出國報告（出國類別：訓練）

第 27 屆國際核子保安訓練

服務機關：行政院原子能委員會
姓名職稱：黃朝群技士
派赴國家：美國
出國期間：107 年 4 月 28 日至 5 月 21 日
報告日期：107 年 7 月 4 日

摘要

自 2001 年 911 美國雙子星大樓恐怖攻擊事件發生後，「反恐」成為國際社會重視的議題，為防止恐怖分子取得大規模毀滅性武器或放射性物質作為犯罪工具進行恐怖攻擊及威脅，聯合國已相繼通過多項重大決議或公約。2004 年聯合國安理會第 1540 號決議案要求各國必須強化核物料管理、實體防護與核子保安等管制與執法作為。2005 年「制止核恐怖主義行為國際公約（International Convention for the Suppression of Acts of Nuclear Terrorism）」更明確要求各會員國嚴懲並制止恐怖行為，並加強國際合作對抗核恐怖主義的威脅。對於核子保安的範圍界定，亦從單純的核物料使用、貯存與運輸安全，逐步納入核設施的運轉安全，防範核物料非法走私、非法取得或使用，以及針對核物料與核設施的蓄意破壞等。

國際原子能總署（International Atomic Energy Agency，IAEA）為強化各會員國防範核設施遭受暴力攻擊（Sabotage）及核物料失竊（Theft）之保安能力，委託美國能源部聖迪亞國家實驗室（Sandia National Laboratories, SNL）辦理「國際核子保安訓練（International Training Course on the Physical Protection of Nuclear Material and Nuclear Facilities, ITC）」，課程範圍包括核子保安系統建構方法，核子保安實體防護學理、防護技術、防護設備，以及國際最新指導原則及建議等。

「國際核子保安訓練」歷史悠久，自 1978 年 11 月舉辦第一屆以來，今年已是第 27 屆，本次計有 40 個會員國，51 個學員完成訓練（總計已有 935 名學員完成訓練），係目前國際間最完整之核子保安訓練。結訓學員遍佈各國核能管制機關、研究機構、核子反應器設施經營者、情治單位及國安系統等，影響力無遠弗屆，建議未來賡續派員參加，相信對於瞭解國際實體防護新知、推動核子保安監管業務及推展核子保安國際合作等均有所助益。

目錄

壹、出國目的

一、緣起

自 2001 年 911 恐怖攻擊事件發生後，「反恐」成為國際重視的議題，2004 年聯合國安理會第 1540 決議案要求各會員國必須強化核物料帳料管理、實體防護與核子保安、邊境管制與防堵走私，以及出（轉）口運輸等管制與執法作為。2005 年「制止核恐怖主義行為國際公約」更明文定義核恐怖主義犯罪、公約適用範圍、締約會員國打擊核恐怖犯罪合作的義務等內容，並明確要求各會員國訂定相關法律，嚴懲恐怖份子、制止恐怖行為，以及加強國際合作對抗核恐怖主義威脅。儘管我國雖非聯合國會員國及「制止核恐怖主義行為國際公約」締約國，但對抗恐怖主義已是普世價值，「制止核恐怖主義行為國際公約」亦屬國際習慣法，不論我國有無簽署加入，同樣受其效力約束。

二、主題

行政院原子能委員會（以下簡稱本會）為我國原子能業務主管機關，負責國內核子反應器設施（核能電廠）有關實體防護與核子保安監督工作。本會參考美國核能管制委員會（Nuclear Regulatory Commission, NRC）有關核子保安法規，要求國內核能電廠建置功能完整的核子保安作業，包括門禁管制、入侵偵測、延遲歹徒，以及應變武裝防衛能力等，並要求加強查察員工及包商，避免發生內部破壞者（Insider）與歹徒裡應外合情形。

本次參加國際原子能總署委託美國能源部在美國新墨西哥州阿布奎基市聖迪亞國家實驗室舉辦的第 27 屆「國際核子保安訓練」（27th International Training Course on the Physical Protection of Nuclear Material and Nuclear Facilities, ITC-27），旨在透過訓練課程，學習國際最新核子保安實體防護學理與技術、國際最新指導原則與建議，以防範核物料、放射性物質及其設施，遭受偷竊、蓄意破壞、未經授權進入、非法轉讓或其他惡意行為之侵害。

貳、 出國行程

本次受訓課程為期三週，自 107 年 4 月 28 日出發至 5 月 21 日返國。課程地點在美國新墨西哥州阿布奎基市聖迪亞國家實驗室舉行。詳細行程如表 1：

表 1 出國行程表

日期	地點	內容
4 月 28 日	台北→舊金山→阿布奎基市	去程
4 月 29 日	阿布奎基市	報到
4 月 30 日～5 月 4 日	阿布奎基市	訓練課程
5 月 5 日～5 月 6 日	阿布奎基市	週末
5 月 7 日～5 月 11 日	阿布奎基市	訓練課程
5 月 12 日～5 月 13 日	阿布奎基市	週末
5 月 14 日～5 月 18 日	阿布奎基市	訓練課程
5 月 19 日～21 日	阿布奎基市→舊金山→台北	返程

參、 研習過程

一、研習方式

本訓練課程係以課堂講授（Lecture）、分組實作（Subgroup Exercises）、示範觀摩（Demonstration）及專題演講（Guest Lecture）等方式進行，主辦單位為確認學員們對課程的瞭解程度，一開始就進行課前測驗，以瞭解學員背景知識，另於每次課堂講授結束後進行小考，針對學員們答錯率較高的部份，請講座進行說明，協助釐清學員觀念，當所有課程結束後進行成果測驗，另再以結訓成果報告（Final Exercise Report）作為總結。

課程講授依照核設施實體防護系統（Physical Protection System, PPS）建構過程三步驟：定義需求（Define Requirement）、系統設計（Design）及系統評估（Evaluation）順序進行，全部課程計有 28 個主要單元，每一單元均由專業講師擔任課堂講座，講授結束隨即進行分組實作，並視課程內容安排示範、觀摩或參訪活動，全程均以英語進行。(學員合影如圖 1)

主辦單位將 51 位學員分為 6 小組，每小組 8 至 10 名學員，進行分組實作練習。實作教材設計一虛構國家「拉卡錫（Lagassi）」，該

虛擬國之國家實驗室設有水池式反應器（Pool Type Reactor, PTR）及中子反應器（Neutron Burst Reactor, NBR）各 1 座。其中水池式反應器為分組實作實體防護系統建構練習標的，由聖迪亞國家實驗室安排資深專家擔任分組指導員（Subgroup Instructor），指導學員進行設施探討、弱點偵測與設計補強等。

最後的成果報告，延續前次（ITC-26）的作法，使用拉卡錫國另外兩個虛擬核設施，包括一個研究用反應器（Hypothetical Atomic Research Institute, HARI）、及一座核電廠（Lone Pine Nuclear Power Plant, LPNPP），進行整體實體防護系統設計。學員需運用自課程中獲得的專業知識，以及自行設計 PTR 的實體防護中所學習到的經驗，自行設計、建構及評估改善上述兩個虛擬核設施之實體防護系統，結訓前須完成製作成果報告，並於訓練最後一天上台報告，接受講師及其他學員之提問及指教。

分組實作期間，各課程講師均會前往各分組指導，協助實作進行。本次參訓被分配到的小組，有來自加拿大、泰國、摩納哥、剛果、哈薩克、波蘭、斯洛伐尼亞等成員，背景有核能管制機關、警察、核設施運轉員等，另由聖迪亞國家實驗室「國際實體保安計畫」資深專家 Carrie O'Hara 擔任指導員，她是聖迪亞國家實驗室負責應變武力教育訓練的專家群之一。

為增加學員身歷其境的臨場感，主辦單位在戶外場地，展示包括電鋸、鋼鋸、電鑽、鐵剪、鐵鎚及焊槍等歹徒常用破壞工具，並由主辦單位工作人員現場操作，破壞鐵條、鐵絲網、鋼板、木板等常用以做為延遲屏障（Delay Barrier）材料，並由學員實地以碼表記錄完成破壞之時間，藉以瞭解運用不同工具破壞不同延遲屏障材料的難易程度。

主辦單位安排學員參訪位於科特蘭空軍基地（Kirtland Air Force Base）內，隸屬美國能源部的「國家實彈射擊訓練中心」及「實兵對抗演練場」，觀看訓練中心射擊教官進行手槍、步槍、輕機槍及槍榴彈發射器等各類型武器實彈射擊，體驗不同武器射程威力，以及聽取射擊教官說明如何訓練學員進行實兵對抗演練，以有助於學員完成包括情境分析、兵棋推演等課程應用。

此外，也安排學員參觀同樣位於科特蘭空軍基地內的「保護區圍籬測試場」(Test Field)，現場觀察包括雷射(Laser)、震動(Vibration)、拉力(Taut Wire)、紅外線(Infrared)、微波(Microwave)、電場(Electric Field)、光纖(Optical Fiber Cable)與影像移動式(Video Motion Detectors)等不同功能用途之各型感測器運用實況，並由學員以分組為單位於各圍籬現場，實際測試感測器靈敏度及感測範圍，並完測試紀錄。

主辦單位安排本組測試延遲測試程序(Dealy Testing Procedure)，實際測試歹徒入侵雙重圍籬、移動至儲存核子原料的緊要區、破壞門鎖至偷走核子原料並成功脫逃等所需的時間，並得到如以下結論：自歹徒成功破壞核子原料貯存場所門鎖並偷走所花時間最短，因此可在此處加強延遲項目（如增加雙重鎖扣），以讓廠內應變武力可及時抵達並弭平歹徒。以上實作練習應用為分組結訓成果報告時，設計、建構及強化整座核能電廠實體防護系統之參考。

圖 1 ITC-27 全體學員及工作人員合影

二、課程內容

國際核子保安訓練課程設計安排，係以核設施實體防護系統（Physical Protection System, PPS）建構過程的：「確認實體防護系統需求」(Define PPS Requirement)、「實體防護系統設計」(PPS Design)、「實體防護系統評估」（PPS Evaluation）三步驟為主軸，PPS 整體建構流程稱作「實體防護設計與評估流程」(Design and Evaluation Process

