of the facility each with a defined P_D and T. Column five is the P_{EP}, which comes from inputting the P_D and T for each layer on each path into EASI.

Column six is the P_{EC} values for the cyber portion of the security system and column seven is the P_E for the whole system (physical and cyber together) using the P_{EC} from column six.

Table 1. Assessment Table

Col 1	Col 2		Col 3		Col 4		Col 5	Col 6	Col 7
	Layer 1		Layer 2		Layer 3				
	P_{D1}	T_1	P_{D2}	T_2	P_{D3}	T_3	P_{EP}	P_{EC1}	P_{E1}
1. Phys. Only	0.3	1	0.7	20	0.5	9	0.215	~	0.215
2. C_1 + Phys.	0.3	1	0.7	20	0.5	9	0.215	0.100	0.294
3. C_2 + Phys.	0.3	1	0.7	20	0.5	9	0.215	0.397	0.527
4. C_1 + C_2 + Phys.	0.3	1	0.7	20	0.5	9	0.215	0.457	0.574

Col 8	Col 9	Col 10	Col 11	Col 12	Col 13	Col 14	Col 15
P_{EC2}	P_{E2}	P_{EC3}	P_{E3}	P_{EC4}	P_{E4}	P_{EC5}	P_{E5}
~	0.215	~	0.215	~	0.215	~	0.215
0.250	0.411	0.500	0.608	0.750	0.804	0.900	0.922
0.497	0.605	0.670	0.741	0.832	0.869	0.933	0.947
0.623	0.704	0.750	0.804	0.937	0.951	0.990	0.992

In order to characterize system behavior completely, a wide range of P_{EC} values was used. "C_1+Phys." path (P_{EC1}) ranged from 0.10 to 0.90, specifically 0.10, 0.25, 0.50, 0.75 and 0.90. The P_{EC} values were selected to demonstrate system behavior and represent arbitrary values and equations for this study.

Because it was assumed that each cyber system path was progressively more difficult for the adversary to defeat, a simple arbitrary equation was used to select values for P_{EC} for C_2+Phys. (P_{EC2}) and C_1+C_2+Phys. ($P_{EC1\text{-}2}$) from P_{EC1} according to a consistent pattern. Equations 2, 3 and 4 indicate how P_{EC1}, P_{EC2}, and $P_{EC1\text{-}2}$ were calculated.

$$P_{EC1} = y \tag{2}$$

$$P_{EC2} = 1-.67(1-y) \tag{3}$$

$$P_{EC1\text{-}2} = 1-[(1-y)^2] \tag{4}$$

These equations represent that an adversary's attack success probabilities against C_1 and C_2 are not completely independent. The $P_{EC1\text{-}2}$ equation was changed for P_{EC}=0.1 and 0.25 because, for these values, equation 4 indicated that an adversary would find it easier to attack *both* C_1 and C_2 than to attack C_2 by itself. Equation 5 depicts the $P_{EC1\text{-}2}$ equation for 0.1 and 0.25.

$$P_{EC1\text{-}2} = .67(1-y)^2 \tag{5}$$

Equation 5 represents that an adversary's success in attacking C_1 is statistically independent from C_2 and the Phys. path.

A full range of P_D values (0.10, 0.30, 0.50, 0.70 and 0.90) was used to see how P_D would affect system behavior. To simplify the assessments, the P_D for Layer 1 was the only P_D value that was varied.

The mean adversary task time was also varied for Layer 1 for some simulations. If T was varied, P_D was given a constant value. When the T simulations were done, the different Layer 1 times were changed so that the adversary total task time was shorter, the same, and longer than the response time, which translates to the response force does not arrive in time, the response force arrives just when the adversary completes the task, and the response force arrives before the adversary completes his task.

From the different attack path metrics, one can then determine the adversary's most desirable path for each P_{EC} value. The path with the lowest P_E is the path that will be the easiest for the adversary to defeat. The different P_{EC} values allow one to see if a different attack path becomes easier as the P_{EC} value increases.

6. Bounding Analysis Approach

6.1 Method

The BAA approach uses a separate value for P_{EC} and P_{EP}. As indicated in equation (6), the product of the probability that the adversary defeats the physical security system ($1-P_{EP}$) and the probability that the adversary defeats the cyber system ($1-P_{EC}$) is subtracted from one to yield P_E.

$$P_E = 1- [(1-P_{EP})*(1-P_{EC})] \quad (6)$$

The P_{EP} value is obtained by defining a P_D and T for all layers of the facility and running EASI with those values.

