National Nuclear Security Administration

SAND2007-6821P

Developing Vulnerable Paths and Worst-Case Scenarios

Insider Protection Course

Learning Objectives

- Identify the most vulnerable protection measures on the protection layers
- Develop most vulnerable paths for threat / target combination
- Estimate likelihood of detection and time for each vulnerable path step
- Be able to develop a timeline for selected scenarios
- Discriminate between continuous and discontinuous time sequences
- Integrate response into the effectiveness analysis and derive P_I and P_E
- Develop worst case scenarios

Develop Most Vulnerable Paths

1. **Select the protection measures most advantageous to the adversary, i.e., the measures with the lowest effectiveness**
   - **Consider the complexity of the actions required to assure that each action and defeat approach is credible**
   - **Be consistent with methods used, for example don't use covert after overt**
2. **Consider the time to defeat, the detection likelihood and adversary capabilities, etc.**
3. **Select the protection measures based on logic and judgment**

This collection of measures leads to the most vulnerable path for a specific threat / target combination

Some Measure Selection Guidelines

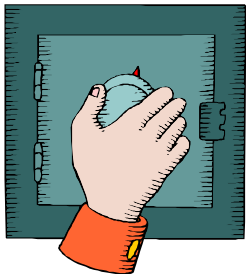
- When several measures are encountered at a step but only one needs to be addressed by the adversary, select the measure that has the lowest detection unless the times to defeat are significantly different
- When several measures must be encountered in the same step, select the highest detection likelihood of all the measures for the effectiveness estimate, or combine them using an agreed upon algorithm

Examples for Developing a Most Vulnerable Path

- We will examine two examples using the bunker case from the previous modules
  - Theft of a goal quantity of NM by the HP tech
- Example 1: Covert abrupt theft under normal operations
- Example 2: Covert abrupt theft by stealing the door combination
- And one example of a different Theft strategy
- Example 3: Protracted Theft or Protracted Diversion
  - Theft of a smaller quantity of NM by a material handler

First Example for Developing Most Vulnerable Path

- **Example 1: covert theft under normal operations**
- **Example 2: covert theft by stealing the door combination**
- **Example 3: Protracted Theft or Protracted Diversion**



Select Measures Along Path: Step 1

Target is the bunker with intent to steal a goal quantity during normal operations

Step	Action	Measures Along Path	Possible methods	Likelihood of Detection	Time (Sec)
1	Enter and traverse PA	Entry control and General observation OR	Normal entry No contraband	Very Low	~~300~~
		Perimeter and General observation	Cut or climb fences	Medium (.36)	25

We should select the first method for both examples because there is no detection here or anywhere before.
Since there is no detection, the time required is not relevant.

Review Possible Methods for Step 2

Step	Action	Measures along path	Possible Methods	Likelihood of Detection	Time (Sec)
2	Enter the bunker	Combination Lock, General observation, MBA custodian oversight	Normal entry	Very Low	120
		Combination lock, General observation	Covertly obtain the combination	Medium	60
		Walls, Door	Breach one of surfaces using tool acquired within facility	High	60 for door 174 for walls

Each of these three methods will lead to a different scenario

Select Possible Method for Step 2

Step	Action	Measures along path	Possible Methods	Likelihood of Detection	Time (Sec)
2	Enter the bunker	Combination Lock, General observation, MBA custodian oversight	Normal entry	Very Low	~~120~~
		Combination lock, General observation	Covertly obtain the combination	Medium	60
		Walls, Door	Breach one of surfaces using tool acquired within facility	High	60 for door 174 for walls

We'll look at this method first - it may be the most vulnerable path since there is no detection here or anywhere before. Again, the time required is not relevant.

Select Possible Method for Step 3

Step	Action	Measures along path	Possible Methods	Likelihood of Detection	Time (Sec)
3	Covertly remove target	General observation, MBA custodian oversight, Cage for product packages, Product package,	Wait until cage and product package opened, take package and hide package inside coat	High	60
		General observation after covert entry	Open cage and product package with hand tools	Low	30
		General observation after overt entry	Open cage and product package with hand tools	Low	30

Ruled out by Previous actions

Select Possible Method for Step 4

Step	Action	Measures along path	Possible Methods	Likelihood of Detection	Time (Sec)
4	Covertly remove a target from the Bunker	General observation, MBA custodian oversight	Normal exit with package hidden under coat	High	60
		General observation after covert entry and removal	Move normally out door and across PA	Medium	60
		General observation after overt entry and removal	Move as quickly as possible out door and across PA	Medium	30

Ruled out by Previous actions

Select Possible Method for Step 5

Step	Action	Measures along path	Possible Methods	Likelihood of Detection	Time (Sec)
5	Covertly remove target from the PA	General observation, Material detectors	Normal exit with explanation that he had gotten contaminated	Medium	90
		General observation, Material detectors	Forceful exit after material detector alarms or is observed with package	High	30
Lowest Detection		Perimeter zone, general observation	Throw package over the zone to the outside for recovery later and leave area	Medium	90

Example 1: Covert Theft under Normal Operations

Step 1. HP Tech enters protected area normally – no detection so time doesn't matter

Step 2. Enter bunker under normal operation – no detection so time doesn't matter

Step 3. Covertly take target package and hide under coat

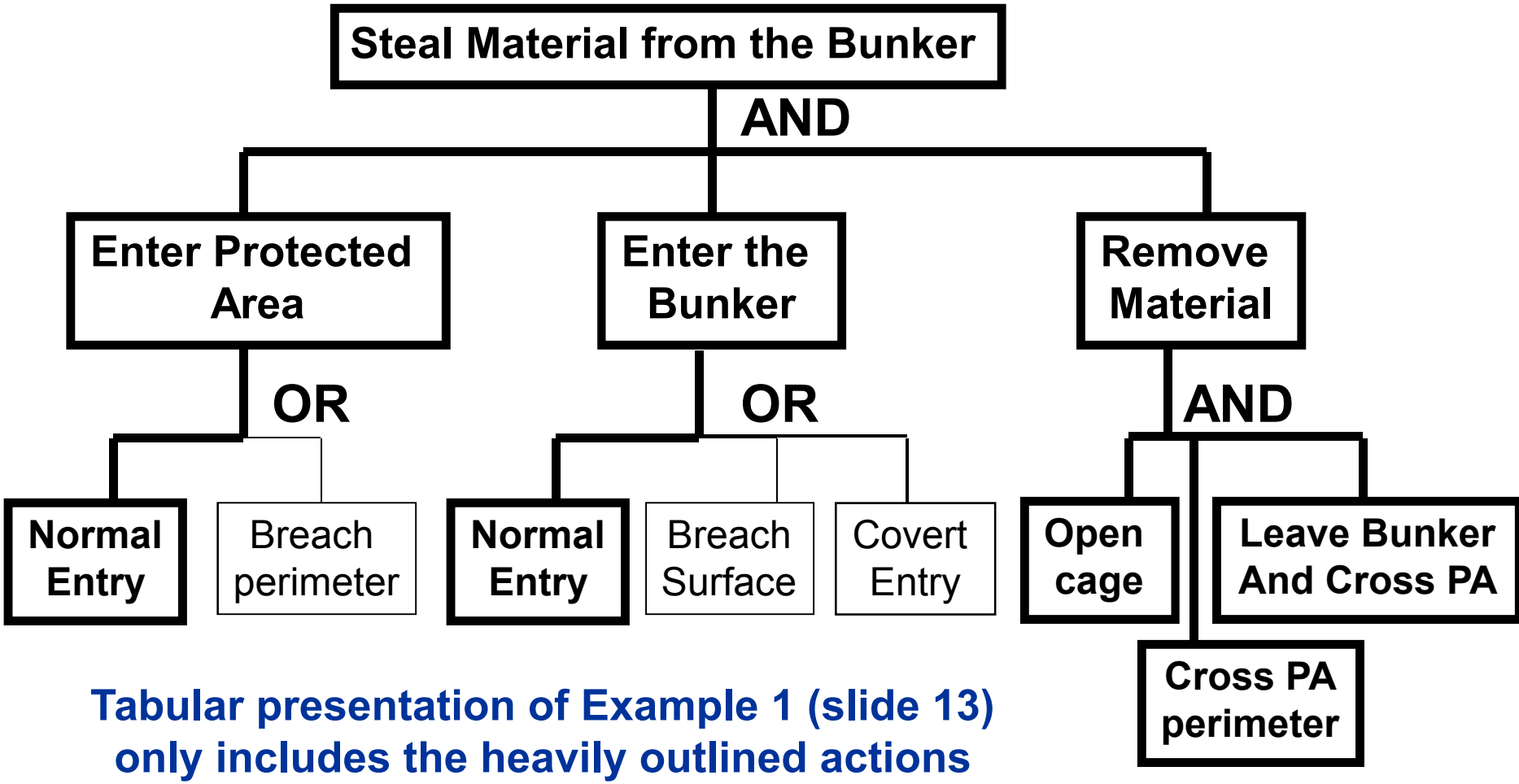
Step 4. Normal exit from bunker

Step 5. Normal walk across area to fence where the package is thrown over the PA boundary

Example 1 – Possibly the Most Vulnerable Path For HP Tech/Bunker

Step	Action	Likelihood of Detection	Time (Sec)
1	Enter protected area normally	Very Low	N/A
2	Enter bunker normally	Very Low	N/A
3	Take package and hide under coat	High	60
4	Walk out of bunker normally	High	60
5	Walk normally to fence and throw package over and leave area	Medium	90

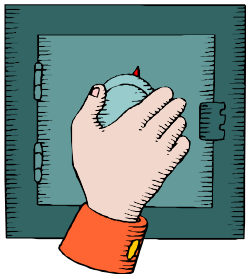
Logic Tree For Example 1



Tabular presentation of Example 1 (slide 13) only includes the heavily outlined actions

Second Example for Developing Most Vulnerable Path

- Example 1: covert theft under normal operations
- Example 2: covert theft by stealing the door combination
- Example 3: Protracted Theft or Protracted Diversion



Select Measures along Path: Step 1

Target is the bunker with intent to steal a goal quantity during normal operations

Step	Action	Measures Along Path	Possible methods	Likelihood of Detection	Time (Sec)
1	Enter and traverse PA	Entry control and General observation OR	Normal entry No contraband	Very Low	~~300~~
		Perimeter and General observation	Cut or climb fences	Medium (.36)	25

Select Possible Method for Step 2

Step	Action	Measures along path	Possible Methods	Likelihood of Detection	Time (Sec)
2	Enter the bunker	Combination Lock, General observation, MBA custodian oversight	Normal entry	Very Low	120
		Combination lock, General observation	**Covertly obtain the combination**	Medium	60
		Walls, Door	Breach one of surfaces using tool acquired within facility	High	60 for door 174 for walls

There are multiple ways to do this – lets explore them.

Some Possible Methods for Getting the Combination

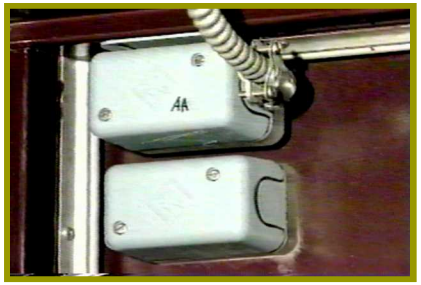
- **Some possible methods to be used by the health physics technician for getting the combination to the bunker**
  - **Covertly look over the shoulder of the material custodian during normal openings**
  - **Obtain the combination from the safe**
  - **Others?**

Let's explore this one.
P_D = Medium (?)

