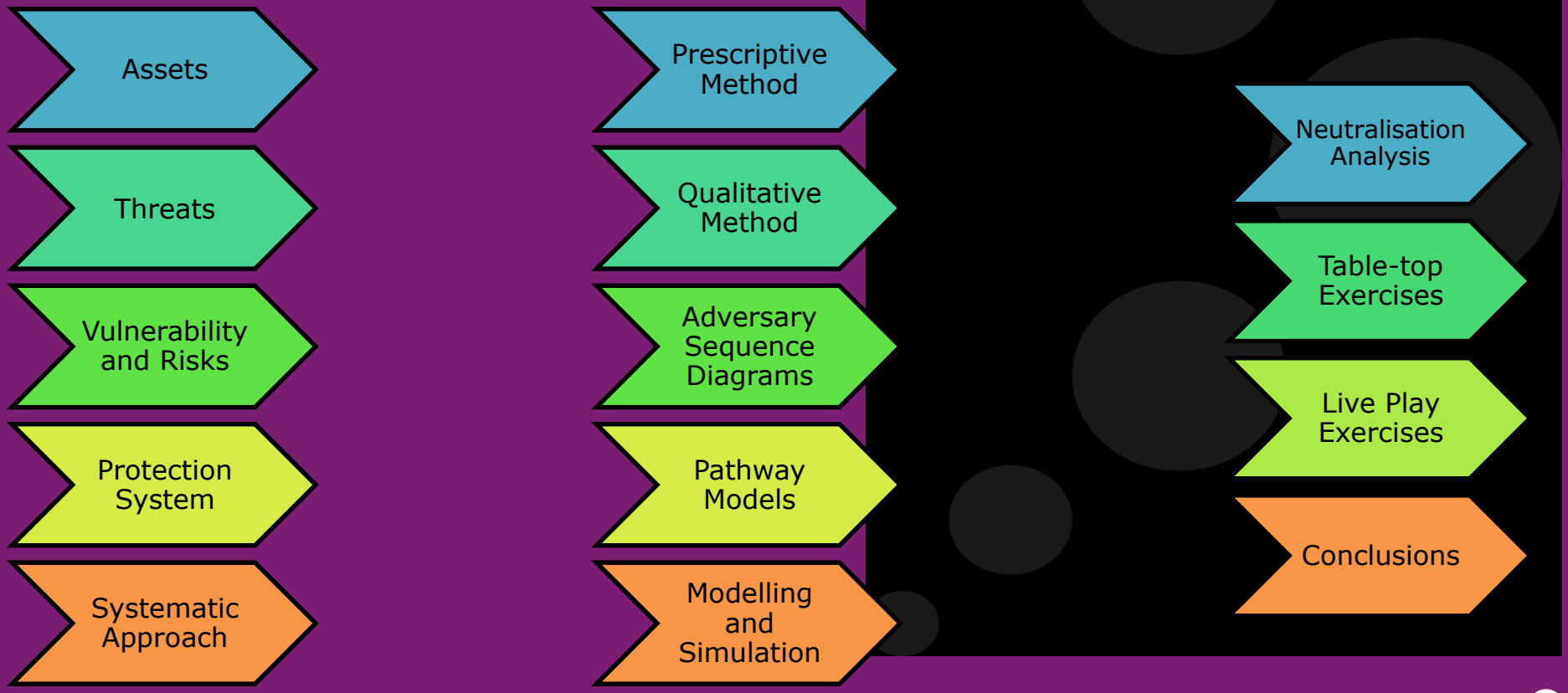
NATIONAL NUCLEAR LABORATORY

Malcolm Baker
Jeremy Edwards
Robert Rodger
Kevin Thompson
Jonathan Scott

The Vulnerability Continuum



Assets

What are you trying to protect (what are the possible targets)?

