EASI is 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 probability of interruption $P_t$. But, since EASI is a path-level model, it can only analyze one adversary path or scenario at time. Path level means that the model analyzes the protection system performance along only one possible adversary path or one adversary scenario. Even so, it can be used to perform sensitivity analyses and analyze PPS interactions and time trade-offs along that path.

For theft or sabotage attempts to be defeated, the response force must be notified of the attempt while sufficient time remains to respond and interrupt the adversary. Communication of the alarm to an operator and to the response force, therefore, is a factor in the analysis. An adversary interruption occurs in the EASI model if the PPS works properly, resulting in confronting the adversary with a response force large enough to prevent them from proceeding further along their path. The input for the model requires (1) detection and communication inputs as probabilities that the total function will be successful and (2) delay and response inputs as mean times and standard deviations for each element. The output will be the $P_t$, or the probability of intercepting the adversary before any theft or sabotage occurs. After obtaining the output, any part of the input data can be changed to determine the effect on the output. However, because EASI is a path-level model, as systems get larger and more complex, better computer models are needed to perform the analysis of multiple paths. This point will be discussed later in the chapter, in the section titled Adversary Sequence Diagrams (ASD). ASDs provide a graphical method to represent the protection elements in a system, which can serve as the interface between a human analyst and computer software.

**The Input**
In the EASI model, input parameters representing the physical protection functions of detection, delay, and response are required. Communication likelihood of the alarm signal is also required for the model. Detection and communication inputs are in the form of probabilities that each of these total functions will be performed successfully. Delay and response inputs are in the form of mean times and standard deviations for each element. All inputs refer to a specific adversary path.

The EASI input for the detection function is the $P_D$ for each sensor encountered by an adversary. As discussed in the text, this probability is highly dependent on the capabilities of the adversary. The $P_D$ is the product of the probability that the detector will sense abnormal or unauthorized activities by the adversary ($P_S$), the probability that an alarm indication will be transmitted to an evaluation or assessment point ($P_T$), and the probability of accurate assessment of the alarm ($P_A$). $P_S$ was discussed in Chapter 5 and assessment was covered in Chapter 8. The relationship among these performance measures for $P_D$ can be summarized as:

$$P_D = P_S \times P_T \times P_A$$

The communication of an alarm condition to the response force is input into EASI as the probability of guard communication, $P_C$. In most PPS, the likelihood of successful communication to the response force increases with time. The value entered into EASI for $P_C$ is the probability of guard communication associated with the guard communication time included in the response force time (RFT). Evaluation of many systems designed and implemented by Sandia National Laboratories indicates that most systems operate with a $P_C$ of at least 0.95. This number can be used as a working value during the analysis of a facility, unless there is reason to believe that this assumption is not valid. If actual testing at a facility yields a different $P_C$, this number should be
used; if guard communication appears to be less dependable, a lower value can be substituted in the model. Factors that may influence $P_C$ include lack of training in use of communication equipment, poor maintenance, dead spots in radio communication, or the stress experienced during an actual attack. This flexibility allows the analyst to vary $P_C$ as needed to correctly represent this function.

The delay time required by an adversary to travel a given path to a target can be thought of as the sum of the times required to perform certain tasks or travel distinct path segments. For the sake of simplicity, both task times and travel times are referred to as adversary task times. In general, it is not possible to predict the exact time interval necessary for the adversary to perform these tasks or proceed across these path segments. This is due to the fact that the adversary (or the response force) will not always perform a task within exactly the same time. For example, the adversary may take more or less time to get through a door or the response force might have trouble starting a vehicle. Over a number of attempts, some variation in delay values will be observed. To allow for this expected variation in EASI, these time intervals are modeled as random variables possessing an average or mean value and a standard deviation. The length of each of these successive adversary task times is input into EASI as a mean time and a standard deviation. Standard deviation is discussed in more detail below.

Response time is modeled in EASI as the time between the generation of an alarm signal by a sensing device and the confrontation of the adversary by a response force adequate to halt the progress of the adversary along the path. This time consists of the successive time increments listed below and in Figure 14-1 in the book.

