出國報告（出國類別：實習）

# 第 28 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：張欽柏技士
派赴國家/地區：美國新墨西哥州
出國期間：108 年 10 月 26 日至 11 月 17 日
報告日期：109 年 1 月 16 日

# 摘要

國際間資訊流通快速，國家安全面對全球性的威脅。恐怖份子滲透、破壞各種重要設施的能力正不斷提升，作戰能力已達到國家等級。另一方面，現今恐怖攻擊所動用的人力、物力以及所運用的技術，已不是單一國家所能應付，必須依賴國際合作，在平時即以反覆推演、縝密佈署達到有效嚇阻的目的，大港倡議就是一個國際合作的成功案例。而在恐怖分子所覬覦的對象中，核物料的敏感性與技術性更在其他安全性議題之上。

有鑒於此，國際間對於攜手執行核物料保安早有共識。為積極防範並嚇阻相關的恐怖攻擊行動，2004 年聯合國安理會通過第 1540 號決議案，要求各國採取有效措施，強化核物料於運送、製造及儲存階段的管理，以有效的執行實體防護與核子保安等管制與執法作為，並透過國際合作以阻止跨國恐怖組織取得核物料；2012 年國際原子能總署（International Atomic Energy Agency，IAEA）成立 Nuclear Security Guidance Committee，統整核子保安相關規範，並建立統一標準以供各國遵循。目前，我國核子保安措施皆參照 IAEA 規範辦理。其中，針對核物料保安的實體防護，以 2011 年發布之 INFCIRC/225/Rev.5 為基礎，執行各項強化措施以符合國際標準規範。

核物料保安的完善有賴於各項措施的精進，國際原子能總署為協助各會員國規劃並執行相關安全措施，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國際規範、實體防護理論及指導原則、防護系統設計及評估、防護技術原理及裝置等，由各領域專家學者授課指導。

「國際核子保安訓練」自 1978 年首次舉辦，今年為第 28 屆，總計已有將近 1,000 位學員參訓。本屆計有 43 個會員國、59 個學員完成訓練，本次訓練係以觀察員(Observer)身份參加。學員主要來自各國核能主管機關，另有研究機構、核子反應器設施經營者、法規制定單位等，共同於三個星期的課程中研習。該課程對於強化核子設施實體防護、推動核子保安監管業務、強化國際交流合作至為重要，建議未來賡續派員參加。

# 目錄

# 壹、 出國目的

## 一、緣起

為阻止恐怖份子利用核物料作為犯罪武器，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）」明文定義核恐怖主義為犯罪行為，各締約會員國負有合作打擊核恐怖犯罪的義務，並明確要求各會員國訂定相關法律，共享情資、嚴懲恐怖份子、消弭核恐怖犯罪威脅。儘管我國非聯合國會員國及「制止核恐怖主義行為國際公約」締約國，但對抗恐怖主義為國際共同認知之重要議題，「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。而 IAEA 為協助各國強化核物料保安技術，定期舉辦訓練課程，以提供最新技術及實務經驗。

## 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，負責監督國內核子反應器設施（核能電廠）執行實體防護與核子保安工作。本會依據我國法規規定，並參考美國聯邦有關核子保安法規，要求我國核能電廠須建置核子保安程序及防護設施，以達到保護核物料免遭破壞或偷竊的目的。重點包括核電廠重要區域門禁、各項重要設施入侵偵測、阻滯歹徒行動的裝置、以及合格應變防衛武力等。此外，為防範內部破壞者（Insider）所產生的危害，要求核電廠加強員工及包商查察，嚇阻犯罪行為並提高警覺，以避免裡應外合的攻擊行為。

此次參加聖迪亞國家實驗室舉辦之第 28 屆「國際核子保安訓練」（28th International Training Course on the Physical Protection of Nuclear Material and Nuclear Facilities, ITC-28），係由國際原子能總署委託美國能源部，於美國新墨西哥州阿布奎基市舉辦，課程結合理論與實務，著重國際最新指導規範與建議、實體防護理論與技術，期望藉由完善的措施以保護我國核物料、放射性物質及其所在設施，並防範核物料偷竊或非法轉讓、蓄意破壞核設施、未經授權進入、或其他惡意行為之侵害，以確保國家安全。

# 貳、 出國行程

本次受訓課程為期三週，自 108 年 10 月 26 日出發至 11 月 17 日返國。訓練課程地點位於美國新墨西哥州，阿布奎基市聖迪亞國家實驗室。詳細行程如表 1：

表 1 出國行程表

| 日期 | 地點 | 內容 |
|---|---|---|
| 10 月 26 日 | 台北→舊金山→阿布奎基市 | 去程 |
| 10 月 27 日 | 阿布奎基市 | 報到 |
| 10 月 28 日～11 月 1 日 | 阿布奎基市 | 訓練課程 |
| 11 月 2 日～11 月 3 日 | 阿布奎基市 | 週末 |
| 11 月 4 日～11 月 8 日 | 阿布奎基市 | 訓練課程 |
| 11 月 9 日～11 月 10 日 | 阿布奎基市 | 週末 |
| 11 月 11 日～11 月 15 日 | 阿布奎基市 | 訓練課程 |
| 11 月 16 日～17 日 | 阿布奎基市→舊金山→台北 | 返程 |