Additional Step

- **The combination may be obtained but how does the insider try to defeat the BMS alarm?**
  - **No defeat - just hurry**
  - **Can he just cut the wires?**
  - **Other technical defeats?**
  - **Can he get to a signal box and compromise the signal there?**
  - **Can he use the procedures to get the alarm ignored**
  - **Other?**

We will use this one for the example but these other questions need to be answered in a full analysis.
P_D = High



Select Possible Method for Step 3

Step	Action	Measures along path	Possible Methods	Likelihood of Detection	Time (Sec)
3	Covertly remove target	General observation, MBA custodian oversight, Cage for product packages, Product package,	Wait until cage and product package opened, take package and hide package inside coat	High	60
		General observation after covert entry	Open cage and product package with hand tools	Low	30
		General observation after overt entry	Open cage and product package with hand tools	Low	30

Ruled out by Previous actions

Select Possible Method for Step 4

Step	Action	Measures along path	Possible Methods	Likelihood of Detection	Time (Sec)
4	Covertly remove a target from the Bunker	General observation, MBA custodian oversight	Normal exit with package hidden under coat	High	60
		General observation after covert entry and removal	Move normally out door and across PA	Medium	60
		General observation after overt entry and removal	Move as quickly as possible out door and across PA	Medium	30

Ruled out by Previous actions

Select Possible Method for Step 5

Step	Action	Measures along path	Possible Methods	Likelihood of Detection	Time (Sec)
5	Covertly remove target from the PA	General observation, Material detectors	Normal exit with explanation that he had gotten contaminated	Medium	90
		General observation, Material detectors	Forceful exit after material detector alarms or is observed with package	High	30
		Perimeter zone, general observation	Throw package over the zone to the outside for recovery later and leave area	Medium	90

Example 2: Covert Theft using Stolen Door Combination

Step 1. HP Tech enters protected area normally – no detection so time doesn't matter

Step 2. Obtain stolen combination – If not detected time doesn't matter

Step 2a. Open bunker door using stolen combination

Step 3. Cut into cage and open product package and take package

Step 4. Move normally out door and across PA

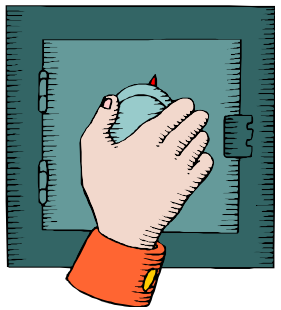
Step 5. Normal exit from PA with talking his way through the reason for the nuclear material alarm

Example 2 – Possibly the Most Vulnerable Path For HP Tech/Bunker

Step	Action	Likelihood of Detection	Time (Sec)
1	Enter protected area normally	Very Low	N/A
2	Obtain combination	Medium	?
2a	Open bunker door using combination	Very Low until the door is opened – P_D = High	60
3	Cut through cage and product package and take package	Low	90
4	Take package, hide under coat and cross the PA	Medium	60
5	Pass through portal	High	90

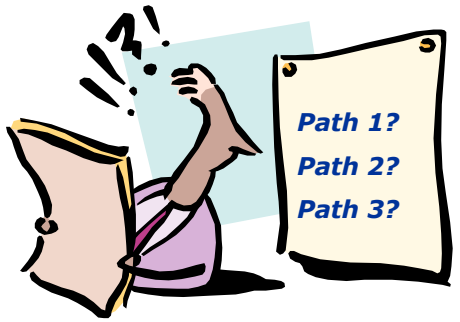
Comments for this Path Example

- Obtaining the combination has some probability of detection but may not be in the same time sequence of the actual theft attempt
- The probability of detection at the portal may be much different if the adversary has significant authority at the facility or responsibilities for the detection systems
- The adversary success could be enhanced by using force at the exit portal



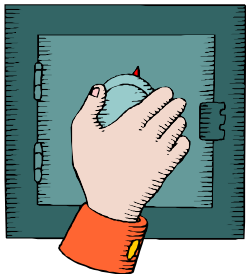
Considerations when Developing Vulnerable Paths

- **Consistent tactics**
  - **Using stealth or deceit after force may not be logical**
  - **If tools are used, include the tool acquisition in the defeating the path measure**
- **If there have been serious questions about measure selection, do another path with the other most credible options**



Third Example for Developing Most Vulnerable Path

- Example 1: covert theft under normal operations
- Example 2: covert theft by stealing the door combination
- Example 3: Protracted Theft or Protracted Diversion



Select Measures Along Path: Step 1

Target is the bunker with intent to steal a small quantity during normal operations

Step	Action	Measures Along Path	Possible methods	Likelihood of Detection	Time (Sec)
1	Enter and traverse PA	Entry control and General observation OR	Normal entry No contraband	Very Low	~~300~~
		Perimeter and General observation	Cut or climb fences	Medium (.36)	25

Normal entry to the area is still the path of least resistance.

Select Possible Method for Step 2

Step	Action	Measures along path	Possible Methods	Likelihood of Detection	Time (Sec)
2	Enter the bunker	Combination Lock, General observation, MBA custodian oversight	Normal entry	Very Low	120
		Combination lock, General observation	Covertly obtain the combination	Medium	60
		Walls, Door	Breach one of surfaces using tool acquired within facility	High	60 for door 174 for walls

Since repeat attempts will be made to get a goal quantity a non-alerting method would be used here

Select Possible Method for Step 3

Step	Action	Measures along path	Possible Methods	Likelihood of Detection	Time (Sec)
3	Covertly remove target material	General observation, MBA custodian oversight,	Access material in normal manner and hide some material on person	Very Low (for mat. handler)	60
Ruled out by Previous actions		General observation after covert entry	Open cage and product package with hand tools	Low	30
		General observation after overt entry	Open cage and product package with hand tools	Low	30

Select Possible Method for Step 4

Step	Action	Measures along path	Possible Methods	Likelihood of Detection	Time (Sec)
4	Covertly remove a target from the Bunker	General observation, MBA custodian oversight	Normal exit with package hidden	Very Low	60
		General observation after covert entry and removal	Move normally out door and across PA	Medium	60
		General observation after overt entry and removal	Move as quickly as possible out door and across PA	Medium	30

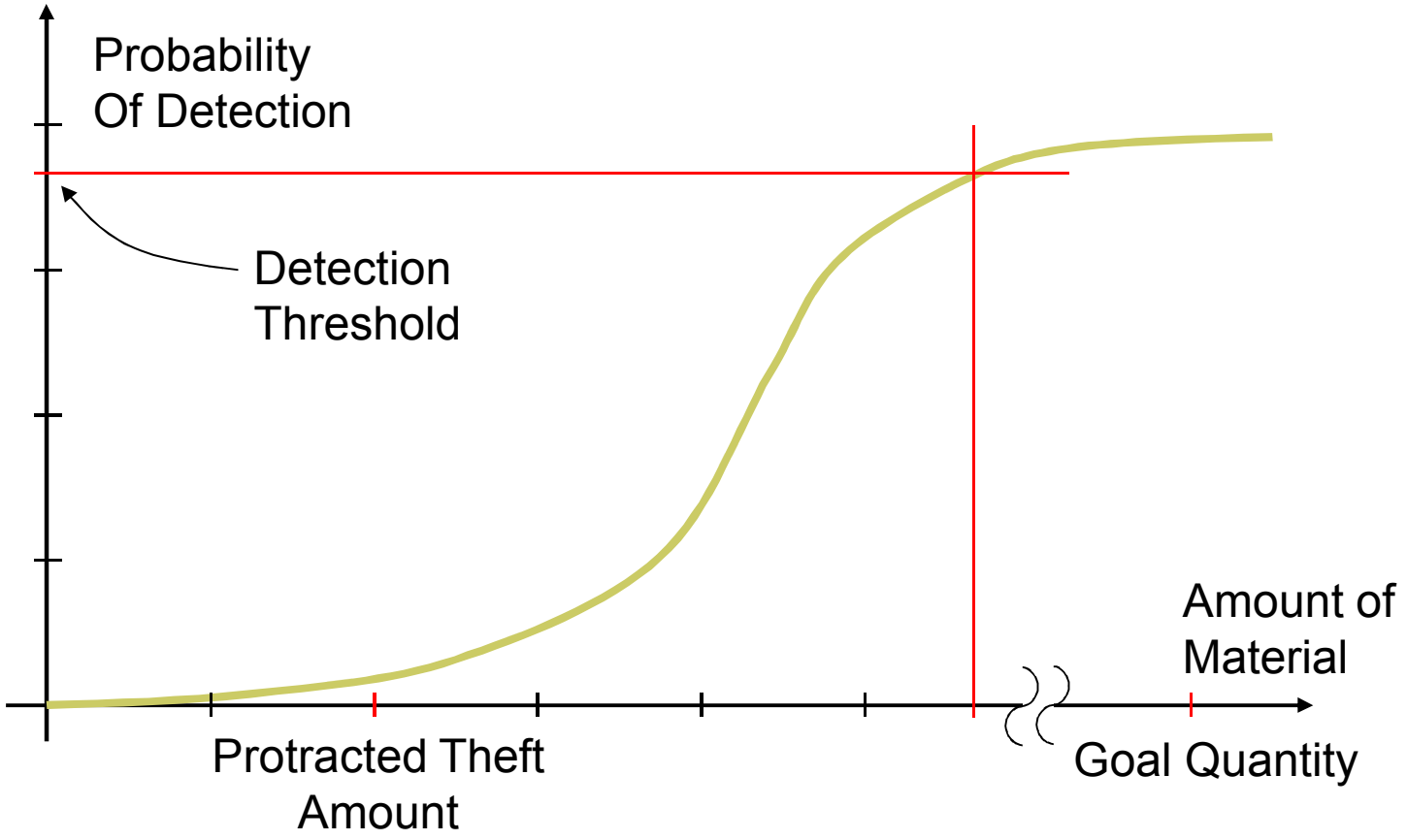
Ruled out by Previous actions

Select Possible Method for Step 5

Step	Action	Measures along path	Possible Methods	Likelihood of Detection	Time (Sec)
5	Covertly remove target from the PA	General observation, Material detectors	Normal exit with explanation that he had gotten contaminated if needed	Low	90
		General observation, Material detectors	Forceful exit after material detector alarms or is observed with package	High	30
		Perimeter zone, general observation	Throw package over the zone to the outside for recovery later and leave area	Medium	90

Detection of lower quantity of material could be much lower than for goal quantity

Detection vs. Quantity tradeoff



Abrupt and Protracted Theft Tradeoffs

- Taking smaller quantities decreases P_D
- Repeated attempts causes accumulation of P_D over multiple attempts (at same detection point)
  - $P_{D\ accumulated} = 1 - (1 - {}_{PD\ attempt})^n$: n = number of attempts
- Timeframe for repeated attempts (enough to get a goal quantity) can bring other detection measures into play
  - Inventory
  - Process alarms

Example 3: Protracted Theft

Step 1. Material Handler enters protected area normally – no detection

Step 2. Enters bunker as part of normal operations

Step 3. Covertly take a small amount of target material and hides to remove from bunker

Step 4. Normal exit from bunker

Step 5. Normal walk across area to Entry Control Point and then process out as normal (hoping not to be detected by SNM detector)

Step 6. Repeat steps 1 - 5 until a goal quantity is achieved

Example 3 - Accumulated Detection Probability

- The accumulated detection probability depends on the number of attempts
- A worst-case, single-event theft quantity can be determined based on the measured capabilities of the detector and the procedural measures in place at the material access point. As an example:
  - An insider may be able to divert up to 500 g with low detection likelihood (0.10), but
  - The SNM detector has a PD of 0.5 for 500 g, but only a PD of 0.05 for 200 g
  - What is the worst-case quantity?
  - Is a protracted scenario better for the Insider?