- alarm communication time
- time required for alarm assessment
- guard communication time
- time required for the guards to prepare, to gather arms, to start vehicles, etc.
- guard travel time
- time required for the guard force to muster and deploy

Response time input to EASI is in the form of a single mean time and standard deviation representing the sum of all the elements shown above. Alarm communication and assessment times are incorporated into RFT within the EASI model to simplify data entry and handling. The use of RFT should not be confused with $P_C$. RFT is a measure of the time it takes to receive, assess, and respond to an alarm; $P_C$ is a measure of the likelihood that there will be successful communication to the response force to carry out the response.

There is one final note on data input to the EASI model. The time data entered into EASI may be in units of seconds or minutes, but not both. Given this constraint, delay and RFT should be in the same unit. If delay times are entered in seconds and RFT in minutes, the discrepancy will affect the accuracy of the output.

**Standard Deviation**
To use the EASI model as effectively as possible, some knowledge of the term standard deviation is required. Standard deviation is a measure of dispersion of a set of related data. Suppose the response time of the guard force at a facility is measured five times and gives the results shown in Table 14-1.
Multiple tests were conducted to measure response force time at a facility. \( X_{avg} \) is the average of the five trials and \( X_i \) is the individual trial result. Using this data, the average response time is \( (9+7+10+11+8)/5 = 9 \) minutes. The standard deviation is a measure of the amount that a given data point is likely to deviate from the mean of all the data. Quantitatively this is calculated as:

\[
s_n = \sqrt{\frac{\sum_{i=1}^{n}(X_i - X_{avg})^2}{n-1}} = \sqrt{\frac{0 + (-2)^2 + 1^2 + 2^2 + (-1)^2}{5-1}} = 1.58
\]

This is the sample standard deviation, based on \( n = 5 \) observations. If we were to collect many observations on the response time, the sample standard deviation, \( s_n \), would tend towards \( S \), the standard deviation for the true distribution of response times. The sample standard deviation, \( s_n \), should not be used in the EASI model. This is because five data points are not sufficient to justify this estimate of the population standard deviation. A better approach would be to collect response time data over several months and divide the data into groups of five. Then find \( s_n \) for each group using the equation above, and average these values to estimate \( S \), the population standard deviation. This will take a minimum of 30 data points, and 6 values of \( s_n \). This average \( s_n \) can then be used in EASI as the standard deviation. As an alternative, tests at Sandia have shown that the standard deviation of a time event can be conservatively estimated at 30% of the mean and, therefore, if there have not been enough tests to establish a statistically significant standard deviation, one can simply use 30% of the estimated mean. These assumptions are equally applicable to delay times, i.e., there is a standard deviation associated with each mean time and the standard deviation can be approximated by using the mean + or - 30%. Use of the standard deviation for RFT and delay times allows consideration of the fact that guards will not always respond in exactly the same time, and that adversaries may take more or less time to penetrate barriers.

If we were to make many measurements of the RFT, we would expect to find a Gaussian distribution of data points as shown in the curve in Figure 14-2 in the book. In a Gaussian (or normal) distribution, 68% of the values are found within the interval \( (X_{avg}-S) \) and \( (X_{avg}+S) \). In the above case, this means that we would expect the RFT to be between 7.42 and 10.58 minutes 68% of the time.

### The Output
The output of the EASI model is an estimate of the probability that a sufficient number of response force personnel will interrupt the adversary at some point before the adversary

<table>
<thead>
<tr>
<th>Trial Number</th>
<th>Response Force Time (minutes)</th>
<th>((X_i-X_{avg}))</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>7</td>
<td>-2</td>
</tr>
<tr>
<td>3</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>11</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>8</td>
<td>-1</td>
</tr>
</tbody>
</table>

**Table 14-1** Guard Response Time Trials. Multiple tests were conducted to measure response force time at a facility. \( X_{avg} \) is the average of the five trials and \( X_i \) is the individual trial result.
completes acts of theft or sabotage. The output is the probability of interruption, $P_i$. If there is one sensor on the path, this probability is calculated as:

$$P_i = P_C \cdot P_D$$

**Using the Model**

To use EASI, the initial step is the selection of an adversary action sequence. The selection should be based on thorough knowledge of the facility and reasonable assumptions about the adversary. Next, select a physical path to the asset corresponding to the chosen sequence. Visualize the adversary tasks along that path, and determine the location of sensors. Then, obtain the required data: (1) the probabilities of detection and communication and (2) the mean and standard deviation of task times and response times. Finally, enter the data into the computer and obtain the results. The real value of the EASI model does not end there, however, because the analyst now has the opportunity to change the input data and see what effect this has on the output. A few examples will demonstrate these effects.

