SAND2013-1826C

Risk-Informed Security Analysis Methodology with Applications to Small Modular Reactors

Christopher Hadlock
Operations Research and Industrial Engineering
The University of Texas at Austin
February 22, 2013

Team Members

Eric Bickel (Asst. Prof., Operations Research)

David Morton (Prof., Operations Research)

Erich Schneider (Assoc. Prof., Nuclear & Radiation Engineering)

Bonnie Canion (MS Student, nuclear)

This work was performed for Sandia National Laboratories, a multi-program laboratory **managed and operated** by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin **Corporation**, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Project Goals

- Develop a game-theoretic model to use as a guideline for decision making of security upgrades to an SMR.
- Perform a cost-benefit analysis of security upgrades based on applied game theoretic model.
- Perform a sensitivity analysis of consequences with respect to probability of adversary type: 1.) an adversary who just needs to reach his target; 2.) an adversary who needs to both reach his target and escape the facility.

Why Game Theory?

- How is the system operated?
- What are the vulnerabilities of the system?
- How can we improve the system's security?

When our system is complex, subtle relationships among system components suggest we should form an "operational model" for the adversary, encoding the adversary's many possible strategies.

Game theory allows us to characterize the damage an adversary, with given capabilities, is capable of inflicting on our system. An important step involves distinguishing the adversary's capabilities and intentions, when formulating the model.

Sometimes observing vulnerabilities suffices to harden the system. Or, we can build an optimization model to optimally harden system defense.

Game Theory in Nuclear Security and Infrastructure Protection

- Optimizing inspection strategies of nuclear material – Gauker et al., Wein et al., Boros et al., Madigan et al., McLay et al., Stroud et al.

- Securing a large-scale network by attempting to thwart an adversary via optimal allocation of detection monitors. Lit. consists of Stackelberg, Cournot, and hybrid models – Atkinson, Dimitrov, Morton, Nehme, Pan, et al.

- Modeling an optimal attack to an electric power system so as to assess system vulnerabilities – Salmeron et al.

- Hardening infrastructure via optimal allocation of detectors within a network-flow-type system – Berry; Murray; Watson (municipal water supply); Paruchuri (airport security); Alderon (municipal transportation networks); Brown (U.S. Strategic Petroleum Reserve)

Why Game Theory?

- PRA attempts to assign probabilities to possible forms of system damage (be it natural/non-deliberate OR adversarial/deliberate).