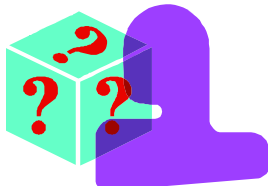
Example 4 - Protracted Diversion

- **If a high probability of detection exists late in the scenario (for example exiting the PA) and is largely independent of amount, it might be advantageous for the insider to remove small quantities of material from the material access area, and accumulate a goal quantity on-site before attempting to remove the material from the site.**

Vulnerable Paths Summary

- Develop most vulnerable paths by:
  - Selecting adversary path with least effective protection measures
  - Considering the time to defeat, the detection likelihood and the adversary capabilities
  - Selecting path measures based on logic and judgment
  - Looking at protracted scenarios as ways to reduce P_D
- Vulnerable paths are developed for each credible threat and target combination

Questions or Comments???



Subgroup Exercise 5: Develop Most Vulnerable Paths

- Utilize the worksheets completed in Subgroup Exercise 4 and develop:
  - Three vulnerable paths
    - Select the protection measures for the most advantage to the adversary, i.e., the measures with the lowest effectiveness
    - Consider both the time to defeat and the detection likelihood and adversary capabilities, etc.
    - Mark the measures selected on the tables
    - Complete a path worksheet
- Present summary to the large group

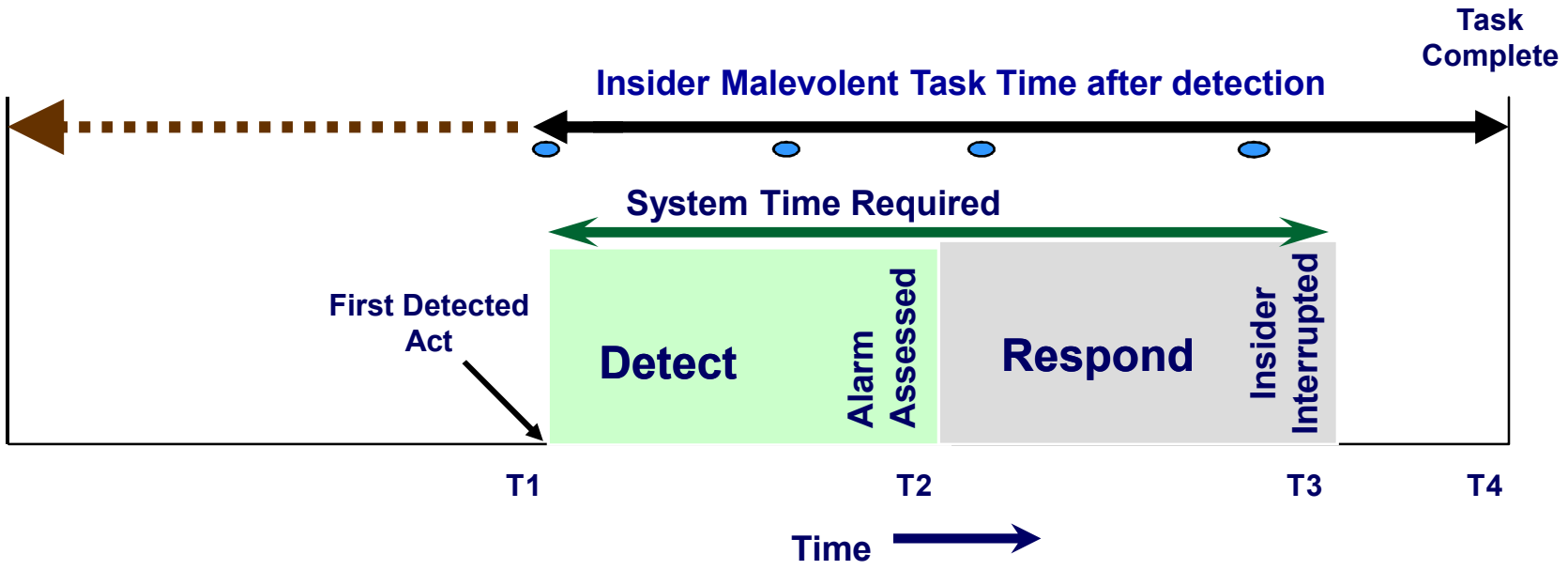
Learning Objectives

- Identify most vulnerable protection measures
- Develop most vulnerable paths for threat / target combination
- Estimate likelihood of detection and time for each vulnerable path step
- Be able to develop a timeline for selected scenarios
- Discriminate between continuous and discontinuous time sequences
- Integrate response into the effectiveness analysis and derive P_I and P_E
- Develop worst case scenarios

Developing Scenario Timelines

- Two types of Timelines
  - Continuous (Abrupt Theft)
    - The classical physical protection “foot race”
    - Time line analysis works well
  - Discontinuous (Protracted Theft or Diversion)
    - Time line is long - may span months
    - detection opportunities occur at multiple steps during the sequence
- Some actions are not related to time
  - Authorized or undetected actions do not include a time component

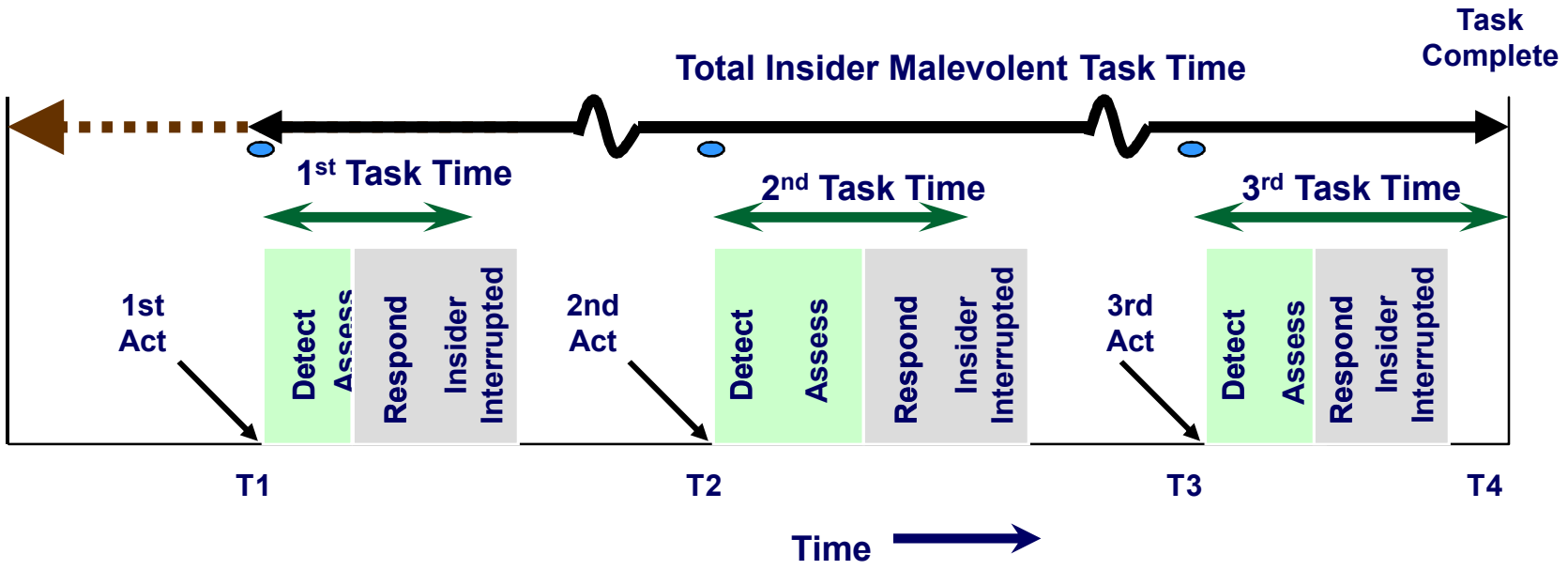
Insider Continuous Sequence



- Detection points

System detection and response time must be less than insider malevolent task time after detection