# 參、 研習過程

## 一、研習方式

本訓練課程的安排大致分成三階段。第一階段為期 6 天，首先進行基礎理論的課堂講授（Lecture），每節課堂講授結束後進行小考(Quiz)，並針對學員答錯率較高的題目，由講座再次講解相關內容，以協助學員釐清正確觀念。小考後即進行分組實作（Subgroup Exercises）或示範觀摩（Demonstration），內容皆與課堂內容緊密結合，學員須應用課堂理論進行案例研討，或經由觀摩活動與課程內容相互對照，可從不同角度思考課堂所講授的理論。

課程內容涵蓋效能基礎方法論（Performance-Based Methodology）主要內容，並依照核設施實體防護系統（Physical Protection System, PPS）的建構、設計及評估過程，分別整合為定義需求（Define Requirement）階段、系統設計（Design）階段及系統評估（Evaluation）階段。各階段內容於全部 32 個課程單元中詳細講授，每一單元均由各領域的專業講師擔任課堂講座，主辦單位並視課程內容搭配各項示範觀摩或演練活動，以強化對授課內容的了解。講授結束隨即分組進行案例討論或實作，全程均以英語進行(學員合影如圖 1) 。主辦單位為了解學員們的

知識背景及專業程度，課程開始前即進行一次課前測驗，全部課程結束後並舉行最終測驗，以呈現學員的學習成果。

本次訓練將 59 位學員分為 8 個小組，每小組 7~8 位學員，分別來自不同國家，並由分組指導員（Subgroup Instructor）帶領於課堂後進行案例研討。分組案例研討的對象，為練習教材所虛構的中亞國家「拉卡錫（Lagassi）」，教材中已詳述該國各項背景資料，包括：政治概況、歷史、地理位置、氣候、經濟條件、國際關係及威脅情資，學員依專業判斷並參考教材內容，進行案例研析。教材中敘明該國之國立研究所設有水池式反應器（Pool Type Reactor, PTR）及小型模組化反應器（Small Modular. Reactor, SMR）各 1 座，案例研討係以水池式反應器為練習標的，實作實體防護系統之建構。分組指導員均由聖迪亞國家實驗室安排資深專家擔任，於實作過程中從旁協助，並依據課程進度指導學員進行設計基準威脅（Design Basis Threat, DBT）之制定、設施弱點研討與保安措施補強等。

第二階段為案例研討結果彙整，為期 4 天，同樣以水池式反應器為對象。各分組依據前一階段中分組研討的成果，進行兵棋推演(Tabletop Exercise)，推演劇本及相關假設皆依據第一階段研討成果與教材制定。進行兵棋推演時，各組成員分成三隊，分別扮演攻方(紅隊)、守方(藍隊)及裁判(綠隊)。過程中每一步驟及細節皆須經過攻方及守方同意，若有爭議則由裁判決定。相關數據可參考教材內容，或由小組成員共同討論，若討論後仍無法達成共識則由裁判判定。以入侵過程為例，入侵歹徒及警衛的行動路徑由各方自行決定，另一方可提出異議，若產生爭議則由裁判裁決。全部討論內容手寫記載於海報上，串連成一完整的兵棋推演報告，包含情境假設、入侵路徑及時序、推演結果，各分組須於第二周最後一天以口頭報告方式向講師說明研討成果，並接受講師講評。

第三階段以成果報告（Final Exercise Report）作為總結。延續前次（ITC-27）訓練課程的作法，各分組以一周的時間，研討 SMR 及拉卡錫國內另外兩個虛擬核設施：包括一個研究用反應器（Material Test Reactor Facility, MTRF）、及一座虛擬核電廠（Lone Pine Nuclear Power Plant, LPNPP）。學員需運用自課程中累積的專業知識，以及分組研討

實體防護的經驗，共同評估上述三個虛擬核設施的設計基準威脅，以進行完整的實體防護系統研究、設計及建構，並針對可能發生的入侵情境進行兵棋推演。除指定研究議題外，本組並額外進行內部破壞者研究以了解其威脅程度。課程最後一天全部分組一同對講師及其他學員簡報，並接受提問及指教，實為一難得的經驗。

本分組由聖迪亞國家實驗室資深專家 Tam Lee 擔任指導員，其專長為電腦模擬，於兵棋推演時亦提供分組成員相當多的指導。此外，各課程講師均輪流前往各分組觀察實作情形，並於實作過程中與學員進行意見交流。本次參訓被分配到的小組，成員分別來自英國、瑞典、阿根廷、波蘭、哈薩克、亞美尼亞及日本等國，專業背景包含核能管制機關、核設施運轉員、研究機構等。

