National Nuclear Security Administration

SAND2007-6887P

Determining Effective Upgrades

Insider Protection Course

Learning Objectives

- Identify how to prioritize security system upgrades
- Recognize the role of scenario development in identifying system upgrades
- Identify methods to present potential upgrades

Upgrade Process

- Establish risk criteria
  - Prioritize based on risk
  - Determine acceptability of risk levels
- Begin by developing upgrade options for scenarios with:
  - Highest consequences and
  - Lowest system effectiveness

  } Highest Risk
- Evaluate other scenario and consequence combinations as deemed necessary
- Develop multiple upgrade options considering the effect on the total system
  - Not only on the scenarios of most concern
- Consider Cost

Prioritize Scenarios by Risk

Threat/Target	Scenario	Risk
HP Technician Product Vault	Protracted Theft - Diverts material to waste stream, allows material shipment from MAA, recovers from sanitary waste	0.92
HP Technician Chip Vault	Protracted Theft - Diverts material to waste stream, allows material shipment from MAA, recovers from sanitary waste	0.85
Machining Operator Machining Area	Protracted Theft - Takes small amount of scrap while working, shields in lunchbox	0.85
…		

When do you stop upgrading?

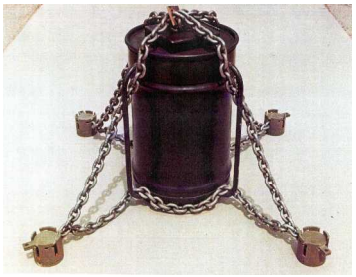
Threat/Target	Scenario	Risk
HP Technician/Product Vault	Scenario 1	0.92
HP Technician/Chip Vault	Scenario 2	0.85
Machining Operator/Machining Area	Scenario 3	0.85
Maintenance/Machining Area	Scenario 4	0.80
Shift Supervisor/Machining Area	Scenario 5	0.80
Plant Manager/Machining Area	Scenario 6	0.65
HP Technician/Machining Area	Scenario 7	0.65
Material Handler/Chip Vault	Scenario 8	0.60
…		
QA Manager/X-ray facility	Scenario m	0.45
…		
Measurement Team/Machining Area	Scenario n	0.18

Where do you move from **unacceptable risk** to **acceptable risk**

This is normally established at a policy level

Developing Upgrade Options

- **Systematically review the scenarios for operational or security changes that provide:**
  - **Earlier and better detection possibilities**
    - **Administrative controls**
    - **Technology**
  - **Increased delays at detection location**
  - **Improved operational and security response possibilities**
  - **Denial of capability, opportunity, tools, etc.**



Look at methods or strategies used

Threat/Scenarios	Methods/Strategies used		
	Step 1	Step 2	Step n
HP Tech Scenario 1	Diverts material to waste stream	allows material shipment from MAA	…
HP Tech Scenario 2	Diverts material to waste stream	allows material shipment from MAA	…
…			

- Look for common methods
  - Are they only used by one Insider group?
  - Do multiple groups use the same methods?
  - Do multiple scenarios utilize the same methods?

Considerations in Formulating Upgrade Options

- Strive for upgrades that affect many scenarios
- Be careful not to introduce upgrades for one scenario that have a negative effect on other scenarios
- Identify if there are unacceptable operational and/or safety impacts
- Document improvement options including rationale for selection
- Review the MPC&A, operational, and safety aspects associated with the scenarios
  - Can something be changed in the operational or safety systems to make scenarios less likely to succeed?