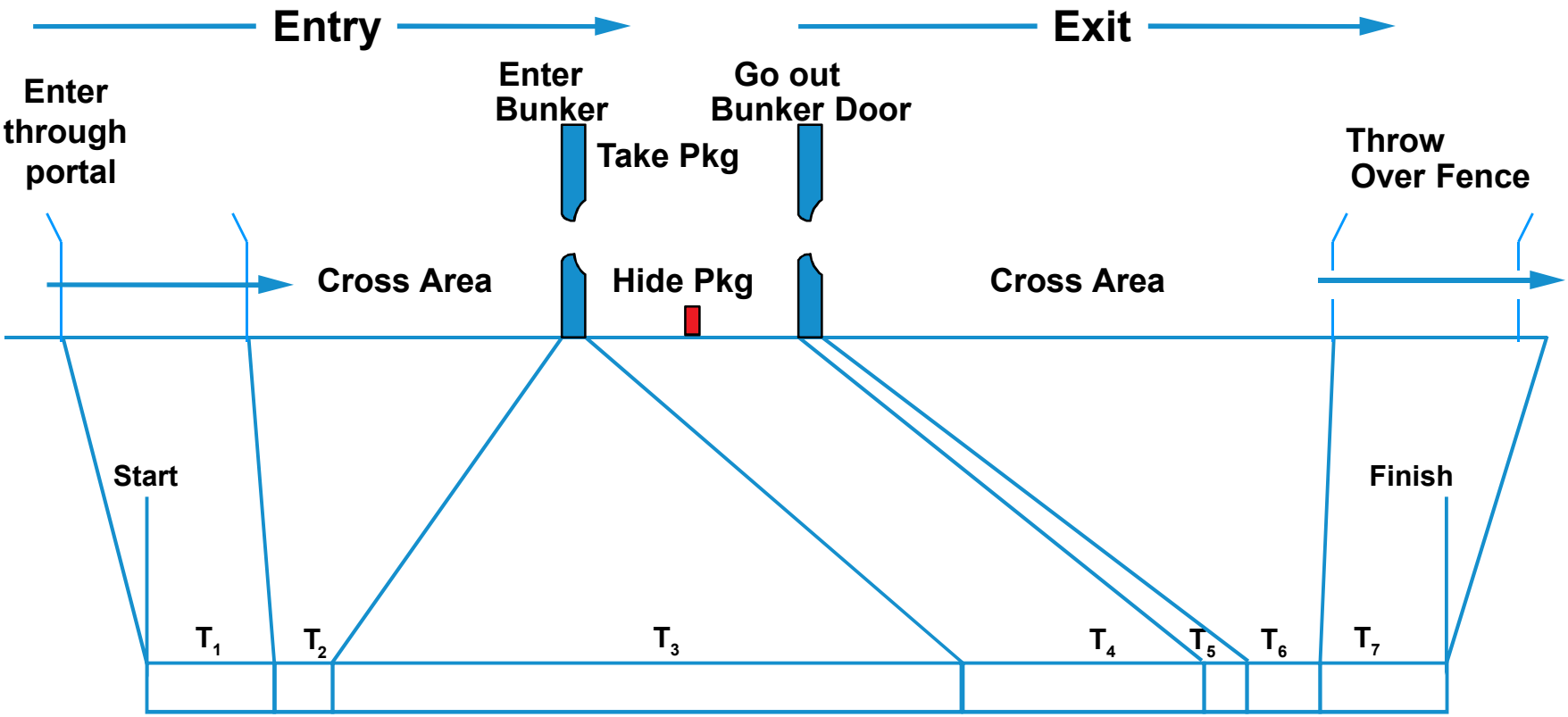
Insider Discontinuous Sequence



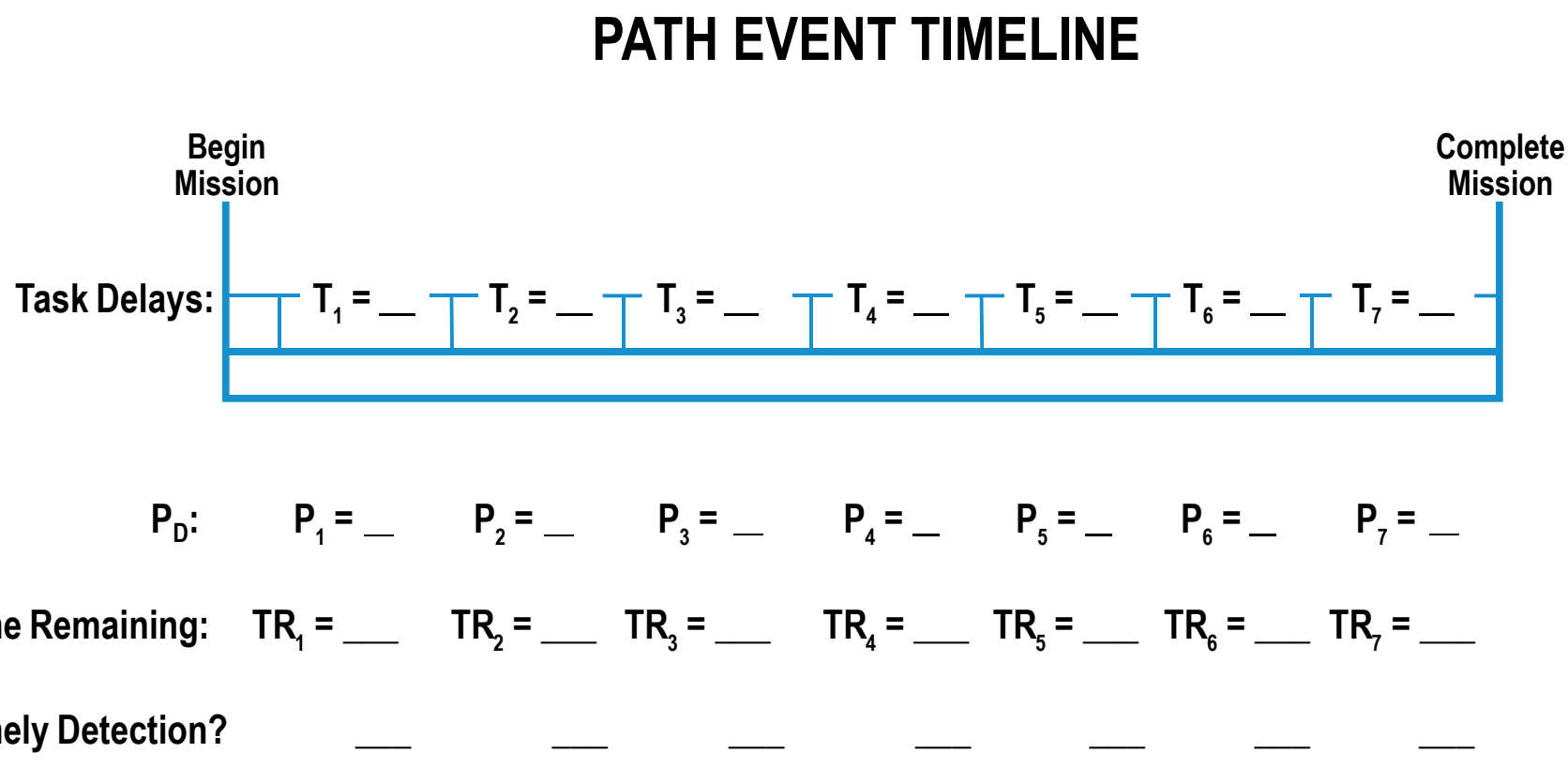
System detection and response time must be less than segmented insider malevolent task time after detection but detection possibilities at T1, T2, T3 may not be complementary as they are in the continuous sequence

Developing Path Event Timelines

Transform location and tasks into delay along a scenario's path



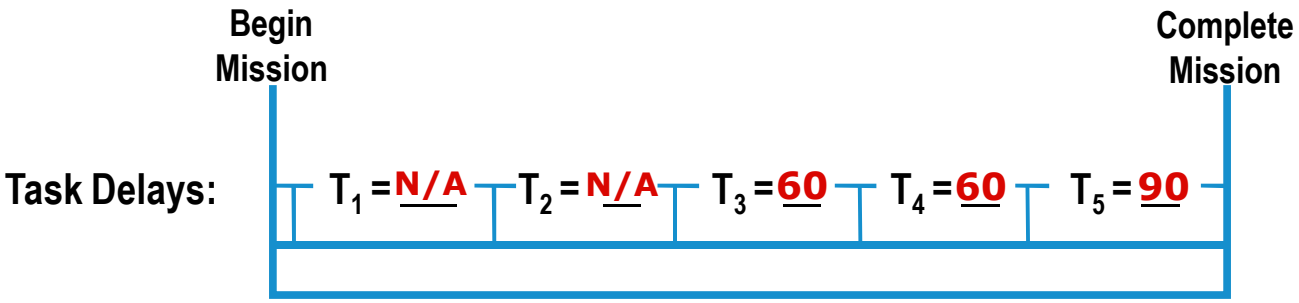
Place Task Delays and Detection Probabilities on the Timeline



Example 1 – Possibly the Most Vulnerable Path For HP Tech/Bunker

Step	Action	Likelihood of Detection	Time (Sec)
1	Enter protected area normally	Very Low	N/A
2	Enter bunker normally	Very Low	N/A
3	Take package and hide under coat	High	60
4	Walk out of bunker normally	High	60
5	Walk normally to fence and throw package over and leave area	Medium	90

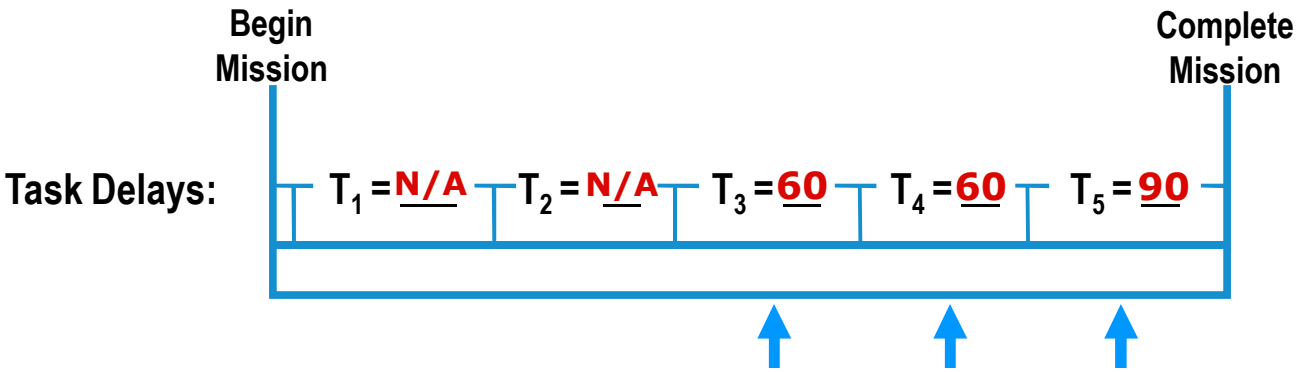
Timeline with Task Times and Detection Probabilities



P_D:	P_1 = ___	P_2 = _	P_3 = H	P_4 = H	P_5 = M
Time Remaining:	TR_1 = ___	TR_2 = ___	TR_3 = ___	TR_4 = ___	TR_5 = ___
Timely Detection?	___	___	___	___	___

Place Detection Locations on the Timeline

Assign detection locations at beginning, middle or end of task delays for the bunker