Outline, DEPO），依據建構流程及其內容計有 28 項專業課程，課程（如圖 2）及各項課程簡介說明如下：

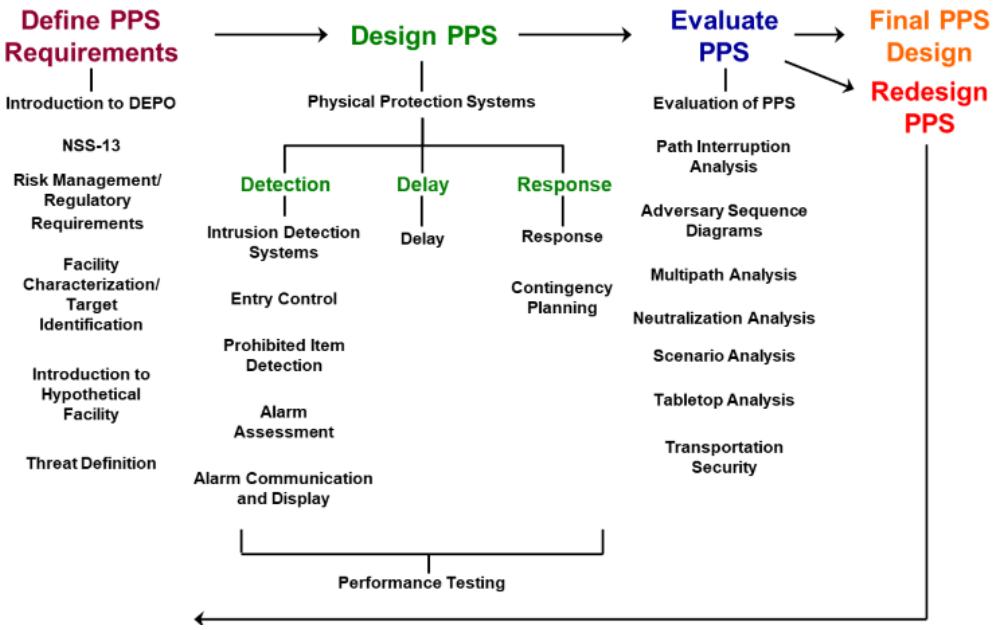


圖 2 實體防護設計與評估流程及其相關專業課程

1. 步驟一：確認實體防護系統需求（Define PPS Requirement），亦即確立實體防護需保護之標的物及定義威脅來源，作為後續系統設計及評估基礎，相關課程內容簡要說明如下：

(1) 實體防護設計與評估流程介紹（Introduction to the DEPO）：

核子保安系統最重要的目的係防止可被用來製造核子武器的核物料於使用、儲存或運輸過程中失竊（Theft），以及保護核設施免於遭受恐怖暴力攻擊（Sabotage）。建構核子保安系統須依照「實體防護設計與評估流程」（Design and Evaluation Process Outline, DEPO）三步驟，依序為「確認需求」（Define Requirement）、「設計」（Design）、「評估」（Evaluation）。

第一步為確認需求，包括：依據核設施的特性，確立防護標的與預期威脅，並據以制定設計基準威脅（Design Basis Threat, DBT），同時也需做好風險管理及滿足法規要求。

第二步為設計核子保安系統之偵測（Dectecion）、延遲（Delay）與應變武力（Reponse）等三大功能，設計時須將「深度防禦（Defence

in Depth）」與「平衡設計（Balanced Design）」原則納入考量，才可建構有效的系統。

最後則是以計算系統效能值（P_E）之效能基礎（Performance-Based）方法，評估所設計之系統是否符合防護需求，如未符合則須重回第二步修改設計，直至符合需求為止。

(2) 國際原子能總署核子保安系列第 13 號(IAEA Nuclear Security Series No.13, NSS-13）報告書（即 INFCIRC/225/Rev.5）建議：

INFCIRC/225 自 1975 年發表第 1 版起，已成為核子保安系統的國際標準，並於 2011 年 1 月發表第 5 版修正（後續更名為核子保安系列第 13 號, NSS-13）。本課程說明 NSS-13 建議內容，包括建構國家實體防護所需之「防止非法竊取核物料（To Protect against Unauthorized Removal）」、「尋回復原失竊核物料（To Locate and Recover Missing Nuclear Material）」、「防範破壞核設施（To Protect against Sabotage）」及「減輕核設施破壞後果（To Mitigate or Minimize Effects of Sabotage）」等四大目標。

另介紹核物料實體防護公約（Convention on the Physical Protection of Nuclear Material, CPPNM）修正版之 12 條基本原則（包含責任界定、國際運輸、深度防禦、安全文化、品質保證等），以及核物料在使用、儲存及運輸時之相關防護建議等，最後特別增加了一項關於資訊安全的規定：用於實體保護、核子保安以及核物料控制的電腦系統和網路必須採取防護措施，以防止網路攻擊、數據操縱或篡改等威脅。

(3) 風險管理與管制要求（Risk Management and Regulatory Requirements）

本課程定義了保安風險與安全風險的差異，所謂保安風險為因個人或團體惡意行為對未來造成傷害或損失的可能性，是由「人」的行為產生的可能性損失，而事件的發生並非隨機的；安全風險則是因一異常的起始事件造成傷害或損失的可能性，其發生機率是隨機的。

風險管理是一種用來降低或減輕因非預期事件發生造成風險的方法。並介紹機率量化風險的觀念，包含自偷竊或破壞可能造

成之後果，找出相應措施，以降低非預期事件發生的機率；另一方面，透過提高防護措施有效性，藉以提升實體防護系統的效能（P_E），以降低攻擊後果發生嚴重性。國家及管制機關則可運用訂定規範（Prescriptive Approach）或效能考核（Performance-Based Approach）方式，檢視業者是否滿足法規管制要求。

(4) 核設施的特性與目標的界定（Facility Characteristization / Target Identification）

為了滿足實體防護系統設計及評估之需要，必須針對核設施的運轉、環境、安全、法規及營運特性等，先進行背景資料蒐集，確認可能遭受的威脅。本課程主要防護目標著重於破壞（避免核物料或核設施遭受破壞產生不可接受的輻射外釋）及偷竊（主要係針對核物料），並依據 NSS-13 之「核物料分類表」（Categorization of Nuclear Material）介紹目前國際最主要之核物料防護等級分類等相關內容，以及訂定核設施緊要區（Vital Area）的步驟等。

(5) 虛擬核設施的介紹（Introductuion to the Hypothetical Facility）

介紹某虛擬國家「拉卡錫（Lagassi）」醫學及物理研究所內，設有水池式反應器（Pool Type Reactor, PTR）、中子反應器（Neutron Burst Reactor, NBR）及放射性廢棄物儲存區等核設施，設施平面圖如圖 3。

課程詳細描述各項設施之規模、設備、位置、佈局，及其現有實體防護設計所使用之各項資料，包含偵測、延遲設備數量，警衛、應變武力組織與日、夜間運作模式等，並輔以簡化之核設施平面圖，具體顯示相關核設施防護現況，包含廠區及各設施的實體區域，相鄰區域間之防護層，及各防護層中包括門窗、牆壁、天花板等防護材料，另提供 3D 電腦動畫模型，讓學員們更加瞭解該核設施結構、運作方式及現行實體防護部署，俾利進行後續一系列設計改良分組實作課程。

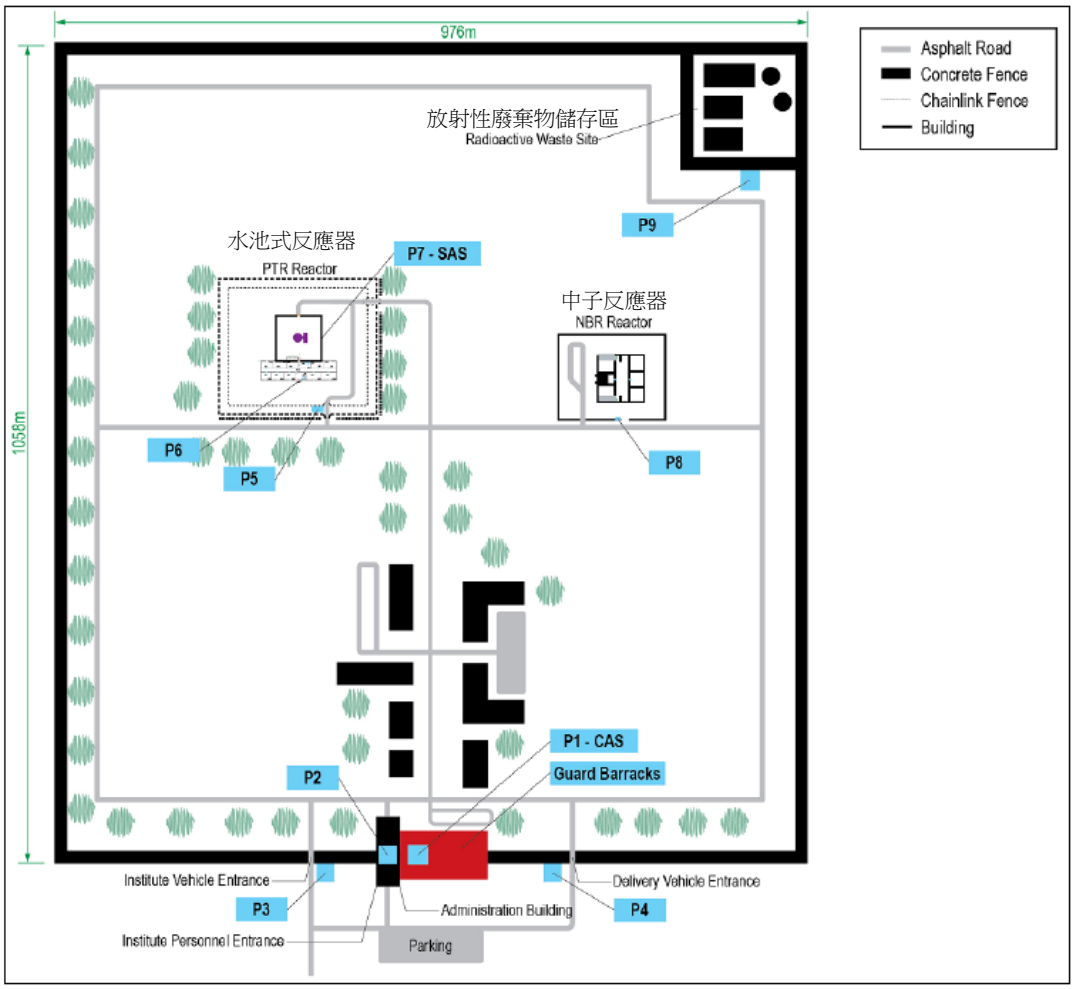


圖 3 拉卡錫核設施平面圖

(6) 威脅定義（Threat Definition）

偷竊（Theft）與暴力攻擊（Sabotage）是實體防護系統對抗之二大威脅，設計者必須以假想可能最大威脅作為實體防護系統設計基準，此一威脅定義為設計基準威脅（Design Basis Threat, DBT）。

本課程介紹評估及制定設計基準威脅的步驟如下：

a. 檢視具可靠來源的威脅情資，例如：歷史情結、地域衝突、恐怖組織類型等。

b. 調查攻擊動機或意圖，例如：意識形態、謀財或報復。

c. 評估犯案能力，例如：人數、武器類型、爆裂物類型與數量、輔助攻擊工具、運輸、移動、專業知識以及內部破壞者等。

經彙整以上資訊後，從中篩選、組合而成各種可能對核設施造成威脅的類型，再考量核設施所能接受最大風險，以決定實體防護系統設計之設計基準威脅。

在評估設計基準威脅時，所參考的背景情資之可靠度非常重要。若低估風險，設計出的實體防護系統將無法抵抗威脅，反之，則會造成資源浪費。

依「核子物料與核設施之實體保護」建議內容，各會員國宜自行訂定設計基準威脅，並據此擬定核設施之保安計畫，而核設施與核物料等均須置於具有實體防護系統且能有效防禦威脅的場所。