Upgrade Considerations

- Operational
  - Set operational limits on quantities in process
  - Set operational limits on materials outside of storage
- Detection
  - Enhance two-person controls
  - Provide duress alarms
- Delay
  - Compensatory measures when delay systems or material controls are not in place (e.g. material is accessed)
- Response
  - Reduce response force deployment time

System Considerations

- **Strive for System Balance**
- **Try to achieve Protection-in-Depth**

Re-evaluate Protection System Effectiveness

- Develop each of the upgrade options in enough detail to re-analyze the system effectiveness
- Go through the effectiveness evaluation again with the improvements
- Prepare a chart showing the changes in risk with the options
  - One chart for each upgrade option or combination of upgrade options

Example Risk Summary Chart

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

Example Risk Summary Chart (Baseline vs. Upgrade)

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

Bunker Example 1: Analysis for Upgrades

- Review the baseline system effectiveness
  - Use the path event timeline
- Discuss methods of improving the system
- Select one or more approaches based on expert judgment
- Re-analyze to determine the improvement in MPC&A system effectiveness with the upgrades

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

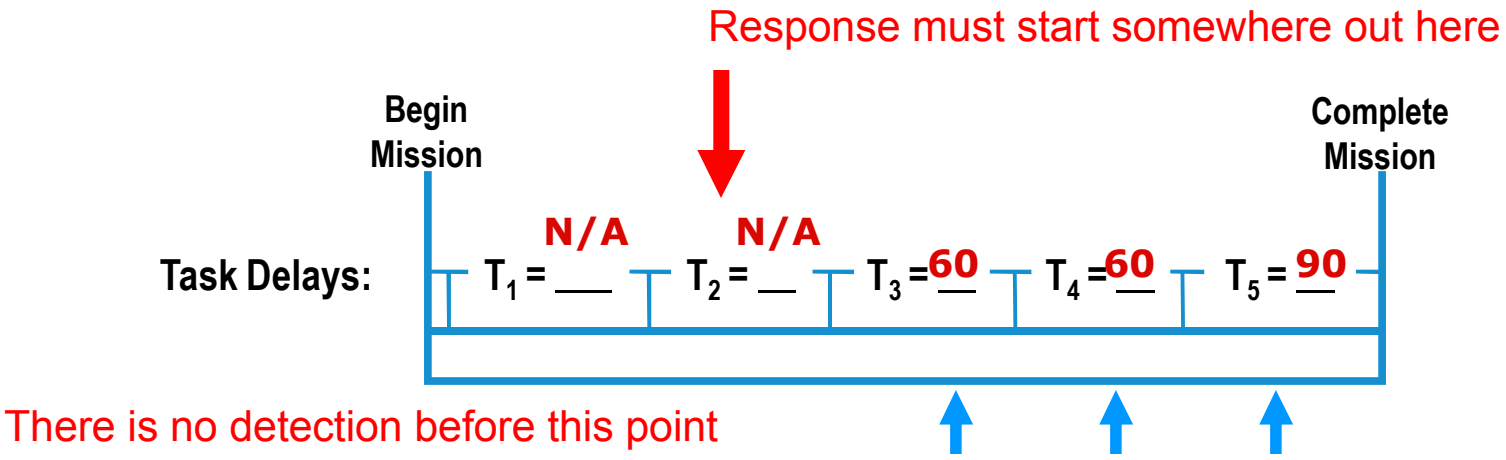
Example 1: Response Time

Example response time table for an adjacent co-worker/ guards – theft from the bunker, HP Tech

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

Example 1: Path Event Timeline

If Response Force Time is 380 (worst-case) – P_I = Zero



How could we improve this situation? Detection? Delay? Response?

Example 1 Upgrade: Posted Guard outside the Bunker

Possible change in detection and perhaps some delay for adding the guard, but BIG change in Response Time

Step	Action	Likelihood of Detection	Delay (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~~ High	90

Example 1 Upgrade: Response Time with Posted Guard outside the Bunker

Response Action	Time taken (seconds) Min	Max
Co-worker identifies malevolent action – Sees material removal – hits the panic button	0	60
Communicate to guards - siren and flashing light on bunker headwall alert posted guard	~~60~~ 0	~~180~~ 0
Guard communication time	~~30~~ 0	
Response prep time	~~50~~ 0	
Travel	~~0 to ECPs~~ 0	~~30 to Bunker~~ 0
Intervene	0	~~60~~ 0
Total	~~140~~ 0	~~360~~ 60

