Security Risk Assessment and Mitigation Prioritization

Stephanie King, PhD, PE

Weidlinger Associates, Inc.

FFC Committee on Physical Security and Hazard Mitigation

July 15, 2008

Outline

- *Introduction*
- *Security Risk Assessment*
  - *Key elements and terminology*
  - *Basic methods (screening)*
  - *Critical issues*
- *Mitigation Prioritization*
  - *Quantified benefit-cost analysis*
  - *Critical issues*
- *Examples*

Introduction

- ***Limited resources + competing priorities***
  - ***Where are the risks?***
  - ***Which risks are acceptable?***
  - ***What should be mitigated first?***
  - ***Which mitigation options are best?***
- ***Specific to security***
  - ***Electronic v. Operational v. Hardening?***
  - ***How much protection is enough?***
  - ***"Rational defense against irrational acts"***

Risk Components and Terminology

General Components of Risk Management

Threat Assessment

Vulnerability Assessment

Criticality/ Consequences

	Daily Decision	Gambling	Natural Hazard	Security
Occurrence	Prob. [rain]	Prob. [roll=7]	Prob. [PGA>0.25g]	Likelihood of successful attack w/ weapon X
Vulnerability	Chance of getting wet if rain occurs	Size of loss if 7 is rolled	Chance of bridge closure if PGA>0.25g	Expected building response to weapon X
Importance	Morning activity; cost of suit; health	Time of day; chips in hand; net worth	Toll revenue; traffic flow; regional economy	Occupancy; function of building; contents of building

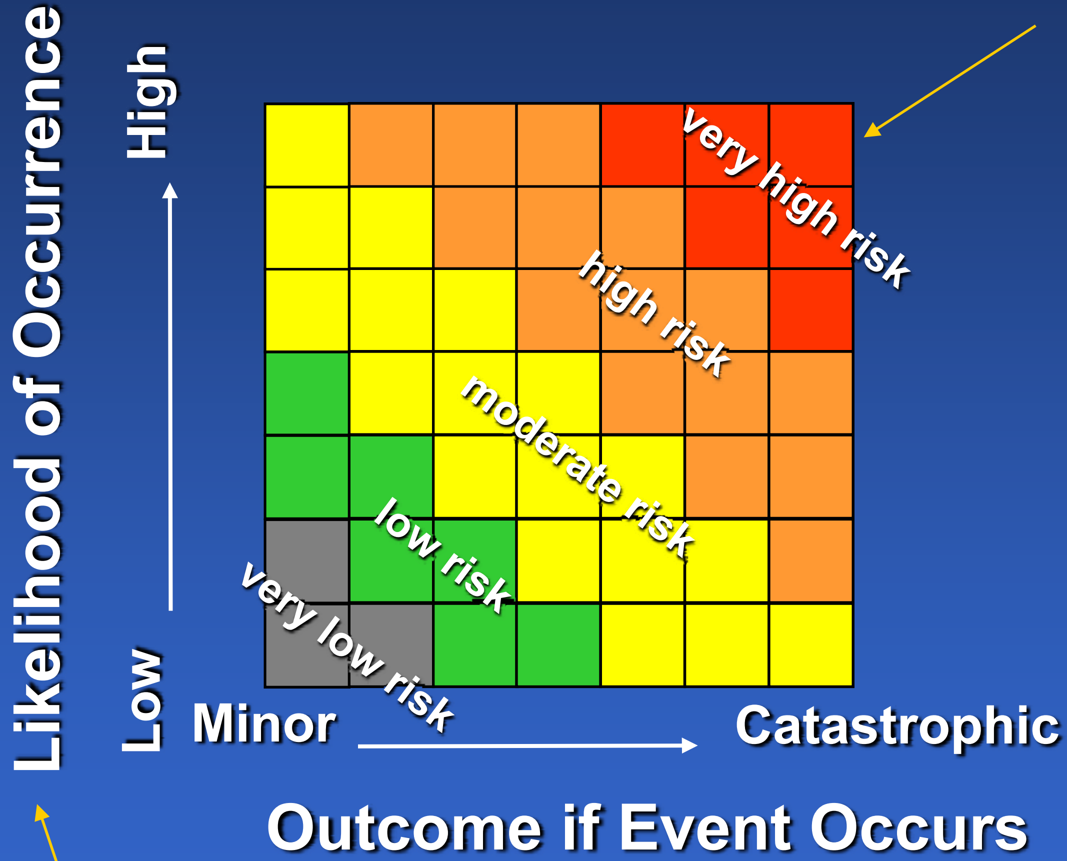
Risk = P[Event] x E[Consequences|Event]

Risk = Vulnerability x Criticality

Risk = Threat x Vulnerability x Consequences

Risk = Occurrence x Vulnerability x Importance

Risk Assessment Methods



Slope of boundaries and definitions depend on risk tolerance

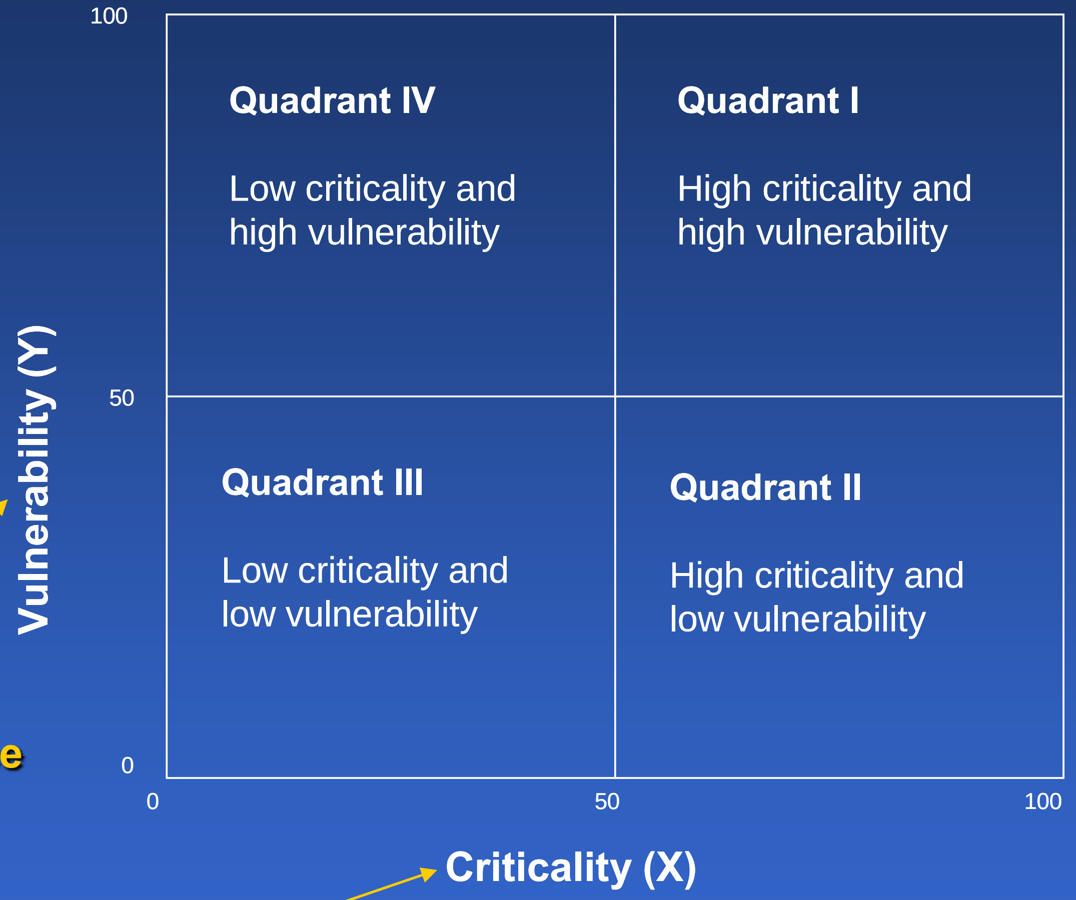
Threat Assessment

Vulnerability Assessment

Criticality or Importance Assessment

Risk Assessment Methods

EXAMPLE:
AASHTO Guide for Bridges & Tunnels (2002)



Vulnerability (Y)

Criticality (X)

Quadrant IV

Low criticality and high vulnerability

Quadrant I

High criticality and high vulnerability

Quadrant III

Low criticality and low vulnerability

Quadrant II

High criticality and low vulnerability

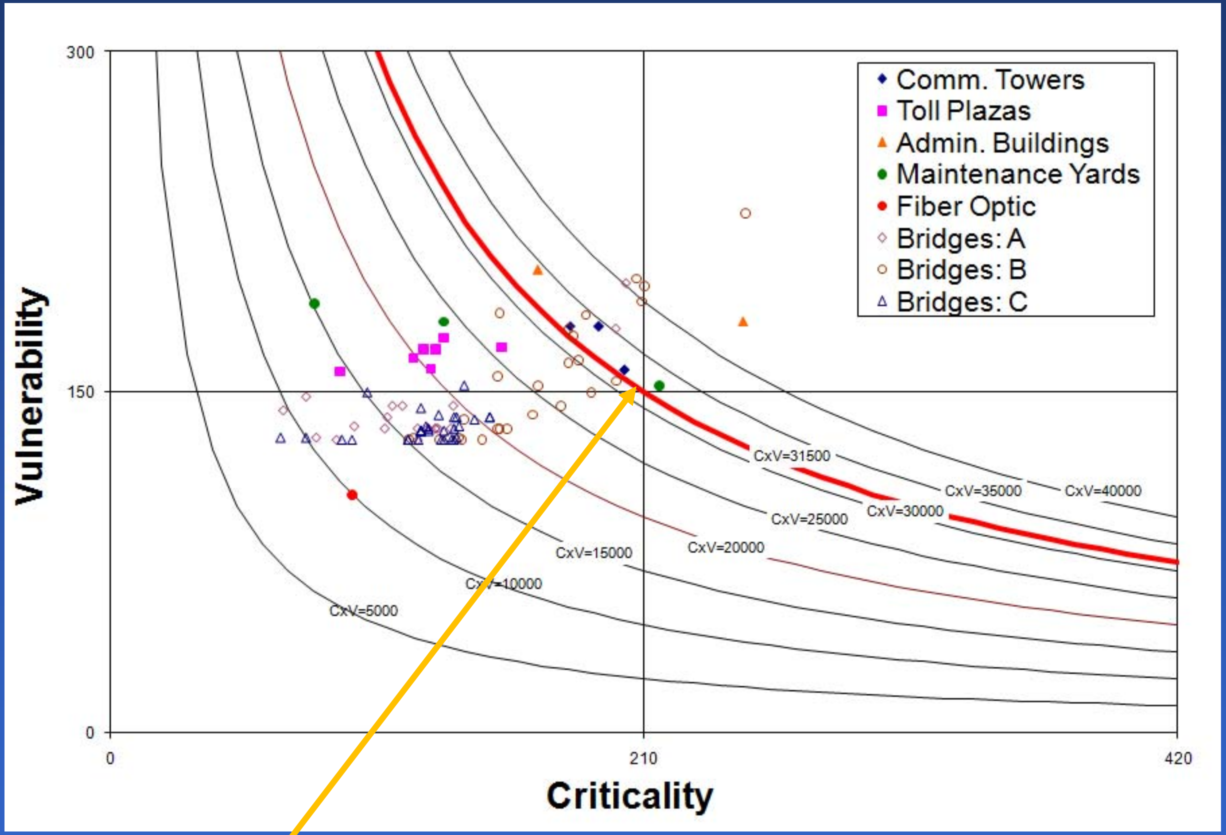
- **Visibility and Attendance**
- **Access to the Asset**
- **Site-specific Hazards**