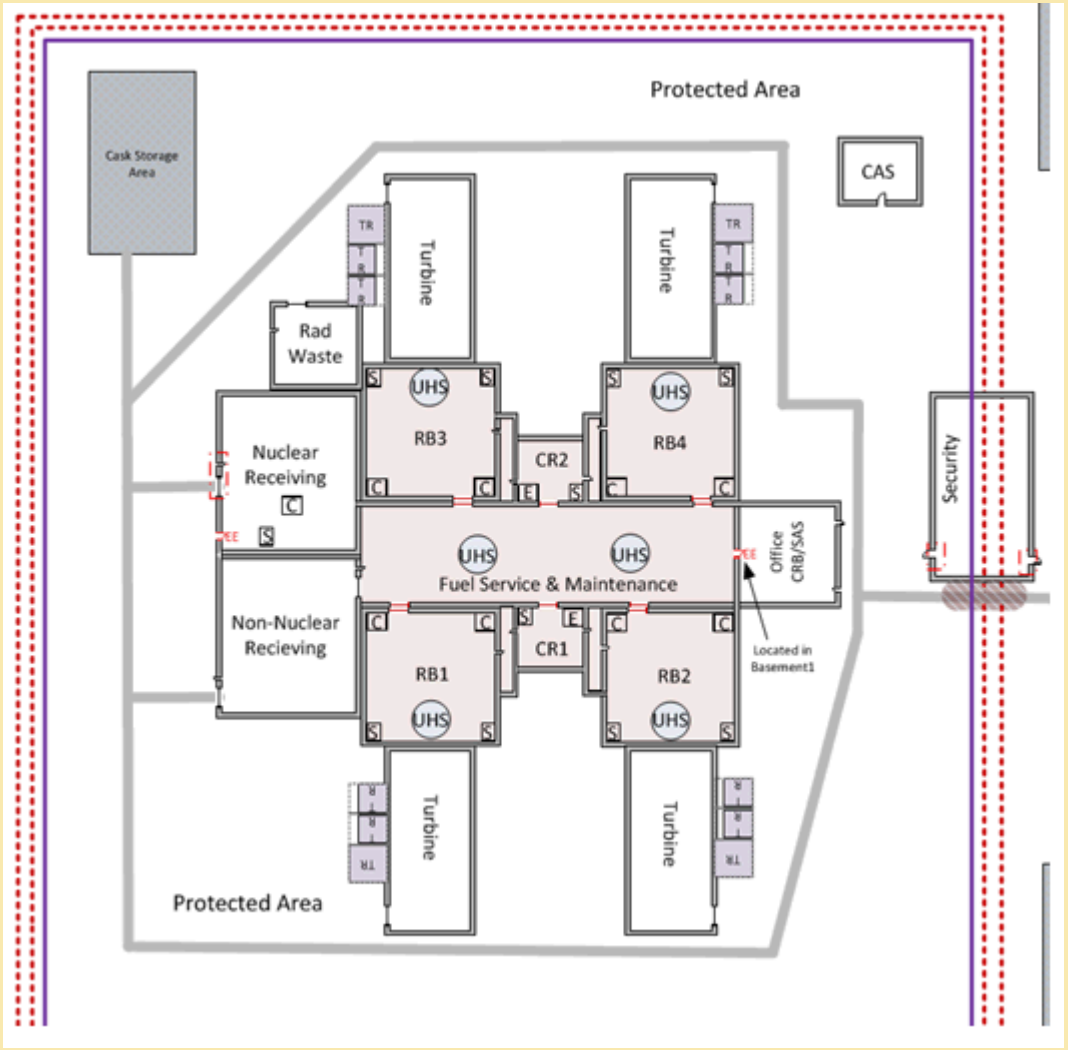
- However, in regard to security, sources suggest that PRA is better suited to non-deliberate threats where these probabilities are well suited to problem inputs. Since adversaries tend to deliberately optimize their objectives, game-theory suggests that the probabilities of specific attack strategies are outputs of the optimization model (NRC, Brown, Cox).

Sequential Play Game

Sequential play (Stackelberg) is appropriate if:

- the defender deploys fixed security measures:
  - passive monitoring systems (cameras, explosives detectors),
  - physical protection installations (gates, door alarms),
  - regular or scheduled events (response times);
- and the adversary has information, knowing
  - what measures are deployed (from blueprints, intelligence, inside information),
  - how they will perform (i.e. detection probabilities);
- and the adversary acts rationally, choosing the best option available.

Generic SMR Plant and Targets



Example of four potential targets:

1) access **radwaste storage** building (small release of radiation);

2) access **spent fuel storage** pool (large release);

3) Sabotage multiple locations within reactor building (**core damage**).

4.) Structural damage to the Protected Area

Defender's valuations of target consequence:

- As the defender, we must assign relative values to an attack of each specific target.

- Defender's valuations of target consequence:

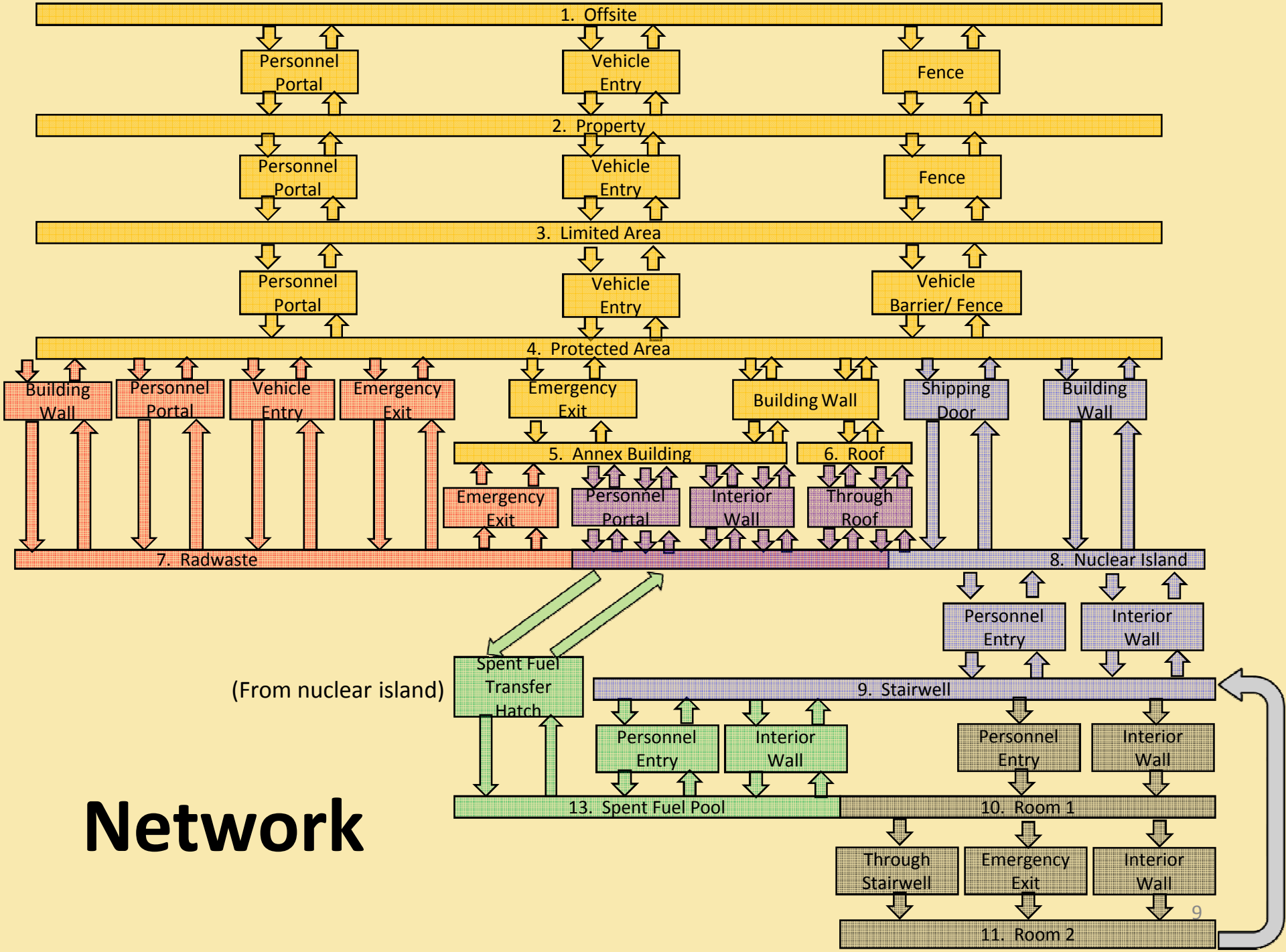
Structural Damage = 1

Radwaste storage = 2

Spent fuel pool = 40

Core damage = 750

This data was constructed for use in student exercises for vulnerability analyst training. This data is not appropriate for use in actual security analyses.


1. Offsite
Personnel Portal
Vehicle Entry
Fence
2. Property
Personnel Portal
Vehicle Entry
Fence
3. Limited Area
Personnel Portal
Vehicle Entry
Vehicle Barrier/ Fence
4. Protected Area
Building Wall
Personnel Portal
Vehicle Entry
Emergency Exit
Emergency Exit
Building Wall
Shipping Door
Building Wall
5. Annex Building
6. Roof
Emergency Exit
Personnel Portal
Interior Wall
Through Roof
7. Radwaste
8. Nuclear Island
Personnel Entry
Interior Wall
(From nuclear island)
Spent Fuel Transfer Hatch
9. Stairwell
Personnel Entry
Interior Wall
Personnel Entry
Interior Wall
13. Spent Fuel Pool
10. Room 1
Through Stairwell
Emergency Exit
Interior Wall
11. Room 2

Network

Security Measures: **Baseline** and **Upgrades**

- A **baseline** set of security measures is in place
  - one or more measures apply on each arc
  - from these, each arc is assigned a baseline **non-detection probability** and **travel time**

- Then the defender is given a **budget** and set of **security upgrades** to choose from
  - each upgrade has a **cost** and might affect the **non-detection probability** and **travel time** on one or more arcs, or it might reduce the **response time** of the security force.

