Critical Infrastructure Security Vulnerability Assessment

A New Approach

Norman Bird - Senior Technical Lead - Nuclear Security

Critical Infrastructure Protection and Resilience Europe (CIPRE)

**Securing Europe’s Critical Infrastructure**

12th – 13th February 2014 – London - UK
Overview

- Based on work undertaken by NNL
- Technology delivery in partnership with ARES Security
- As this case study involves a real nuclear facility I cannot discuss specific results
Background - Critical Infrastructure

• Desire:
  • Steady-state operations
  • No incidents *(man-made, natural or malicious)*

• Mitigation:
  • Appropriate regulation
  • Appropriate threat / risk mitigation
  • Good design (incorporating appropriate resilience)
  • Good operation (incl. effective security at all times)
  • Effective maintenance and guarding
  • Human aspects - best practices, reliability, awareness

• Financial:
  • Justify expenditure and investment decisions, *(CapEx, OpEx, etc.)*
  • Optimise return on investment (ROI)

*CapEx – Capital Expenditure, OpEx – Operational Expenditure, ROI – Return On Investment*
Background - (Nuclear) Critical Infrastructure?

Desire:
- Steady-state operations
- No incidents (man-made, natural or malicious)

Mitigation:
- Appropriate regulation
- Appropriate design/maintenance/mitigation
- Good design (resilience)
- Good operational effectiveness and capability at all times
- Effective management and guarding
- Human aspects - Best practices, reliability, awareness

Financial:
- Justify expenditure and investment decisions, (CapEx, OpEx, etc.)
- Optimise return on investment

Essentially the same drivers
Background – NNL – At a glance

• Strategic:
  • International nuclear R&D centre of excellence
  • Support new build and clean up
  • Safeguard nuclear expertise, facilities and skills
  • Trusted advisor
  • Collaborations/Partnerships/Links
  • Socio-economic focus

• Operational:
  • Nuclear infrastructure operator
  • Do our own threat assessments
  • Operate nuclear facilities requiring ‘outcome-based’ security compliance
Background – Infrastructure information

Infrastructure information:

- Now readily available
- Excellent quality
- Continually improving

Imagery from Bing Maps
Background – Modelling / Simulation

- Not new
- Often confused with CAD etc.
- Extensively used in civil nuclear sector to date (safety, process, design, etc.)
- An emerging technique (for security)
- Modelling of infrastructure is now an international, open source and leisure time activity

Imagery from Google Earth and Google Streetview
Iraqi Insurgency Group Utilizes 'Google Earth' for Attack Planning

Case Study – M and S Approach

- Established and matured in US for over a decade
- Proven and endorsed technology for significant government programmes
- Accredited in US:
  - DHS (Certified)
  - DoD (Accredited)
  - DoE (Accreditation in Progress)
- Used by NNL in their national early adopter role for nuclear industry and critical national infrastructure
Case Study - Aims

• Evaluate against a **complex** UK nuclear infrastructure asset

• Evaluate if there are substantial benefits over existing techniques

• Illustrate possible wider UK national infrastructure use in future

• Provide independent reach back, technical / software support / assessment services and training
Process - Overview - (5 Steps)

DATA PHASE

MODELLING PHASE

SIMULATION PHASE

OUTPUT PHASE

VERIFICATION PHASE
Process - (Data) – Step 1

DATA PHASE

2D CAD information
3D CAD information
GIS information
Aerial Photography
Satellite Imagery
Facility Record Drawings
Facility Security Measures
Security Performance Data
  • Physical
  • Systems / Sensors
  • Guard Force
Adversary Performance Data
Environmental Criteria
Plant Operational Criteria
Threat Scenario Criteria
Vulnerability of Facility
DATA PHASE

- 2D CAD information
- 3D CAD information
- GIS information
- Aerial Photography
- Satellite Imagery
- Facility Record Drawings
- Facility Security Measures
- Security Performance Data
  - Physical
  - Systems / Sensors
  - Guard Force
- Adversary Performance Data
- Environmental Criteria
- Plant Operational Criteria
- Threat Scenario Criteria
- Vulnerability of Facility

MODELLING PHASE

- Facility Characterization
  - Site Layout
    - Infrastructure
    - Security layers
    - Elevation / terrain
  - Barrier Systems
    - Perimeter structure
    - Barriers
    - Delay systems
- Detection Systems
  - Sensors & cameras
  - Command / control
  - Communications
- Response Force
  - Patrol & response
  - Capabilities
  - Training
Process - (Simulation) – Step 3

DATA PHASE
- 2D CAD information
- 3D CAD information
- GIS information
- Aerial Photography
- Satellite Imagery
- Facility Record Drawings
- Facility Security Measures
- Security Performance Data
  - Physical
  - Systems / Sensors
  - Guard Force
- Adversary Performance Data
- Environmental Criteria
- Plant Operational Criteria
- Threat Scenario Criteria
- Vulnerability of Facility

MODELLING PHASE
- Security Modeling
- Facility Characterization
  - Site Layout
  - Infrastructure
  - Security layers
  - Elevation / terrain
- Barrier Systems
  - Defenses / controls
  - Barriers
  - Delay systems
- Detection Systems
  - Sensors & controls
  - Command / control
  - Communications
- Response Force
  - Human & response
  - Capabilities
  - Training

SIMULATION PHASE
- Define Scenarios
  - Threat capabilities
  - Targets
- Constructive Simulation
  - Attack planning or vulnerability
  - Overall system response to attack
  - Determine KPIs: system effectiveness, detections, interruption, neutralization
- Virtual Simulation
  - Response of real and virtual agents to scenario
  - Compare human response to anticipated/optimal response
  - Determine KPIs: exposure and response time, neutralization given response
Process - (Output) – Step 4