為增加學員對於破壞工具的了解，主辦單位在戶外場地，展示 Broco 火焰切割機、氧乙炔火焰切割機、電漿火焰切割機、氣動電鋸、砂輪機、往復式電鋸、螺栓切割機等歹徒常用破壞工具，並由主辦單位工作人員現場操作，實際示範破壞鎖頭、鍊條、鋼筋、鋼板、鉸鏈等延遲屏障（Delay Barrier）的常用材料，並由學員以碼表記錄完成破壞的時間，實地感受各種工具的攜帶及操作方法、所需配件，以及破壞不同延遲屏障材料的難易程度、破壞時所可能發出的噪音。此示範課程的主要目的，在於教導學員評估延遲時間的具體方法。另外，在設計阻滯設施時，主辦單位教導學員利用簡單的方法提高破壞難度，例如以煙霧或黏膠增加操作難度等。

主辦單位針對實體防護評估的演練，除課堂內容與分組討論外，另以位於科特蘭空軍基地（Kirtland Air Force Base）內，隸屬美國能源部的 Technical Area V(TAV)作為實習地點。首先由講師分批帶領學員講解設施內的各項防護措施，包含保安監控中心、圍籬、CCTV 等，並觀看 Force-On-Force 的演練。各組於講師講解後對 TAV 的實體防護設施進行測試，演練保安設施的評估過程。本組測試項目為圍籬區 CCTV 辨識率之及盲區檢測。

由於感應器為保安設施的重點之一，為強化學員對於其特性的了解，主辦單位特地安排於測試場地進行講解。感應器種類可依其作用原理區分為：電子圍籬（Electric Field）、微波（Microwave）、雷射（Laser）、

震動（Vibration）、拉力線（Taut Wire）、主動及被動式紅外線（Infrared）、光纖（Optical Fiber Cable）等，現場除介紹其特性外，並講解設計時所需考量的因素，包括地形、高度、角度、交錯排列方式、氣候影響等，均可能會影響感應器的效能。因此，講師特別強調感應器安裝後須進行檢測，以確保防護能力達到設計要求。

圖 1　ITC-28 全體學員及工作人員合影

二、課程內容

核設施實體防護系統的設計遵循一套標準流程，如圖 2 所示，設計者必須透過評估與改善的過程，不斷強化系統防護能力，以確保在面對設計基準威脅時，系統可發揮要求的防護強度。因此，設計者必須先蒐集足夠的資訊，包括核設施的特性、設計基準威脅、應變程序等，藉此設計新系統或評估現有系統。下一步則需評估系統效能，以確認系統是否達到防護需求標準。由於防護系統的複雜度高，評估過程必須借助各種模型或電腦軟體，若評估後發現弱點，則進入系統修改及再評估程序。核子保安訓練課程的安排，亦遵循上述系統建構過程，區分成三大步驟：1.定義實體防護系統需求（Define PPS Requirement）；2.實體防護系統設計（PPS Design）；3.實體防護系統評估（PPS Evaluation）。此一流程統稱為「實體防護設計與評估流程」（Design and Evaluation