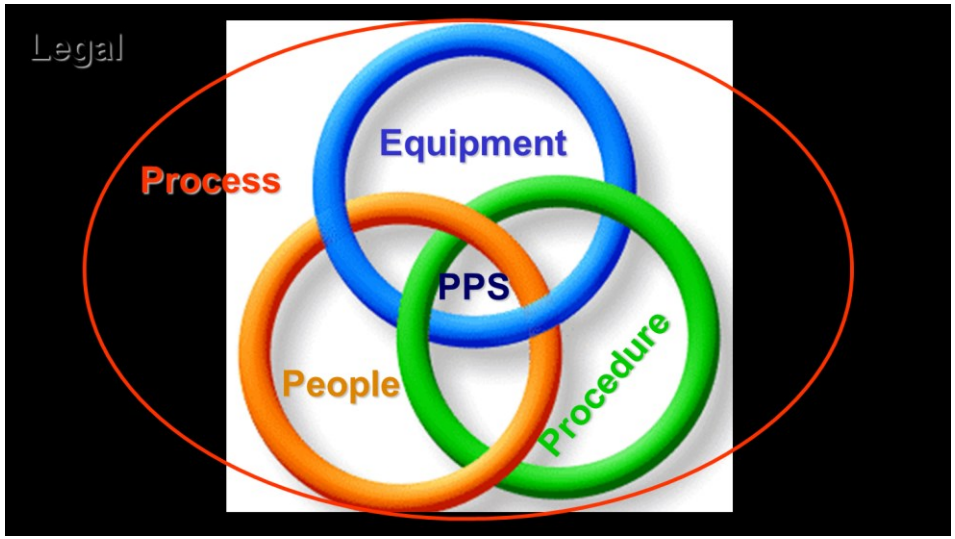
- People
- Nuclear Material
- Other Radioactive Materials
- Structures, Systems and Components

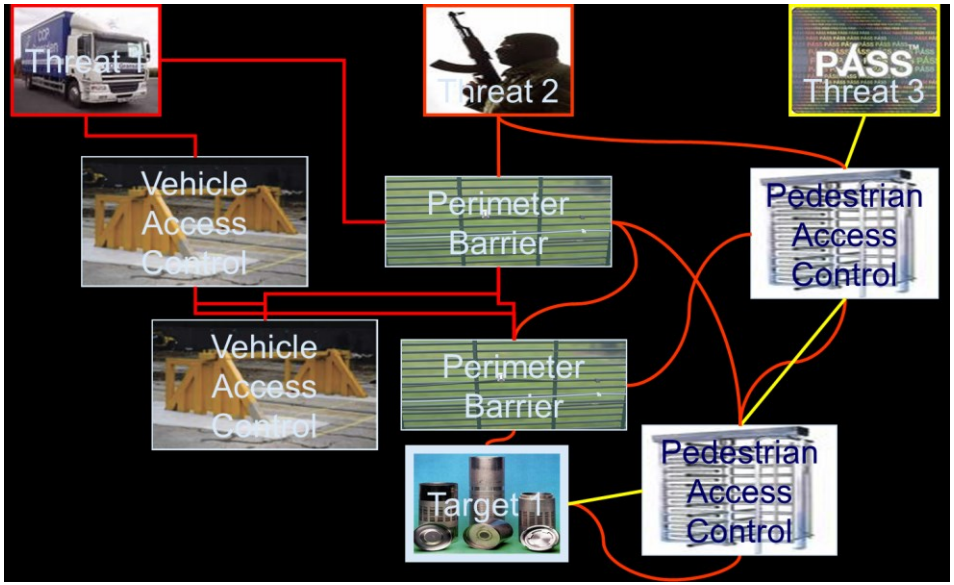
Threats

NATIONAL NUCLEAR LABORATORY

Design Basis Threat

Vulnerability and Risks





Adversary →  ← Response

Physical Protection System (PPS)

- Designed to address vulnerabilities and manage risk
- Assessment can be difficult
  - Subjective
  - Many methods
- When is it "good enough?"