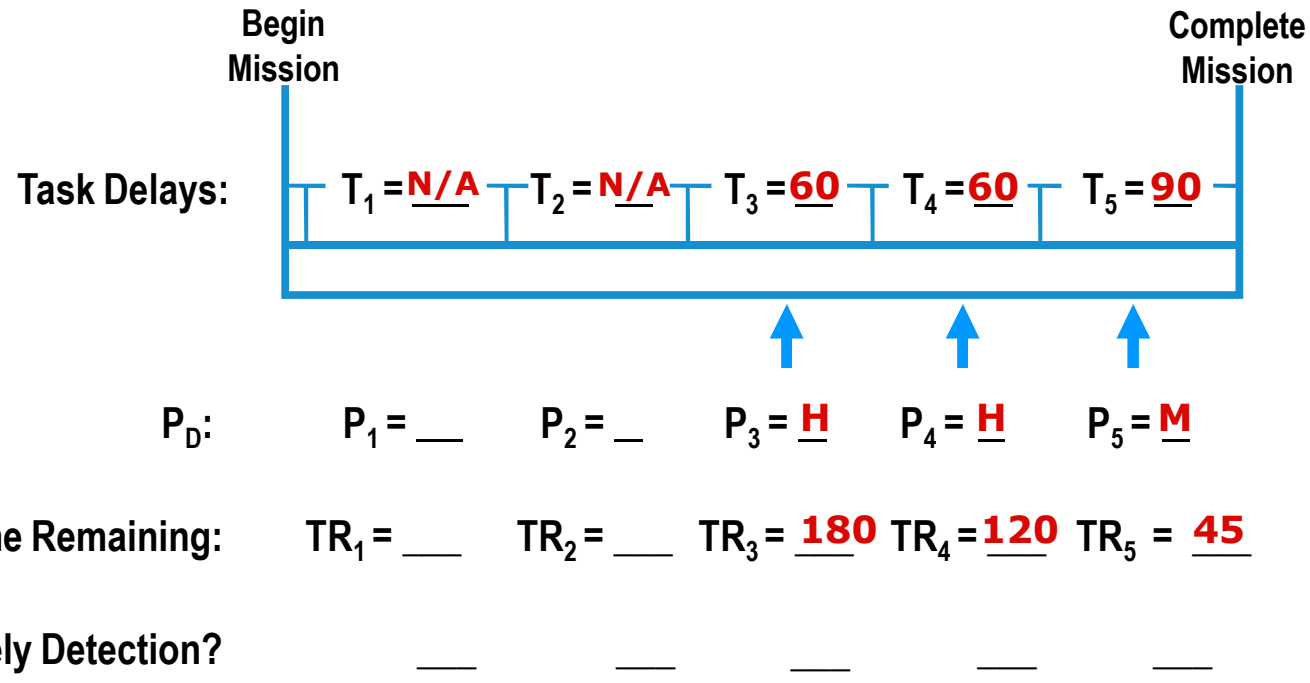


P_D: P_1 = ___ P_2 = _ P_3 = H P_4 = H P_5 = M

Time Remaining: TR_1 = ___ TR_2 = ___ TR_3 = ___ TR_4 = ___ TR_5 = ___

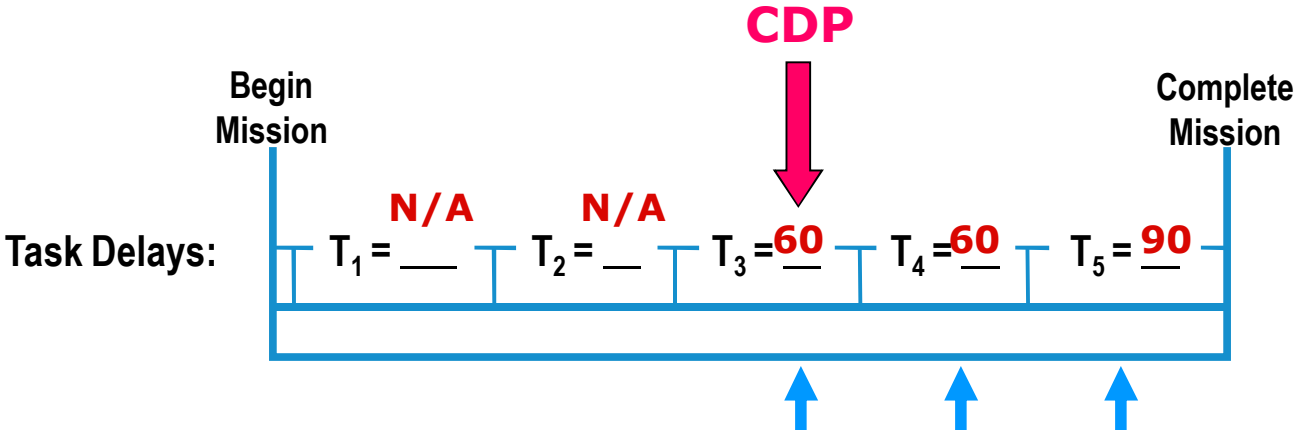
Timely Detection? ___ ___ ___ ___ ___

Add Time Remaining Before Completion of Adversary Tasks



Add Response Time and Determine Timely Detection

Determine where (if) we have timely detection by comparing Response Time and Time Remaining



Assume RT=150

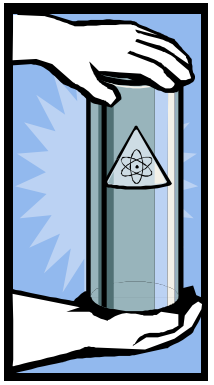
Developing Effectiveness Measures

- **Probability of Interruption (P_I)**
  - **The probability that the MPC&A system will detect and respond to adversary actions in a timely manner**
- **Probability of System Effectiveness (P_E)**
  - **The probability that the MPC&A system will detect and effectively stop adversary actions in a timely manner**
- **Risk (R)**
  - **A graded measure of system effectiveness that takes the consequence of successful insider activities into account**

- **Interrupting and stopping insider activities is the function of response**

Response

- Response is intended to prevent undesirable consequences
- The type of response depends on the type of adversary actions
- The type of response also depends on where detection occurs in the action sequence



- If response is not in time to prevent undesirable consequences, it can mitigate those consequences
  - Emergency management system
  - Safety systems

Response Effectiveness

- Determine the response type
  - Employees and/or guards for non-violent insider
  - Guards for violent insider
- Determine the time taken for the response
  - Include all time elements
- Determine the ability of the response to stop the adversary
  - Use testing results
  - Data provided by studies and simulations
  - Expert opinion

Large Group Discussion: Who will Respond?

- **Who will respond for the given situation:**
  - **Procedural error (may be malevolent)?**
  - **BMS alarm?**
  - **Person seen taking material?**
  - **Person discovered attempting to acquire combination?**
  - **Person entering faulty data in MC&A system?**

Protective Force Response for Insiders

- **Procedure may call for different deployments**
  - **How does the response force know if it is an insider or outsider alarm?**
  - **Response to Outsider actions**
    - **Respond to target location**
    - **All responders available deploy**
  - **Response to Insider actions**
    - **Probably depends on insider action – if known**
    - **Respond to exit points**
    - **Respond to target location and perhaps miss the insider**
    - **Only 1 to 2 responders needed to apprehend so full force can cover several points**

Other Responders

- Adjacent co-workers
  - Response time is essentially zero
  - Are they trained to respond in any way?
    - Query each other about unusual activity?
    - Physically restrain other workers?
  - If they are trained to contact the guards:
    - How do they do this?
    - How long does it take?
- Casual observers
  - Probably only contact guards in exceptional cases

How to Estimate Probability of Interruption (P_I)

For Abrupt Theft scenarios

1. **List task times**
2. **Identify response elements and response time**
3. **Use the response time to calculate the point in time where response must start if the malevolent action is to be stopped before completion**
4. **Calculate the cumulative likelihood of detection at or before this point**

Example 1 – Possibly the Most Vulnerable Path For HP Tech/Bunker

Step	Action	Likelihood of Detection	Time (Sec)
1	Enter protected area normally	Very Low	N/A
2	Enter bunker normally	Very Low	N/A
3	Take package and hide under coat	High	60
4	Walk out of bunker normally	High	60
5	Walk normally to fence and throw package over and leave area	Medium	90

Who is the responder to each of these detections?

Questions about the Response for these Detection Locations?

- In the Bunker
  - Other workers?
  - What is the response time if they detect?
  - Does the adversary stop if detected?
  - Do they stop the action or call the guards?
- Crossing the PA
  - Other workers? Response time?
  - Guards in towers?
- Throwing package across the perimeter
  - Other workers? Response time?
  - Guards in towers? Entry Control Point?

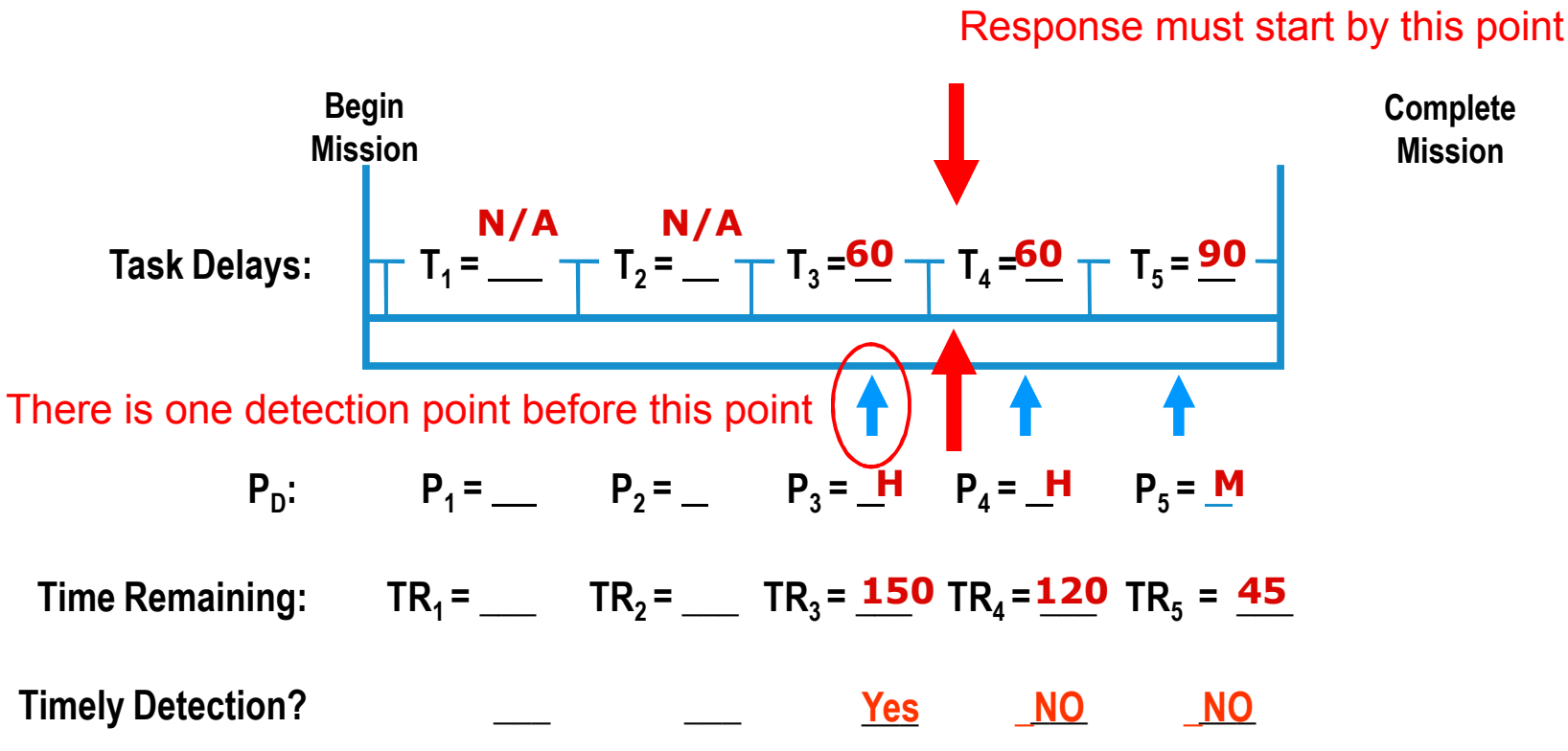
Example 1: Response Time Table for an adjacent co-worker and Guards

Response Action	Time taken (seconds) Min	Max
Co-worker identify malevolent action – Sees material removal – assume detection at this point	0	60
Communicate to guards	60	180
Guard communication time	30	
Response prep time	50	
Travel	0 to ECPs	30 to Bunker
Intervene	0	60
Total	140	380

This example has several uncertainties – Who? Where? When?