- **Defer/Defend Factors**
- **Loss and Damage Consequences**
- **Consequences to Public Services**
- **Consequences to the General Public**

Risk Assessment Methods

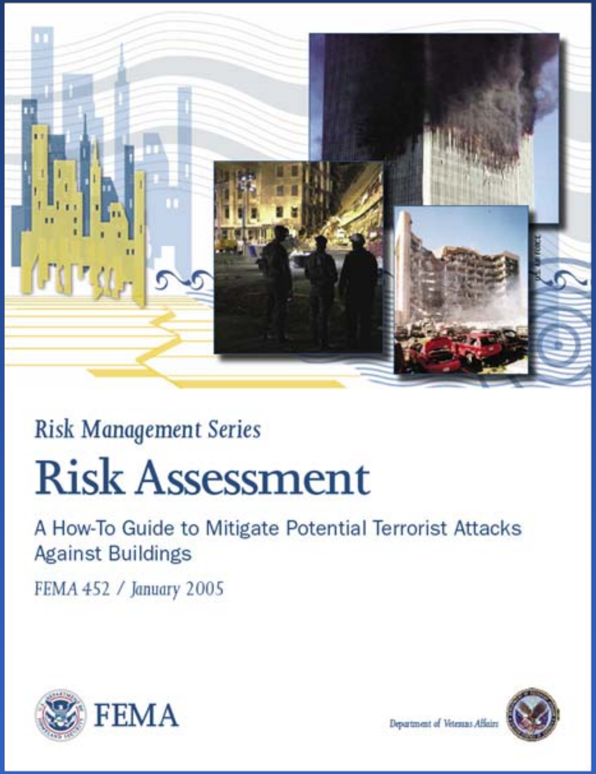
EXAMPLE:

DHS ODP State Homeland Security Assessment and Strategy Program: Special Needs Jurisdiction Tool Kit (2003)



High Risk Threshold

Risk Assessment Methods



Risk Management Series

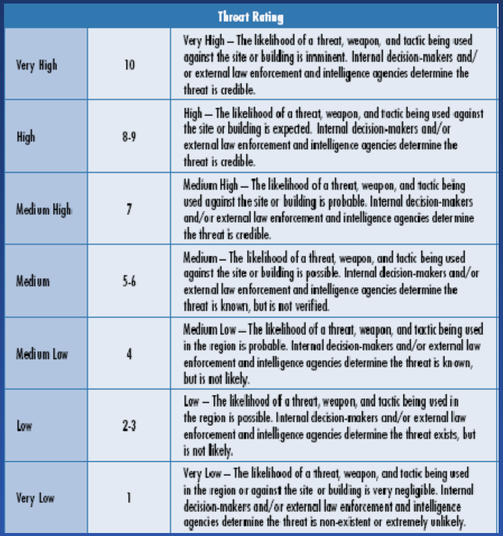
Risk Assessment

A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings

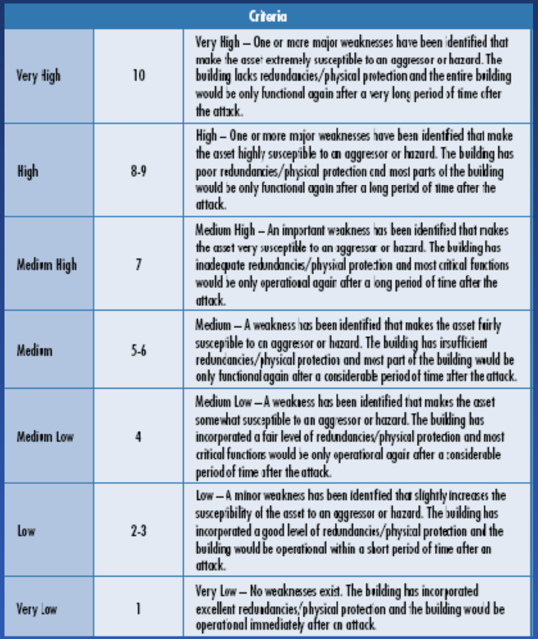
FEMA 452 / January 2005

FEMA

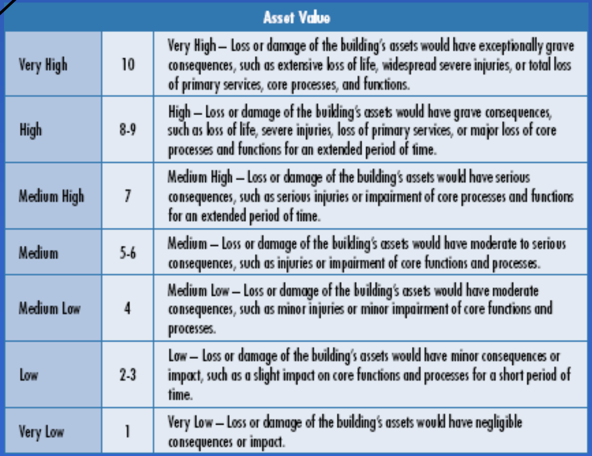
Department of Veterans Affairs



Threat Rating		
Very High	10	Very High – The likelihood of a threat, weapon, and tactic being used against the site or building is imminent. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is credible.
High	8-9	High – The likelihood of a threat, weapon, and tactic being used against the site or building is expected. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is credible.
Medium High	7	Medium High – The likelihood of a threat, weapon, and tactic being used against the site or building is probable. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is credible.
Medium	5-6	Medium – The likelihood of a threat, weapon, and tactic being used against the site or building is possible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is known, but is not verified.
Medium Low	4	Medium Low – The likelihood of a threat, weapon, and tactic being used in the region is probable. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is known, but is not likely.
Low	2-3	Low – The likelihood of a threat, weapon, and tactic being used in the region is possible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat exists, but is not likely.
Very Low	1	Very Low – The likelihood of a threat, weapon, and tactic being used in the region or against the site or building is very negligible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is non-existent or extremely unlikely.



Criteria		
Very High	10	Very High – One or more major weaknesses have been identified that make the asset extremely susceptible to an aggressor or hazard. The building lacks redundancies/physical protection and the entire building would be only functional again after a very long period of time after the attack.
High	8-9	High – One or more major weaknesses have been identified that make the asset highly susceptible to an aggressor or hazard. The building has poor redundancies/physical protection and most parts of the building would be only functional again after a long period of time after the attack.
Medium High	7	Medium High – An important weakness has been identified that makes the asset very susceptible to an aggressor or hazard. The building has inadequate redundancies/physical protection and most critical functions would be only operational again after a long period of time after the attack.
Medium	5-6	Medium – A weakness has been identified that makes the asset fairly susceptible to an aggressor or hazard. The building has insufficient redundancies/physical protection and most part of the building would be only functional again after a considerable period of time after the attack.
Medium Low	4	Medium Low – A weakness has been identified that makes the asset somewhat susceptible to an aggressor or hazard. The building has incorporated a fair level of redundancies/physical protection and most critical functions would be only operational again after a considerable period of time after the attack.
Low	2-3	Low – A minor weakness has been identified that slightly increases the susceptibility of the asset to an aggressor or hazard. The building has incorporated a good level of redundancies/physical protection and the building would be operational within a short period of time after an attack.
Very Low	1	Very Low – No weaknesses exist. The building has incorporated excellent redundancies/physical protection and the building would be operational immediately after an attack.



Asset Value		
Very High	10	Very High – Loss or damage of the building's assets would have exceptionally grave consequences, such as extensive loss of life, widespread severe injuries, or total loss of primary services, core processes, and functions.
High	8-9	High – Loss or damage of the building's assets would have grave consequences, such as loss of life, severe injuries, loss of primary services, or major loss of core processes and functions for an extended period of time.
Medium High	7	Medium High – Loss or damage of the building's assets would have serious consequences, such as serious injuries or impairment of core processes and functions for an extended period of time.
Medium	5-6	Medium – Loss or damage of the building's assets would have moderate to serious consequences, such as injuries or impairment of core functions and processes.
Medium Low	4	Medium Low – Loss or damage of the building's assets would have moderate consequences, such as minor injuries or minor impairment of core functions and processes.
Low	2-3	Low – Loss or damage of the building's assets would have minor consequences or impact, such as a slight impact on core functions and processes for a short period of time.
Very Low	1	Very Low – Loss or damage of the building's assets would have negligible consequences or impact.