Example: Arc Non-Detection Probabilities

Path	Path Description	Fences/ Walls	Emergency Exit	Personnel Portal	Stationed guards	Random Searches	Non Guard Personnel	Roaming Guards	Alarmed Detection Device	Video Surveillance	Two person Rule	Non-Detection Probability
8 → 9	Personnel Portal			1.00	2.00	1.00	1.00	1.00		1.00	1.00	
				0.56	0.95	0.74	0.97	0.84		0.97	0.91	0.27
8 → 9	Interior Wall	1.00					1.00	1.00		2.00		
		0.56					0.97	0.84		0.67 & 0.80		0.24
9 → 10	Personnel Portal			1.00			1.00	1.00		1.00	1.00	
				0.56			0.97	0.84		0.97	0.91	0.41
9 → 10	Interior Wall	1.00					1.00	1.00		2.00		
		0.56					0.97	0.84		0.67		0.21
10 → 11	Personnel Portal			1.00			1.00	1.00		1.00	1.00	
				0.56			0.97	0.84		0.97	0.91	0.41
10 → 11	Emergency Exit		1.00				1.00	1.00	1.00	2.00		
			0.67				0.97	0.84	0.74	0.67		0.18
10 → 11	Interior Wall	1.00					1.00	1.00		2.00		
		0.56					0.97	0.84		0.67		0.21
8 → 13	Spent Fuel Transfer	1.00					1.00	1.00		1.00		
		0.56					0.97	0.84		0.80		0.37
9 → 13	Personnel Portal			1.00			1.00	1.00		1.00	1.00	
				0.56			0.97	0.84		0.97	0.91	0.41
9 → 13	Interior Wall	1.00					1.00	1.00		2.00		
		0.56					0.97	0.84		0.67		0.21