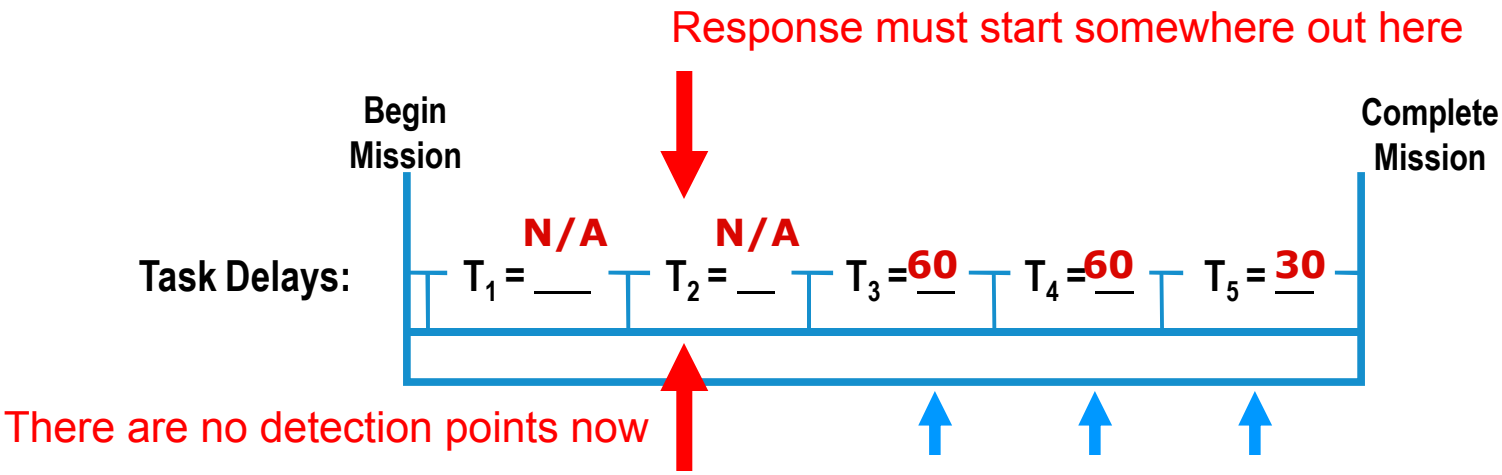
Insider Continuous Timeline

If Response Force Time is 140 sec, P_I = High



Insider Continuous Timeline

If Response Force Time is 380 sec, P_I = zero



Example: Protracted Diversion

Step 1. Material Handler enters protected area normally – no detection

Step 2. Enters bunker as part of normal operations

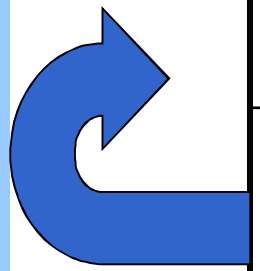
Step 3. Covertly take a small amount of target material and hides to remove from bunker

Step 4. Normal exit from bunker to stash material

Step 5. Repeat steps 1 - 4 until a goal quantity is achieved

Step 6. Access stash, walk across area to Perimeter, throw material across to pick up later, leave area

Example: Protracted Diversion by Material Handler



Step	Action	Likelihood of Detection	Time (Sec)
1	Enter protected area normally	Very Low	N/A
2	Enter bunker normally	Very Low	N/A
3	Take material and hide on person	Very Low	30
4	Walk out of bunker normally and stash material	Very Low	60
5	Gather material. walk normally to perimeter and throw accumulated material over fence, leave area	Medium	90

Response to Protracted Diversion

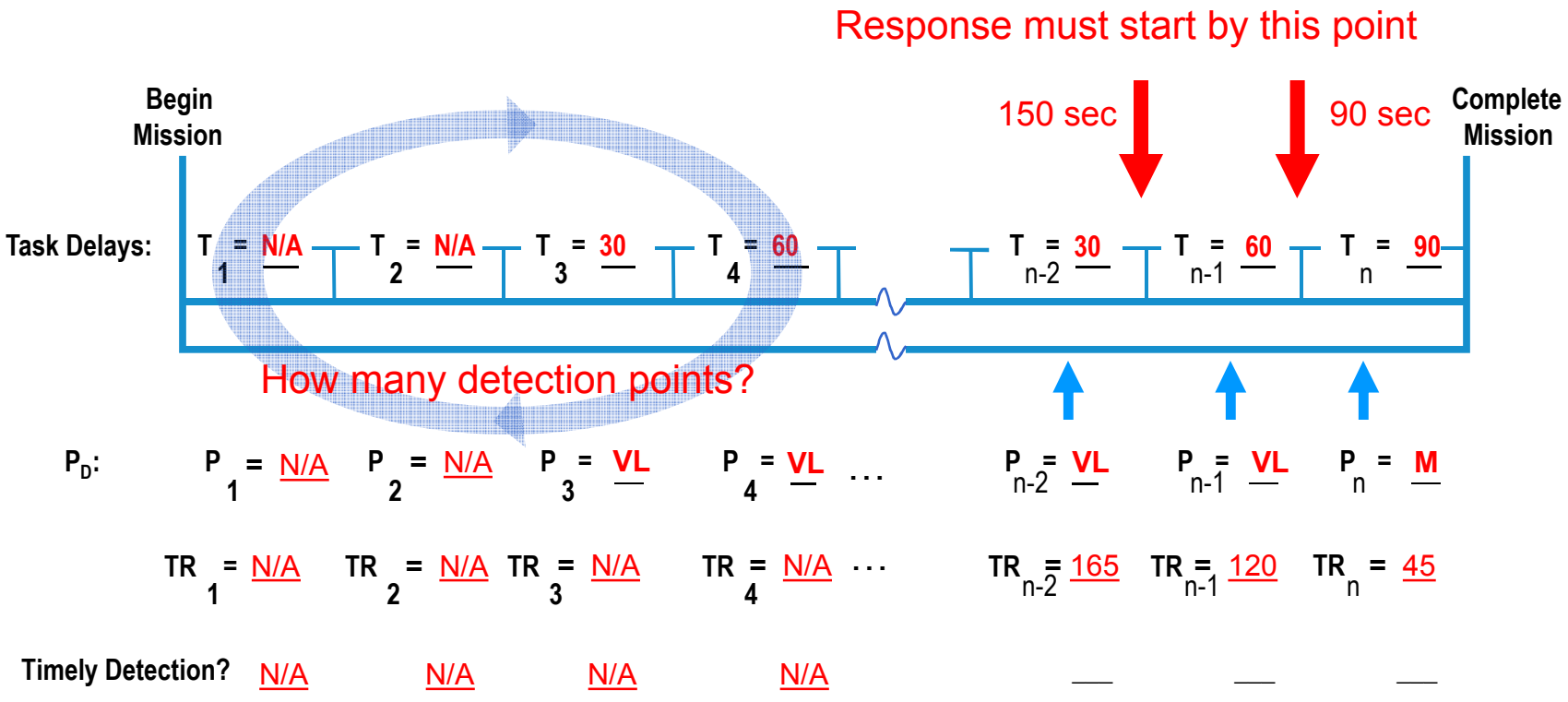
- **If we are protecting against theft of a "goal quantity" of material, we assume:**
  - **If Insider has accumulated less that a goal quantity:**
    - **Insider will stop actions when identified (will not become violent)**
    - **Detection of actions is the measure of effectiveness**
  - **If Insider has accumulated goal quantity and is on final actions (removing from area):**
    - **Response is necessary**
    - **Insider may turn violent to complete actions**

Response Actions to Insider Actions

Step	Action	Response Action	Response Time
1	Enter protected area normally	None	N/A
2	Enter bunker normally	None	N/A
3 < GQ	Take material and hide on person	Co-worker identification Insider surrenders	N/A
4 <GQ	Walk out of bunker normally	Co-worker identification Insider surrenders	N/A
3 w/ GQ	Take material and hide on person	Co-worker identification, communication to guards, guard response	90 - 150
4 w/ GQ	Walk out of bunker normally	Co-worker identification, communication to guards, guard response	90 - 150
5	Gather material, walk normally to perimeter, throw accumulated material over fence, leave area	Co-worker identification, communication to guards, guard response	90 - 150

Protracted Diversion Timeline

If Response Force Time is 90 to 150 sec, P_I = ?

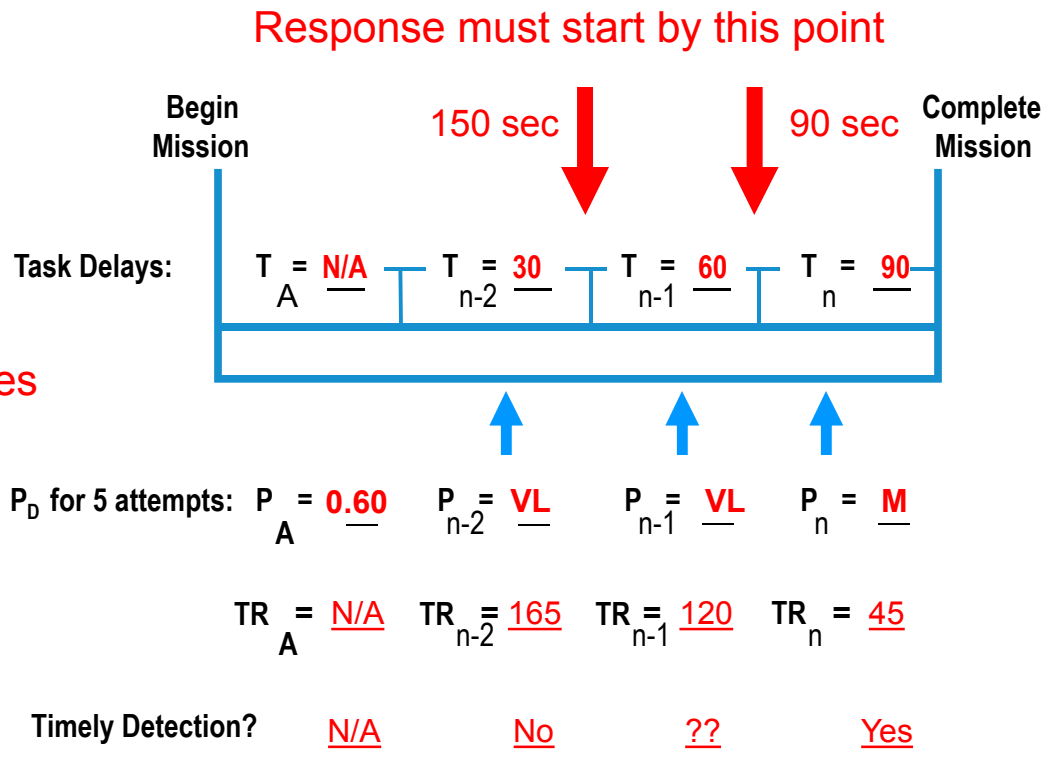


Probability of Detection for Protracted Diversion

- If five diversions attempts are required to accumulate a goal quantity the probability of detecting repeated diversion attempts is :
  - PD for step 3 and 4 = 1 - (1-0.05)**8 = 0.34
- If ten diversion attempts are required to accumulate a goal quantity the probability of detecting repeated diversion attempts is:
  - PD for step 3 and 4 = 1 - (1-0.05)**18 = 0.60