**EASI Examples**

Consider the example where the adversary intends to sabotage a target in a vital area as shown in Figure 14-3. The adversary intends to penetrate the fence, travel to the building, force open a door, travel to the vital area, force open another door, and set and detonate an explosive device on the critical asset. Detection and delay values are shown in Figure 14-4 and the RFT is 300 seconds.

![Figure 14-3](image.jpg) Adversary Path to Asset in a Vital Area. The adversary must cross the fence, approach the building, enter the outer door, travel to the asset location, enter an inner door, and then set up the explosive charge at the asset.
After entering this data in EASI, the result shows the probability of interruption is 0.48, as shown in Figure 14-4. The analyst may decide that this $P_i$ is too low and that something should be done to improve this result. If a fence sensor with a probability of detection of 0.9 were added to the outer fence, the input would be as shown in Figure 14-5. The $P_i$ in this upgraded case is 0.58, which may be satisfactory and may justify the installation of the fence sensor system.

**Figure 14-4** Results of EASI Analysis for Adversary Path. $P_i$ is 0.48 for this path.
Figure 14-5 Results of EASI Analysis after Upgrade. A fence sensor with $P_D$ of 0.9 was added to the outer fence resulting in an improved $P_I$ of 0.58.

Exercise
The model is already open if you followed the download model instructions. Toggle between this page and the Excel EASI model using the Windows tool bar at the bottom of the screen to work the exercises along with the discussion below.

Task 1:
Replace $P(Detection)$ from 0 to 0.9 (verify the result is .58 as shown above) If this value is still not acceptable, an additional upgrade could be modeled. For example, if the RFT is also reduced to 200 seconds, the new $P_I$ is 0.90 (see Figure 14-6). This is a significant improvement and only required relocating guards closer to the target, i.e., low or no additional cost. Or, if preferred, guards could be left at their current location (RFT still 300 seconds) and delay can be doubled at the asset, perhaps by enclosing it in a hardened case. This would result in a $P_I$ of 0.84 (see Figure 14-7). This is not quite as high as the previous upgrade, but might be easier or cheaper to implement or operationally be more acceptable. When the $P_I$s along all paths are approximately equal, the PPS is said to be balanced, i.e., all paths are equally difficult for the adversary to achieve their goal. Note that balance is achieved by mixing detection, delay and response components and that there are a number of possible combinations that will result in acceptable system performance. This provides the opportunity to select combinations that meet cost and operational requirements without compromising system effectiveness.
Figure 14-6 EASI Analysis after Reduction in Response Force Time. Reduction of RFT and detection at the fence has increased $P_i$ to 0.90.

Figure 14-7 EASI Analysis after Addition of Delay at Asset. With detection at the fence and delay at the target, $P_i$ is now 0.84.
These results demonstrate the utility of the EASI model, i.e., the ability to adjust protection elements and their performance in order to predict overall system effectiveness prior to implementation. Further manipulation of detection and delay components at different points on the path will emphasize the value of the security principles discussed throughout the text. These include detection early on the path and prior to delay, effectiveness of delay at the asset, the relationship among detection, delay and response functions, timely detection, and the principles of protection-in-depth and balanced protection.

**Critical Detection Point**
As described in Chapter 13 in the text, the critical detection point, or CDP, is the point on the path where the delay time remaining first exceeds the response force time. EASI cannot locate a CDP because the delay and response force times are random variables in a distribution, so there is a chance any point on the path will be the CDP during the actual attack. The concept of a CDP is too important to dismiss, however, because it gives valuable guidance on where to put additional protection, that is, add detection before or at the CDP and delay after.