2. 步驟二：實體防護系統設計(PPS Design)，依據保護標的與威脅來源，設計實體防護系統，相關課程為概述如下：

(7) 實體防護系統設計簡介（Introduction to the Design of Phyicl Protection Systems）

有效的實體防護系統設計，包括「嚇阻」（Deter）、「打擊」（Defeat）歹徒等二大策略，課程內容為：實體防護系統設計三大功能（偵測、延遲及反應）設計過程、防護系統工程設計原則（深度防禦、平衡設計及可靠度要求）、衡量效能方式（計算偵測機率、延遲時間、應變時間、攔截機率及弭平機率），以及內部破壞者（Insider）之防範措施等。

(8) 入侵偵測系統（Intrusion Detection Systems）

為防範入侵行為，偵測系統應具備入侵偵測之功能，在異常狀況下，偵測器應發出警報信號。應用範圍包括：歹徒入侵偵測器（通常設置於核設施周界與核設施建物）、偵測器發出警報信號的傳遞與顯示及評估、門禁管制（Access Control）及違禁品管制（Contraband Control）等。

偵測器的選擇必須考量偵測機率（Probability of Detection）、誤動作率（Nuisance and False Alarm Rates）與弱點（Vulnerability to Defeat）。一般來說，偵測率愈高愈能發現非法侵入，但誤動作率也會提高，增加了保安人員的負擔，因此如何選擇最佳的偵測器，需在兩者間進行取捨。

最後，因不同的偵測器有不同的弱點及適用環境，因此，在選用偵測器種類時，必須對背景環境、氣候條件、偵測標的、偵測效率等作通盤考量；不同形式偵測器間亦可相互搭配使用，以建立完整連續的偵測系統，提高成功偵測的機率。

感測器可依其技術原理、偵測方式及佈置方式加以分類：

a. 依技術原理：可分為雷射（Laser）、震動（Vibration）、拉力（Taut Wire）、紅外線（Infrared）、微波（Microwave）、電場（Electric Field）、光纖（Optical Fiber Cable）與影像移動式（Video Motion Detectors）等。

b. 依偵測方式：可分為隱藏式（Covert）或外顯式（Visible）、線偵式（Line Detection）或體偵式（Volumetric Detection）、主動式（Active）或被動式（Passive）。

c. 依佈置方式：可分為埋地型（Buried-Line）、圍籬型（Fence-Associated）或立柱型（Freestanding）等。

各類型偵測系統功能之特性上亦有錯誤接受率（False Acceptance）與錯誤拒絕率（False Rejection）等不同差異。基本上，使用在內圈區域（即保護區、緊要區及內部區）應儘量選擇錯誤接受率低產品，以提高偵測效率。在外圍區域（限制區）若因成本考量，則稍可容忍使用錯誤拒絕率高產品，以避免因天候牽動或動物誤觸等誤動作發生，增加保安監控之負擔。

(9) 門禁管制（Entry Control）

目的在建立保護區域，其功能為僅允許獲授權人員的進出，並監控保護區域進出狀況。本課程介紹不同類型門禁管制系統的原理，包含依據進出人員所知道的〔如密碼（PIN）〕、所擁有的（如識別證、鑰匙）、天生的生物識別特徵（如指紋）、虹膜（Iris）及語音辨識（Voice Recognition Identify Verification）等特性加以設計。

不同門禁管制系統各有其優點及限制，例如識別證可以很快速的通過門禁，但是被盜用的機率也高，所以，在選擇門禁管制系統時，也需進行通盤考量，不同特性的檢查方式若能搭配使用，可提升實體防護系統的有效性。

良好的門禁管制系統，須考量下列因素：無法輕易被旁通、人員可監視、可提供應變武力人員防護、檢查過程中可隔離受檢者、針對未通過系統查驗者執行人工檢查及全程均由保安監控中心監看等。

(10) 違禁品偵測（Prohibited Item Detection）

就核設施而言，違禁品包括：武器、爆裂物、工具、攝影器材及放射性物質等。當人員、行李、車輛進出保安區域時，須執行違禁品偵測，通常只允許經授權物品的進出，並限制違禁品（如武器、破壞工具、爆裂物）進入及管制核物料的流出等。其管制項目必須依據所訂定的設計基準威脅來評估歹徒可能攜帶的違禁品種類或攜帶方式，並依照不同保安層級區域調整限制措施。

違禁品的偵測方式有以下幾種類型，包含人工檢查、金屬偵測（用以檢查是否攜有武器、配壞工具、爆裂物及智慧型手機等）、X 光掃描（用以檢查行李、背包有無夾帶違禁品)及輻射偵測器(用以檢查放射性物質)等。其中，以人工檢查（含緝毒犬）具備高機動性及敏感度但較費時，且起始成本雖低但維護成本高；若改以儀器偵測雖成本較高，但相對節省檢查時間。因此要建立一個良好的違禁品管制偵測系統，亦可搭配不同種類的偵測方式，以提升對違禁品偵測的有效度。

(11) 警報評估（Alarm Assessment）

警報評估是入侵偵測系統的最後一環，偵測後若發現異常，系統應立即發出警報，判斷是否為雜訊幹擾（如天候）或異物（如動物）誤觸，並評估警報內容，提供應變武力正確的訊息以迅速弭平入侵。如僅有警報而無法評估及判斷狀況，則警報偵測系統無法發揮功能。

評估可分為人力評估及科技評估兩種，人力評估包括由警衛、應變武力或當地員警進行人工評估；科技評估主要係透過影像系統進行自動評估。人力評估優點為機動性較強，可適用於特殊狀況，但缺點則是人力成本高；而科技評估優點為可長時間連續性的監測，並記錄相關影像，缺點是儀器後續維護費用高。科

技評估最主要是透過影像系統執行自動評估作業，影響影像評估系統效能最主要的三大因素則為：相機、鏡頭及光源。

因此，在建置影像評估系統時，必須針對核設施周遭不同環境、天候（如下雨、下雪、霾及霧）等狀況，搭配不同的影像組合，建構一全時性且具有完整覆蓋範圍的偵測器統，並避免造成誤判，或因攝影角度不當而產生視線死角，形成偵測漏洞。常見的影像系統包括：閉路電視系統（Closed Circuit Television, CCTV），熱成像攝像機（Thermal Cameras）及影像動作感測器（Video Motion Detection）等。

(12) 警報通訊與顯示（Alarm Communication and Display）

其主要功能是將實體防護系統蒐集到的各項資料（例如:入侵偵測警報、門禁管制、CCTV 影像監視與評估等）提供給相關應變人員（例如：警衛、應變武力等），於不法份子入侵時能及時有效應變；此外通訊系統應考慮其資料傳輸保密性且不易遭受干擾，系統顯示方式最好將人因工程納入考量，並依重要性分層顯示，以便監看人員能掌控全部狀況，一旦發現異常能立即通報給相關應變人員及時處理緊急情況。

(13) 延遲（Delay）

針對入侵者可能選擇之途徑，預先或臨時設障礙物以延遲入侵者行動，增加其作業時間，並替應變武力爭取時間，讓應變武力能及時抵達現場阻止入侵者行動。核設施中典型之兩種屏障系統為：

a. 被動型屏障（Passive Delay）：一般而言，稱之為「結構屏障」（Structural Barrier），屏障效果最為直接確實，例如廠界圍牆、大門出入口、車輛進出通道、牆壁、門窗、屋頂、樓地板等。

b. 主動型屏障（Active Delay）：需要啟動，又分為散佈材料屏障（Dispensable Barrier），例如運用煙霧、泡沫、黏著劑等方式延緩敵人動作及行進；及彈出式車輛屏障(Pop-up Vehicle Barrier)。除此，崗位駐警也具有遲延功能。

一般而言，良好屏障應具有：偵測到異常時可立即發揮延遲作用、同時也需考量平衡設計及深度防禦等特性。

(14) 應變武力（Response Force）

不同於一般警衛（Guard）負責檢查、監視、通報及防止未獲授權人士及物的進出等例行勤務，應變武力屬於具特種戰鬥能力的快速打擊部隊，主要職責有二：其一為當接獲歹徒入侵之通報後，必須及時趕往歹徒所在地或欲破壞的目標，執行攔截並阻止其行為；其二為狙殺或逮捕歹徒以防止其達成破壞目的。

成功的攔截，必須依靠精確的偵測、警報評估、可靠的通訊傳遞及是否能及時趕往歹徒所在地或目標地點等。一個完整的實體防護系統時間計算是從第一次警報成功偵測至應變武力趕往目標地點的時間，包含與應變武力之通訊、準備、集合、部署及行動等所需之時間，不包括應變武力對抗威脅或是阻止歹徒完成破壞目標的這段應變時間。因此需精確評估應變時間能否及時制止歹徒不法活動。建置應變武力亦需有周詳的計畫、訓練合格的人員、精實的訓練以及確切的評估過程，並需經常進行實兵對抗演練，以維持任務執行效率及能力。

(15) 核子計畫方案（Nuclear Program Plans）

相對於核能安全（Nuclear Safety）的緊急計畫（Emergency Plan），核子保安（Nuclear Security）對於核物料的偷竊及核設施的破壞等，須事先擬定「保安計畫（Security Plan）」，保安計畫是核設施平時整備的一部分。計畫的內容包含：目的、範圍、威脅想定情況、運作概念、計畫發展及維護等項目，同時也包含針對偷竊或惡意攻擊採取應對的保安應變計畫（Contingency Plan）。保安應變計畫內容重點包括：通訊聯繫、資源共用、各友軍間合作支援及聯合演習等項目，需定期訓練、測試及評估，並視需要定期檢視更新。

(16) 效能測試（Performance Testing）

包含針對偵測、延遲及應變武力等的效能測試。測試型態包括操作及功能測試（Operability and Functional Tests）、子系統測

試（Subsystem Performance Test）、全部系統測試（Whole System Performance Tests）及評估測試（Evaluation Tests）。測試流程首先要規劃一個測試方案、接著針對該方案測試的結果進行蒐集、分析並記錄結果，其目的在於評估實體防護系統成功偵測到不法入侵的機率及應變武力成功攔截並制伏不法份子的機率。

3. 步驟三：實體防護系統評估（Evaluation of Physical Protection Ssystems），係運用效能基礎（Performanc-based）方法，量化評估分析實體防護系統及其效益，是否足以排除設計基準威脅（DBT），相關課程簡述說明如下：

(17) 實體防護系統評估（Evaluation of Physical Protection Ssystems）

實體防護系統的有效性（P_E）可藉由 P_I 值及 P_N 值來決定，能將實體防護系統的有效性以量化方式呈現，〔$P_E = P_I \times P_N$ ，P_I＝實體防護系統成功攔截（Interruption）威脅的機率，P_N＝PPS 成功弭平（Neutralization）威脅的機率〕，P_I 值可由「路徑分析」方式獲得。當防護標的與歹徒入侵路線確認後，於路經分析程式中輸入相關參數後，即可由電腦軟體程式計算最後的結果，課程中使用的路徑分析程式係聖迪亞國家實驗室自行開發的教學程式，原則不對外開放。P_E 值除可由「情境分析」方式獲得外，亦可由兵棋推演及實兵對抗等方式得出。