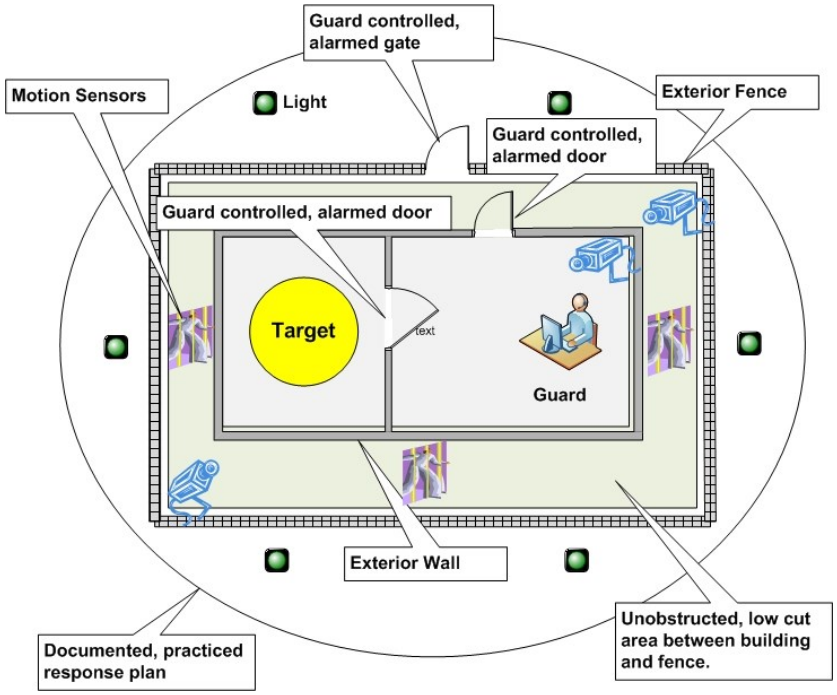


Image Credit; Tom Olzak (TechRepublic)

Systematic Approach

Information, Assessment, Decision and Process

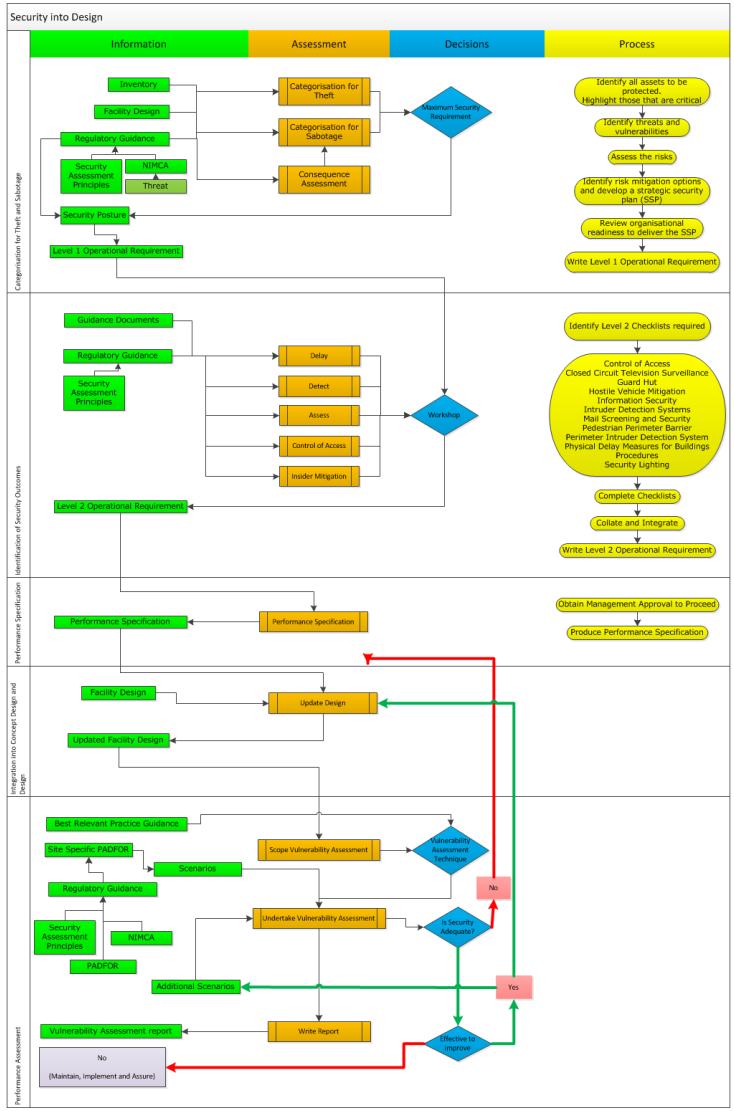
Categorise Assets for Theft and Sabotage

Identify requirements for:

- ★Delay;
- ★Detect;
- ★Assess;
- ★Control of Access; and
- ★Insider Mitigation

Design including Performance Specification

Vulnerability Assessment



Prescriptive Methods

Checklist approach
(NSS11, Appendix 4)

- ✓ Very simple
- ✓ No expertise required
- ✓ Quick and Inexpensive
- ✓ Repeatable
- ✓ Can include non-quantitative aspects (Security Management etc.)