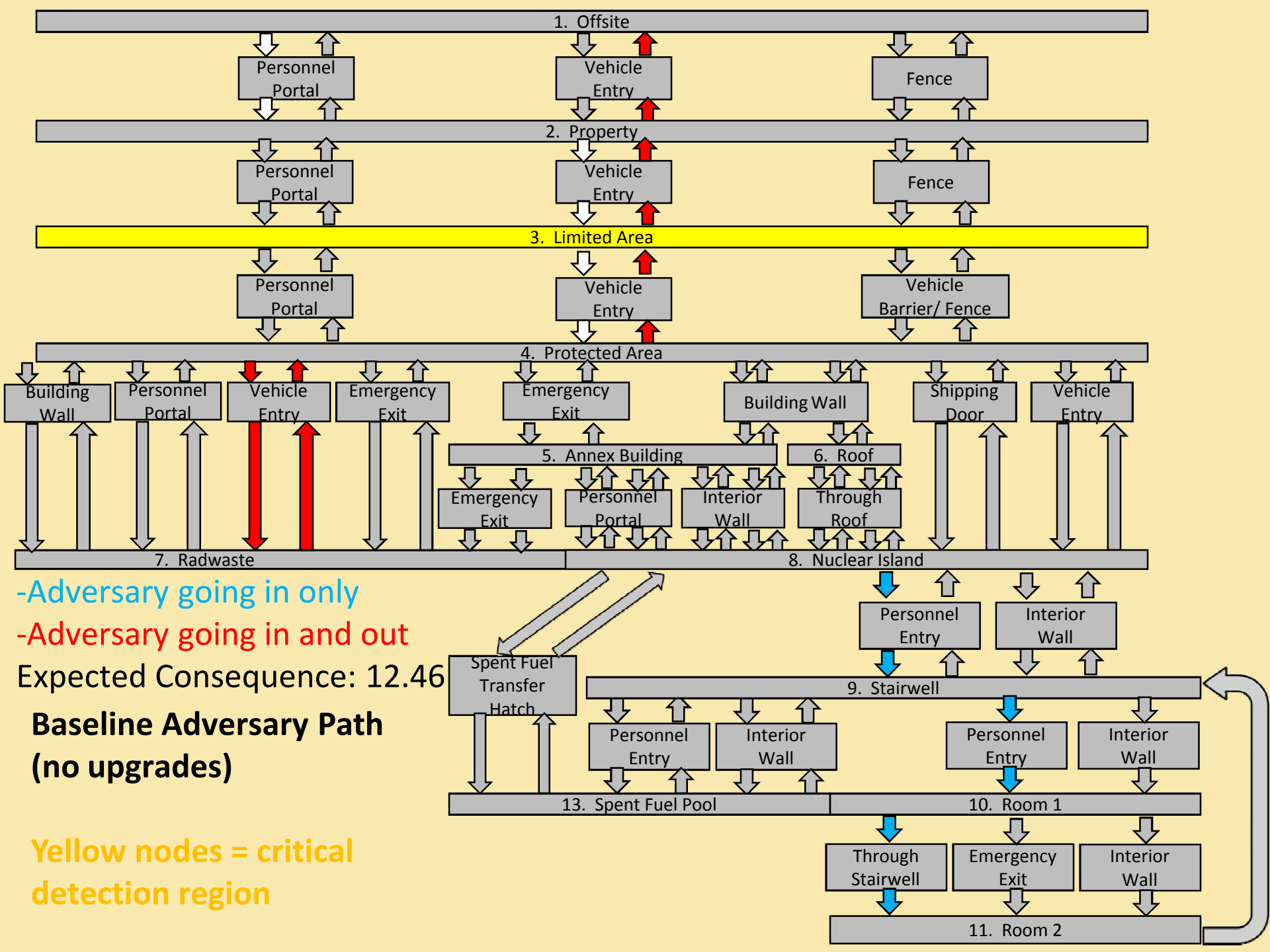
This data was constructed for use in student exercises for vulnerability analyst training. This data is not appropriate for use in actual security analyses.

Overview of Arc Travel Times (Non lockdown state)

Path		Travel Time	Obstacle Time	TOTAL
1 → 2	Pers Port	300	5 X 1	305
	Veh Ent	30	5 X 1	35
	Fence	300	30 X 1	330
2 → 3	Pers Port	54	5 X 1	59
	Veh Ent	15	5 X 1	35
	Fence	54	30 X 1	84
3 → 4	Pers Port	54	5 X 1	59
	Veh Ent	15	5 X 1	20
	Fence	54	30 X 2	114
4 → 5	Pers Port	10	5 X 1	15
	Em Exit	10	60/5 X 1	70/15
	Thru Wall	10	180 X 1	190
4 → 6	Up Wall	0	120/90 X 1	120/90
4 → 7	Pers Port	10	5 X 1	15
	Em Exit	10	60/5 X 1	70/15
	Veh Ent	10	5 X 1	15
	Thru Wall	10	180 X 1	190
4 → 8	Pers Port	10	5 X 1	70/15
	Veh Ent	10	5 X 1	15
	Thru Wall	10	180 X 1	190

Path		Travel Time	Obstacle Time	TOTAL
5 → 7	Pers Port	10	5 X 1	15
	Thru Wall	10	180 X 1	190
5 → 8	Pers Port	10	5 X 1	15
	Thru Wall	10	180 X 1	190
6 → 7	Thru Roof	0	180 X 1	180
6 → 8	Thru Roof	0	180 X 1	180
8 → 9	Pers Port	10	5 X 1	15
	Thru Wall	10	300 X 1	310
9 → 10	Pers Port	10	5 X 1	15
	Em Exit	10	90/5 X 1	100/15
	Thru Wall	10	300 X 1	310
10 → 11	Pers Port	20	5 X 2	30
	Em Exit	10	90/5 X 1	100/15
	Thru Wall	10	300 X 1	310
8 → 13	SF Hatch	10	500 X 1	510
9 → 13	Pers Port	10	5 X 1	15
	Thru Wall	10	300 X 1	310
7, 13	Sabotage	10	50 X 1	60
Core	Sabotage	10	50 X 2	110

This data was constructed for use in student exercises for vulnerability analyst training. This data is not appropriate for use in actual security analyses.