Process Outline, DEPO），主辦單位將完整流程區分為 32 項專業課程，各項課程內容簡介說明如下：

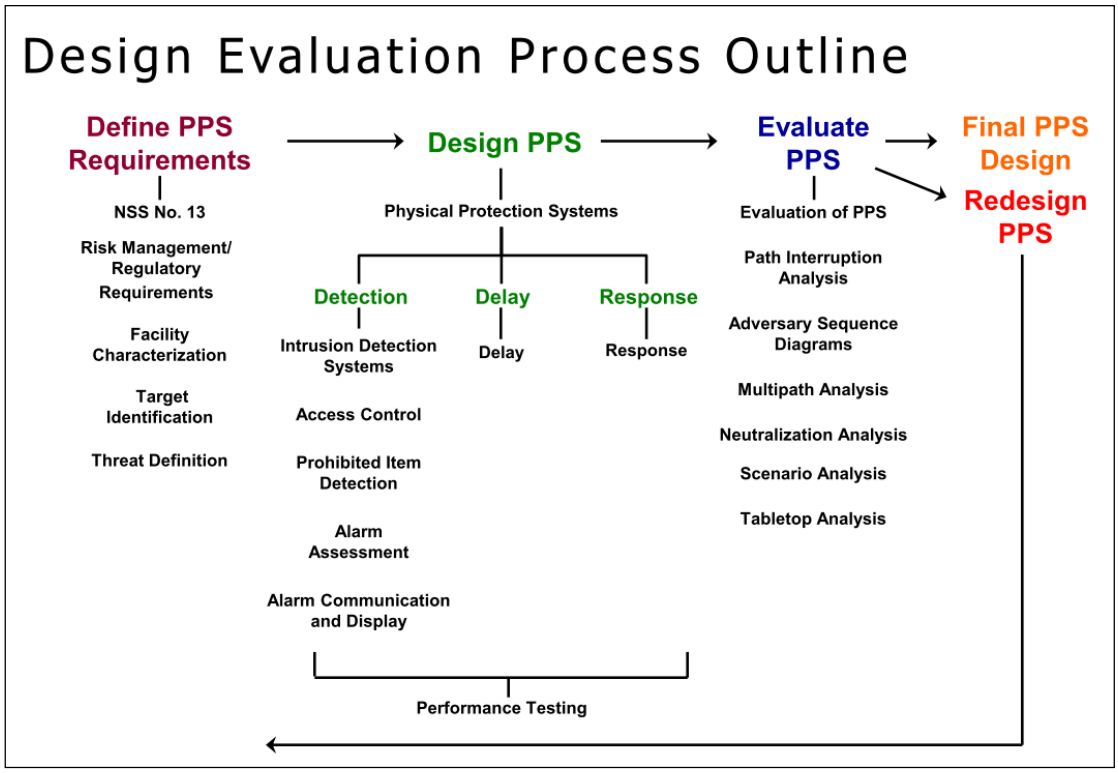


圖 2 實體防護設計與評估流程

**步驟一、定義實體防護系統需求（Define PPS Requirement）。**

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），於第 3.10 節中要求各國必須依據相關評估結果，定義實體防護系統需求。系統需求經明確定義後成為系統設計及評估的基礎，即可進入下一階段作業。

此步驟中所涵蓋的作業內容包括：界定防護對象及標的物特性、定義威脅的種類、確認法規要求。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）：

本訓練課程使用 DEPO 流程進行實體防護系統的建構，該流程將整個系統的設計及評估流程區分為三大步驟：

步驟 1 為需求定義階段,設計者必須先蒐集設施的相關資訊，包括設施的運轉狀況、現有建築物、地理環境、現有防護設施等。設計者還必須確認設施面對的威脅，包括威脅的型態及來源、可能具有的威脅能力、以及可能採取的戰術。綜合設施及威脅來源

的資訊，並結合法規與風險管理的要求後，設計者可確認出一個或多個標的物，作為系統設計的防護目標。

步驟 2 為實體防護系統設計階段。設計者必須決定防護設施(例如圍籬)與人員的最佳組合方式，以發揮保安系統的三大目標功能，即偵測（Detection）、延遲（Delay）與應變（Response）。除此之外，設計時須考量「平衡設計（Balanced Design）」原則、「深度防禦（Defense-in-Depth）」、「偵測先於延遲（Detection before Delay）」，以建構符合要求的防護系統。

步驟 3 為實體防護系統評估，目的在於確認系統設計結果是否達到設計要求。為求評估結果的客觀性及一致性，本課程中採取一定量方法計算系統效能，即效能基礎（Performance-Based）方法，可針對複雜的防護系統評估其防護效能，並尋找系統的弱點。若評估後系統防護效能未達要求，必須重新回到步驟 2 進行設計變更。

(2) NSS-13 報告書介紹：

NSS-13 報告書即為 INFCIRC/225 第 5 版，由國際原子能總署於 2011 年 1 月發布，為國際間共通之重要核子保安規範。本課程說明其主要條文，並介紹重要改版內容。

NSS-13 將核子保安工作區分為三大角色：設施所在國家、主管機關及執照持有者，強調三者間的層級、分工及責任；三者間必須緊密合作，以共同完成實體防護四大目標：「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）」。

NSS-13 本次改版的主要目的，在於處理更多的威脅種類，例如無人機的普及化。另一目的即為配合核物料實體防護公約（Convention on the Physical Protection of Nuclear Material, CPPNM）的增訂，該公約於增訂內容中提出 12 條基本原則（包含國家責任界定、國際運輸責任、法規框架、深度防禦、品質保證、應變計畫

等），內容涵蓋核子保安的各重要項目。課程中特別針對此 12 條原則與 NSS-13 內容進行比對，以說明兩者間的緊密關係。

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

課程中將保安風險定義為：惡意行為在未來某時間點造成傷害或損失的機率。由於惡意行為經過事先計畫，因此保安風險並非隨機產生。風險雖然無法完全消除，但其後果可經由風險管理措施來降低、避免或轉移，使其損害程度降低至可接受範圍。課程中指出，降低風險可透過三種途徑：降低攻擊的發生機率（$P_A$）、降低攻擊成功所造成的損害、提高實體防護系統的效能（$P_E$）。對於核物料保安工作而言，風險主要來自於核物料的偷竊及核設施的破壞。

課程中主要針對攻擊造成的損害以及系統效能 $P_E$，提出系統性的改進方法。在攻擊損害方面，平時應做好物料管理，並強化防護措施，以降低攻擊成功機率；另外，預想攻擊成功後的狀況並建立控管措施，以減少或迅速彌補可能造成的損害。在系統效能方面，課程提出以成功攔截威脅機率（$P_I$）及成功弭平威脅機率（$P_N$）計算系統效能，亦即 $P_E = P_I \times P_N$，設計者可參考公式以找出最佳的效能組合，或尋找可能的改善機會。