Risk = Asset Value x Threat Rating x Vulnerability Rating

Risk Assessment Methods

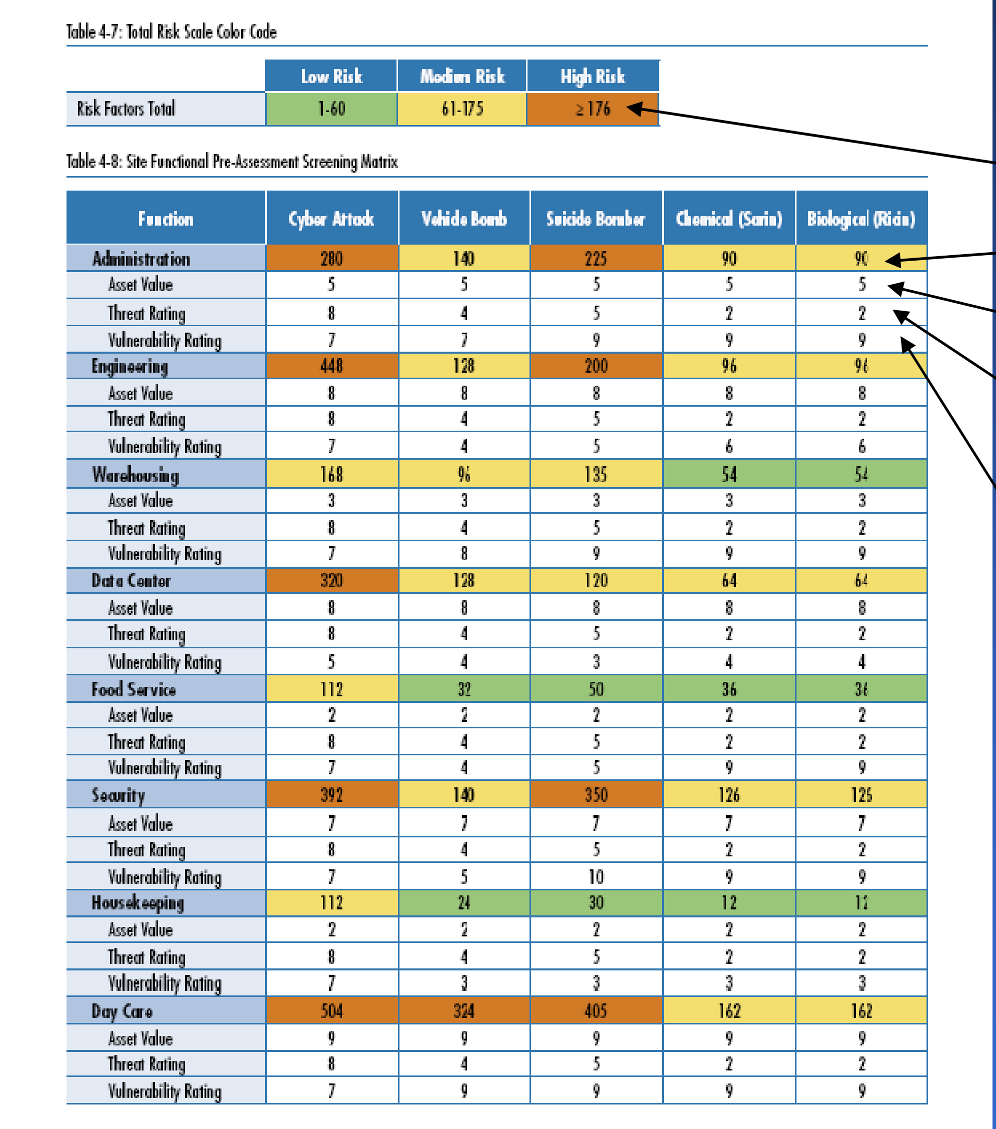


Table 4-7: Total Risk Scale Color Code

	Low Risk	Medium Risk	High Risk
Risk Factors Total	1-60	61-175	≥ 176

Table 4-8: Site Functional Pre-Assessment Screening Matrix

Function	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Administration	280	140	225	90	90
Asset Value	5	5	5	5	5
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	7	9	9	9
Engineering	448	128	200	96	96
Asset Value	8	8	8	8	8
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	4	5	6	6
Warehousing	168	96	135	54	54
Asset Value	3	3	3	3	3
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	8	9	9	9
Data Center	320	128	120	64	64
Asset Value	8	8	8	8	8
Threat Rating	8	4	5	2	2
Vulnerability Rating	5	4	3	4	4
Food Service	112	32	50	36	36
Asset Value	2	2	2	2	2
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	4	5	9	9
Security	392	140	350	126	125
Asset Value	7	7	7	7	7
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	5	10	9	9
Housekeeping	112	24	30	12	12
Asset Value	2	2	2	2	2
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	3	3	3	3
Day Care	504	324	405	162	162
Asset Value	9	9	9	9	9
Threat Rating	8	4	5	2	2
Vulnerability Rating	7	9	9	9	9

Risk

=

Asset Value

X

Threat Rating

X

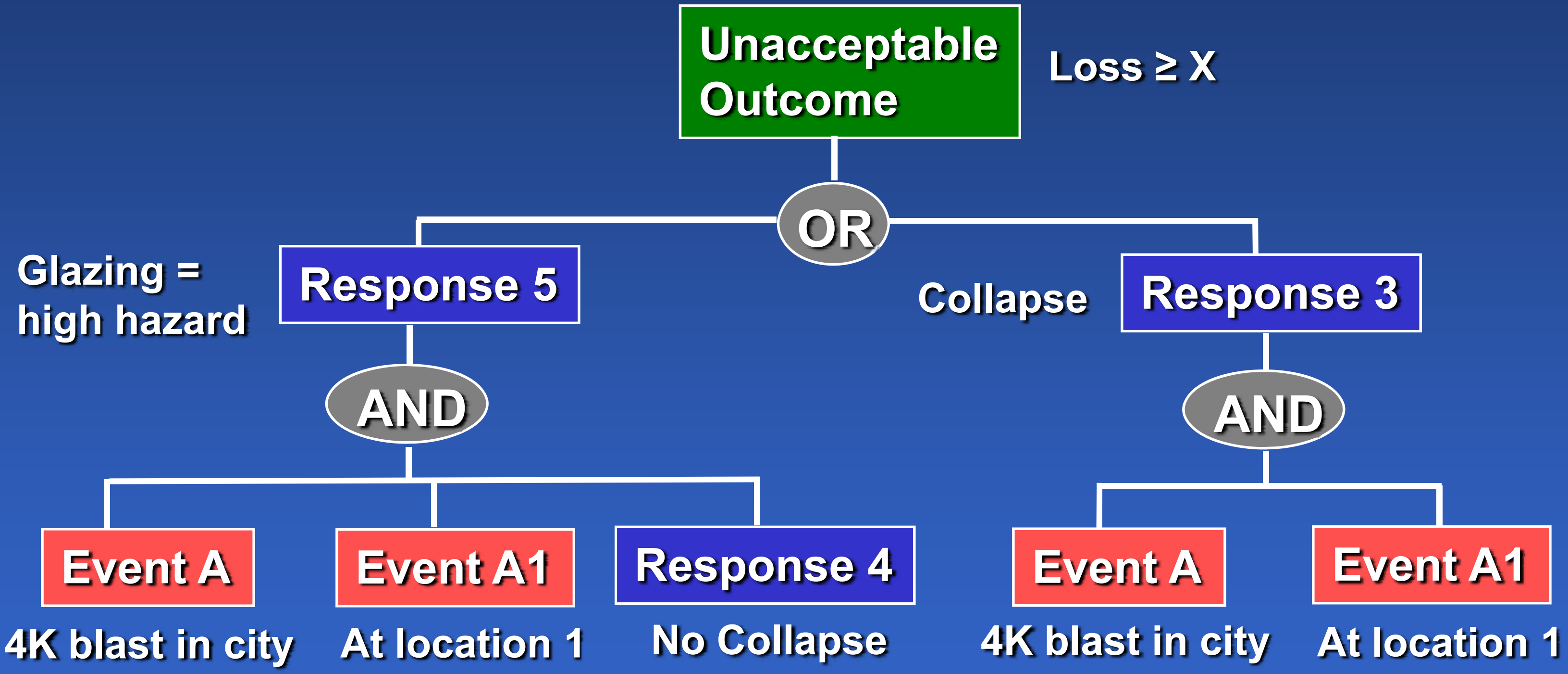
Vulnerability Rating

EXAMPLE:

Results from FEMA 452 (2005)