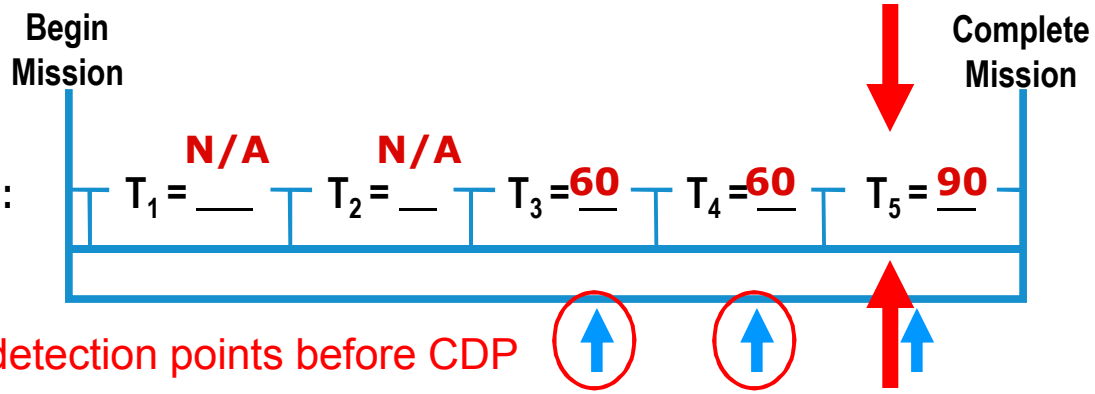
Significant change in response time and communication time assuming the guard is the response

Example 1 Upgrade: Timeline with Posted Guard outside the Bunker

Response Force Time is now 60 sec in the worst-case

P_I = (H+H) = VH

Response must start by this point



There are now 2 detection points before CDP

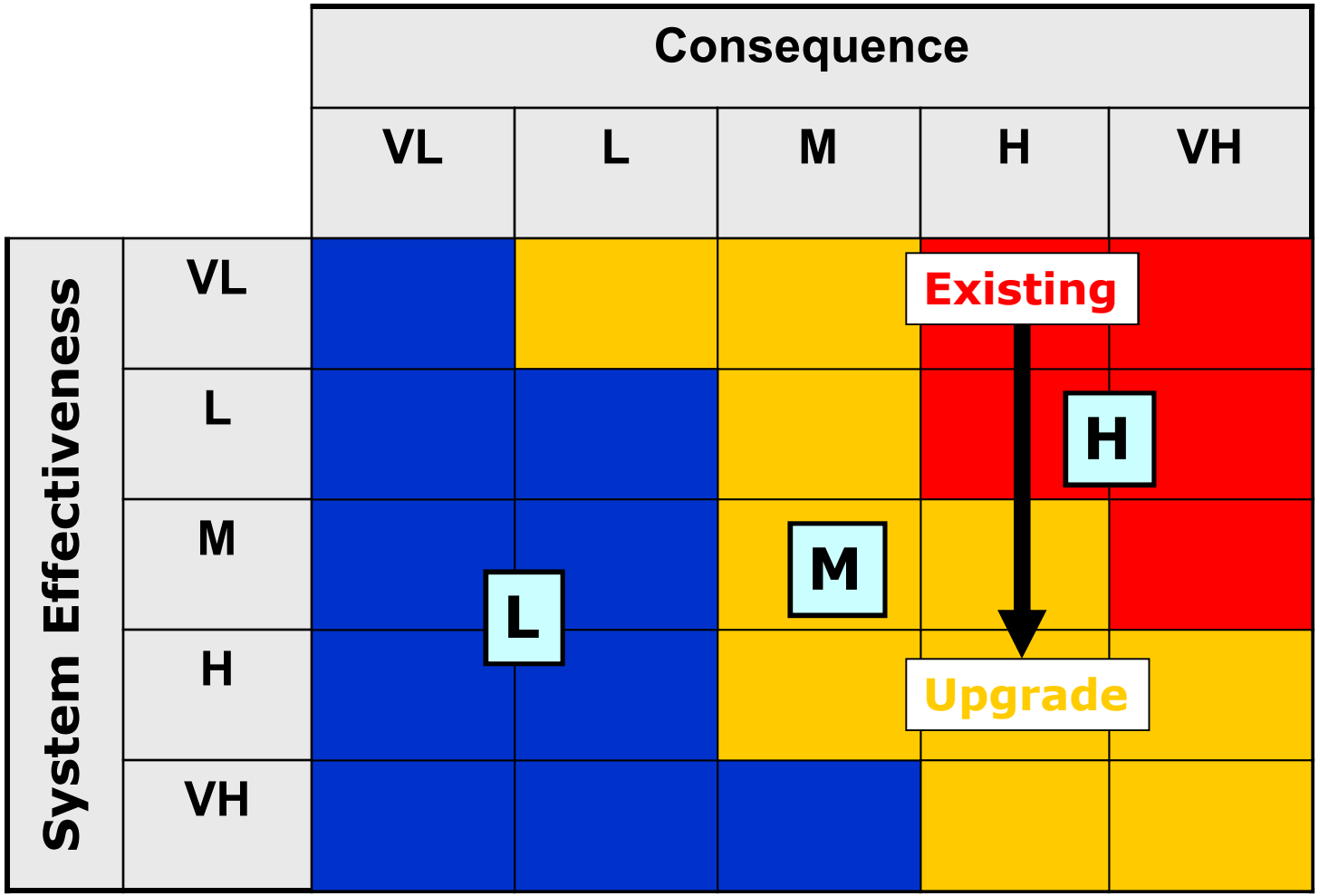
P_D:	P_1 = ___	P_2 = _	P_3 = H	P_4 = H	P_5 = H
Time Remaining:	TR_1 = ___	TR_2 = ___	TR_3 = 180	TR_4 = 120	TR_5 = 45
Timely Detection?	___	___	Yes ~~NO~~	Yes	No