(4) 威脅定義（Threat Definition）

NSS-13 第 3.10 節中，要求國家必須針對核物料實體防護系統定義設計基準威脅（Design Basis Threat, DBT），且評估範圍必須涵蓋偷竊（Theft）與暴力破壞（Sabotage）。主管機關、情報機關及設施經營者都必須參與評估流程，並提供相關資料。本課程介紹評估及制定 DBT 流程如下：

a. 首先由威脅評估作業開始，經由公開的或機密的管道蒐集有關威脅情資，內容包括動機、目標及攻擊能力。蒐集後分析資料的可靠性，將情資彙整作為下一階段的分析基礎。

b. 檢視前一階段所彙整的資料，依據合理性及可行性判斷，篩選出可能發動攻擊的威脅來源，例如恐怖組織的動機是否強烈、目標是否與核物料有關、攻擊能力是否足夠等。攻擊能力又可

細分為組織人力、武裝程度、持有的爆裂物數量、手持工具、通訊設備、運輸能力、相關專業技術以及內部破壞者等。

c. 將篩選後的威脅來源組合、轉化成一具體模型，並檢視模型的合理性；尤其須注意在建立模型的過程中，不可單純將最嚴重的威脅條件組合起來，而須配合各項情資與背景條件進行綜合判斷。

d. 最後依據政策或法規要求進行調整，例如依據國家政策或財政限制進行調整。另外，必須考量設施本身承擔的極限，並將超出極限的部份納入超越設計基準威脅(Beyond Design Basis Threat, BDBT)。

經過上述步驟制定出核設施的設計基準威脅，主管機關可將其納入法規或指引中，要求設施經營者遵循；或要求作為效能評估的基礎，例如於威脅情境中以 DBT 作為假設條件。

(5) 針對內部破壞者的措施（Measures Applied to Insider Threat）

內部破壞者的威脅在於其潛伏的特性不易被察覺，且獲得授權可出入特定區域。此外，內部破壞者常因工作性質得以獲取重要知識或技能，對於設施可能造成的破壞更大。內部破壞者除自行發動攻擊，也可能與外部破壞者合作，採取裡應外合的策略，防不勝防。有鑑於防範內部破壞者的重要性，IAEA 發行 NSS-8 (Preventive and Protective Measures against Insider Threats , Implementing Guide)，作為主管機關及設施經營者的指引。

課程中將內部破壞者區分為被動與主動兩類。被動的內部破壞者僅單純提供相關知識，主動破壞者則參與行動，包括暴力破壞行為在內。內部破壞者的動機可分為意識形態、財務問題、報復、心理狀態異常、受脅迫或被利用等。

由於內部破壞者具有相當明顯的優勢，在防範作為方面必須更加注重規劃與執行。首先於聘僱員工前，進行安全查核，例如調查犯罪紀錄、查核確認財務狀況等；聘僱後仍必須定期或不定期進行員工行為評估或執行適職能力(Fitness for Duty)檢測，例如透過健康檢查確認有無身心方面問題、以尿液或血液篩檢有無濫用藥物等。其次對於設施內特定區域的出入管制，定期檢討授權

的對象是否合適，人數是否過多，對於 Two-Man-Rule 是否確實執行。

在防護措施方面，應依循偵測－延遲－應變的策略對付內部破壞者，並盡量消弭各種惡意行為成功的機會，例如即時更新通行證的有效性、定期檢視通行證出入紀錄、教育員工注意設施內狀況等。

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

核物料管理的目的，在於使設施經營者能隨時掌握核物料的數量及儲存狀況，避免核物料遭偷竊或移置於其他處所。同時，良好的核物料管理是應對內部破壞者的基本措施。

核物料料帳管理與控制系統經由運作良好的庫存物追蹤措施，即時且完整掌握設施內核物料的所有資訊，包含數量、型態、位置。其資訊的可靠性，來自於有效執行的行政及技術措施，協助設施經營者降低核物料遭竊風險。在竊取或遺失事件發生時，管理系統亦可協助追查行動，迅速擬定補救措施。

該系統強調核物料的管理紀錄必須以數字形式呈現，若出現差異(稱為 Material Unaccounted For, MUF)，則代表異常事件發生。而系統的運作則依賴 MBA(Material Balance Area)的管理，包含該區域內的物料數據統計、運轉程序、人員控管、以及其他保安措施的執行。

(7) 核設施特性描述(Facility Characteristization)

進行實體防護系統設計前，必須先蒐集設施重要資訊，並且清楚描述設施特性，課程中所列舉之重點包括：

- 廠址特性，包括廠界環境、地理條件、週邊道路、廠房位置、出入口、廠房建築等；
- 設施運轉情形，包括員工人數、值勤排班、正常運轉及緊急運轉程序、後勤作業(包括資訊網路、設備維修、物料管理等)；
- 設施運轉程序書，包括保安及運轉安全相關、核安文化、訓練及應變等相關程序書；