(17) 路徑攔截分析（Path Interruption Analysis）

根據所有歹徒可能入侵的途徑，分析實體防護系統中有效偵測時間點及後續延遲時間後，能計算出 P_I 值，其值等於 1－（關鍵偵測點前各點偵測設備失敗機率乘積），其中關鍵偵測點（Critical Detection Point, CDP）係最後一個可及時阻止歹徒入侵的時間點。例如關鍵偵測點前若有三個偵測點 D_1、D_2 及 D_3，其相對成功偵測機率為 P_{D1}、P_{D2} 及 P_{D3}，則 $P_I=1-(1-P_{D1})(1-P_{D2})(1-P_{D3})(1-P_{CDP})$。關鍵偵測點可利用歹徒完成任務時間軸（Adversary Timeline）與實體防護系統應變時間軸（Response Timeline）找出，概念如圖 4，入侵偵測系統必須於關鍵偵測點之前發出警報，才能有效攔截歹徒行動。

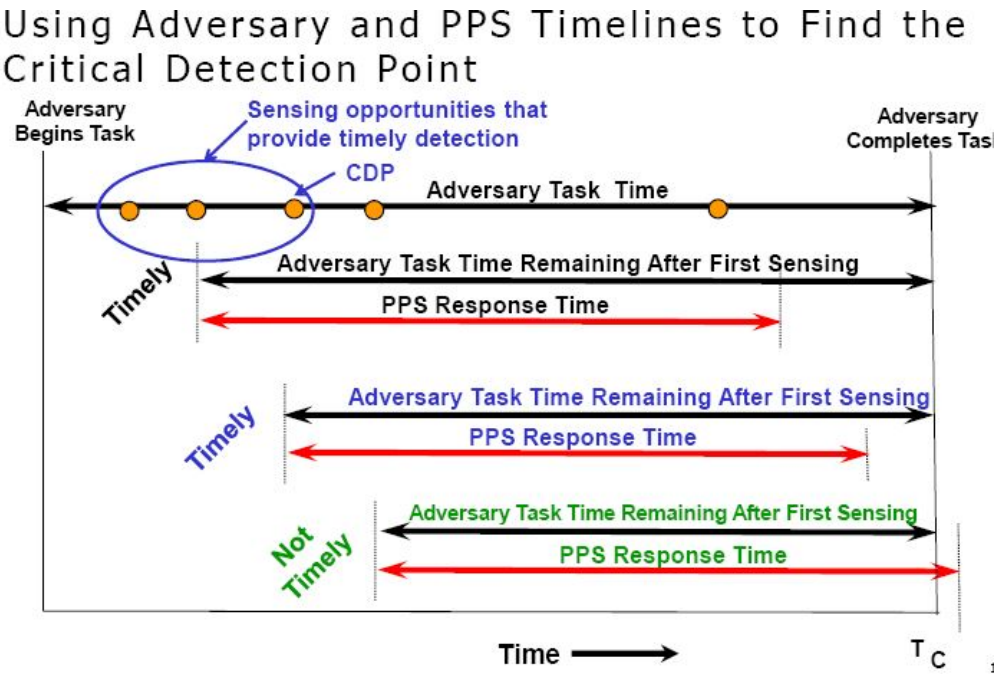


圖 4 關鍵偵測點概念示意圖

(18) 侵入者滲透入侵路徑圖（Adversary Sequence Diagrams, ASD）

依據現場實況，設定目標物及歹徒所有可能入侵路徑，繪出詳細的路徑順序，概念如圖 5。首先需定義出各實體區域（Physical Areas）、各防護層（Protection Layer）及防護標的物，接著針對各實體區域分配最小偵測機率及延遲時間，最後建立出滲透入侵路徑圖模型，藉此實際評估實體防護系統在防護上的優弱點。

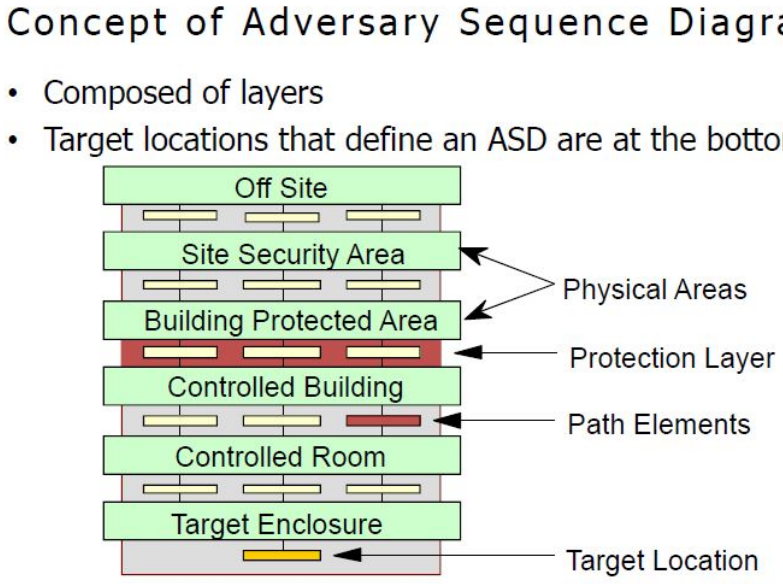


圖 5 滲透入侵路徑示意圖

(19) 多重路徑分析（Miltipath Analyis）

歹徒入侵通常會有很多可能路徑，為了評估最脆弱的路徑，聖迪亞國家實驗室開發 MPVEASI 軟體（Multi-Path Very-simplified Estimate of Aversary Sequence Interruption, MPVEASI）來算出歹徒最可能入侵到目標物的途徑，亦即算出最脆弱之路徑。

執行方式有三步驟，首先需輸入歹徒入侵路徑圖數據，包括每一區域或標的物之偵測機率及其延遲時間，接著輸入應變數據，包括實體防護系統的應變時間及應變策略（針對直接武力、祕密行動或欺騙等三種情形採取的策略），最後按下分析功能鍵得到輸出結果，該結果即歹徒最可能進行滲透入侵的途徑。

(20) 弭平能力分析（Neutralization Analysis）

假設敵我雙方之武器裝備、人員素質等客觀條件均一致的前提下，可透過查詢聖迪亞國家實驗室提供之表 2「不同敵我數量弭平機率對照表」來得出成功弭平威脅之機率：P_N（Probability of Neutralization），惟表 2 係聖迪亞國家實驗室提供之參考資料，理論上各國均應參考設計基準威脅建立自己的數據。

表 2 不同敵我數量弭平機率對照表

Number of Adversaries	Number of Responders																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	0.50	0.83	0.96	0.99	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
2	0.17	0.50	0.78	0.92	0.98	0.99	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
3	0.04	0.23	0.50	0.74	0.89	0.96	0.99	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
4	0.01	0.08	0.26	0.50	0.72	0.86	0.94	0.98	0.99	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
5	0.00	0.02	0.11	0.28	0.50	0.70	0.84	0.92	0.97	0.99	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
6	0.00	0.01	0.04	0.14	0.30	0.50	0.68	0.82	0.91	0.96	0.98	0.99	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
7	0.00	0.00	0.01	0.06	0.16	0.32	0.50	0.67	0.81	0.90	0.95	0.98	0.99	1.00	1.00	1.00	1.00	1.00	1.00	1.00
8	0.00	0.00	0.00	0.02	0.08	0.18	0.33	0.50	0.66	0.79	0.88	0.94	0.97	0.99	0.99	1.00	1.00	1.00	1.00	1.00
9	0.00	0.00	0.00	0.01	0.03	0.09	0.19	0.34	0.50	0.65	0.78	0.87	0.93	0.96	0.98	0.99	1.00	1.00	1.00	1.00
10	0.00	0.00	0.00	0.00	0.01	0.04	0.10	0.21	0.35	0.50	0.65	0.77	0.86	0.92	0.96	0.98	0.99	1.00	1.00	1.00

Probability of Neutralization for Different Numbers of Adversaries and Responders

(21) 情境分析（Scenario Analysis）

情境分析是一種分析實體防護系統有效性（P_E）的方法，藉由考慮不同的攻擊情境，包括歹徒採取偷竊或破壞之攻擊方式、可能採取的路徑、具備的專業知識水準及所擁有的資源等，來分析包含核設施之實體防護系務統整體防禦能力、保安應變計畫、

保安政策與程序及跨單位支援協調等各方面的弱點，作為後續改進之參考。

(22) 兵棋推演分析（Tabletop Analysis）

兵棋推演可將人員分成攻擊方（Adversary Team）、防守方（Guard and Response Force Team）、評估組（Evaluation Team）及裁判組（Exercise Moderator）等四組，主要用於模擬歹徒攻擊設施時，評估實體防護系統效能。攻守雙方針對假想的攻擊情境進行模擬推演，特別在重要事件發生點（例如歹徒何時破壞偵測設備進入廠區、何時抵達目標物執行偷竊或破壞、應變武力何時與歹徒進行對抗等）進行討論並記錄結果，結束之後評估核設施實體防護系統之防禦弱點，進而提出改善建議。

(23) 運送安全（Transportion Security）

運送型式可分為空運、海運、陸運，運送威脅包含遭遇海盜、脅持、埋伏及破壞等。關於核物料運送之實體防護系統設計，原則上是比照固定廠區（Fixed Site）核設施「實體防護設計與評估流程」，惟兩者最大不同處在於運輸是以動態方式進行，故無法建立保護區，且路徑會隨環境變化，因此評估過程改以「情境分析」取代「路徑分析」，且通常偵測時間無法提前，所以須加強延遲功能以爭取應變時間，另外偵測、評估、通訊及應變、請求外援等工作，亦需全由押運應變武力負責處理。

4. 其他補充課程，簡述說明如下：

(24) STAGE 軟體介紹（Simulation Tookit and Generation Environment, STAGE）

STAGE 軟體係由聖迪亞國家實驗室開發來評估 P_N 值，這套軟體必須輸入大量的實測數據以獲得較準確的結果。其優點可以透過 3D 立體的方式模擬歹徒入侵路徑，另一方面可呈現應變武力接獲通報後趕赴現場部署、與歹徒交鋒並弭平事件的過程，因此可以從中獲得核設施實體防護系統需改進的地方。

(25) 核物料料帳管理與控制系統（Nuclear Materials Accounting and Control）

現行的核設施實體防護系統，主要應用於防範外部攻擊，無法針對內部破壞者偷竊核物料的行為有相應防範措施。依據NSS-13 建議，核設施運轉員必須有能力確保掌控核設施內所有核物料的數量、類型及儲放位置。

核物料料帳管理與控制系統的功能是透過整合行政及技術的措施，對於核物料的儲存，透過建立一套完整的庫存追蹤系統，協助設施經營者能完全掌控有關在設施內核物料的所有資訊，以降低失竊風險。該系統主要應用於偵測由內部破壞者未經合法授權的使用或提取核物料，亦可用來偵測長時間微量偷竊核物料的行為；在失竊事件發生時，可用來追查遭竊核物料的種類及數量，以掌握追查目標，儘速採取相應補救措施。

(26) 針對內部破壞者威脅的預防及防護措施（Preventive and Protective Measures Against Insider Threat）

內部破壞者主要具備有三項特性，包含可接近（Access）、獲授權（Authority）及具備核設施相關知識（Knowledge）。其動機方面需考量是否具有意識形態（包含對於政治或宗教狂熱）、個人財務問題、身心狀況及是否遭人脅迫等。

