Integration of Security into a Concept Design for a Facility

Malcolm Baker
Jeremy Edwards
Robert Rodger
Ken Owens
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

Performance and Vulnerability Assessment
Categorisation for Theft and Sabotage

Need to Understand Assets and Potential Consequences
Assets

Nuclear Material
Other Radioactive Materials
Structures, Systems and Components
Threat

Design Basis Threat

Malicious Capabilities ➔ Potential Adversarial Forces ➔ Scenarios
Identification of Security Outcomes

Understand Physical and Technical Regulatory Expectations

Categorisation drives required ‘Security Outcomes’
Once Security Outcomes are Specified then Performance Specifications can be Provided to ‘Design and Engineering’ Teams
Updated Design is then Tested against Credible Scenarios (based on the Design Basis Threat)
Improvements to the Design are made as Required
Iterative Process for Designing and Testing Concept Design

Ensures Appropriate Inclusion of Security at an Early Stage

Enables Safety and Security to be Discussed Before Large Investment Decisions are Made

Leads to a ‘Right First Time’ Result

Project Cost and Operational Efficiencies are Delivered
Integration of Security into a Concept Design for a Facility

Any Questions?

robert.m.rodger@nnl.co.uk