- 設施有關的法規及指引；
- 員工聘僱程序及相關保安要求；
- 其他資訊，例如對運轉安全與設施保安的協調、設施經營者的運轉目標。

上述資訊部分可由設施經營者直接提供，部份必須由實體防護系統設計者實地觀察或分析後取得，蒐集後的大量資訊即為後續分析設計作業的基礎。

(8) 目標界定（Target Identification）

進行核物料保安作業時，首先必須釐清的是：保護的對象是甚麼？它在哪裡？它的價值是什麼？對於恐怖攻擊而言，核物料依其元素以及重量所造成的危害也有所不同，因此，防護系統的等級也必須加以區分。為方便對核物料進行分級，課程以 NSS-13 之「核物料分類表」（Categorization of Nuclear Material），作為劃分核物料防護等級的依據。在 NSS-13 中，亦要求國家必須對核物料的防護措施進行分級，包括劃分防護區域的等級、定義 URC(unacceptable radiological consequences)的限值等，相關作業都必須依據核物料分類表的分級進行。

(9) 虛擬核設施介紹（Introductuion to the Hypothetical Facility）

課程所設定之虛擬國家「拉卡錫（Lagassi）」，其核設施(如圖 3)位於該國醫學及物理研究所，其內設置有水池式反應器( Pool Type Reactor, PTR）、小型模組化反應器（Small Modular. Reactor, SMR）、以及放射性廢棄物儲存設施各一座。

教材中已設定設施的地理位置及周邊道路，並描述設施本身的保安系統，包括保安人力、警衛配置、武器及通訊設備、巡邏及執勤方式。對於實體防護設施部分，已設定偵測設備、圍籬設計及出入口位置，包含 CCTV 的數量及位置、圍籬及出入口的感測器、燈光照明等。以上各項內容皆以文字及圖面顯示，具體呈現評估所需之各項資訊。另外針對入侵時所可能經過的重要出入口，特別詳細描述其細節，包括出入動線、刷卡設備、車輛檢查程序及大門開關位置。

針對核設施本身設定其運轉條件及安全設施，包括控制室、燃料儲存設施、緊急冷卻系統等。對於威脅來源部分，教材中說明拉卡錫國內的各恐怖組織及其概況，以利學員設定設計基準威脅。