1. Offsite
Personnel Portal
Vehicle Entry
Fence
2. Property
Personnel Portal
Vehicle Entry
Fence
3. Limited Area
Personnel Portal
Vehicle Entry
Vehicle Barrier/ Fence
4. Protected Area
Building Wall
Personnel Portal
Vehicle Entry
Emergency Exit
Emergency Exit
Building Wall
Shipping Door
Vehicle Entry
5. Annex Building
6. Roof
Emergency Exit
Personnel Portal
Interior Wall
Through Roof
7. Radwaste
8. Nuclear Island
-Adversary going in only
-Adversary going in and out
Expected Consequence: 12.46
Baseline Adversary Path (no upgrades)
Yellow nodes = critical detection region
Personnel Entry
Interior Wall
Spent Fuel Transfer Hatch
9. Stairwell
Personnel Entry
Interior Wall
Personnel Entry
Interior Wall
13. Spent Fuel Pool
10. Room 1
Through Stairwell
Emergency Exit
Interior Wall
11. Room 2

Security Upgrades

ID	Description	Cost
A	**Bolster the strength of the security force**, reducing the response time from 120 seconds to 70 seconds.	**$$$**
B	**Provide additional search equipment and stationed guards between the Protected Area and Rad. Waste Storage.**	**$**
C	**Provide increased surveillance and alarms at the Spent Fuel Hatch**.	**$$**
D	**Station additional guards between Offsite and the Protected Area.**	**$$**
E	**Add an additional room to the Vital Area**	**$**
F	**Provide additional search equipment and stationed guards at the Protected Area.**	**$**
G	**Provide additional search equipment and stationed guards at the Vital Area.**	**$**
H	**add an additional set of redundant systems in the vital area, forcing adversary to sabotage more equipment**	**$**