為了降低此類人員成為內部破壞者的風險，可以在雇用人員前進行一些安全查核，例如透過背景查核確認有無犯罪紀錄、信用查核可確認有無財務問題、利用醫療檢驗確認有無身心方面問題、藥物篩選確認有無濫用藥物等。

(27) 核子保安可信賴計畫介紹（Introduction to Nucler Security Trustworthiness Programs）

核子保安可信賴計畫能夠幫助確認在核設施中擔任重要職位人員品性是否正直、可信賴、及可勝任該職位。另外所有核設施的風險須考慮到「人」的因素，在預防保安事件發生方面，人員扮演一個正面的角色，但是在某些情況下人員也可能扮演一個

負面的角色，例如：人員缺乏保安意識、疏忽、甚至可能是內部破壞者。

(28) 資訊安全（Information Security）

類似實體防護系統，資訊安全可採用深度防禦概念來防護，先將廠內系統依據重要性加以分類，最重要的系統（例如安全系統）可採取最嚴密的防護措施、次重要的系統則採用嚴密的防護、較不重要的系統則採行原則性的防護。

另外確保資訊安全作法可分為以下三方面：

a. 行政面（Administrative）：針對電腦的使用進行管制，並告知工作人員電腦使用規範。

b. 實體防護面（Physical）：對於電腦、數位系統及網路設備、特殊伺服器所在區域，應加強實體防護（例如增加門鎖、安排電腦使用監管人員及防火設備等）。

c. 技術面（Technical）：架設防火牆、防毒軟體、進出管制等。

上述 28 項課程完成後，訓練倒數 2、3 天為「學員討論」期間，每一位學員均須於分組研究室中相互討論、腦力激盪（討論過程如圖 6、圖 7），合作完成「結訓成果報告」簡報，成果報告須充分運用訓練課程所學知識，以及分組實作水池式反應器（PTR）時計算、討論之結論及經驗數據，依組別題目分別設計虛擬核設施之實體防護，並自我評估、量化系統防護效能，若有不足處須再檢討、精進防護措施，直至達成防護目標值為止。

本次虛擬核設施有二項：其一為研究用反應器（Hypothetical Atomic Research Institute facility，HARI）、另一為核電廠（Lone Pine Nuclear Power Plant，LPNPP），本次依照主辦單位規劃為針對 HARI 進行整體實體防護設計及評估。

訓練最後一天為「結訓成果報告」，全體學員以分組為單位，依抽籤順序上臺報告 20 分鐘，所有學員皆須上臺報告（報告過程如圖 8），並接受所有講師、分組指導員及全體學員的質詢及指正，最後由班主任講評，合格學員即可獲頒結訓證書（結訓成果報告簡報資料如附件）。

圖 6 分組研討-資料蒐集

圖 7 分組研討-路徑分析

圖 8 結訓成果上臺報告

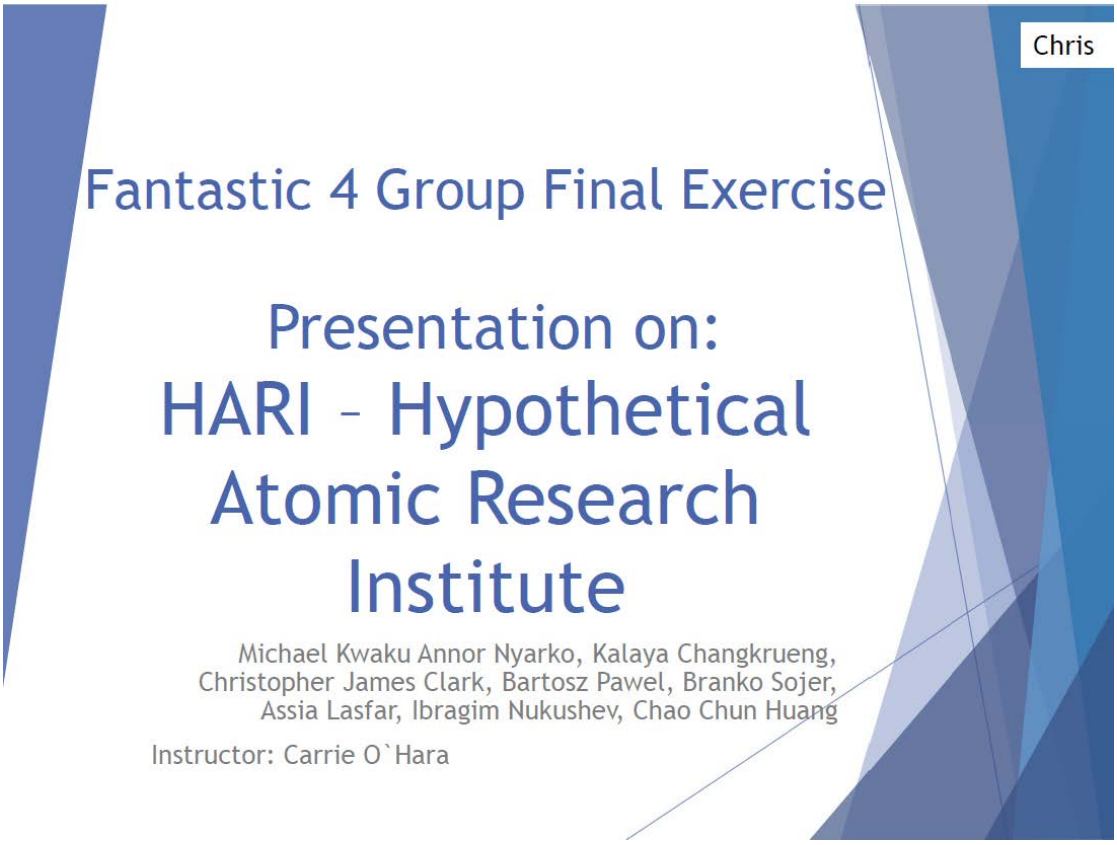
肆、 心得及建議

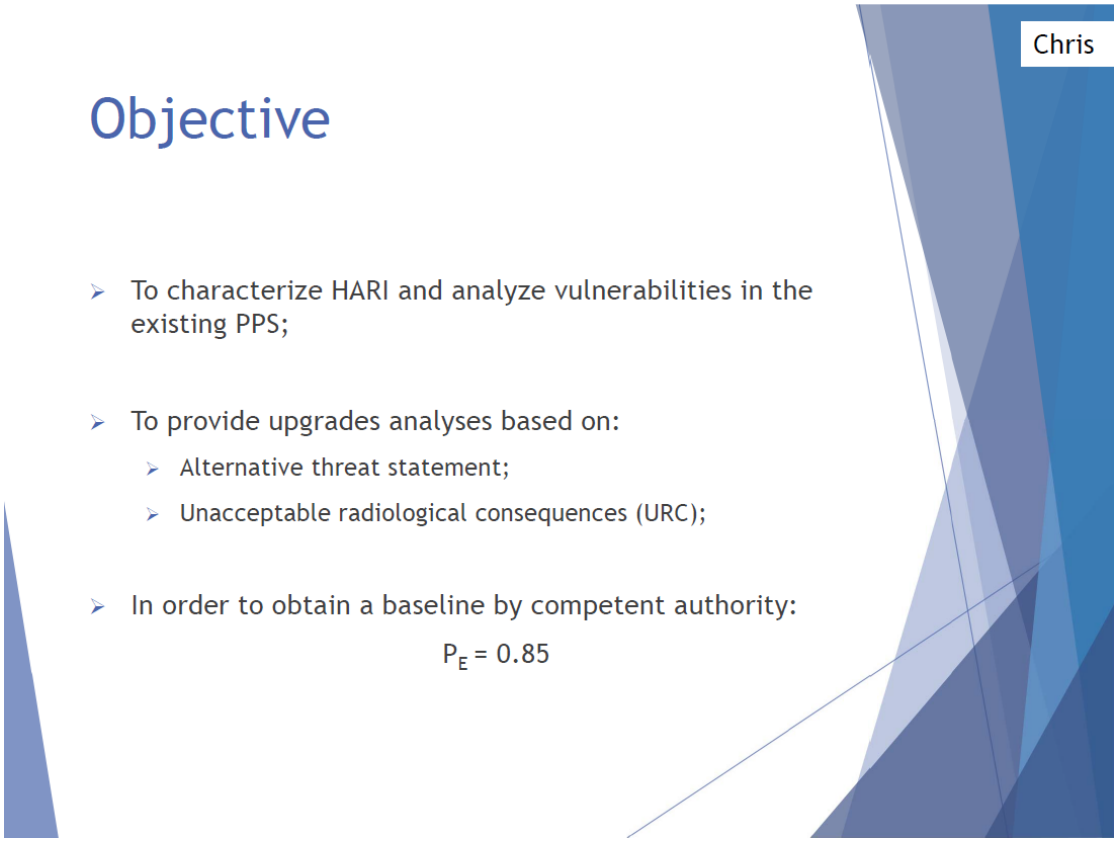
一、 影響核子保安三要素為「人員」、「設備」、「程序」，其中最重要的因素就是「人員」，故核能電廠應建立良好的核子保安文化，以降低由內部破壞者造成實體防護失效。因此如何有效地落實核子保安文化，有賴業者持續的努力。

二、 核子保安同緊急應變，均屬隱而不顯的業務，亦即其績效不易彰顯出來，惟核能電廠屬於國家關鍵基礎設施之一，核能電廠仍應做好相關核子保安工作，杜絕可能潛在危險，以確保核能電廠運轉及工作人員安全。

三、 我國雖非 IAEA 正式會員國，本次訓練係以觀察員（Observer）身分參加，透過台美民用核能合作會議，台美雙方達成加強保安議題交流之共識，並將該訓練納入「台美民用核能合作計畫」合作項目後，多年來我國均獲邀參加，參訓人員不僅可從課程中學習到專業的保安識能，還與各國學員交流，從中瞭解不同國家之核能電廠的實體防護，對於管制機關及設施經營者本身都是一大助益，建議能持續派員參與學習，特別是設施經營者更應派員參加。

伍、附件


Chris
Fantastic 4 Group Final Exercise
Presentation on:
HARI – Hypothetical Atomic Research Institute
Michael Kwaku Annor Nyarko, Kalaya Changkrueng, Christopher James Clark, Bartosz Pawel, Branko Sojer, Assia Lasfar, Ibragim Nukushev, Chao Chun Huang
Instructor: Carrie O`Hara


Chris
Objective
To characterize HARI and analyze vulnerabilities in the existing PPS;
To provide upgrades analyses based on:
Alternative threat statement;
Unacceptable radiological consequences (URC);
In order to obtain a baseline by competent authority:
$P_E = 0.85$

Define Problem and determine PPS Requirements

Branko

- Facility Characterization (Vital Areas)
  - Control Rod Drive Bridge
  - Reactor Block / Pool Tank Wall
  - Both Heat Exchanger rooms (2)
- Target identification
  1. Control Rod Drive Bridge (600s)
  2. Reactor Block / Poll Tank Wall (900s)
  3. ECCS Water Tank (300s)
  4. Both Heat Exchanger rooms (600s)
- Use State DBT
- Create ASD and Response Force Time
- Path analysis by MP VEASI Software