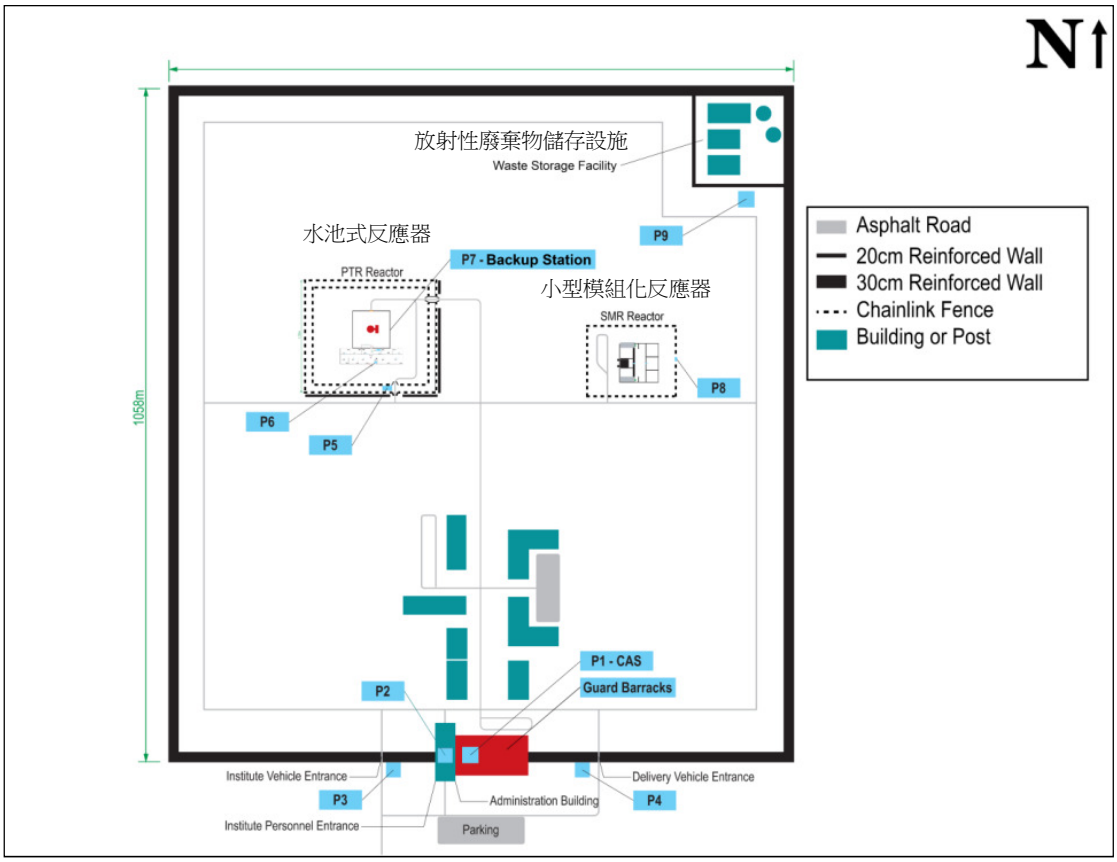


圖 3 拉卡錫核設施平面圖

**步驟二：進入實體防護系統設計(PPS Design)階段。**

設計者應以步驟一所彙整的資料為基礎，依循課程所提供的指引及原則進行系統設計。此步驟的課程內容概述如下：

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

NSS-13 中說明實體防護系統的三大功能為偵測、延遲及應變，課程中針對各項功能可採取的措施舉例說明，並於實作課程中進行介紹。在系統設計上，則須運用深度防禦及分級策略(Graded approach)以達到適當的防護效能。

防護系統的設計方向不外乎「嚇阻」(Deter)與「打擊」(Defeat),各有其適用場合與優缺點。課程中亦介紹數項重要設計原則及重點,作為實體防護系統設計參考:

- 及時偵測原則:從開始偵測到異常,到歹徒完成破壞的時間點,其時間差應長於反應時間,以使應變武力有充分的餘裕完成任務。
- 深度防禦原則:在可能的入侵途徑上,利用多重的防護措施達到延遲甚至阻滯攻擊行動的目的,同時可強化攻擊行動的不確定性,嚇阻歹徒入侵的信心。
- 平衡設計:在入侵途徑上,整個系統的防護效能等同於最脆弱位置的效能,因此,在設計上須避免過度強化某些元件,而忽略不同路徑間的平衡。

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

入侵偵測系統作為整體防護系統的”哨兵”及第一道防線,其設計的良窳決定應變作為的結果。在防護系統中,入侵偵測雖然不具備主動的防護功能,但在偵測到異常狀況時可立即發出警報,經警衛評估後採取適當應變行動。因此,歹徒在行動時必須評估偵測系統的作用,產生一定的嚇阻效果。

前段的描述中已提到構成偵測系統的三大元素:偵測設備、訊號傳輸及電力、警報顯示裝置。課程中說明可從以下三個面向評估偵測設備性能,包括偵測機率(Probability of Detection)、誤動作率(Nuisance and False Alarm Rates)與偵測弱點(Vulnerability to Defeat)。在設計系統時,應盡量選擇高偵測機率與低誤動作率的偵測器;同時仔細評估偵測弱點,以程序管制(例如 Two-Man Rule)、定期檢測或以多種偵測器互相支援,避免弱點遭歹徒利用。

偵測器可分類如下:

a.主動式與被動式:主動式偵測器會先發送能量(Energy,例如紅外線),再與回傳能量比較,若出現差異即代表環境中有物體移動。被動式則不發出能量,僅接收環境物體所發出的能量(例如震動),若偵測到能量即代表環境出現變化。

b.隱藏式與外顯式：如同字面意義，隱藏式偵測器可設置於其他物體中，例如牆壁內或地面下，外觀無法察覺，使入侵者難以察覺並避開，可提高偵測效果。外顯式較易安裝，但也易於避開。

c.體偵式(Volumetric Detection)與線偵式(Line Detection)：體偵式偵測整個立體空間的信號，入侵者一旦進入空間內即會被察覺，難以迴避。線偵式僅偵測單一直線上的信號，若設計不良，可能會產生偵測盲點。

d.外部式與內部式：外部式主要用於偵測開放空間的狀態，內部式則用於偵測密閉空間以及邊界上的變化。

選擇偵測器必須與環境結合，例如在視線不佳或易有遮蔽的狀況，應加強照明或選擇震動型偵測器。在重要區域例如核物料儲存場所，可加裝平衡磁力開關(Balanced Magnetic Switch)或主動式紅外線感測器。各類型偵測系統在不同環境下有不同的誤動作率，設計時必須參考氣候因素、環境條件、偵測對象、甚至可能出現的野生動物等作通盤考量，避免造成警衛過度負擔。必要時以多種偵測器相互搭配，降低偵測盲點，以提高偵測成功率。

(12)門禁管制（Entry Control）

門禁管制常見於各種重要場所的保護，由於牽涉到人員或車輛進出動線，常成為歹徒入侵或夾帶管制物品的重要途徑。門禁管制的主要作法，是在保護區域外圍的邊界上，執行人員及物品進出管制，以維護保護區域的安全。因此需要使用各種方式以識別人員、物品及車輛，本課程首先介紹人員身分識別，可分為 What you know(如密碼)、What you have(如證件、鑰匙)、What you are(如指紋、虹膜、語音)。針對需加強管制的區域，也可採取多種類識別，例如於核物料管制區同時要求密碼及指紋識別。