Example MPC&A System Effectiveness Summary Chart

Threat Group	Bunker C = H	X-ray Facility C = H	Chip Vault C = H	Machining area C = H
Plant Manager	*Zero → H*			
Shift Supervisor	*Zero → H*			
Machining Operator	*Zero → H*			
Health Physics Technician	*Zero → H*			
Operations Support	*Zero → H*			
Maintenance Manager	*Zero → H*			
Maintenance Personnel	*Zero → H*			

Example Risk Criterion

RED is HIGH RISK, ORANGE MEDIUM and BLUE LOW



Example Numerical Risk Criterion

System Effectiveness	Consequence				
	VL	L	M	H	VH
VL	15	10	6	3	1
L	19	14	9	4	2
M	22	18	13	7	5
H	24	21	17	11	8
VH	25	23	20	16	12

1 is highest priority, 2 next highest and so on

Example Risk Summary Chart for Posted Guard Upgrade

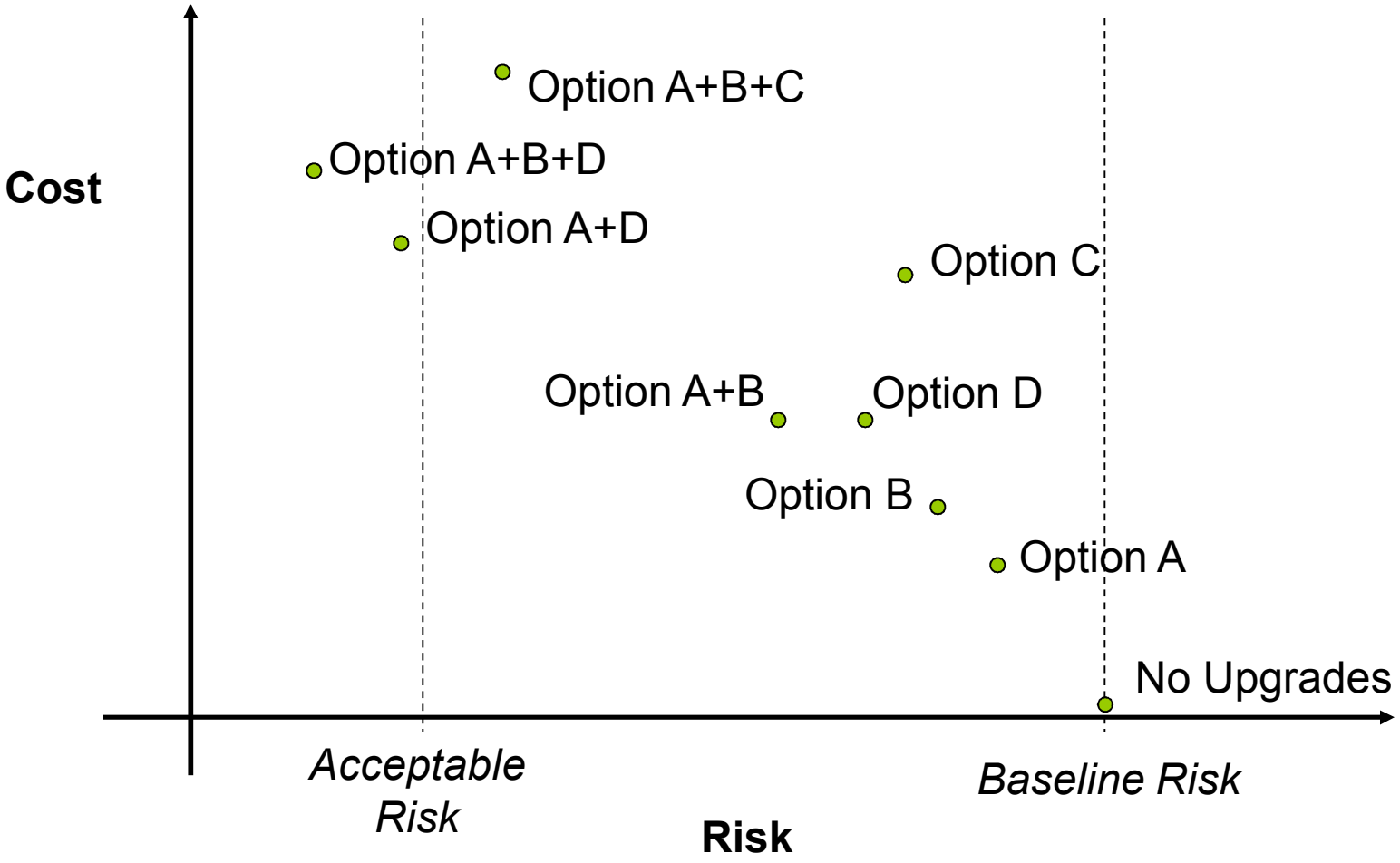
Threat Group	Target			
	Bunker	X-ray Facility	Chip Vault	Machining area
Plant Manager	*H* → *M*			
Shift Supervisor	*H* → *M*			
Machining Operator	*H* → *M*			
Health Physics Technician	*H* → *M*			
Operations Support	*H* → *M*			
Maintenance Manager	*H* → *M*			
Maintenance Personnel	*H* → *M*			

This particular Upgrade might not apply to other targets or other scenarios

Cost Effective Upgrades

- Identify cost constraints
- Develop Upgrade Options
  - Single upgrades
  - Upgrades packages
- Identify life-cycle costs for upgrade options
  - Separate maintenance and operating costs
  - Include safety costs as well

Example Cost Benefit Chart for Upgrade Options



Learning Objectives

- Identify how to prioritize security system upgrades
- Recognize the role of scenario development in identifying system upgrades
- Identify methods to present potential upgrades

Questions or Comments??

Subgroup Exercise 7: Upgrade Analysis

- Review the security system effectiveness and consequences and derive the risk for your specific scenario
- Discuss relevant security and operational options
- Develop an upgrade option for improving the overall system
  - Describe why your team selected that option
- Mark up your original tables to show the changes in P_E and risk for this option
- Present your option to the group with a brief discussion of the other alternatives considered