- X No quantification
- X Is that equipment good enough?
- X No scoring – pass or fail

"So you have a gate?"…

Image Credit; Wikimedia Commons

Image Credit; Newgate UK

NATIONAL NUCLEAR LABORATORY

Software Questionnaire

(Automated Questionnaire with scoring)

- ✓ Easy to use
- ✓ No expertise required
- ✓ Quick and Inexpensive
- ✓ Repeatable
- ✓ Can test non-quantitative aspects

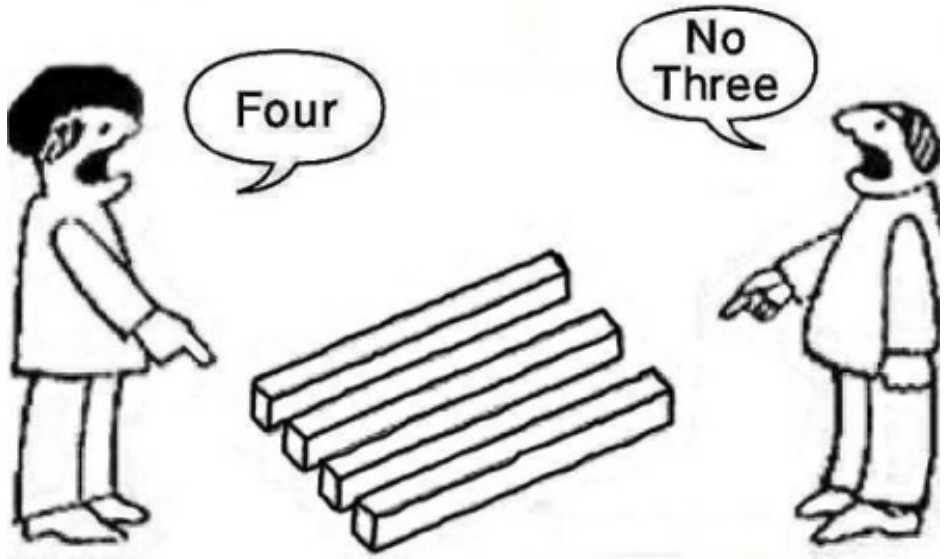


Image Credit; MISCW.com

- X Arbitrary quantification and scoring
- X Subjective (is that a 3 or a 4?)

Adversary Sequence Diagrams

- ✓ Customisable – can be simple or complex
- ✓ Quantifies Delay vs. Response
- ✓ Predominantly user driven
- ✓ Route comparison/assessment
- ✓ Understanding of PPS

- X Data dependent
- X No consideration of e.g. security management
- X Transit delays difficult to reconcile
- X Requires some expertise
- X Takes longer than Prescriptive/Qualitative