Protracted Diversion Timeline
Ten attempts required

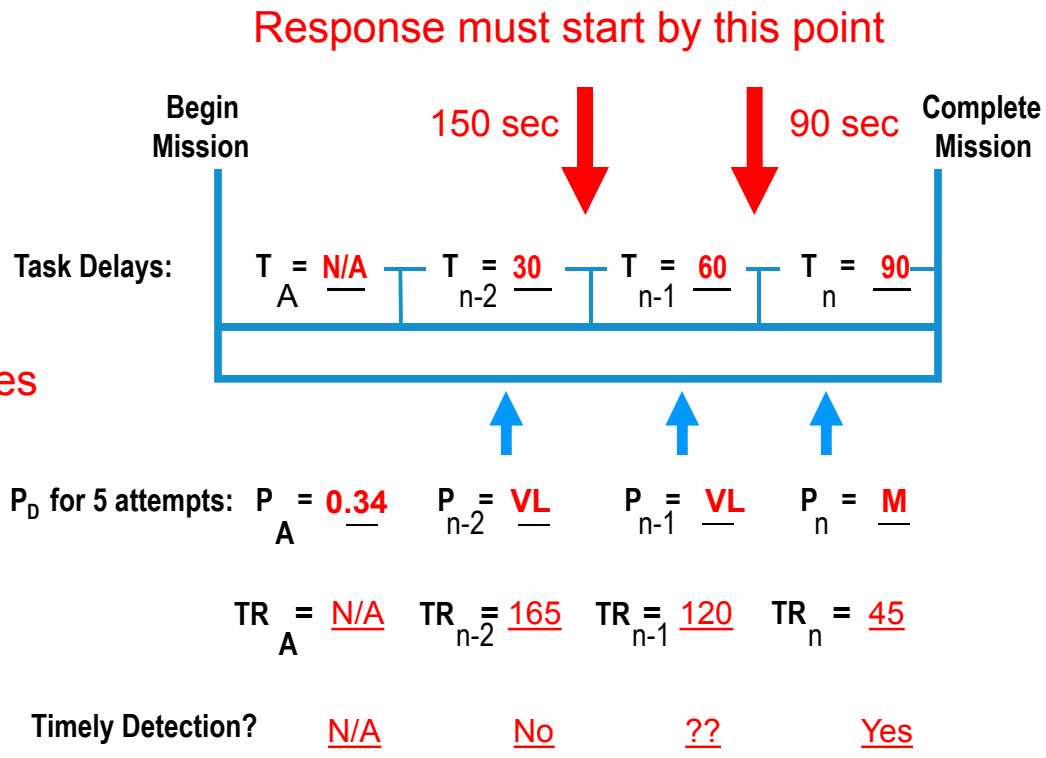
If Response Force Time is 90 to 150 sec, P_I = 0.64 to 0.62



T_A, P_A, TR_A are accumulated values over the diversion attempts

Protracted Diversion Timeline Only Five attempts required

If Response Force Time is 90 to 150 sec, P_I = 0.40 to 0.37



T_A, P_A, TR_A are accumulated values over the diversion attempts

Suggested Simple Rules For Deriving Cumulative Likelihood – Example Table

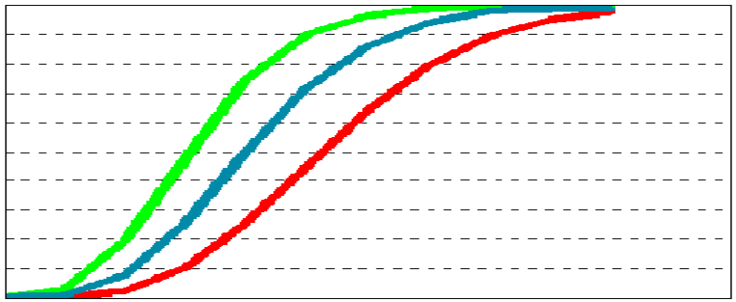
Measures in Sequence	*Cumulative Likelihood*
VL & VL	VL
VL & VL & VL	L
VL & L	L
VL & VL & L	L
L & L	M
L & L & L	M
L & M	M
L & L & M	H
M & M	H
L & H	H
M & H	H
M & M & H	VH
H & H	VH

More Response Integration

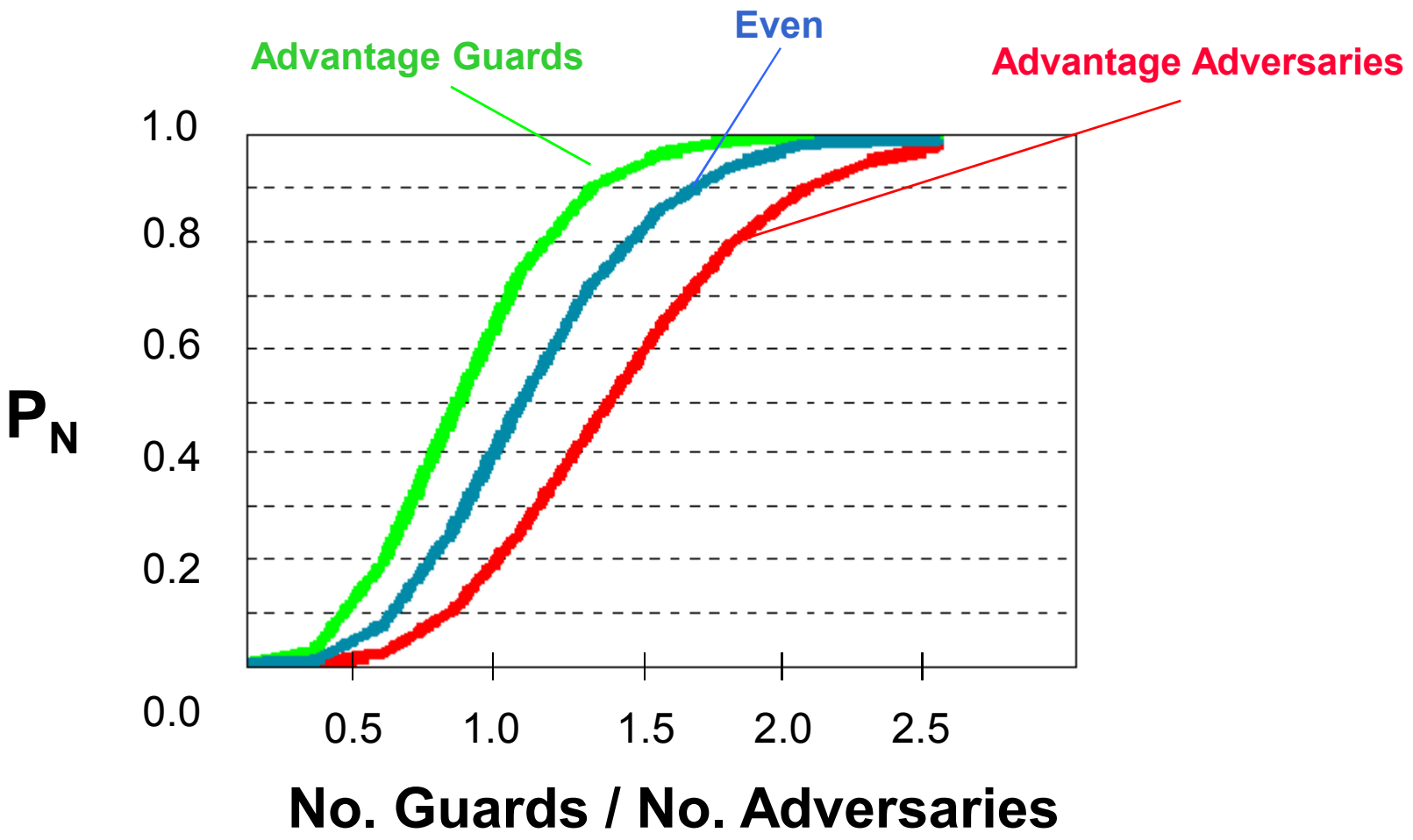
- The Response Time helps to determine if detection is timely (in time to prevent Insider success)
- We also need to consider the effectiveness of the response in the case of active violent Insiders
- This effectiveness is captured as the probability of Neutralization (P_N)
- For non-violent Insiders, P_N is 1.0
- For violent Insiders, it depends

A Simple Probability of Neutralization Estimate for Insiders

- If an insider is violent but does not have a weapon, use the P_N curve on the next page, but give the guard the advantage
  - 1 armed guard to 1 Violent Insider - $P_N = 0.7$
  - 2 armed guards to 1 Violent Insider - $P_N = 1.0$
- If the insider has a weapon, and the advantage of surprise, use the curve with adversary advantage
  - 1:1 - $P_N = 0.15$
  - 2:1 - $P_N = 0.85$



Simple Estimate for P_N



Overall System Effectiveness (P_E)

- **Probability of System Effectiveness is the product of the Probability of Interruption and the Probability of Neutralization**
  - $P_E = P_I * P_N$
- **Relies on concept of timely Detection (Critical Detection Point)**
- **Relies on independence of P_I and P_N**
- **Since the process combines P_I & P_N we need to identify how to combine numbers and qualitative designators. One method is to map qualitative values to quantitative values**

Qualitative to Quantitative Mapping

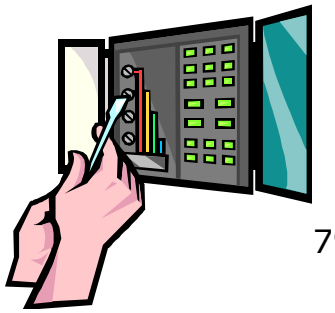
Quantitative Range	Qualitative Value	Quantitative Value
0.9 - 1.0	Very High	0.95
0.7 – 0.9	High	0.8
0.3 – 0.7	Medium	0.5
0.1 – 0.3	Low	0.2
0.0 – 0.1	Very Low	0.05

Effectiveness Analysis Summary

Scenario	PI	PN	PE
Bunker Target, HP technician, abrupt theft, RT = 140 sec	High 0.95	0.15	0.14
Bunker Target, HP technician, abrupt theft, RT = 380 sec	0.0	N/A	0.0
Bunker Target, Material Handler, protracted diversion, RT = 90 sec	0.64	1.0	0.64
Bunker Target, Material Handler, protracted diversion, RT = 150 sec	0.62	0.7	0.43

Worst Case Considerations

- We may have identified the most vulnerable paths but are these necessarily the paths for the worst cases after we add response considerations?
- Consider known vulnerabilities and see if they can be exploited by the adversary
- Can the insider delay or eliminate the response?
- Can the insider prevent the alarms from being generated or communicated?
- Can the insider utilize authority to reduce assessment effectiveness of an action?
- Can diversionary actions be used to assist in successful scenario completion?



Using System Effectiveness to find the Worst-case Scenario

- Look for the lowest Probability of MPC&A System Effectiveness (P_E)
  - Multiply P_I for the path with the lowest P_I by its P_N
  - See whether there is a path with a higher P_I but a much lower P_N
    - If so, compute the product of the P_I and P_N
  - Take the smaller of these two products as P_E for that target and Insider
- These approaches concentrate mostly on P_I – look at P_N also
  - Can the adversary delay or neutralize the response force in the adversary path?

Possible Impacts on P_N

- A non-violent insider won't actively interact forcefully with the guards BUT
  - Can he divert them?
  - Delay them?
- A violent insider has the advantage over the guards in the early stages of a confrontation – could eliminate at least one guard without generating an alarm
  - This confrontation could be at the end of the path - perhaps in the Entry Control Point

Developing Worst Case Scenarios

- Distinguish between continuous and discontinuous insider threat time sequences
- Use response time to calculate where response must start to stop a continuous malevolent event
- Use the standard timeline for continuous scenarios
- Use segmented analysis for discontinuous scenarios like protracted theft and protracted diversion

Developing Scenario Summary

- Discriminate between continuous and discontinuous time sequences
- Integrate response into the effectiveness analysis and derive P_I, P_N and P_E
- Develop worst case scenarios

Questions or Comments??