Many of the more complex analysis tools, like SAVI or ASSESS, that find most-vulnerable paths use only the mean delay and response force times, because their algorithms fail when variation is introduced. Experience with these tools over the years has shown that effective systems can be designed by assigning the CDP based on the mean times, and then adding detection before this CDP and delay after it. This CDP, based on the mean values, will be what we refer to as the CDP in this chapter, rather than the more precise definition found in Chapter 13. For example, in Figure 14-4, the CDP is at the first door. To illustrate why this CDP is important for effective design, we will incorporate detection (P_D =0.9) at the target itself and show the results in Figure 14-8. The P_I is 0.48, which is the same as the baseline system. In Figure 14-9, 20 seconds of delay has been added at the fence, again resulting in a P_I of .48. Both of these upgrades were on the wrong side of the CDP and both had negligible effect on performance.

---

**Figure 14-8** EASI Analysis with Addition of Detection at the Asset. The P_I remains at 0.48.
While it is practical to set the CDP based on mean delay and response force times, this must be done carefully, with the understanding that there will be variation in times. In Figure 14-4, the mean time remaining at the CDP exceeds the mean response force time by only 10 seconds—not a lot of leeway. Considering that the standard deviation for the response force time is 90 seconds, while that for the time remaining is 27 seconds, we see that 10 seconds leeway is probably insufficient to assure that any detection at this door will be effective. Typically, 30 seconds or more is desirable. This does not mean that a very large difference between RFT and time remaining on the path is by itself a design criterion, but it could become one if most of the detection is located on the path near the CDP.

Use of Location Variable in EASI
At this point, all but one of the required input elements to the EASI model have been discussed. This last input falls in the column labeled Location in the previous figures. Note that each of these results have a B in this column. The Location column is used to describe where in the model detection falls relative to delay for the specific protection element. Consider that if detection and delay both exist at an element, the detection may start before delay, at the end of delay, or somewhere in-between. Due to these possibilities, EASI allows assignment of detection relative to delay to more accurately model system effectiveness. To do this, entries are B for detection before delay, M for detection during delay (middle), and E for detection after, or at the end of, delay. Where there is no detection associated with the delay the location parameter will not matter. When the location is B, the delay time is calculated using the mean delay time for that element plus/minus the standard deviation; when an E is entered, EASI uses 0 as the time delay for this task. Use of an M indicates that the delay happens somewhere in between the before and end values, so is approximated as the one-half the mean plus/minus the standard deviation. The mathematical calculations for these assumptions are shown in Appendix B. Use of this location parameter allows the model to better allocate credit to the standard deviation of the delay time. This in turn allows the analyst to achieve a more realistic view of the probability of interruption by

Figure 14-9 EASI Analysis with Addition of Delay at the Fence. The $P_i$ remains at 0.48.
calculating the PI based on the relationship of detection and delay time at each protection element. This is a complex point that may be best explained through the use of examples.

For example, a locked door with a balanced magnetic switch sensor might be assigned a location of E. This is because the sensor will not register an alarm until the door is opened a small distance. An attack on the door might be to pick the lock, then enter through the door. In this case, most of the delay came from the time to pick the lock, not to pass through the door, so the detection came at the end of the delay, which limits the effectiveness of the delay. An example of use of the M location parameter might be for the case where an adversary will use an explosive to penetrate a wall. In this case, the adversary must take time to set-up the explosive charge, then retreat to a safe distance during the detonation. At this point, the explosion would presumably be detected, but the adversary still has to return to the wall and get through the hole to continue the attack, so some delay still remains after detection. Use of the B parameter in the location column is exemplified by a volumetric sensor in a room monitoring a door. In this case, as soon as the adversary starts to penetrate the door, the sensor will detect the intrusion, and the adversary still must finish penetrating the door to get to the asset. The volumetric sensor detects before the door delay, so use of a B is appropriate.

## Part C Questions: Design and Evaluation of Physical Protection Systems

1. Using Figure 14-4, add the following steps and performance measures that represent an adversary theft scenario, instead of sabotage. Assume RFT= 300 seconds and P_C= 0.95. What is the PI? Where is the CDP, based on mean delays and RFT? What detection and delay improvements could be made?