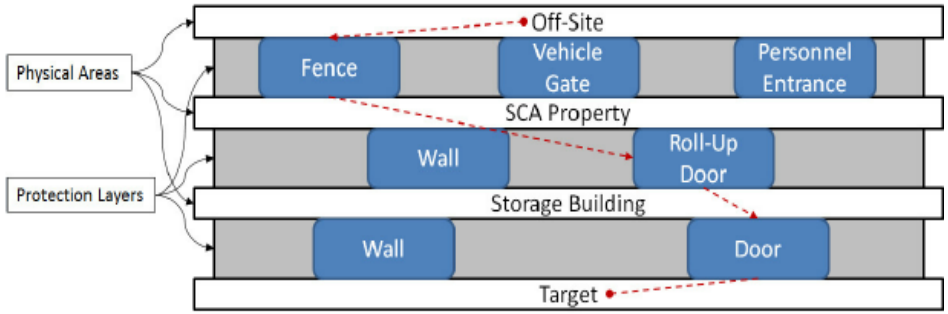


Image Credit; M. L. Garcia

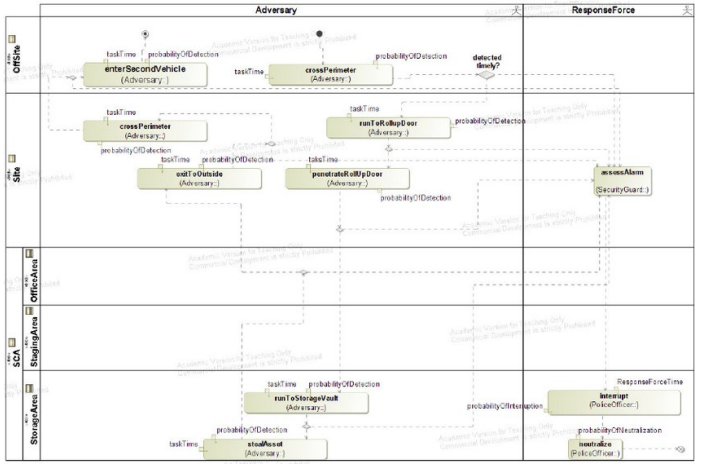


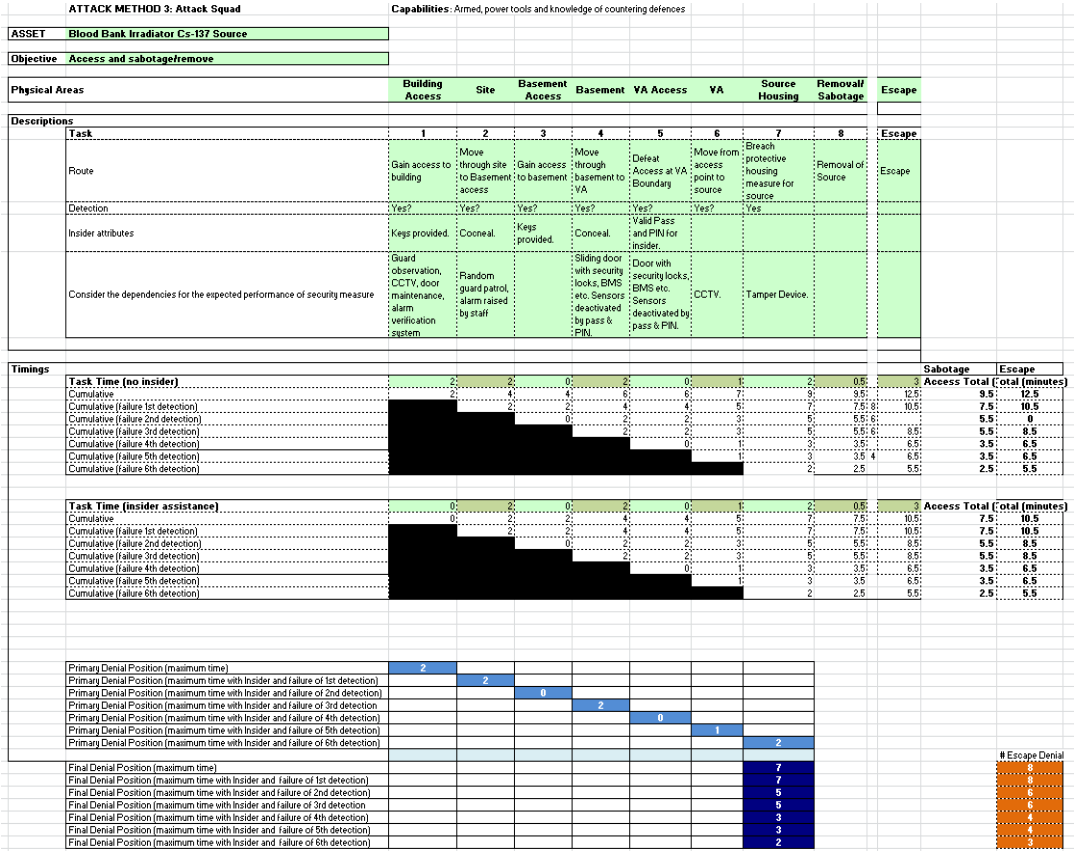
Image Credit; S Bassam

Pathway Methods

Simple Pathway

- ✓ Customisable – can be simple or complex
- ✓ Quantifies Delay vs. Response
- ✓ Scenario based
- ✓ Route comparison/assessment
- ✓ Understanding of PPS

- ✗ Data dependent
- ✗ No consideration of e.g. security management
- ✗ Requires expertise
- ✗ Takes longer than Prescriptive/Qualitative



ATTACK METHOD 3: Attack Squad — **Capabilities**: Armed, power tools and knowledge of countering defences

