The Vulnerability Continuum

- Assets
- Threats
- Vulnerability and Risks
- Protection System
- Systematic Approach

- Prescriptive Method
- Qualitative Method
- Adversary Sequence Diagrams
- Pathway Models
- Modelling and Simulation

- Neutralisation Analysis
- Table-top Exercises
- Live Play Exercises
- Conclusions
What are you trying to protect (what are the possible targets)?

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

Malicious Capabilities → Potential Adversarial Forces → Scenarios
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.)

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

“So you have a gate?”...
Qualitative Methods

Software Questionnaire
(Automated Questionnaire with scoring)

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

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

Image Credit; MISCW.com
Adversary Sequence Diagrams

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

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

Image Credit; M. L. Garcia
Image Credit; S Bassam
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
Modelling and Simulation

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

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

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

- Expensive to organise and run
- Potential for confirmation bias
- Requires significant expertise and knowledge
- 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’