State DBT for Lagassi Country

Branko

Likelihood of Potential Action	
Theft	XX
Sabotage	High (Antinuclear terrorism)
Other	
Motivations	
Ideological	High (Antinuclear terrorism)
Economic	Low
Personal	Low
Capabilities	
Number of attackers	2
Type of weapons	Sub magazine gun, sub automatic pistol
Explosive (type and quantity)	N/A
Transportation	Vehicle
Power and hand tools	Portable manual tools and power tools
Technical skills	Skills -weapons, communication, vehicle, well trained
Level of funding	N/A
Infrastructure Collusion with Insider (passive or active)	1 Passive/non-violent insider

Branko

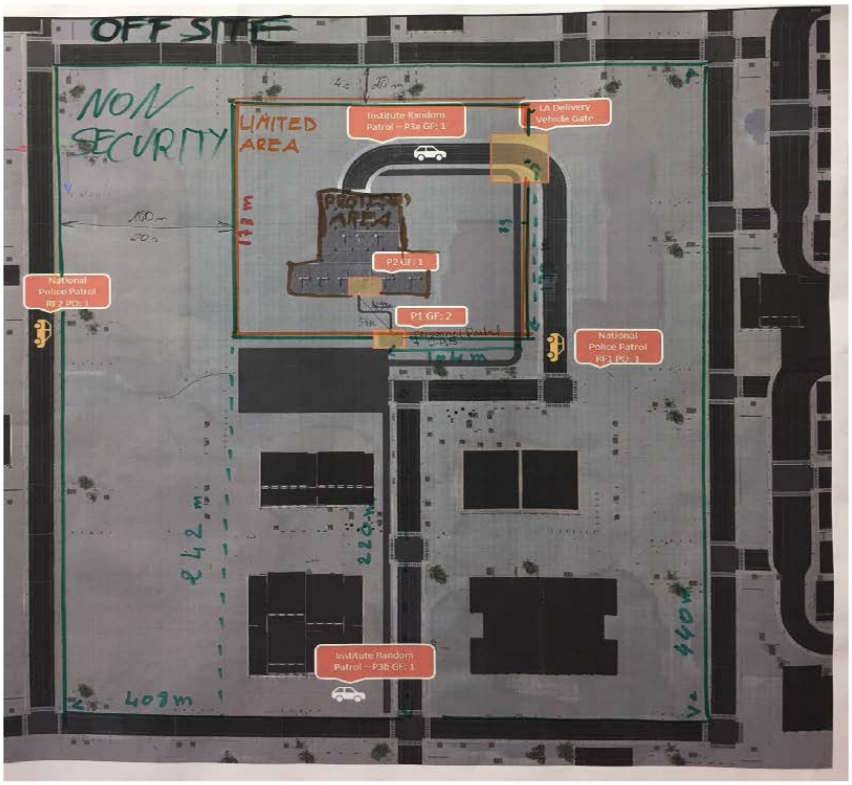
Analyze existing PPS

- Task Time at Target
  1. Control Rod Drive Bridge 10 min = 600s
  2. Reactor Block / Poll Tank Wall 20 min = 1200s
  3. Both Heat Exchanger rooms (2) 15 min = 900s
- 3 Path analysis
  - PATH 1 - running: Main entrance - Limited area Fence - Window - Window in classroom - Target 1 - **NO CDP, task time 691s**
  - PATH 2 - vehicle: Fence Campus - Limited area Fence - Shipping Door in the back of Reactor Hall - Target 1 - **NO CDP, task time 620s**
  - PATH 3 - running: Fence Campus - Limited area Fence - Shipping Door in the back of Reactor Hall - Target 1 - **NO CDP, task time 818s**
- Guard and Response Force Times:

Team	Number	Response Time	Probability of neutral. P_N
P3 Guard Random Patrol	2	146s	0
NP1+ NP2 Nat. Police	2	461s	0,5
NP Tactical Response NP	6	851s	0,99

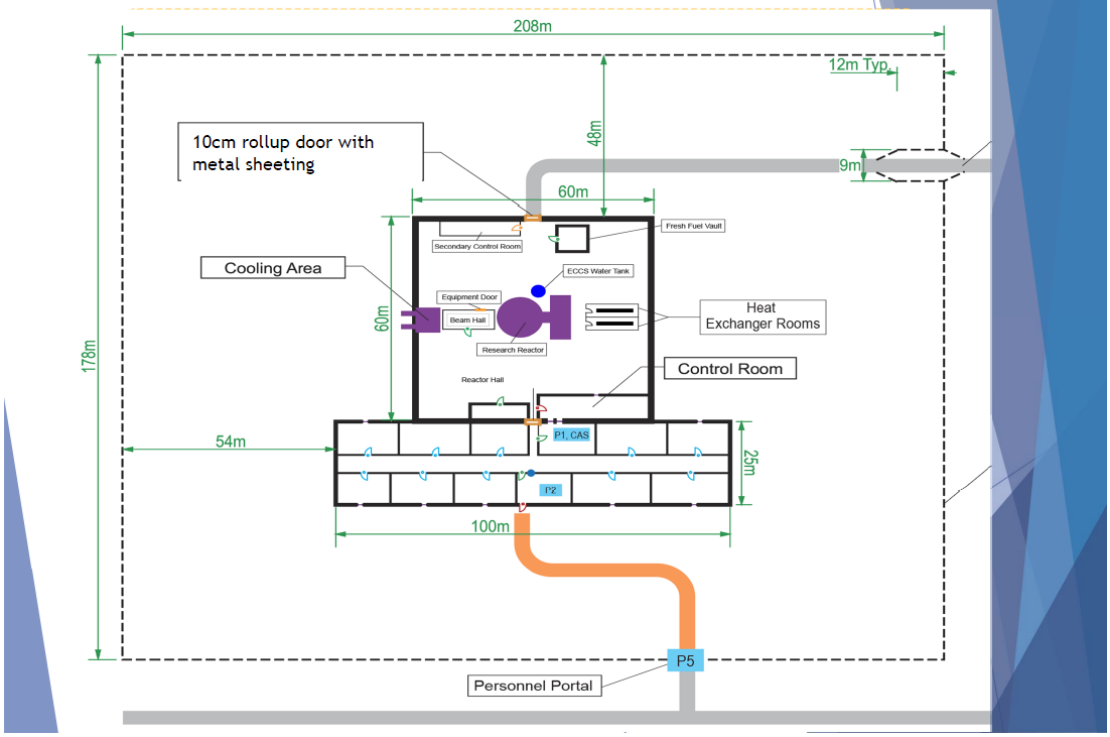
Present situation in HARI

Huang



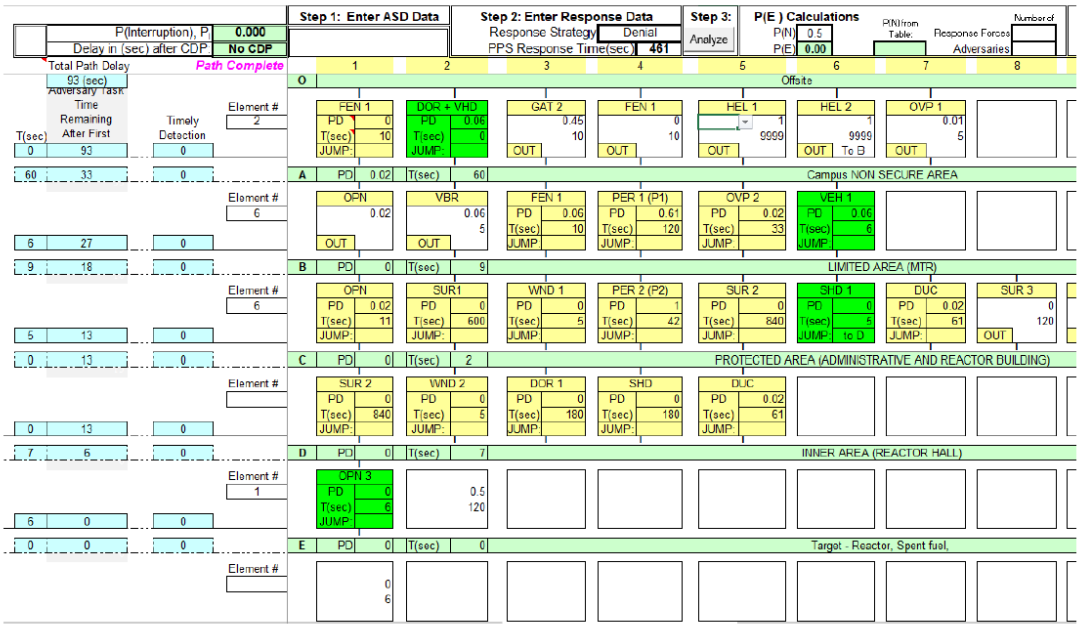
Present situation in HARI MTR

Huang



Path Analysis by MPVEASI Software

Huang



Analyze existing PPS assumption

Mike

- P_I = 0,00
- **NO CRITICAL DETECTION POINT (CDP)**
- Detection - Low scale (BMS)
- Delay - Not effective (Turn stile)
- Response - Not effective (too long time to alarm assessment, preparation and travel time)

Evaluate PPS and Upgrades

Mike

- Upgrade of PPS
  - Detection
    - Active IR, Microwave and taut wire in isolation zone
    - BMS on critical doors
    - Sensors on windows
    - Interior sensors
    - Vibration sensors on barriers
  - Delay
    - Inner fence - 2.5-m chain-link mesh with outriggers 4-mm x 50 mesh
    - Isolation zone - 10m width
    - Entry control
    - Bars on windows
    - Mesh cage on exterior venting
    - Vehicle denial system in search portal