ASSET: Blood Bank Irradiator Cs-137 Source

Objective: Access and sabotage/remove

Physical Areas	Building Access	Site	Basement Access	Basement	YA Access	YA	Source Housing	Removal/ Sabotage	Escape

Descriptions

Task	1	2	3	4	5	6	7	8	Escape
Route	Gain access to building	Move through site to Basement access	Gain access to basement	Move through basement to YA	Defeat Access at YA Boundary	Move from access point to source	Breach protective housing measure for source	Removal of Source	Escape
Detection	Yes?	Yes?	Yes?	Yes?	Yes?	Yes?	Yes		
Insider attributes	Keys provided.	Cocneal.	Keys provided.	Conceal.	Valid Pass and PIN for insider.				
Consider the dependencies for the expected performance of security measure	Guard observation, CCTV, door maintenance, alarm verification system	Random guard patrol, alarm raised by staff		Sliding door with security locks, BMS etc. Sensors deactivated by pass & PIN.	Door with security locks, BMS etc. Sensors deactivated by pass & PIN.	CCTV.	Tamper Device.		

Timings

Task Time (no insider)									Sabotage	Escape
	2	2	0	2	0	1	2	0.5	3 Access Total (minutes)	
Cumulative	2	4	4	6	6	7	9	9.5	12.5	9.5 / 12.5
Cumulative (failure 1st detection)		2	2	4	4	5	7	7.5	8 10.5	7.5 / 10.5
Cumulative (failure 2nd detection)			0	2	2	3	5	5.5	6	5.5 / 0
Cumulative (failure 3rd detection)				2	2	3	5	5.5	6	5.5 / 8.5
Cumulative (failure 4th detection)					0	1	3	3.5	6.5	3.5 / 6.5
Cumulative (failure 5th detection)						1	3	3.5	4 6.5	3.5 / 6.5
Cumulative (failure 6th detection)							2	2.5	5.5	2.5 / 5.5

Task Time (insider assistance)									Sabotage	Escape
	0	2	0	2	0	1	2	0.5	3 Access Total (minutes)	
Cumulative	0	2	2	4	4	5	7	7.5	10.5	7.5 / 10.5
Cumulative (failure 1st detection)		2	2	4	4	5	7	7.5	10.5	7.5 / 10.5
Cumulative (failure 2nd detection)			0	2	2	3	5	5.5	8.5	5.5 / 8.5
Cumulative (failure 3rd detection)				2	2	3	5	5.5	8.5	5.5 / 8.5
Cumulative (failure 4th detection)					0	1	3	3.5	6.5	3.5 / 6.5
Cumulative (failure 5th detection)						1	3	3.5	6.5	3.5 / 6.5
Cumulative (failure 6th detection)							2	2.5	5.5	2.5 / 5.5

Primary Denial Position (maximum time)	2						
Primary Denial Position (maximum time with Insider and failure of 1st detection)		2					
Primary Denial Position (maximum time with Insider and failure of 2nd detection)			0				
Primary Denial Position (maximum time with Insider and failure of 3rd detection				2			
Primary Denial Position (maximum time with Insider and failure of 4th detection)					0		
Primary Denial Position (maximum time with Insider and failure of 5th detection)						1	
Primary Denial Position (maximum time with Insider and failure of 6th detection)							2
Final Denial Position (maximum time)							7
Final Denial Position (maximum time with Insider and failure of 1st detection)							7
Final Denial Position (maximum time with Insider and failure of 2nd detection)							5
Final Denial Position (maximum time with Insider and failure of 3rd detection							5
Final Denial Position (maximum time with Insider and failure of 4th detection)							3
Final Denial Position (maximum time with Insider and failure of 5th detection)							3
Final Denial Position (maximum time with Insider and failure of 6th detection)							2