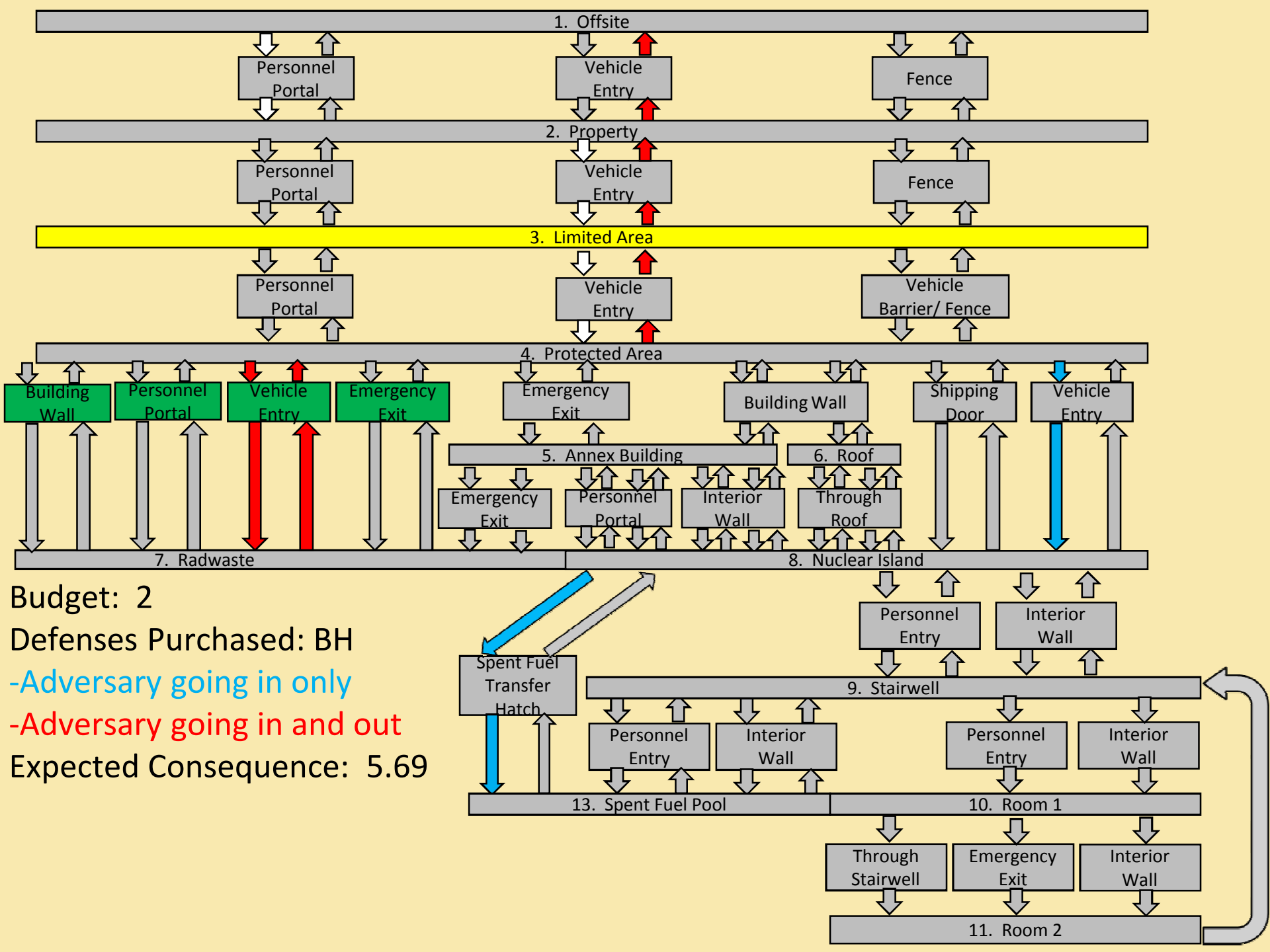
Consequences Versus Scenario Difficulty

- Green markers = zero budget, Blue = all upgrades applied
- The upgrades aim to make all adversary path choices equally ‘bad’.