The BAA assumes that if an adversary "infiltrates" a cyber system he can then eliminate from the attack path those elements of the PPS that are controlled by that cyber network. Whether the cyber system controls an alarm element (e.g., alarm or sensor) or a physical barrier or delay element (e.g., magnetic lock), the adversary can essentially eliminate that element in the physical path to make the physical attack path quicker and/or easier.

Table 2 is an example of a BAA assessment. The mean response force time used in EASI is 30 minutes, which is at the same mean total adversary time for the physical-only path. The X's in the chart are those metrics that are controlled by the cyber network noted in column one. For this example the C_1 network controls the P_D and T metrics for the Layer 1 and C_2 controls P_D for Layer 2 and P_D for Layer 3. If the adversary can defeat *both* C_1 and C_2 then they have the ability to zero out the P_D and T for Layer 1, the P_D for Layer 2 AND the P_D for Layer 3. The different P_{EP} for the attack paths and their eliminated metrics are in column five. When compared to Table 1, the changes in the P_{EP} values can be seen on the paths with elements whose effectiveness have been eliminated via cyber attack. As shown with this example, depending on the

protective value of the cyber networks, the most advantageous path for the adversary starts out as the C_1 + Phys. path and as P_{EC} increases, it changes to the physical-only path.

Table 2. BAA Example

	Layer 1 P_{D1}	T_1	Layer 2 P_{D2}	T_2	Layer 3 P_{D3}	T_3	P_{EP}	P_{EC1}	P_{E1}
1. Phys. Only	0.3	1	0.7	20	0.5	9	0.215	~	0.215
2. C_1 + Phys.	X	X	0.7	20	0.5	9	0.093	0.100	0.184
3. C_2 + Phys.	0.3	1	X	20	X	9	0.150	0.397	0.487
4. C_1 + C_2 + Phys.	X	X	X	20	X	9	0.000	0.457	0.457

P_{EC2}	P_{E2}	P_{EC3}	P_{E3}	P_{EC4}	P_{E4}	P_{EC5}	P_{E5}
~	0.215	~	0.215	~	0.215	~	0.215
0.250	0.250	0.500	0.875	0.750	0.938	0.900	0.975
0.497	0.497	0.670	0.670	0.832	0.832	0.933	0.933
0.623	0.623	0.750	0.750	0.937	0.937	0.990	0.990

Many assessments were done with different T for Layer 1 and the previously mentioned range of P_D. For each assessment different combinations of cyber-controlled elements were selected. Some assessments had C_1 and C_2 each controlling only one element, and so combined only control two elements out of the six possible for the three layers. Other assessments were done where one cyber network controlled two elements and the other one element and so combined, controlled three. As seen in Table 1 there were assessments done with each cyber network controlling two physical elements and so four combined, etc.

6.2 Observations

This method indicates that if the P_D for all layers of physical security is low, it is not profitable for the adversary to disable the physical elements through cyber networks. It would be easier to attack the asset by the purely physical path than to introduce the added complexity and uncertainty of a cyber attack. Also, if the P_{EC} for a facility's cyber networks is high, the physical path will be the most desirable adversary path. The combined physical-cyber attack path is most desirable only when the cyber system's vulnerabilities are significant and it controls physical protection assets whose defeat would significantly help the adversary. Thus, it is not advantageous for a facility to protect its cyber networks when its physical security is lacking or vice versa. Physical and cyber security must be balanced to effectively deter or thwart an attack.

7. Expected Value Approach

The EVA finds the average P_D and T values between the cyber and non-cyber attacks. These values were then entered into the cyber-controlled elements of EASI to obtain total system effectiveness.

The EVA calculates P_E on the basis that only those metrics that are cyber-controlled will be affected by the P_{EC} value. Table 3 is an example of Path 2 $P_{EC} = 0.25$, Path 3 $P_{EC} = 0.497$ and Path 4 $P_{EC} = 0.623$. These values correspond to Table 1's column seven values. The shaded values are the cyber-controlled metrics of each layer and the values are the original P_D or T multiplied by the appropriate P_{EC} for that path. The physical-only path is included here simply for reference purposes and is not part of the EVA method.