Escape Denial
2
8
5
5
3
3
2

Image Credit; IAEA NUSAM

Modelling and Simulation

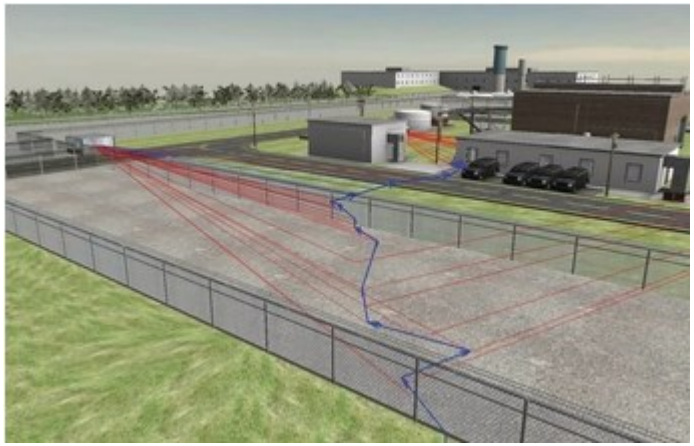
NATIONAL NUCLEAR LABORATORY

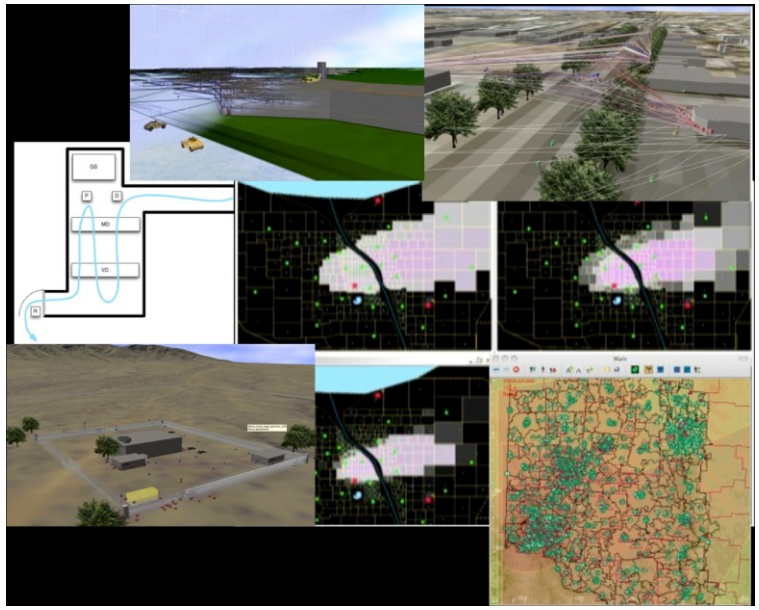
Pathway/Scenario Tools
(e.g. AVERT, Simajin)

- ✓ Detailed pathway analysis
- ✓ Highly quantitative
- ✓ Thorough assessment of PPS
- ✓ Repeatable
- ✓ Modifiable

- X Expensive
- X Time consuming
- X Requires significant expertise
- X Needs high volume of data
- X No qualitative assessment

Image Credit; Ares Corp





Neutralisation analysis (ConOps)

- ✓ Customisable – can be simple or complex
- ✓ Specialist input
- ✓ Consideration of expected human responses
- ✓ Consideration of security management
- ✓ Understanding of PPS

- ✗ Potential for confirmation bias
- ✗ Requires significant expertise and knowledge
- ✗ Rarely accounts for human error

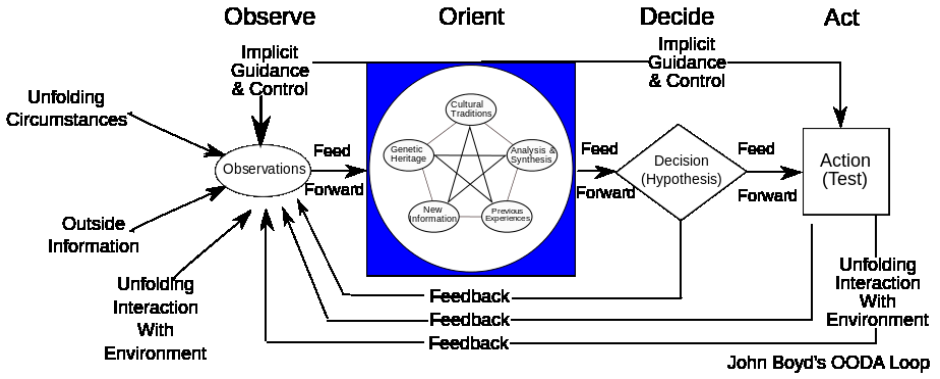
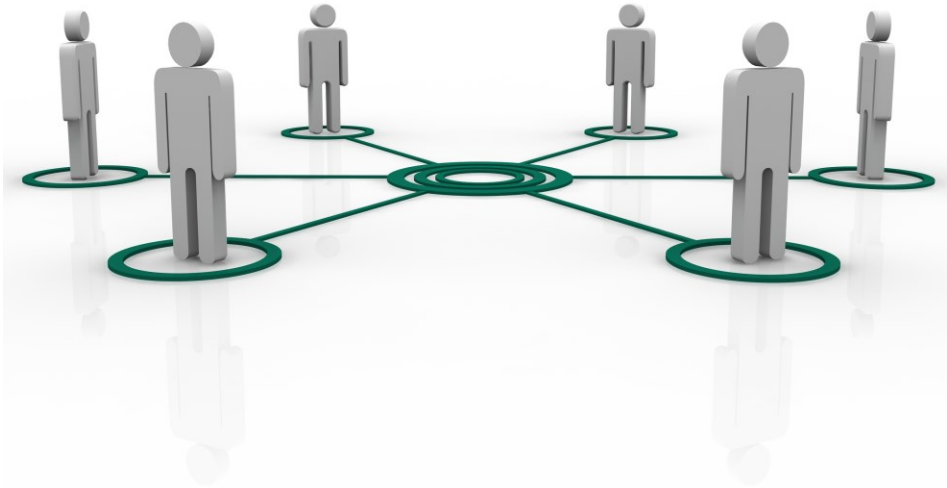