DATA PHASE
- 2D CAD information
- 3D CAD information
- GIS information
- Aerial Photography
- Satellite Imagery
- Facility Record Drawings
- Facility Security Measures
- Security Performance Data
  - Physical
  - Systems / Sensors
  - Guard Force
- Adversary Performance Data
- Environmental Criteria
- Plant Operational Criteria
- Threat Scenario Criteria
- Vulnerability of Facility

MODELLING PHASE
- Security Modeling
- Facility Characterization
  - Site Layout
  - Infrastructure
  - Security layers
  - Elevation / terrain
- Barriers
  - Master barrier structures
- Delay systems
- Detection Systems
  - Sensors / devices
  - Communications
- Response Force
  - Training
  - Capabilities

SIMULATION PHASE
- Security Simulation
- Define Scenarios
  - Threat capabilities
  - Targets
- Constructive Simulation
  - Attack planning
  - Vulnerability
  - Countermeasures
- Virtual Simulation
  - Performance of real and virtual agent to scenario

OUTPUT PHASE
- Exercise Metrics
Process - (Verification) – Step 5

DATA PHASE
- 2D CAD information
- 3D CAD information
- GIS information
- Aerial Photography
- Satellite Imagery
- Facility Record Drawings
- Facility Security Measures
- Security Performance Data
  - Physical
  - Systems / Sensors
  - Guard Force
- Adversary Performance Data
  - Environmental Criteria
  - Plant Operational Criteria
  - Threat Scenario Criteria
  - Vulnerability of Facility

MODELLING PHASE
- Facility Characterization
  - Site Layout
  - Infrastructure
  - Security layers
  - Elevation / terrain
- Barrier Systems
  - Perimeter structures
  - Barriers
- Delay systems
- Detection Systems
  - Sensors / cameras
  - Command / control
- Response Force
  - Target & response
  - Capabilities
  - Training

SIMULATION PHASE
- Constructive Simulation
  - Attack planning or vulnerability
  - Overall system response to attack
  - Determine KPIs: system effectiveness, detection, interruption, neutralization
- Virtual Simulation
  - Response of real and virtual agents to scenario
  - Simulate human response to anticipated / optimal response
  - Data from KPIs: exposure and response time, neutralization given response

OUTPUT PHASE

VERIFICATION PHASE (Future)

Exercises
- Update data libraries and results based on ‘real’ performance outcomes
Early results (Typical)
Early learning

• Accurate model information
• Early risk review mechanism
• Alignment with site visits (both site & model verification)
• Model simplification (don’t need to model everything)
• Access to timely technical support / SMEs
• Early pooling of expert opinion around a centric model
• Early operational appreciation

SME = Subject Matter Expert
Early challenges

- Inaccuracy in as built records
- Obtaining as built knowledge
- Obtaining verified performance data
- Managing sensitive data and results
- Managing the what if syndrome (*and preventing scope creep*)

*These challenges were all overcome in the case study*
Typical examples of results output
Performance-based infrastructure assurance

- Quantitative performance assessment (Graded RAG approach)
- Challengeable and demonstrable threat mitigation
- Threat scenario is capable of being rehearsed / exercised
- Model can be re-verified from further exercises
- Managing output expectations:
  - Practical
  - Cost effective
  - Operationally achievable
  - Acceptable

Note: The % threshold levels defined on this slide are also being used as a methodology to assess nuclear security effectiveness / threat mitigation at US nuclear infrastructure sites.

RAG = Red, Amber, Green.
Case study – M and S benefits

- Improved quantitative infrastructure assessment
- Enhanced security appreciation / optimisation
- Core model for determining minimum performance standards
- Reproducible / repeatable demonstration of assurances
- Efficient re-assessment of DBT impact

- Auditable platform (for further exercising, testing and improved consistency of approach for cost benefit analysis)

Outcome – Modelled / measured security effectiveness
Conclusions

• Facilitates improved decision making

• Demonstrates operational effectiveness

• Helps to manage / mitigate the threat to infrastructure

• Helps to optimise security standards, costs, performance, compliance and expectations

• ......Future?
Future - *(Dynamic)* threat assessment

**ALL THREATS ‘STATUS’ VIEW**

**National (and Public) Expectation**
(I.e. Design Basis)

**Infrastructure Operation**
(I.e. Outcome-based)

**THREAT SCENARIO**

Strategic aim being closer parity between expectation (design) and infrastructure operation (delivery) using M and S
Summary

• Wider infrastructure uses:
  • Transport Hubs
    • Airports, Ports etc.
  • Transport networks and movements
  • Utilities, Telecomms
  • Chemicals, Oil and Gas
  • Key national infrastructure points
  • Energy
  • Defence, Borders and Emergency Services
  • Commerce
  • National and international risk governance / agencies
  • Foreign embassies
  • Temporary hardened assets (Events etc.)
  • Contingency planning and resilience

Where risk reduction and resilience are essential to continuity
Acknowledgements

• NNL Modelling and Simulation Team

• NNL Site Security Management

• ARES Security

• Civil Nuclear Constabulary (CNC)

• University of Central Lancashire (UCLan)
  
  (Joint authors of the case study summary
  Norman Bird – NNL and
  Prof. Laurence Williams - UCLan)
Thank you for listening

Questions?

For further information contact: Norman Bird

norman.bird@nnl.co.uk

or visit

www.nnl.co.uk/commercial-services/security.aspx