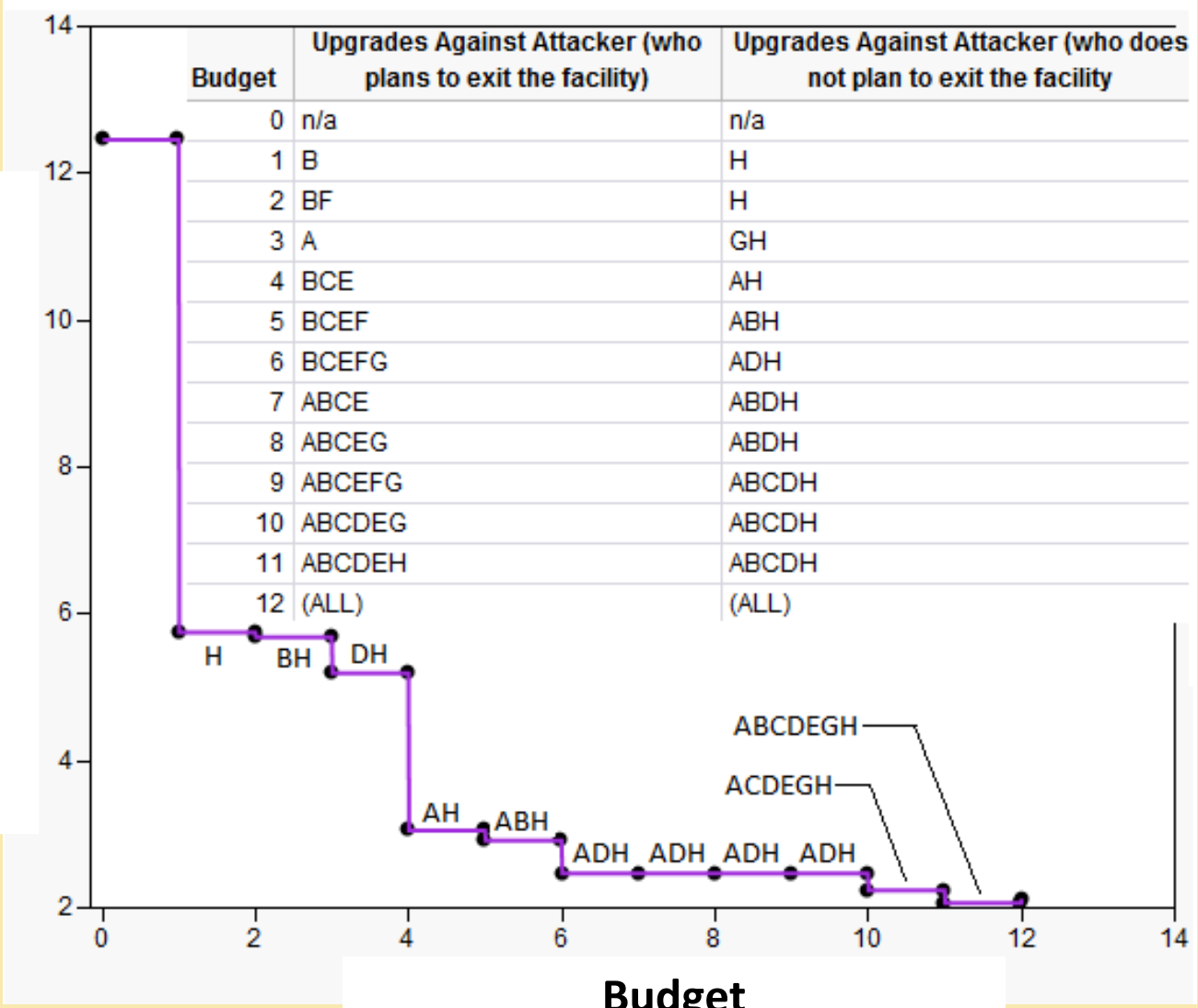
Increase Budget from 0 to 2 Units

- At a **budget of 1**, the defender's optimal strategy is to purchase an additional set of redundant systems in the vital area, forcing adversary to sabotage more equipment (H).

- Given a **budget of 2**, the defender's optimal strategy is to keep "H" implemented, but also to purchase additional search equipment and stationed guards between the Protected Area and Rad. Waste Storage (B).


1. Offsite
Personnel Portal
Vehicle Entry
Fence
2. Property
Personnel Portal
Vehicle Entry
Fence
3. Limited Area
Personnel Portal
Vehicle Entry
Vehicle Barrier/ Fence
4. Protected Area
Building Wall
Personnel Portal
Vehicle Entry
Emergency Exit
Emergency Exit
Building Wall
Shipping Door
Vehicle Entry
5. Annex Building
6. Roof
Emergency Exit
Personnel Portal
Interior Wall
Through Roof
7. Radwaste
8. Nuclear Island
Budget: 2
Defenses Purchased: BH
-Adversary going in only
-Adversary going in and out
Expected Consequence: 5.69
Spent Fuel Transfer Hatch
Personnel Entry
Interior Wall
9. Stairwell
Personnel Entry
Interior Wall
Personnel Entry
Interior Wall
13. Spent Fuel Pool
10. Room 1
Through Stairwell
Emergency Exit
Interior Wall
11. Room 2

Efficient Frontier:
Expected Consequence versus **Budget**



Budget	Upgrades Against Attacker (who plans to exit the facility)	Upgrades Against Attacker (who does not plan to exit the facility
0	n/a	n/a
1	B	H
2	BF	H
3	A	GH
4	BCE	AH
5	BCEF	ABH
6	BCEFG	ADH
7	ABCE	ABDH
8	ABCEG	ABDH
9	ABCEFG	ABCDH
10	ABCDEG	ABCDH
11	ABCDEH	ABCDH
12	(ALL)	(ALL)

This data was constructed for use in student exercises for vulnerability analyst training. This data is not appropriate for use in actual security analyses.

Conclusions / Next Steps

- Perform a sensitivity analysis providing “expected damage” dependence upon probability of adversary type.
- Incorporate non-unitary defeat probability
- Model the presence of both an onsite and offsite security force in conjunction with non-unitary defeat probabilities
- Additional targets and security measures