Table-top Exercises

- ✓ Customisable – can be simple or complex
- ✓ Specialist input
- ✓ Some consideration of expected human responses
- ✓ Some consideration of security management
- ✓ Understanding of PPS and response force
- ✓ Easily re-run

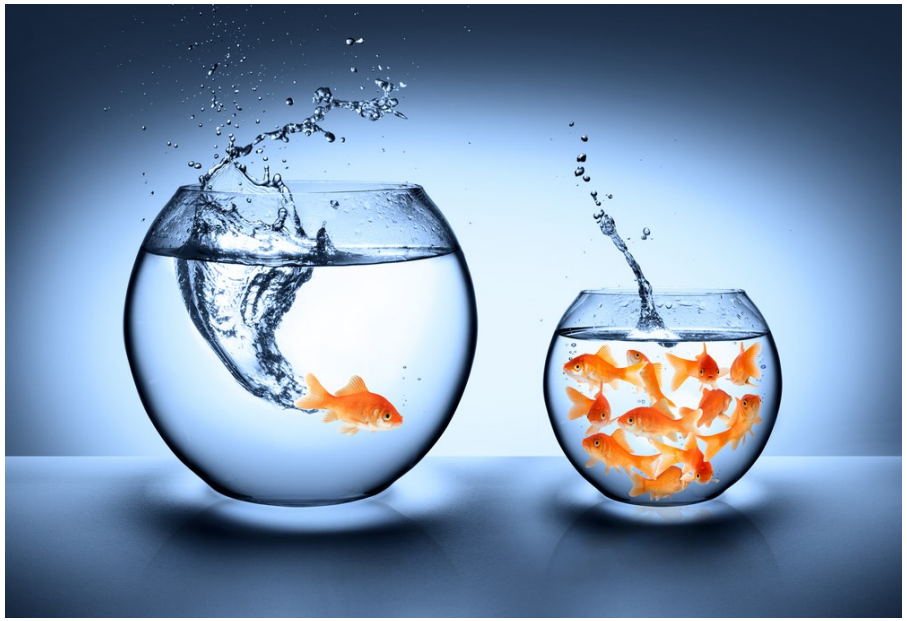
- ✗ Potential for confirmation bias
- ✗ Requires some expertise and knowledge
- ✗ Rarely accounts for human error
- ✗ Force on Force interactions may benefit first action



Live Play Exercises

- ✓ Customisable – can be simple or complex
- ✓ Specialist input
- ✓ Consideration of expected human responses
- ✓ Consideration of security management
- ✓ Understanding of PPS and response

- X Expensive to organise and run
- X Potential for confirmation bias
- X Requires significant expertise and knowledge
- X Limited repeatability



Conclusions

There are many ways to assess the performance of Physical Protection Systems

Each has their own strengths (cost, scope, schedule, detail) but also their own weaknesses (depth, coverage, completeness)

Some require considerable investment in preparation for the assessment to maximise the value of the output

No individual method will be all encompassing

No method will ENSURE that the system will perform as expected when challenged for ‘Real’