Subgroup Exercise 6: Estimate System Effectiveness (P_E)

- Complete the tables developed in Subgroup Exercise 5 describing the most vulnerable paths:
  - Determine the response type
  - Determine the time taken for the response
  - Determine the ability of the response to stop the adversary
  - Derive a P_E for all three vulnerable paths giving three potential worst case scenarios
    - Do you think these are the worst case scenarios?
- Present summary to the large group

National Nuclear Security Administration

Risk Determination

Insider Protection Course

Learning Objectives

- **Understand the benefits of using Risk a metric of MPC&A System effectiveness**
- **Identify how to estimate Risk using two different approaches**

Risk

- Use of Risk to measure MPC&A system effectiveness allows the system to:
  - Protect pencils like pencils
  - Protect diamonds like diamonds
- Risk incorporates the consequence value of the targets
- P_E and P_I do not have to be as high for lower consequence targets to have equal risk

Two Approaches to Estimating Risk

- **Qualitative**
  - **Utilizes the qualitative designators**
  - **Advantage: More openly demonstrates the qualitative nature of the insider analysis**
- **Quantitative**
  - **Converts all relevant factors to numbers**
  - **Advantage: Can be easily combined with risk numbers often used for outsider adversaries to provide an overall summary of MPC&A system effectiveness**

Combine Results for all Targets

- We have only done the analysis on a few paths for a few threat / target combinations
- A complete system analysis includes ALL reasonable paths for ALL credible threat / target combinations
- Many of the lower threat group scenarios can often be easily evaluated based on the analysis of the high threat group scenarios
- The result: a defendable composite picture of system effectiveness and vulnerabilities

Qualitative Approach

- Create a MPC&A system effectiveness table using the estimated values for P_I
  - Assumes P_N is similar for all scenarios
  - Equates system effectiveness to P_I
- Include all reasonable threat/target combinations
- Identify and qualitatively define the consequences expected for successful completion of each threat/target scenario
- Utilize a P_I vs. C chart to determine relative risk for each scenario

Example System Effectiveness Table

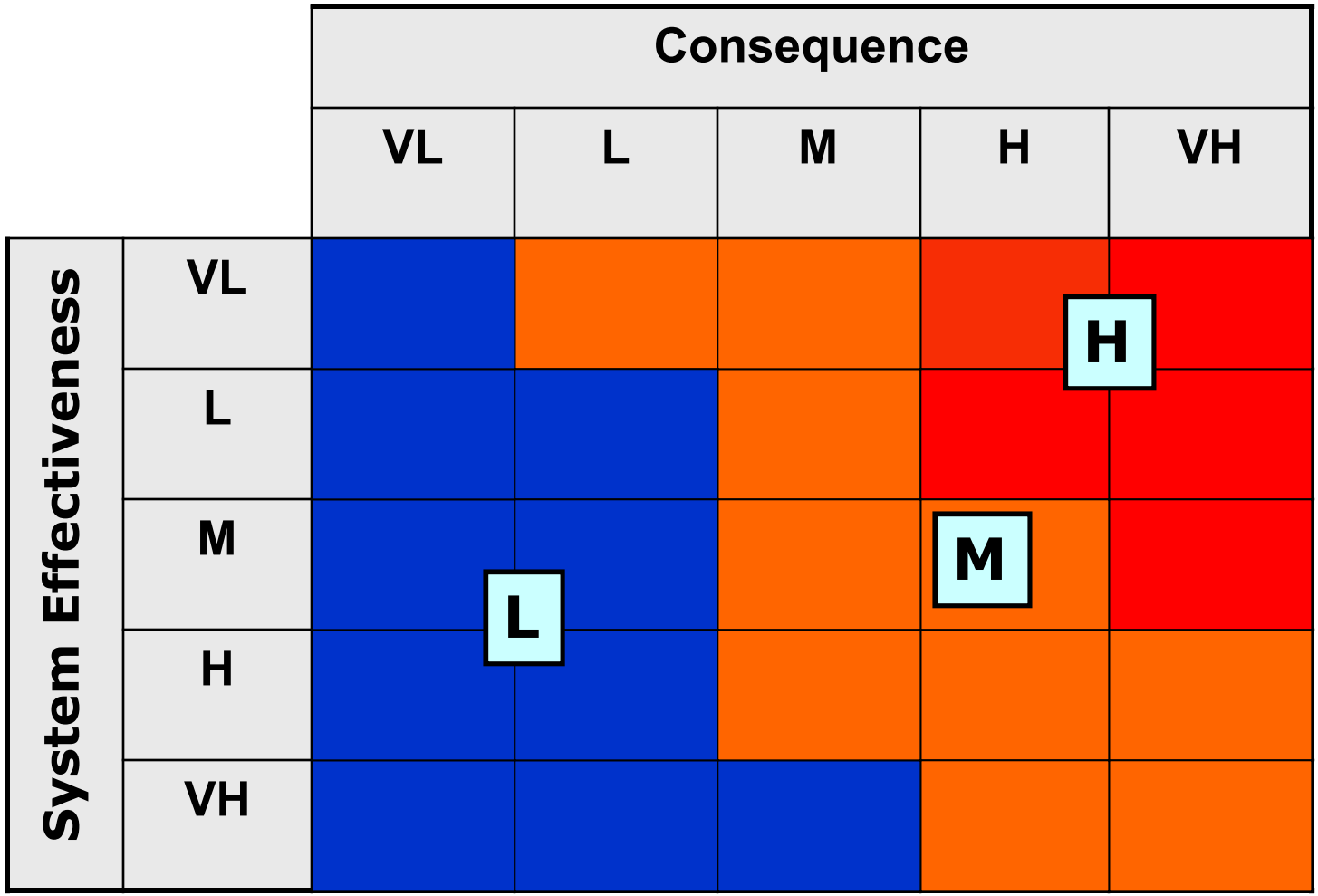
Threat Group	Product Vault	X-ray Facility	Chip Vault	Machining area
Plant Manager	H			
Shift Supervisor		M		
Machining Operator			H	L
Health Physics Technician				
Operations Support				
Maintenance Manager				
Maintenance Personnel				

Add Target Consequences to the System Effectiveness Table

Threat Group	Product Vault C = High	X-ray Facility C = Med	Chip Vault C = High	Machining area C = High
Plant Manager	H			
Shift Supervisor		M		
Machining Operator			H	L
Health Physics Technician				
Operations Support				
Maintenance Manager				
Maintenance Personnel				

Example Risk Criterion

RED is HIGH RISK, ORANGE MEDIUM and BLUE LOW



Example Qualitative Risk Summary Chart

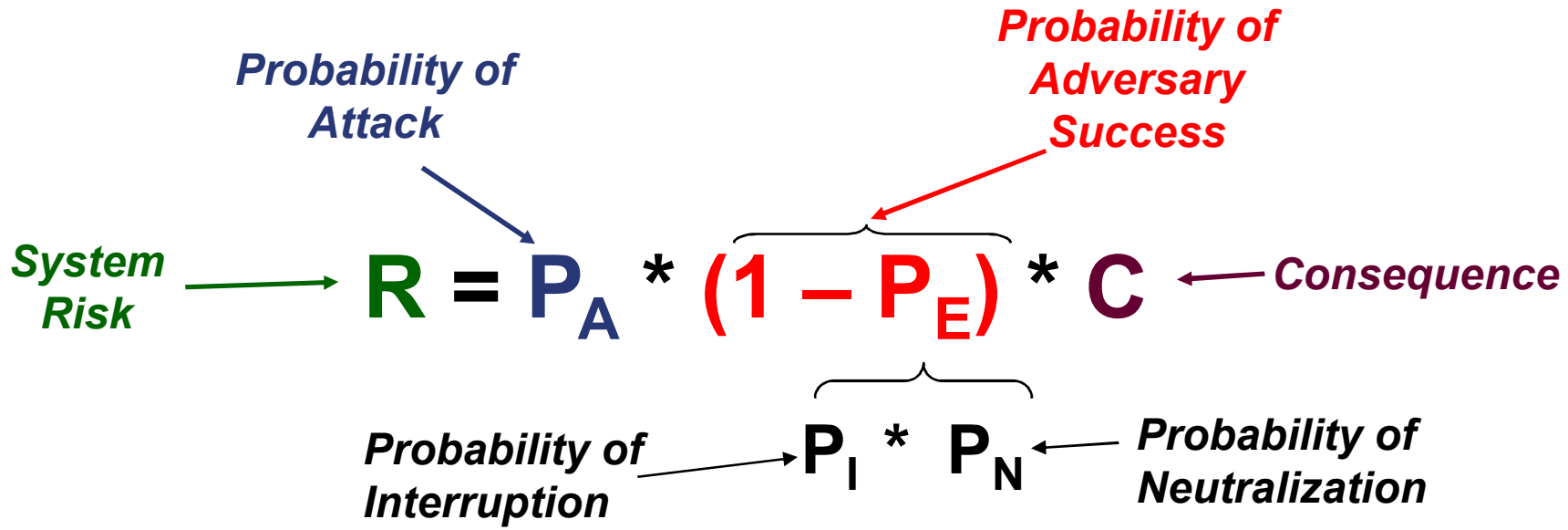
Threat Group	Product Vault C = High	X-ray Facility C = Med	Chip Vault C = High	Machining area C = High
Plant Manager	M			
Shift Supervisor		M		
Machining Operator			M	H
Health Physics Technician				
Operations Support				
Maintenance Manager				
Maintenance Personnel				

Quantitative Approach

- Use the risk equation
- Convert all qualitative values to numbers
- Include all reasonable threat/target combinations
- Identify the consequences expected for successful completion of each threat/target scenario
- Utilize the numerical result to determine relative risk for each scenario

Estimating Risk with the Risk Equation

- Integrates system effectiveness measures into a single, consistent approach for determining risk



The Conditional Risk Equation

For High-Consequence Targets, we often assume that the Probability of Attack is equal to 1.0

Probability of Adversary Success

System Risk → $R = 1.0 * (1 - P_E) * C$ ← *Consequence*

Probability of Interruption → $P_I * P_N$ ← *Probability of Neutralization*

We call the resulting equation the Conditional Risk Equation:

$$R_C = (1 - P_E) * C$$

Estimating Insider Risks

- $R_C = (1 - \underbrace{(P_I * P_N)}_{P_E}) * C$

- We know P_E , P_I and P_N
- We determine the Consequence Value - C in Target Characterization
- We can calculate Conditional Risk

Example Quantitative Risk Summary Chart

Threat Group	Product Vault	X-ray Facility	Chip Vault	Machining area
Plant Manager	0.60	?	?	?
Shift Supervisor	0.80	?	?	?
Machining Operator	0.75	?	?	?
Health Physics Technician	0.92	?	?	?
Operations Support	0.35	?	?	?
Maintenance Manager	0.80	?	?	?
Maintenance Personnel	0.65	?	?	?

Learning Objectives

- Understand the benefits of using Risk a metric of MPC&A System effectiveness
- Identify how to estimate Risk using two different approaches

Questions???