Risk Assessment Methods

Fault-tree / Consequence-based Assessment



Unacceptable Outcome

Loss ≥ X

OR

Glazing = high hazard

Response 5

AND

Event A

4K blast in city

Event A1

At location 1

Response 4

No Collapse

Collapse

Response 3

AND

Event A

4K blast in city

Event A1

At location 1

Consequence Assessment

Vulnerability Assessment

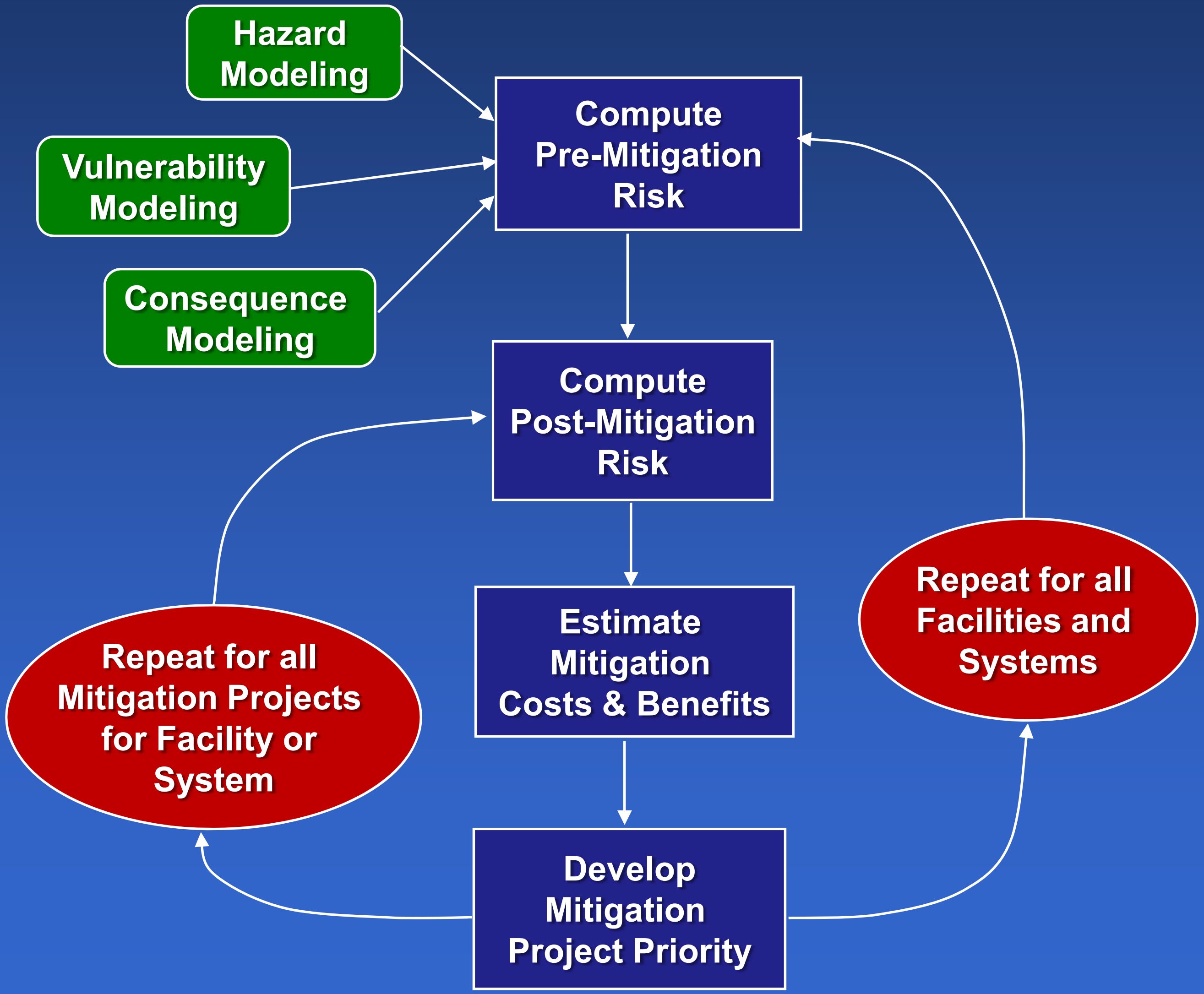
Threat Assessment

Useful for multi-hazard risk assessment

Critical Issues: Assessment

- Definition of Risk Metric
    - Stakeholders input and buy-in
- Subjectivity, Uncertainty, Quantification
    - Transparent, rational, unbiased
    - Consistency among assessors
    - Simplifying assumptions
    - Limitations on results
- Snapshot in Time = Re-Assess

Mitigation Prioritization



Hazard Modeling

Vulnerability Modeling

Consequence Modeling

Compute Pre-Mitigation Risk

Compute Post-Mitigation Risk

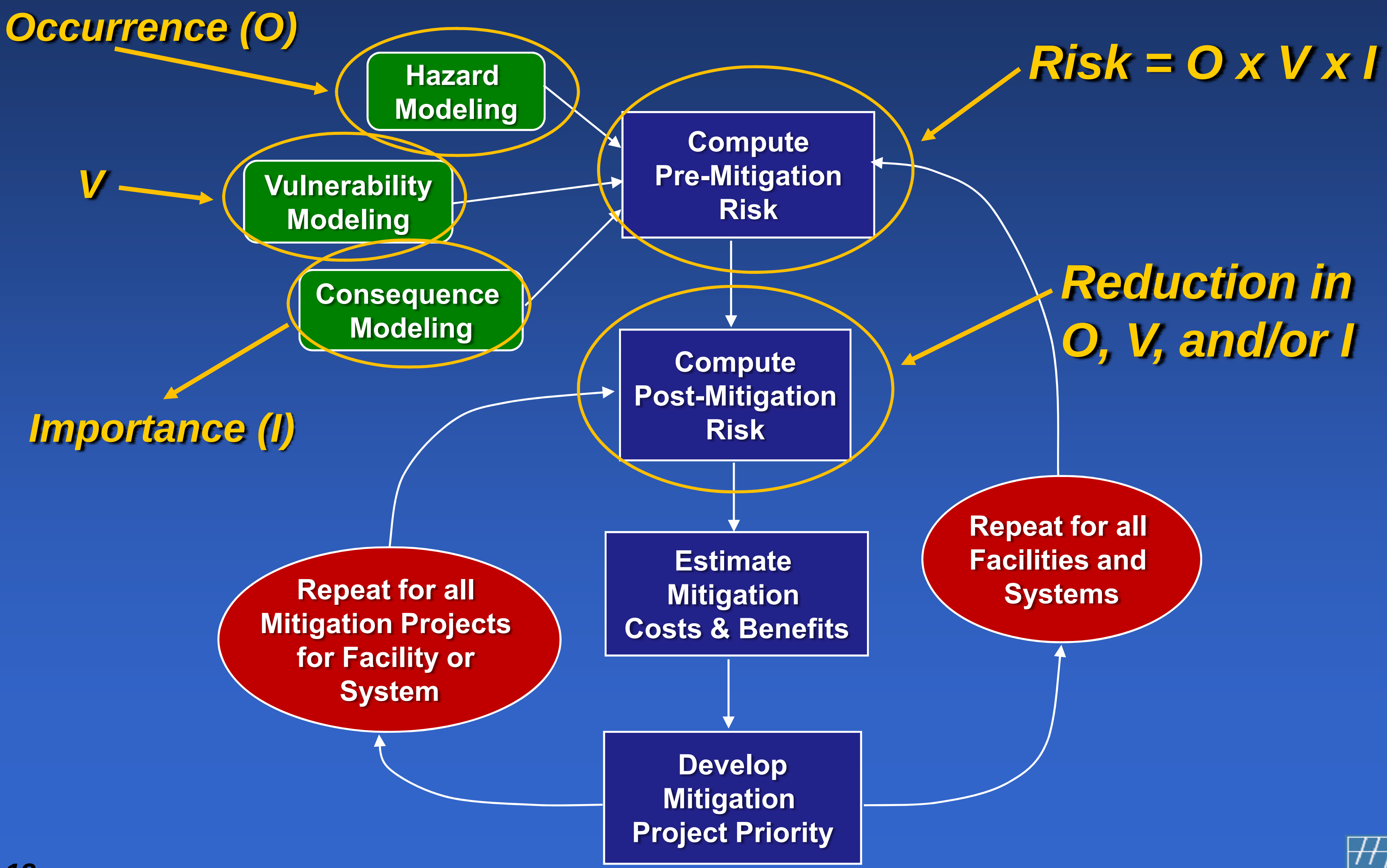
Estimate Mitigation Costs & Benefits

Develop Mitigation Project Priority

Repeat for all Mitigation Projects for Facility or System

Repeat for all Facilities and Systems

Mitigation Prioritization



Occurrence (O)

Hazard Modeling

V

Vulnerability Modeling

Consequence Modeling

Importance (I)