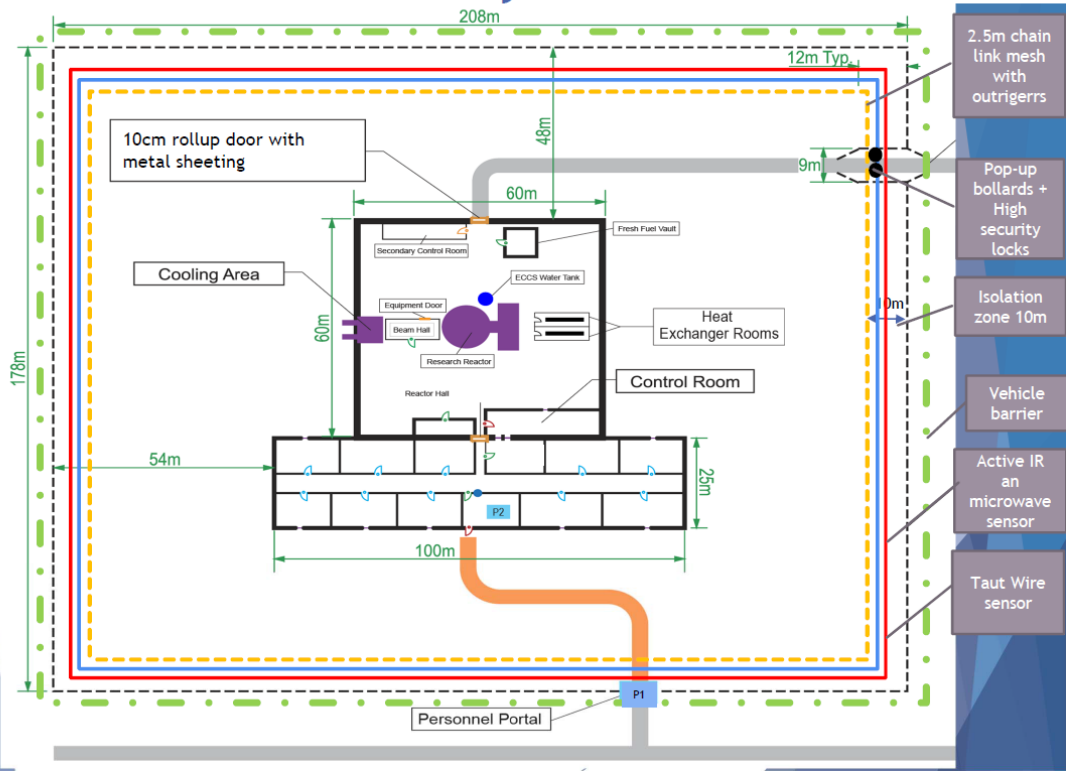
Evaluate PPS and Upgrades

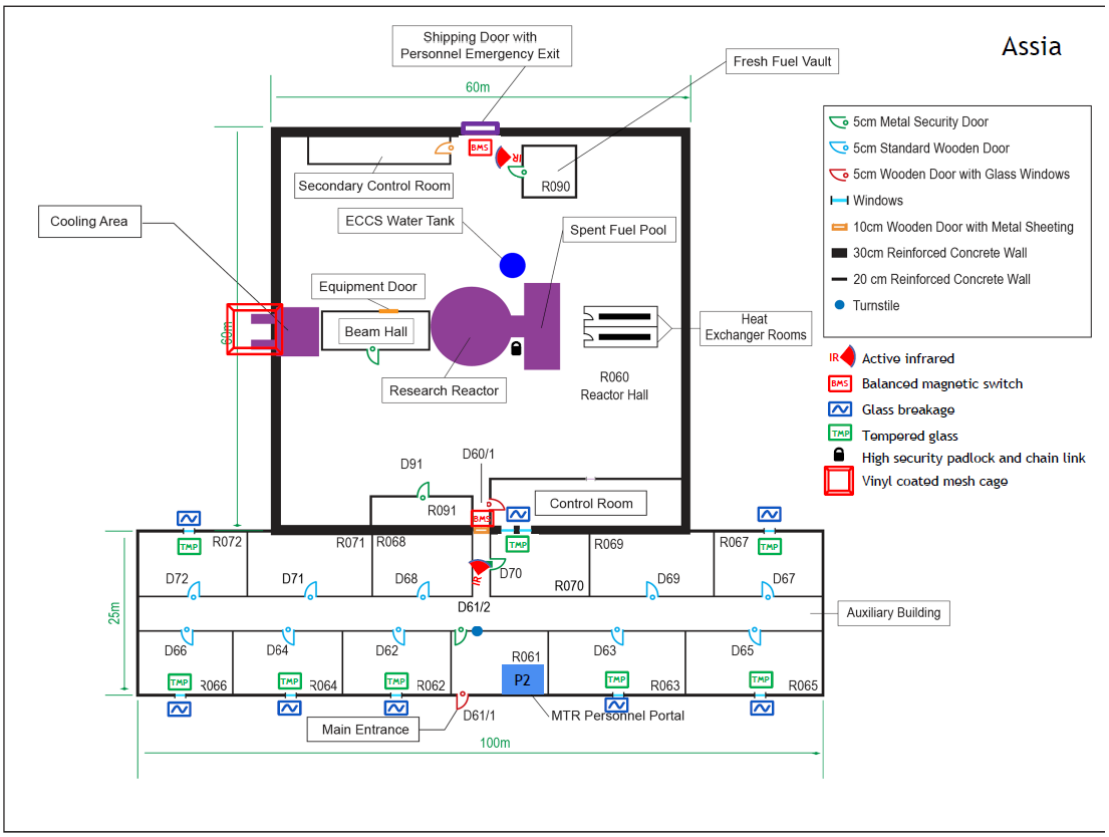
Mike

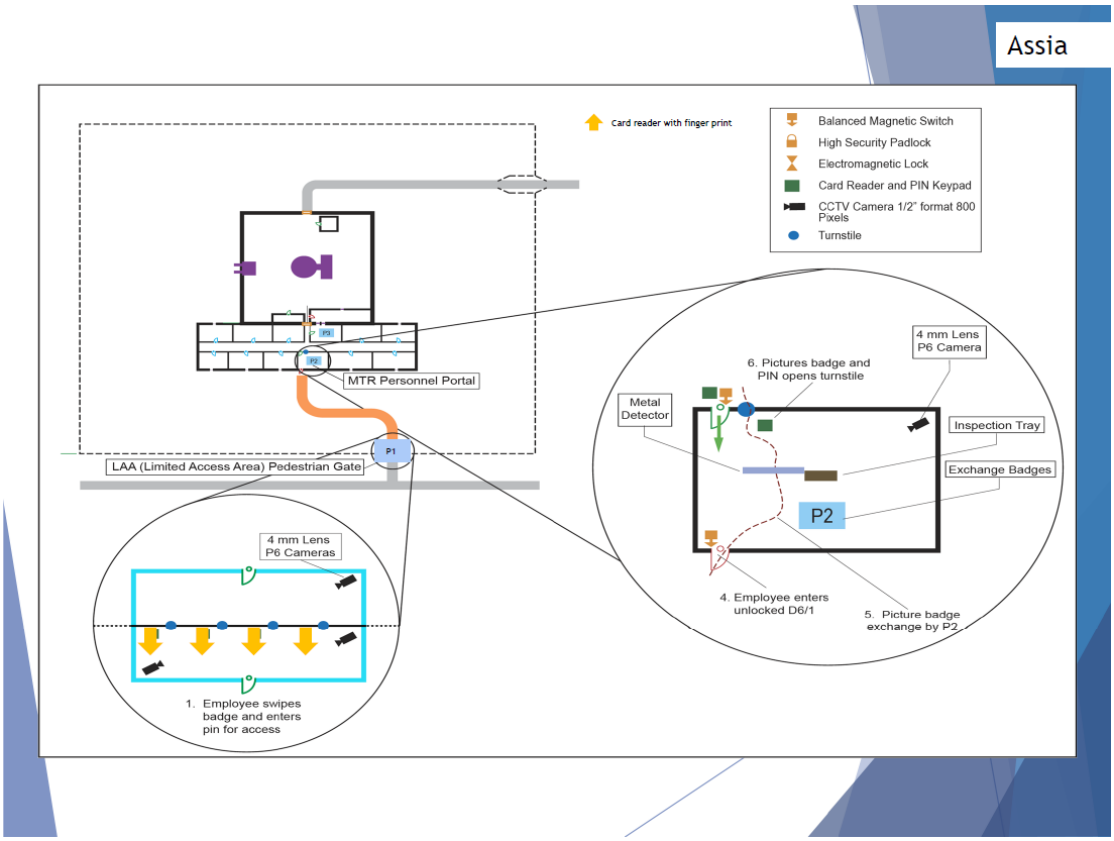
- Upgrade of PPS
  - Assessment
    - Adding cameras in isolation zone
    - Interior cameras
    - Exterior cameras
  - Response
    - Reduce alarm assessment time
    - Reduce alarm response time
    - Re-characterized response force