<table>
<thead>
<tr>
<th>Description</th>
<th>P_D</th>
<th>Location</th>
<th>Delay Mean</th>
<th>Standard Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>6. Remove asset</td>
<td>0.0</td>
<td>B</td>
<td>60</td>
<td>18</td>
</tr>
<tr>
<td>7. Exit Vital Area door</td>
<td>0.9</td>
<td>B</td>
<td>10</td>
<td>3</td>
</tr>
<tr>
<td>8. Run to 2nd outer door*</td>
<td>0.0</td>
<td>B</td>
<td>20</td>
<td>5</td>
</tr>
<tr>
<td>9. Exit outer door</td>
<td>0.9</td>
<td>B</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10. Run to gate</td>
<td>0.0</td>
<td>B</td>
<td>15</td>
<td>4.5</td>
</tr>
<tr>
<td>11. Exit facility</td>
<td>0.2</td>
<td>B</td>
<td>12</td>
<td>3.6</td>
</tr>
</tbody>
</table>

*This is not the same door that they entered through; it is the other door leading out of the building.

**Answer to Question 1**

2. Using the initial theft scenario from question #4 above, assume the RFT is 600 seconds. What is the PI? What if the RFT changed to 150 seconds?

**Answer to Question 2**
3. Using the sabotage scenario described in Figure 14-4, change the following locations and record the change in $P_i$. Explain your results. Be sure to change the location back to the initial value before making the next change.

a) Task 1, cut fence, change to M.
b) Task 6, sabotage target, change to E.
c) Task 3, open door, change to E.
d) Task 3, open door, change to M.

Answer to Question 3

4. Using the example from Figure 14-4, change the probability of communication to 0.8, 0.7, and 0.5. Record the new $P_i$ for each of these values. Explain your results. What are some possible reasons for lowering the probability of communication in a PPS?

Answer to Question 4

Answers

Answer to Question 1:
$P_i = 0.46$  
CDP is at Task 3, Open Door. This would explain why $P_i$ didn't change much-detection and delay are not integrated together into an effective system.

Add detection at the fence of 0.9, $P_i = .57$ Add 60 seconds delay at other outer door (note that it isn't the same one they used to come in, had a crash bar on it, that's why it was 0). $P_i = .76$. Might be OK, but do one more. An obvious one is to add delay at the target, but this one was done previously, so encourage them to use something different. Add 50 seconds delay at vital area door, $P_i = 0.86$. Not bad. Do as many as you want, decide what is acceptable.

Answer to Question 2:
RFT= 600 seconds, $P_i = 0.05$
RFT= 150 seconds, $P_i = 0.92$

Answer to Question 3:
a) Task 1, cut fence, change to M. $P_i = 0.48$ (no change). This is because there is no detection here. In this case, there is no relationship between detection and delay.

b) Task 6, sabotage target, change to E. $P_i = 0.48$ (no change). Same as (a). We have maximized the value of delay at the target without detection. This should also reinforce the effectiveness of delay at the target and the lack of effectiveness of detection at the target for a sabotage scenario.

c) Task 3, open door, change to E. $P_i = 0.20$. When the location is B, we have delay before detection, and the calculation uses the mean delay time ±standard deviation. The calculation is now changed to using 0 as the mean value ±standard deviation. This means we get less credit for delay, which means we have less of a chance of success.

d) Task 3, open door, change to M. $P_i = 0.33$. The calculation is now made using the mean value as half the mean ±standard deviation, so we get more credit for the delay remaining after detection.

Answer to Question 4:
$P_C = 0.8, P_i = 0.40$
$P_C = 0.7, P_i = 0.35$
$P_C = 0.5, P_i = 0.25$
The probability of communication could change due to transmission failure of the sensor signal (broken wire or intermittent connection), low/no battery power in response force radios (bad maintenance), guards not sure how to operate radio (bad training), if an adversary is jamming communications, or under the stress of a simulation exercise/attack, guards forgot how to operate radio features. The idea here is that a number of things can influence the probability of communication, ranging from equipment failure to bad training. It is important to consider this in the analysis of the system. If you are uncertain of how good your system communication is, test it to decide. If you know that under certain weather or operational conditions (such as lightning storms or non-operational hours), your communication system is less reliable, this may require lowering the $P_C$ used.

For example, if a PPS used wireless (RF) transmission of alarm signals, bad weather or adversary interference could prevent adequate transmission of the alarm condition. This would justify using a lower value to recognize the uncertainty within the system.

Back to Top

Created by Ryan Bedoe
April 3, 2001
Disclaimer