Compute Pre-Mitigation Risk

Risk = O x V x I

Compute Post-Mitigation Risk

Reduction in O, V, and/or I

Estimate Mitigation Costs & Benefits

Develop Mitigation Project Priority

Repeat for all Mitigation Projects for Facility or System

Repeat for all Facilities and Systems

Mitigation Prioritization

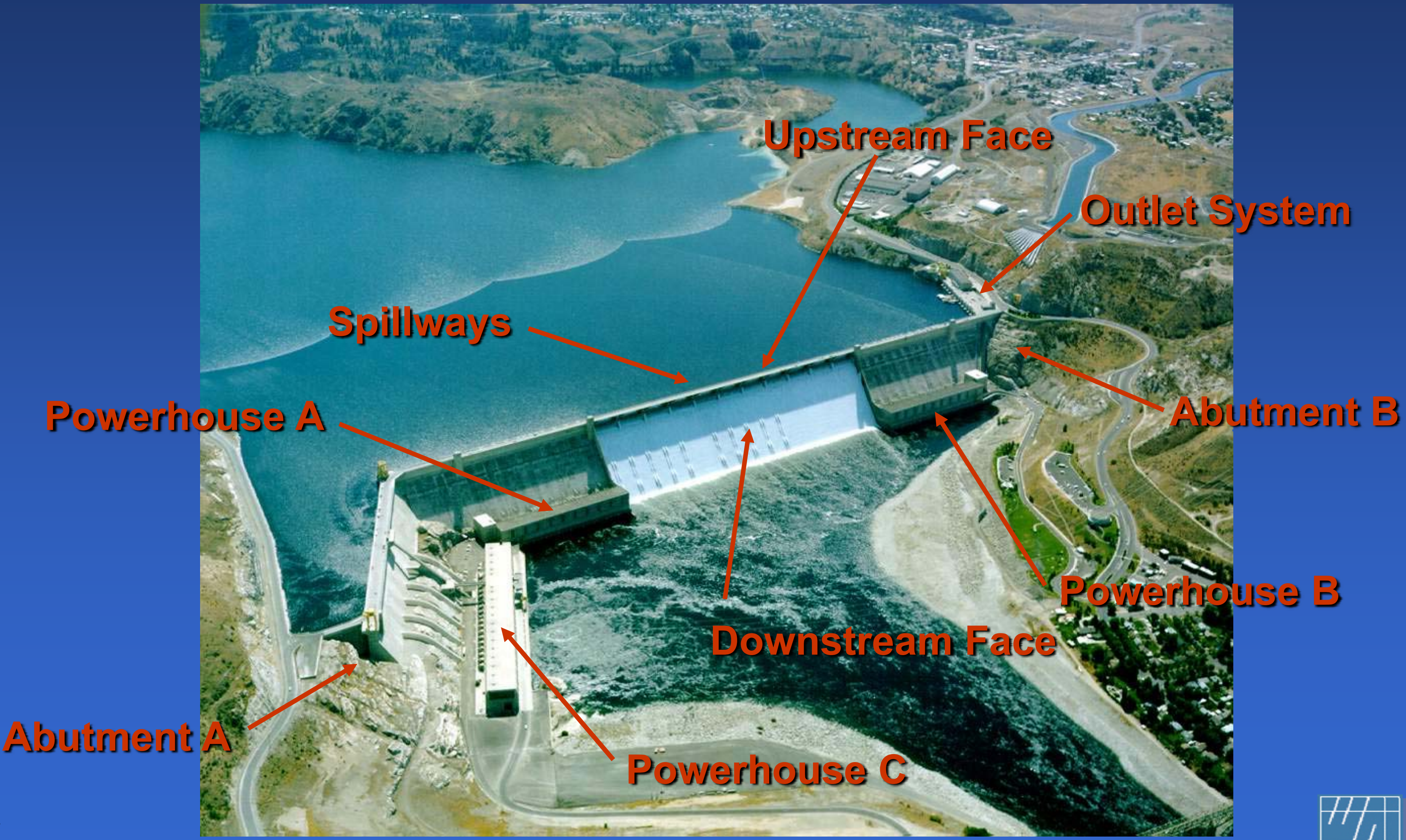
- *Threat scenario-based assessment*

$$Risk = \sum_{i=1}^{n} [O_i \times V_i] \times I$$

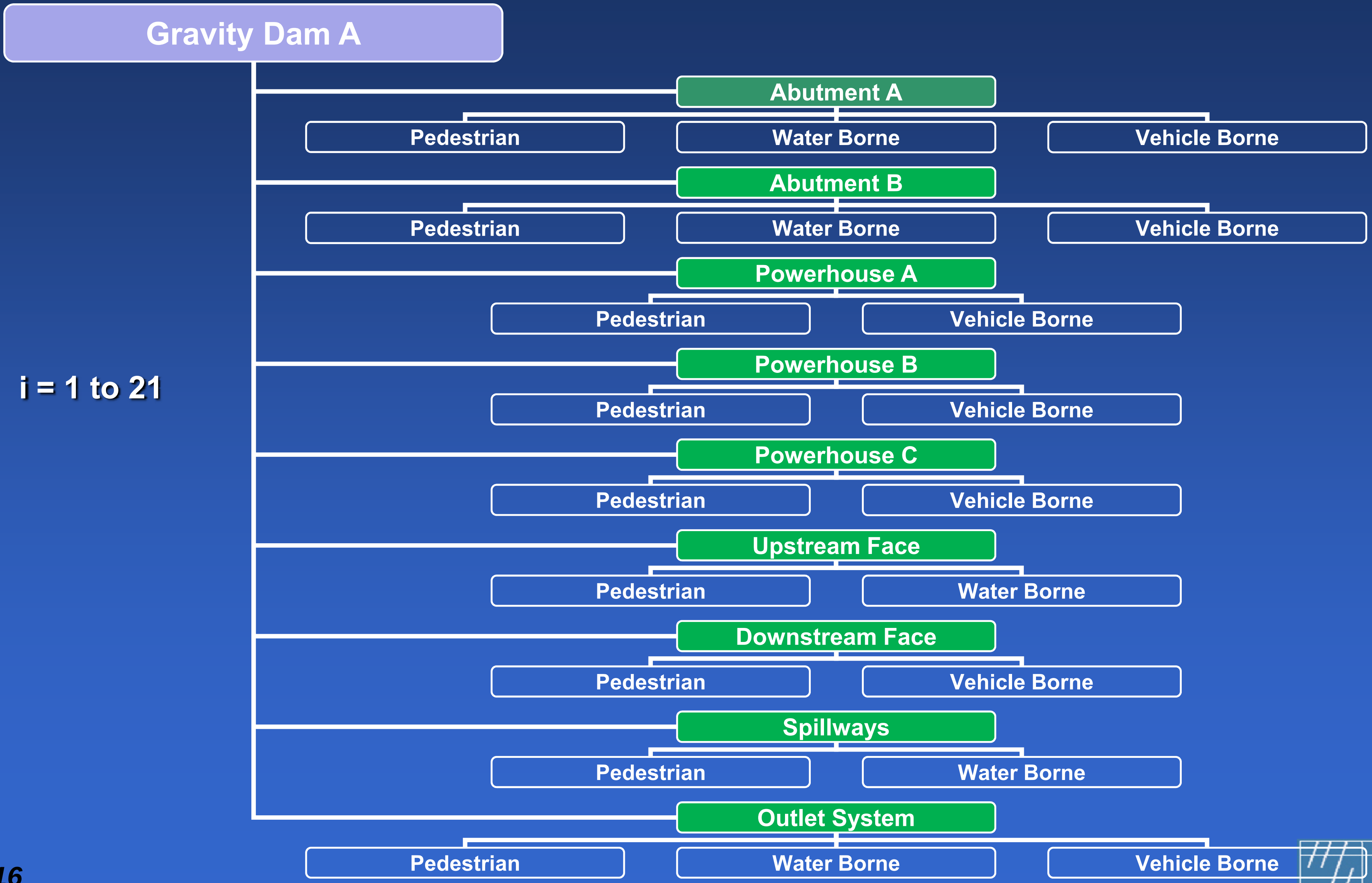
threat scenarios

  - *Similar to earthquake insurance loss estimation methods*
  - *Transparent impact of mitigation (hardening v. operational v. electronic)*

Example I: Gravity Dam (HYPOTHETICAL)



Threat Scenario Definition



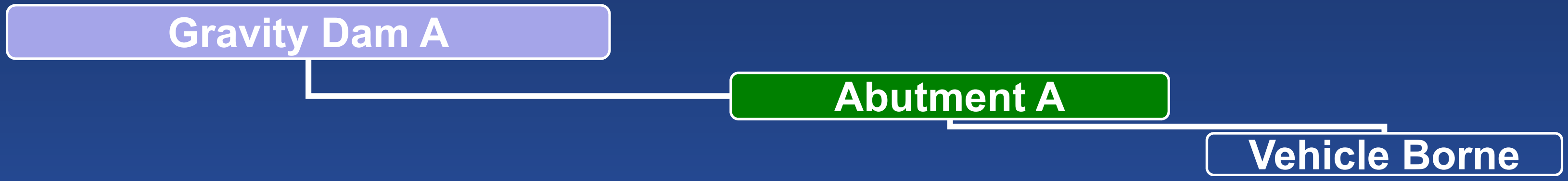
- Gravity Dam A
  - Abutment A
    - Pedestrian
    - Water Borne
    - Vehicle Borne
  - Abutment B
    - Pedestrian
    - Water Borne
    - Vehicle Borne
  - Powerhouse A
    - Pedestrian
    - Vehicle Borne
  - Powerhouse B
    - Pedestrian
    - Vehicle Borne
  - Powerhouse C
    - Pedestrian
    - Vehicle Borne
  - Upstream Face
    - Pedestrian
    - Water Borne
  - Downstream Face
    - Pedestrian
    - Vehicle Borne
  - Spillways
    - Pedestrian
    - Water Borne
  - Outlet System
    - Pedestrian
    - Water Borne
    - Vehicle Borne

i = 1 to 21

$$\sum_{i}^{n}[O_i \times V_i] \times I$$

Occurrence

- *Computed for each threat:*



Gravity Dam A

Abutment A

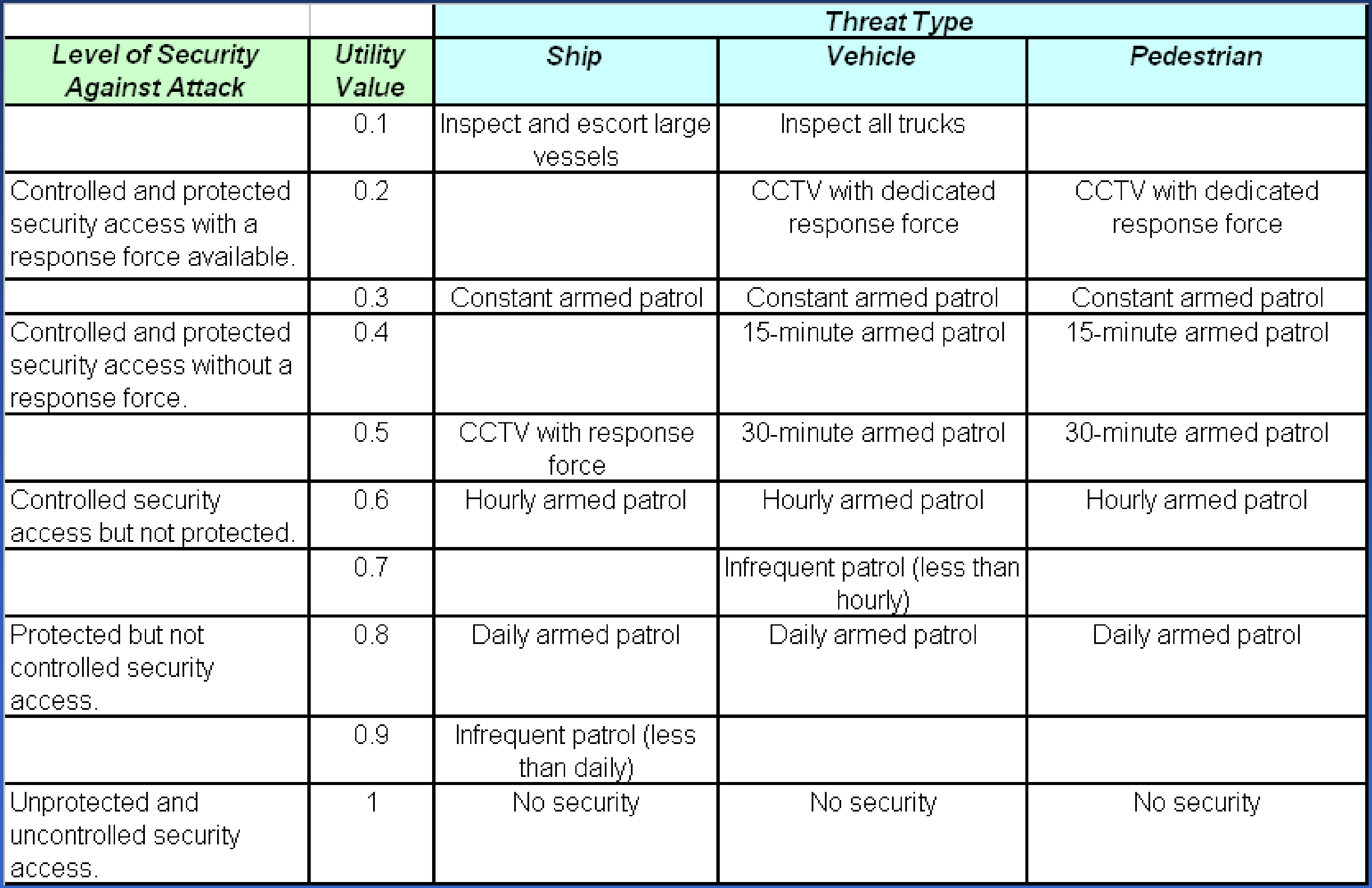
Vehicle Borne

- *Weighted sum of pseudo-utility values:*

$$O_i=\sum_{j=1}^{4} x_j w_j$$

- *Attributes mapped to quantitative scale*
  - *Access for attack*
  - *Security against attack*
  - *Attractiveness as a target*
  - *Capability of aggressor*