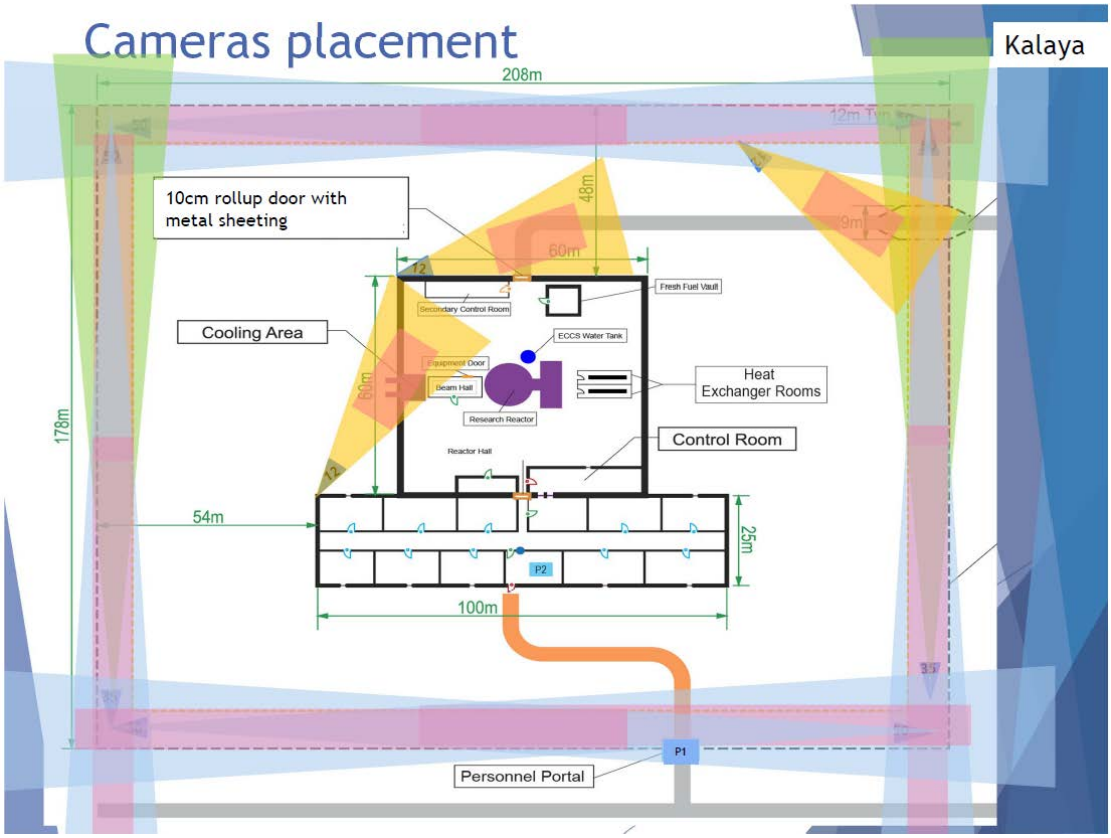
Detection and delay

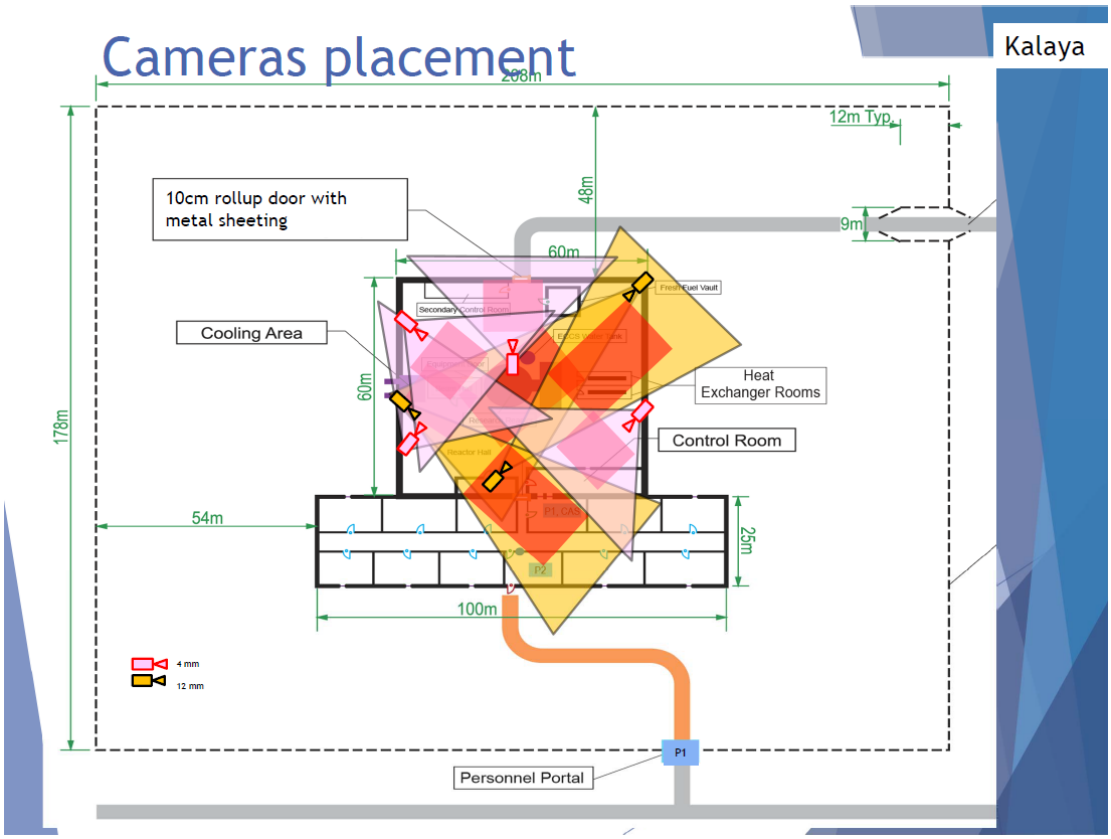
Assia




Assia
Shipping Door with Personnel Emergency Exit
Fresh Fuel Vault
60m
Secondary Control Room
R090
Cooling Area
ECCS Water Tank
Spent Fuel Pool
Equipment Door
Beam Hall
Heat Exchanger Rooms
Research Reactor
R060 Reactor Hall
D91
D60/1
R091
Control Room
R072
R071
R068
R069
R067
D72
D71
D68
D70
R070
D69
D67
D61/2
Auxiliary Building
25m
D66
D64
D62
R061
D63
D65
R066
R064
R062
P2
R063
R065
Main Entrance
D61/1
MTR Personnel Portal
100m
5cm Metal Security Door
5cm Standard Wooden Door
5cm Wooden Door with Glass Windows
Windows
10cm Wooden Door with Metal Sheeting
30cm Reinforced Concrete Wall
20 cm Reinforced Concrete Wall
Turnstile
Active infrared
Balanced magnetic switch
Glass breakage
Tempered glass
High security padlock and chain link
Vinyl coated mesh cage

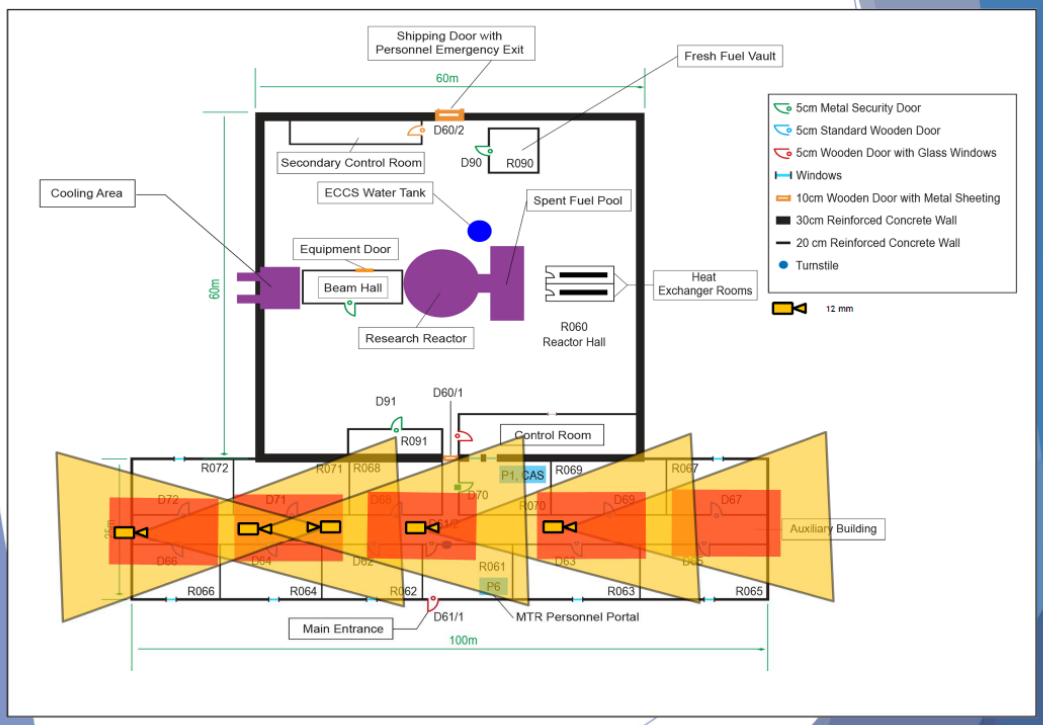

Assia
Card reader with finger print
Balanced Magnetic Switch
High Security Padlock
Electromagnetic Lock
Card Reader and PIN Keypad
CCTV Camera 1/2" format 800 Pixels
Turnstile
MTR Personnel Portal
LAA (Limited Access Area) Pedestrian Gate
P1
4 mm Lens P6 Cameras
1. Employee swipes badge and enters pin for access
4 mm Lens P6 Camera
6. Pictures badge and PIN opens turnstile
Metal Detector
Inspection Tray
Exchange Badges
P2
4. Employee enters unlocked D6/1
5. Picture badge exchange by P2


Cameras placement
Kalaya
208m
12m Typ
48m
9m
60m
10cm rollup door with metal sheeting
Cooling Area
Heat Exchanger Rooms
Control Room
Fresh Fuel Vault
Secondary Control Room
ECCS Water Tank
Equipment Door
Beam Hall
Research Reactor
Reactor Hall
178m
60m
54m
25m
100m
P2
P1
Personnel Portal


Cameras placement
Kalaya
208m
12m Typ
48m
9m
60m
10cm rollup door with metal sheeting
Cooling Area
Heat Exchanger Rooms
Control Room
Fresh Fuel Vault
Secondary Control Room
178m
60m
54m
25m
100m
P2
P1
Personnel Portal
4 mm
12 mm

Cameras placement

Bartosz



Path 1

Ibragim

P(Interruption), P	0.954
Delay in (sec) after CDP	600
Total Path Delay	Path Complete
859 (sec)	

Step 1: Enter ASD Data — Step 2: Enter Response Data — Response Strategy: Denial — PPS Response Time(sec): 125 — Step 3: Analyze — P(E) Calculations — P(N): 0.92 — P(E): 0.88 — P(N) from Table: 0.92 — Response: Adver

T(sec)	Adversary Task Time Remaining After First	Timely Detection		1	2	3	4	5	6	7
			O	Offsite						
0	859	0.06	Element # 2	FEN 1: PD 0.06, T(sec) 10, JUMP:	VEH: PD 0.06, T(sec) 0, JUMP:	GAT 2: 0.45, 10, OUT	FEN 1: 0, 10, OUT	HEL 1: 1, 9999, OUT	HEL 2: 1, 9999, OUT To B	OVP 1: 0.01, 5, OUT
60	799	0.02	A	PD 0.02	T(sec) 60	Institute Limited Area				
33	766	0.8	Element # 3	ISO: PD 1, T(sec) 26, JUMP:	PER: PD 0.95, T(sec) 60, JUMP:	OVP: PD 0.8, T(sec) 33, JUMP:	VEH: PD 0.96, T(sec) 19, JUMP:	OVP 2: 0.42, 33, OUT		
9	757	0	B	PD 0	T(sec) 9	PTR Protected Area				
140	617	0.75	Element # 6	SUR 1: PD 0.9, T(sec) 600, JUMP:	WND 1: PD 0.9, T(sec) 35, JUMP:	PER: PD 0.8, T(sec) 60, JUMP:	SUR 2: PD 0.9, T(sec) 840, JUMP: To D	SHP: PD 0.9, T(sec) 185, JUMP: To D	DUC: PD 0.75, T(sec) 140, JUMP: To D	EMX 1: 0.4, 12, OUT To D
0	617	0	C	PD 0	T(sec) 2	PTR Reactor Building				
0	617	0	Element #	DOR 1: PD 0.8, T(sec) 95, JUMP:	DOR 2: PD, T(sec) 10, JUMP:	SUR 1: PD 0.9, T(sec) 600, JUMP:				
7	610	0	D	PD 0	T(sec) 7	Reactor Hall				
10	600	0	Element # 1	DOR 2: PD 0, T(sec) 10, JUMP:	SUR 6: PD 0.5, T(sec) 120, JUMP:					
0	600	0 CDP	E	PD 0	T(sec) 0	Target Area - Products Vault R091				
			Element # 1	CRD: PD 0, T(sec) 600, JUMP:						

Tabletop exercise 1

Ibragim

Start t.	Adversary active.	End t.	Start t.	Adversary active.	End t.
0	Drive to PER 1 (12)	12	0		
12	Overpass (climbing) (33s)	45	0		
45	Go to Duct (26)	71	0	Police detection and asses (10)	10
71	Break Duct (80s)	151	10	Communicate to Police HQ (10)	20
151	Crawling cross Duct (22s)	173	30	Preparation & travel time (300)	330
173	Go to door 2 (30s)	203	330	NP1&NP2 on site (0)	330
203	Break door 2 (10s)	213	630	NP tactical team on-site (600)	630
213	Go to CRD (5s)	218	630	On-site deployment NP (90)	720
218	Sabotage (600)	818	800	Enter MTR hall and neutralize	

Ibragim

Re-Characterize Response Force

- Reduced alarm assessment time by adding cameras to the isolation zone and interior of the Protected Area
- Replaced the two mobile guards with Campus Police
- Comprised a 4 man on-site response team as opposed to a 6 man off-site team, resulting in a maximum response time of 125 seconds to P1.

Tabletop exercise 2

Chris

Start t.	Adversary active.	End t.	Start t.	Adversary active.	End t.
0	Overpass (climbing) (33s)		0	Patrol Detection	1
			1	Assessment in CAS	10
			11	Communicate alarm	21
33	Run to duct (26)	59	21	Respond to alarm	65
59	Breach duct (140)	199	65	Dismount and transit through P1	10
			75	Move to duct	50
			125	Engage/neutralize adversary	130

Chris

Final Outcome

- Probability of Interruption: .954
- Probability of Neutralization: .92
- Probability of Effectiveness: .88
- Successful neutralization of adversary prior to entry into the MTR.