Table 3. EVA Layer Layout

	PEC	Layer 1 P_{D1}	Layer 1 T_1	Layer 2 P_{D2}	Layer 2 T_2	Layer 3 P_{D3}	Layer 3 T_3
1. Phys. Only	~	0.3	1	0.7	20	0.5	9
2. C_1 + Phys.	0.250	0.3*0.25	1*0.25	0.7	20	0.5	9
3. C_2 + Phys.	0.497	0.3	1	0.7*0.497	20	0.5*0.497	9
4. C_1 + C_2 + Phys.	0.623	0.3*0.623	1*0.623	0.7*0.623	20	0.5*0.623	9

Once the cyber-affected metric values are calculated, they are entered into EASI to determine the total P_E. Again, the response force time used in EASI was 30, which is the same total adversary time for the path before any P_{EC} has been taken into consideration. EVA integrates the P_{EC} values with the P_E EASI run. Table 4 is an example of an EVA evaluation with the layer values calculated from Table 3. Column five shows the P_E values for the cyber system and the PPS.

Table 4. EVA Example

	Layer 1 P_{D1}	Layer 1 T_1	Layer 2 P_{D2}	Layer 2 T_2	Layer 3 P_{D3}	Layer 3 T_3	P_E
1. C_1 + Phys.	0.075	0.250	0.7	20	0.5	9	0.122
2. C_2 + Phys.	0.3	1	0.348	20	0.249	9	0.183
3. C_1 + C_2 + Phys.	0.187	0.623	0.436	20	0.312	9	0.138

The EVA method also allows the user to determine the most desirable adversary path from the P_E values. In this example Path 1 would be the easiest path for an attack. Many assessments were done with different layer metric combinations under cyber control.

The EVA method only models those attacks involving cyber networks so it does not predict the level of P_{EC} needed to push the adversary to "switch" from cyber to pure physical attacks. The EVA values could not be compared to a physical-only path run through EASI because that pure physical path would never be the easiest path because the EVA calculations for all cyber systems will be a lower P_E.

The EVA method would be useful for a facility that only wants to assess the cyber and physical security combined. With this type of assessment a facility would be able to compare all cyber networks combined with a physical attack and determine which of their cyber networks is the most vulnerable and attractive to an adversary for an attack.

8. Comparisons and Conclusions

The two methodologies described in this paper were examined to determine their applicability to the cyber and physical security modeling problem. Many assessments were done with each methodology with varying metric values to characterize system behaviors. Each method brought new insights and considerations for analyzing the cyber and physical security integration. However, there were some distinct differences between the two methods that caused us to select the BAA approach for continuing research.

The EASI program used with both methods is non-linear because it is based on the combination of multiple normal distribution functions. Because the BAA is applied after the EASI run, as the BAA conditions increase, EASI gives a greater value between zero and one. Therefore, the BAA can be less conservative and the EVA biases P_E values low. This is not to say one method's values are more "right" than the other, only that the two methods should not be compared in one facility. These methods can be used to determine how facilities compare to each other but the same method should be used for these comparisons to obtain relative values.

The BAA method is more applicable to our assessments for the cyber and physical security modeling problem because it allows us to see what happens if an adversary is able to "zero-out" an element through a cyber network, thereby eliminating it ability to detect the adversary. A focus of our analysis is how the increasing reliance on cyber technology impacts the physical security systems. If an adversary can gain access to the cyber networks, he may have full control over all physical security elements that are controlled by that network. The BAA allows us to examine whether or not eliminating an element reduced the P_E enough for the adversary to want to continue on that specific path. This ability is very beneficial because a facility can determine what elements have the biggest impact on P_E. If there is an element that does not affect P_E if it is eliminated, the facility can avoid spending the money on protecting that element further since its effect on the overall security posture is minimal.

Comparatively, the EVA only models the probability that the adversary can eliminate an element. The P_{EC} for that path is calculated into EASI and so there is no way to observe the consequences of reducing that element to zero, just the probability that the adversary can do it. Without the ability to eliminate an element, it is difficult to see if one element is more critical than another.

This study examined the pure physical attack path and how it relates and compares to the cyber and physical attack paths. The BAA method includes the purely physical attack path and so is more suited to our assessments. A focus of the study is how good the physical security has to be to deter and thwart an attack. This study also examined how well-protected all cyber networks must be to force the adversary to pursue a purely physical attack scenario. The BAA allows for

manipulation of the physical path elements to determine how much a change in one layer would affect the P_E. A facility would have the capability to see if it would be more cost-effective to strengthen the physical security (e.g., more responders) or the cyber security (e.g., stronger firewalls).