Example Utility Value Mapping

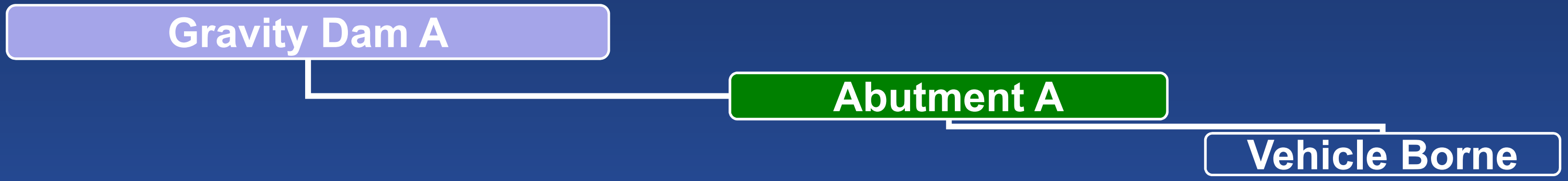


		Threat Type		
Level of Security Against Attack	*Utility Value*	*Ship*	*Vehicle*	*Pedestrian*
	0.1	Inspect and escort large vessels	Inspect all trucks	
Controlled and protected security access with a response force available.	0.2		CCTV with dedicated response force	CCTV with dedicated response force
	0.3	Constant armed patrol	Constant armed patrol	Constant armed patrol
Controlled and protected security access without a response force.	0.4		15-minute armed patrol	15-minute armed patrol
	0.5	CCTV with response force	30-minute armed patrol	30-minute armed patrol
Controlled security access but not protected.	0.6	Hourly armed patrol	Hourly armed patrol	Hourly armed patrol
	0.7		Infrequent patrol (less than hourly)	
Protected but not controlled security access.	0.8	Daily armed patrol	Daily armed patrol	Daily armed patrol
	0.9	Infrequent patrol (less than daily)		
Unprotected and uncontrolled security access.	1	No security	No security	No security

$$\sum_{i}^{n}[O_i \times V_i] \times I$$

Vulnerability

- Computed for each threat:



Gravity Dam A

Abutment A

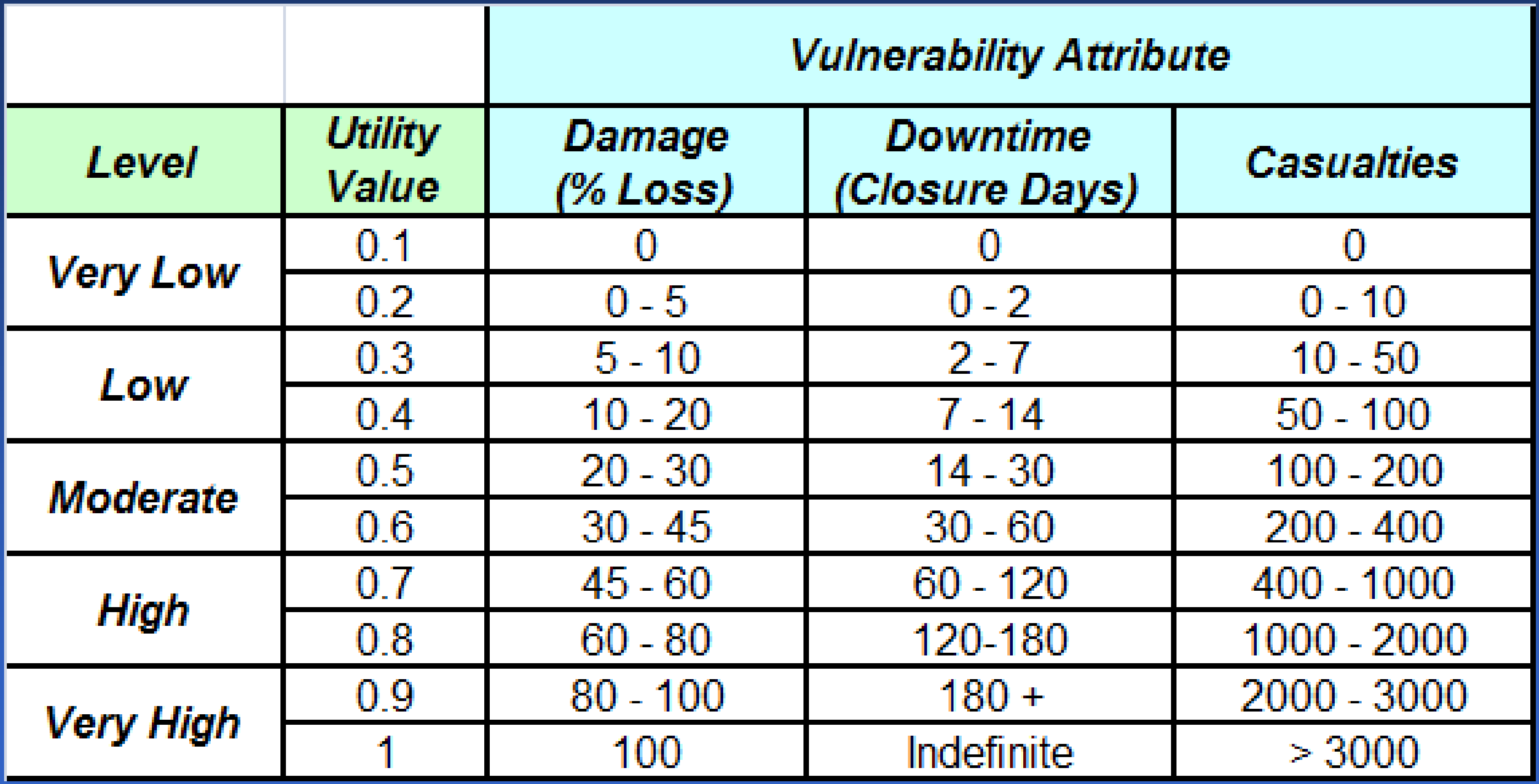
Vehicle Borne

- Weighted sum of pseudo-utility values:

$$V_i = \sum_{j=1}^{3} x_j w_j$$

- Attributes mapped to quantitative scale
  - Expected damage
  - Expected closure
  - Expected casualties

Example Utility Value Mapping



		Vulnerability Attribute		
Level	Utility Value	Damage (% Loss)	Downtime (Closure Days)	Casualties
Very Low	0.1	0	0	0
	0.2	0 - 5	0 - 2	0 - 10
Low	0.3	5 - 10	2 - 7	10 - 50
	0.4	10 - 20	7 - 14	50 - 100
Moderate	0.5	20 - 30	14 - 30	100 - 200
	0.6	30 - 45	30 - 60	200 - 400
High	0.7	45 - 60	60 - 120	400 - 1000
	0.8	60 - 80	120-180	1000 - 2000
Very High	0.9	80 - 100	180 +	2000 - 3000
	1	100	Indefinite	> 3000

$$\sum_{i}^{n}[O_i \times V_i] \times I$$

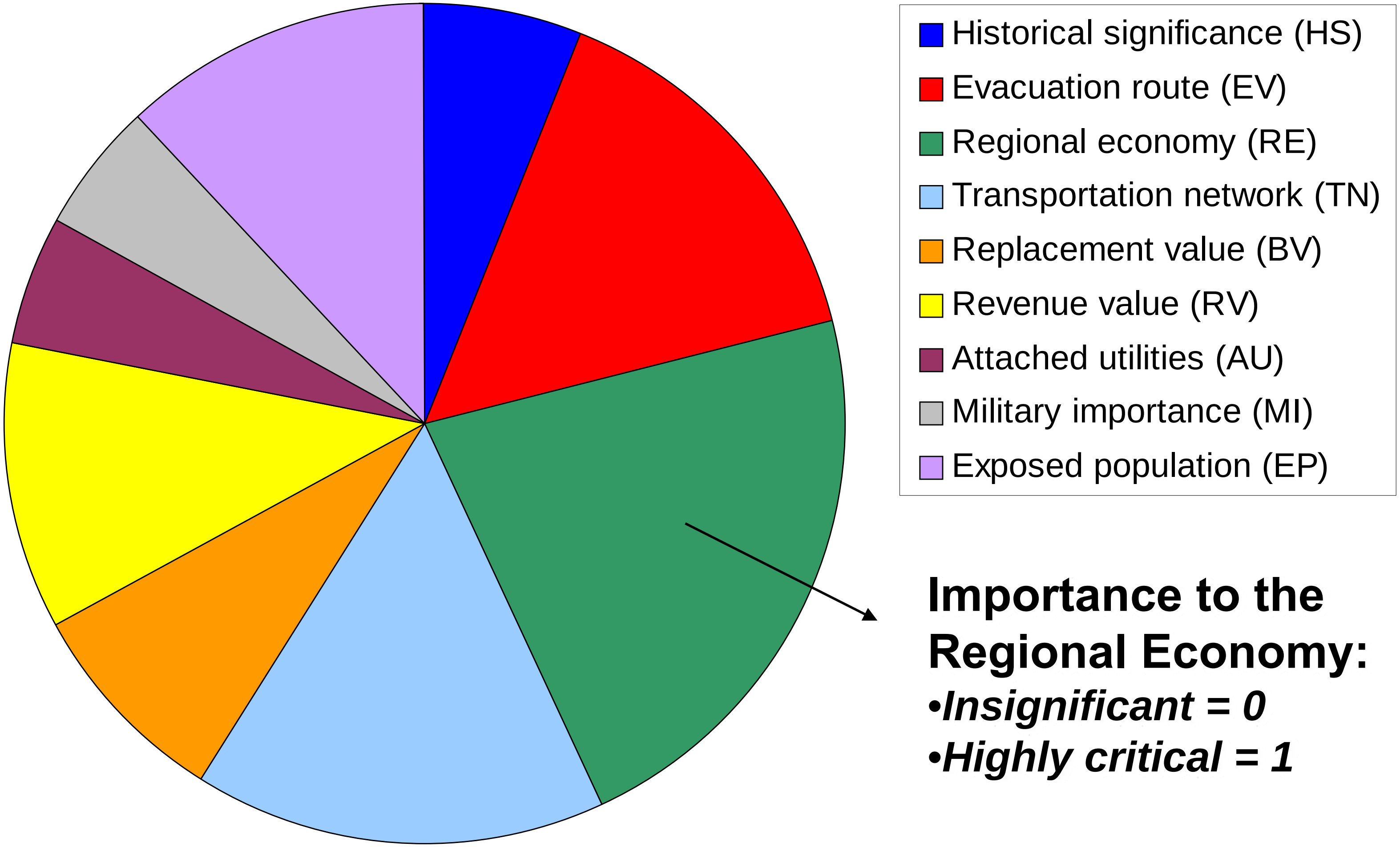
Importance

- Computed once for the facility
- Weighted sum of pseudo-utility values:

$$I=\sum_{j=1}^{8} x_j w_j$$

- Attributes mapped to quantitative scale
  - Exposed population
  - Historical/symbolic importance
  - Replacement value
  - Importance to regional economy
  - Importance to irrigation system
  - Importance for power generation
  - Importance to transportation network
  - Annual revenue

Importance Modeling Example

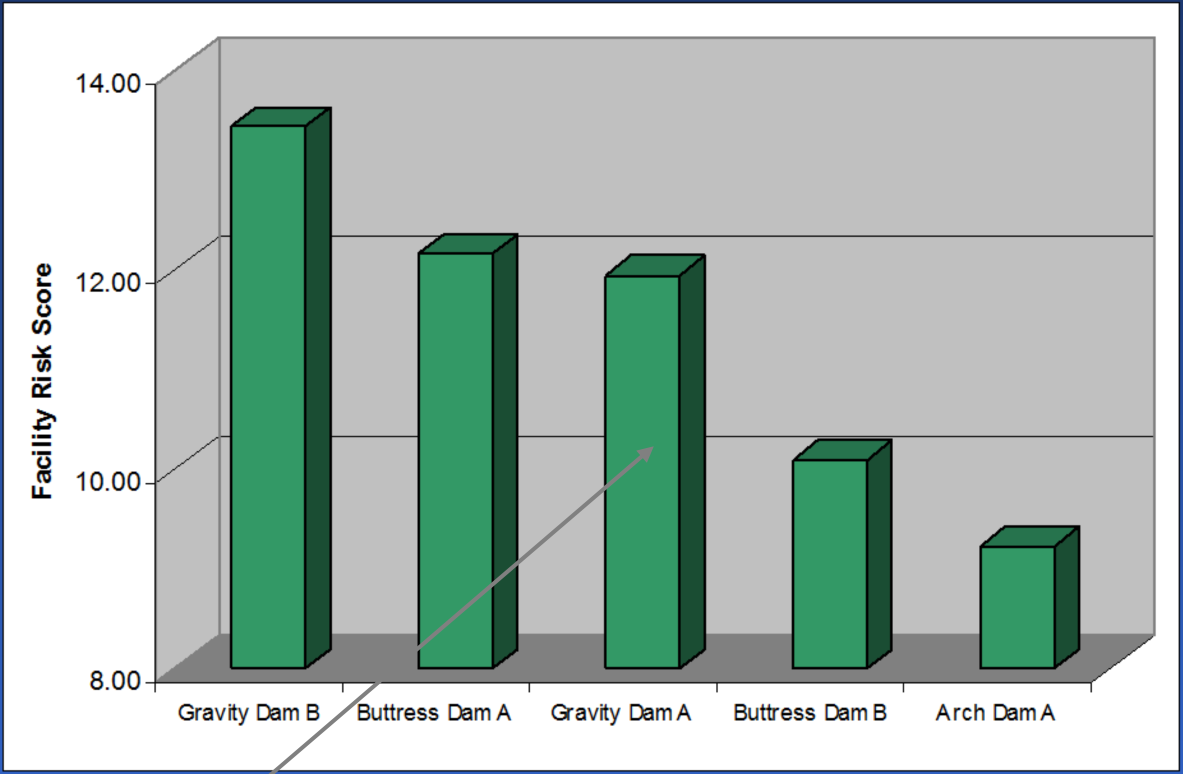


Importance to the Regional Economy:

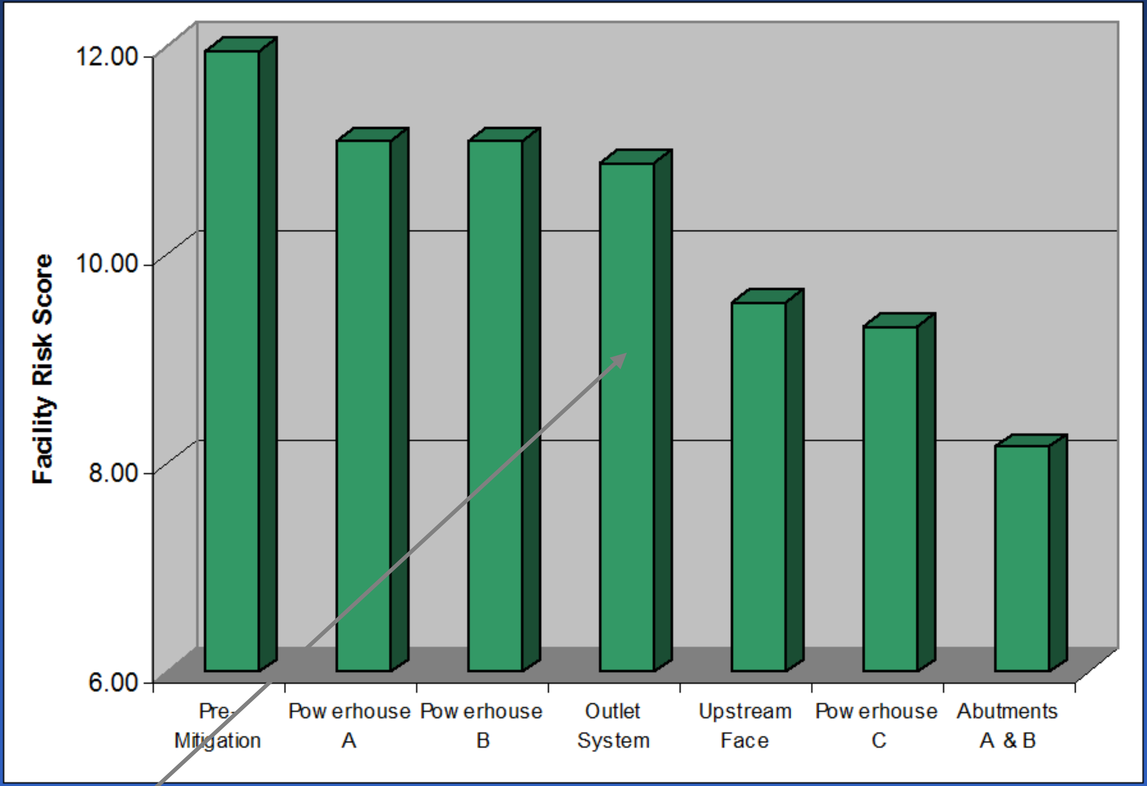
- ***Insignificant = 0***
- ***Highly critical = 1***

Pre-Mitigation Risk Scores (HYPOTHETICAL EXAMPLE)

Threat Location	Transport	Risk = OxVxI
Abutment A	Water Borne	0.36
Abutment A	Pedestrian	0.65
Abutment A	Vehicle Borne	0.31
Abutment B	Water Borne	0.52
Abutment B	Pedestrian	0.71
Abutment B	Vehicle Borne	0.54
Powerhouse A	Pedestrian	0.72
Powerhouse A	Vehicle Borne	0.11
Powerhouse B	Pedestrian	0.68
Powerhouse B	Vehicle Borne	0.18
Powerhouse C	Pedestrian	0.88
Powerhouse C	Vehicle Borne	0.78
Upstream Face	Water Borne	0.85
Upstream Face	Pedestrian	0.82
Downstream Face	Pedestrian	0.89
Downstream Face	Vehicle Borne	0.92
Spillways	Pedestrian	0.29
Spillways	Water Borne	0.69
Outlet System	Water Borne	0.67
Outlet System	Pedestrian	0.09
Outlet System	Vehicle Borne	0.29
	SUM	11.95