Figure 3 illustrates that the EVA approach is neither conservative nor non-conservative, which is apparent from the EVA 0.1 curve crossing over the BAA 0.1 curve. The "bends" in the BAA curve represent a switch in attack paths, from physical-only to cyber-enabled physical, as P_D increases. These shifts in attack paths are not captured by the EVA method.

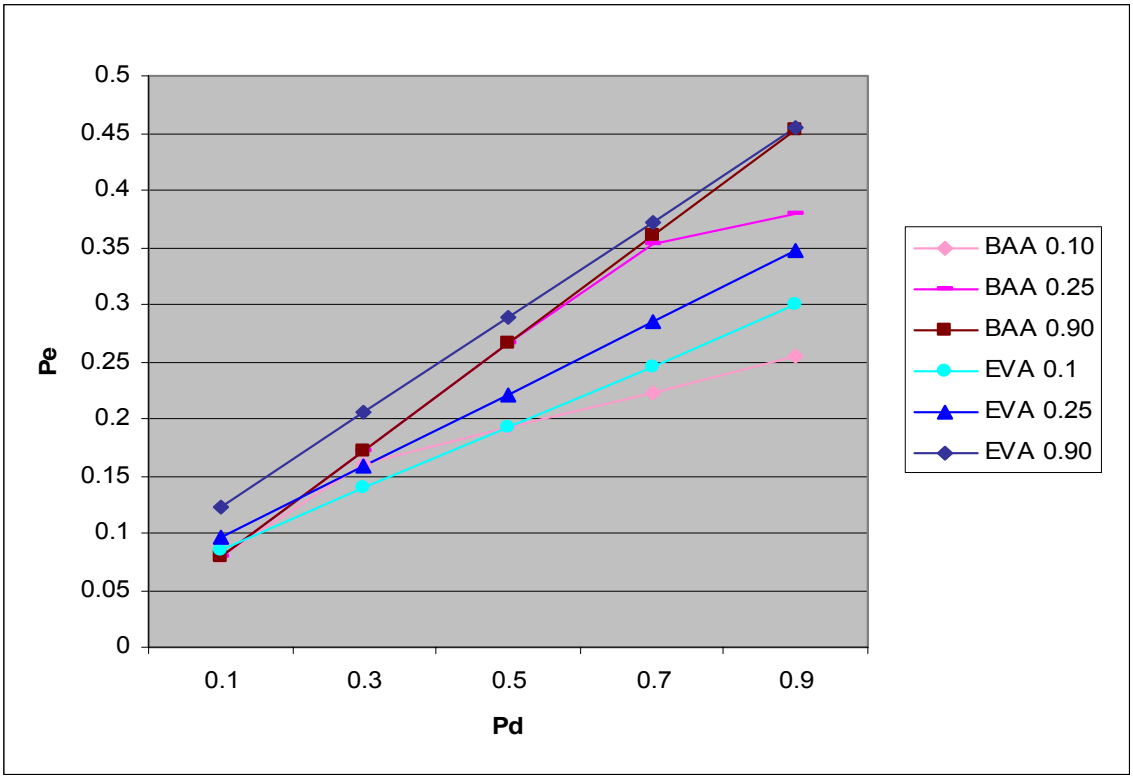


Figure 3. EVA and BAA Results Graph

The two methodologies in this paper were assessed for their applicability to cyber security and physical security integration modeling. Many assessments were performed with each method varying the cyber-controlled elements and their combinations. The assessments provided insight on an adversary's behavior depending on P_D and T values as well as what part of the PPS is cyber-controlled. This study concluded that the BAA is a more suitable approach because of its flexibility and its ability to identify and model the change in the adversary's most desirable attack path as the P_D, T, or P_{EC} vary.

References

[1] M. L. Garcia, *The Design and Evaluation of Physical Protection Systems*, Butterworth-Heinemann, Woburn MA 2001

Distribution

3	MS	0757	Kristl A. Gordon
2		0757	Gregory D. Wyss
1		0757	Carla Ulibarri
1		1368	Jennifer Depoy
2	MS	9018	Central Technical Files, 8945-1
2		0899	Technical Library, 04536