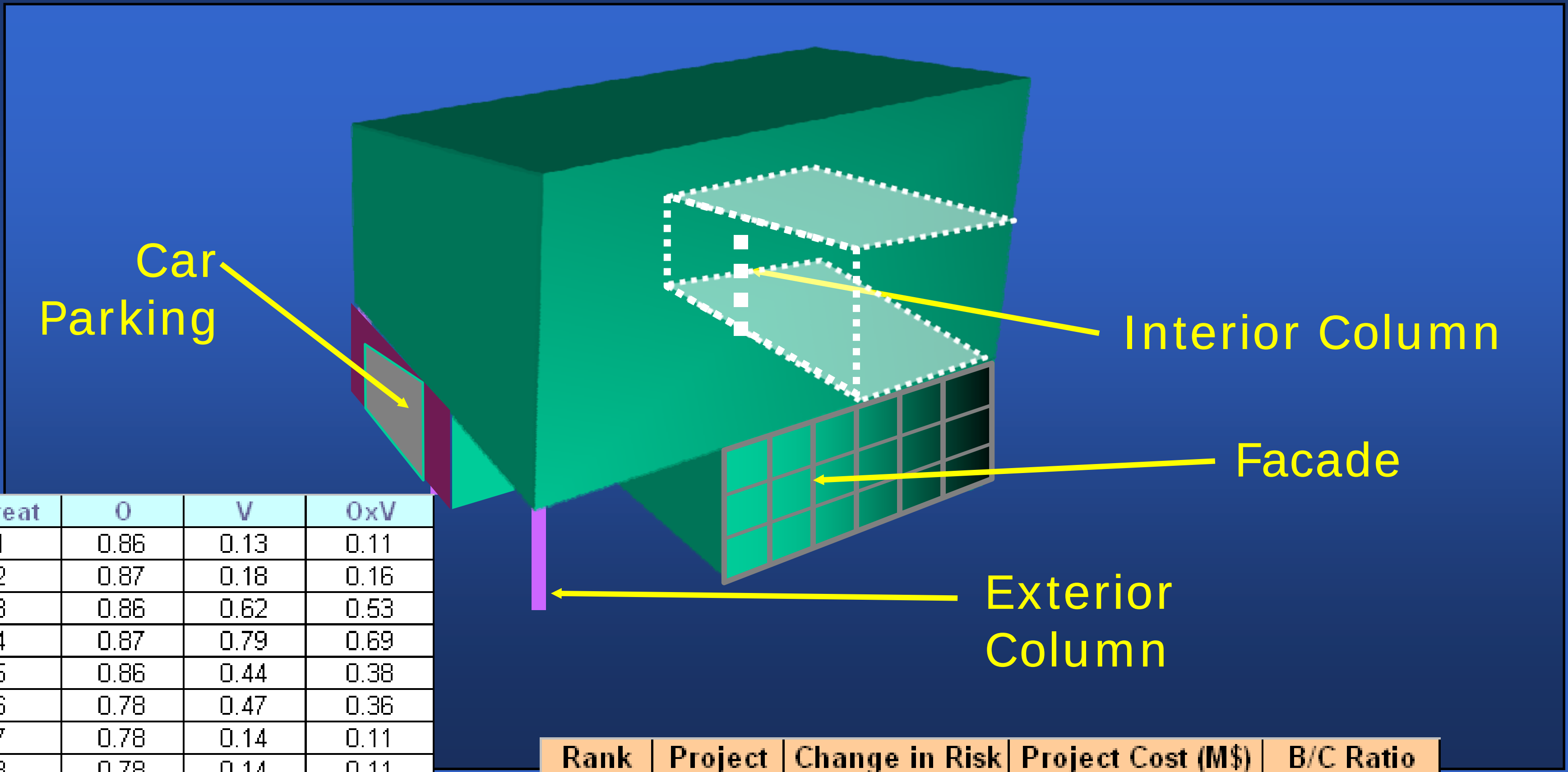


Post-Mitigation Risk Scores (HYPOTHETICAL EXAMPLE)



Mitigation Project	Cost ($1000)	Risk = OxVxI
Outlet System	750	10.88
Powerhouse A	2,840	11.09
Powerhouse B	2,840	11.09
Upstream Face	12,360	9.54
Powerhouse C	13,940	9.32
Abutments A & B	30,870	8.16

Example II: Existing Building (HYPOTHETICAL EXAMPLE)



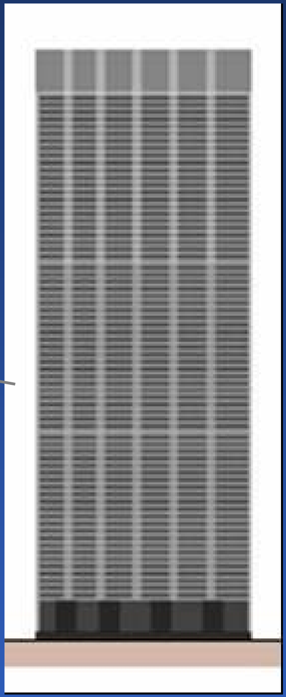
Threat	O	V	OxV
1	0.86	0.13	0.11
2	0.87	0.18	0.16
3	0.86	0.62	0.53
4	0.87	0.79	0.69
5	0.86	0.44	0.38
6	0.78	0.47	0.36
7	0.78	0.14	0.11
8	0.78	0.14	0.11
9	0.70	0.62	0.43
10	0.65	0.79	0.51
11	0.70	0.78	0.54
12	0.65	0.93	0.60
		Sum	4.55
		I	0.62
		Risk	2.82

Rank	Project	Change in Risk	Project Cost (M$)	B/C Ratio
1	B	0.30	0.19	1.61
2	F	0.34	0.82	0.41
3	E	0.23	0.70	0.34
4	D	0.05	0.74	0.07
5	C	0.10	3.18	0.03
6	A	0.03	2.05	0.02

Example III: New Design (HYPOTHETICAL EXAMPLE)

Example: truck explosive at curbside

Threat	O	V	OxV
1	0.90	0.10	0.090
2	0.84	0.20	0.168
3	0.75	0.36	0.270
4	0.70	0.46	0.322
5	0.63	0.55	0.347
6	0.54	0.65	0.351
7	0.46	0.70	0.322
8	0.32	0.70	0.224
9	0.25	0.82	0.205
10	0.18	0.95	0.171
		Sum	2.470
		I	0.85
		Risk	2.099



Mitigation Alternative	Option	Change in R	Change in Cost ($)	B/C Ratio
Harden Glazing	Glazing Option 1			
	Glazing Option 2			
	Glazing Option 3			
Harden Walls	Wall Option 1			
	Wall Option 2			
Harden Columns	Column Option 1			
	Column Option 2			
	Column Option 3			
Access Control	Screening Option 1			
	Screening Option 2			
	Bollard Option 1			
	Bollard Option 2			

Critical Issues: Prioritization

- *Based on rational, rigorous, and unbiased risk assessment*
- *Assumptions and limitations*
- *Benefits and costs*
- *Objectives and constraints*
- *Time frame*
- *Decision support*

Example IV: Existing Tunnel

- ***Single deterministic threat***
- ***Prioritize on all benefits and costs***

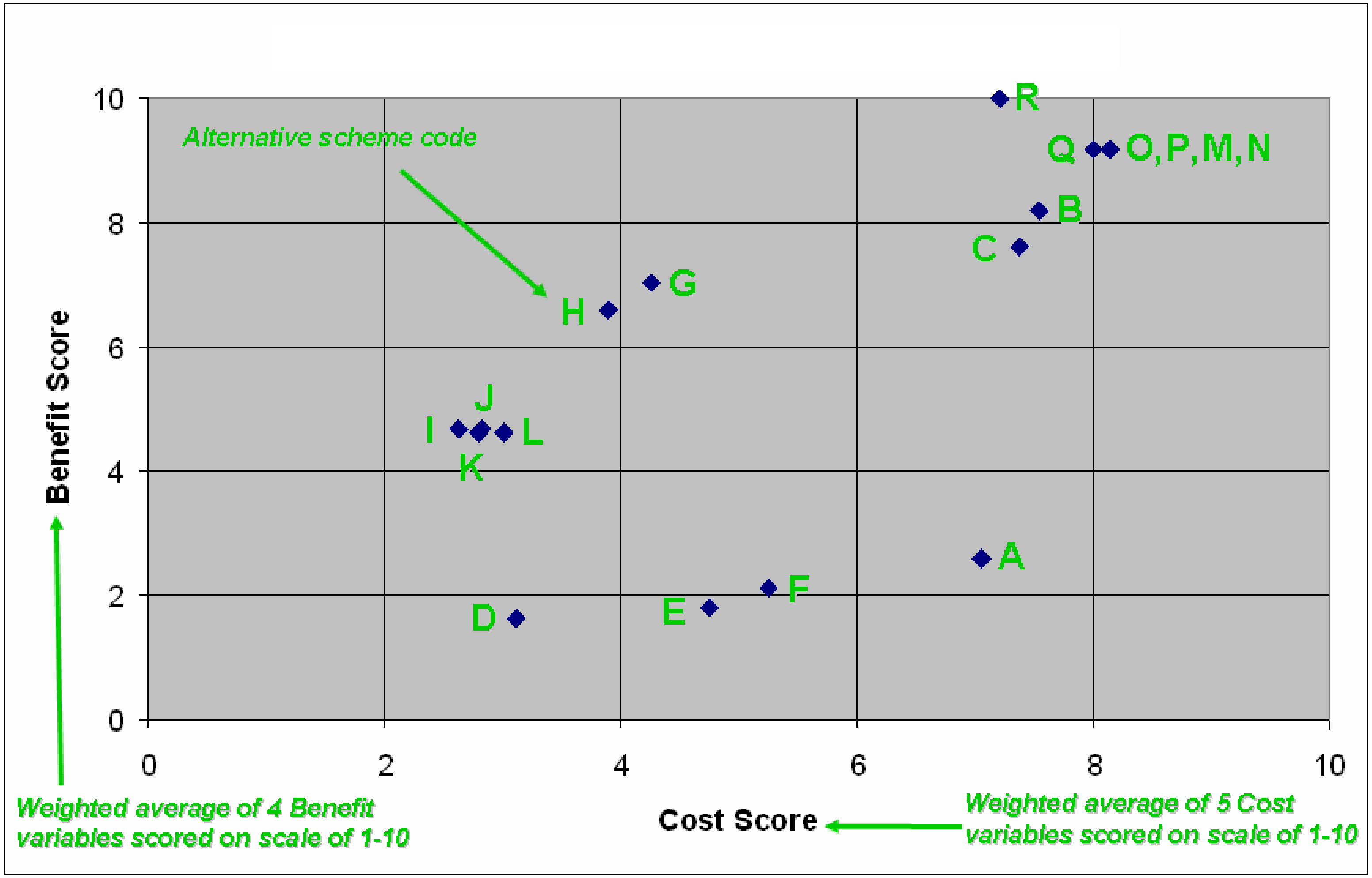
Benefits:

- *Expected Performance (Reliability)*
- *Ease of Tunnel Repair*
- *Benefit to Emergency Response*
- *Secondary/Other Benefits*

Costs:

- *Construction Cost*
- *Construction Risk*
- *Construction Duration*
- *Impact on Operations During Construction*
- *Impact on Operations Long Term*

Benefit-Cost Comparison



Alternative scheme code

Weighted average of 4 Benefit variables scored on scale of 1-10

Weighted average of 5 Cost variables scored on scale of 1-10

Concluding Remarks

- *Security risk assessment*
  - *Components, basis, terminology*
  - *Screening methods*
  - *Assumptions and limitations*
- *Mitigation prioritization*
  - *Risk-based, quantitative benefit/cost*
  - *Rational unbiased approach*
  - *Several other influences*
    - *Economic, social, legal, political*
    - *Rational assessment provides data*