一般而言，越易於執行的管制系統越容易被突破，例如識別證有易於被複製或竊取的風險。而指紋雖不易偽造，但錯誤發生率卻較高。以目前最常被採用的生物識別而言，就容易受到環境與身體因素的影響而辨識失敗。因此，針對不同防護等級的區域，應注重 FAR(False Acceptance Rate)及 FRR(False Rejection Rate)的配

合，例如，高風險區域應採取低 FAR 的設備，以避免發生誤放的機率。

(13)違禁品偵測（Detection of Prohibited Items）

違禁品偵測為門禁管制的一環，目的為管制物料進出。就核設施的違禁品偵測作業，課程中依偵測對象的性質及所使用的設備分開討論，內容說明如下：

- 金屬探測器：主要針對武器、爆裂物及零組件、工具、通訊及攝影設備等，其原理是利用金屬物品對電磁波所造成的感應，又可依偵測原理分成主動式與被動式。一般常見的金屬探測器外型分成門框式及手持式，經常搭配使用。

  就常見的主動式金屬探測器而言，由於其偵測效果來自金屬物體在電磁場中產生的渦電流(Eddy Current)，任何影響渦電流的因素都會影響偵測效能，包括物體的大小、形狀、與電磁場的夾角、材質、移動速度等。
- 包裹檢查：指以人工或 X 光、電腦斷層掃描對包裹或行李進行檢查，以防止違禁品被夾帶出入。以人工進行檢查較為費時但成本較低，檢查技巧須經過訓練。至於電腦斷層掃描的技術日益進步且普及，已可即時呈現受測物體的 3D 立體影像，方便進行辨識。
- 爆裂物偵測：主要是偵測爆裂物所含有之特定化學物質，通常利用警犬或設備進行偵測。
- 放射性物質偵測：課程中主要介紹 Gamma Ray 偵檢器，包括碘化鈉偵檢器、純鍺偵檢器等，形式可分成攜帶型與固定式。

(14)警報評估（Alarm Assessment）

當偵測系統發現異常狀況後發出警報，保安人員應立即評估警報內容，警報來源包括監視器螢幕、崗哨值勤人員、應變武力、蜂鳴器等。評估方式可分為兩類，一類是由監控人員於監控室內

進行，另一類則由應變武力於崗哨或巡邏中進行，本課程主要針對第一類進行介紹，即由監控人員透過 CCTV 進行警報評估。

課程中講師一再強調：” No Assessment, No Detection.”，若缺乏正確的判斷力，輕則浪費人力處理雜訊干擾，重則可能導致歹徒入侵成功，可謂是關鍵的環節。在評估作業所接收到的訊息並進行判斷時，首先必須排除雜訊（如下雨）或異物（如鳥類），若經評估後確認為入侵事件，須提供正確資訊以進行武力佈署，包括人數、時間、入侵位置、入侵方式、裝備等。

CCTV 為評估資訊的主要來源，其構成元件包括：相機及鏡頭、照明系統、信號傳輸系統、控制設備、影像儲存設備、監視器等，包括系統所使用的作業系統及程式。

在設計 CCTV 時，首先應考慮監控區域的幾何形狀，設法達到最大範圍的監控，尤其應重視可能的入侵位置，例如圍籬和出入口。同時應配合監控範圍內的感測器位置，預想警報發生時需透過 CCTV 確認的區域。此外，設計者必須考量設施環境中可能出現的各種氣候條件，例如大雨、颱風、暴雪、濃霧等，適度強化 CCTV 及照明系統的功能。基於 CCTV 的重要性，主辦單位特別安排學員實際以 TAV 為場地，教導評估 CCTV 設置的方法，包括如何辨識及消除監視範圍的盲區、如何確認解析度是否符合需求。

(15)警報通訊與顯示（Alarm Communication and Display,AC&D）

AC&D 的主要功能是將警報及信號由入侵偵測系統、門禁管制系統或CCTV 傳輸至監控中心，呈現於螢幕或其他監控裝置上，由應變人員或警衛進行後續的評估及應變程序。AC&D 作為偵測系統與應變人員之間的介面，首要目標是完整呈現必要資訊，使應變人員清楚掌握現場狀況，並能即時與應變武力進行聯繫，以利人員佈署與行動協調。此外，考量到緊急應變狀態的需求，顯示方式應依資訊重要性排序，將最重要資訊(例如警報位置的 CCTV 畫面)置於中間，其他依序排列。盡量以圖像資訊顯示，或以聲音、簡單訊提提示，避免以大量文字造成理解上的錯誤。

(16)延遲（Delay）

延遲裝置一般設置於可能的入侵途徑，藉由阻滯歹徒行動，使應變武力可於歹徒達成目的前加以阻止。由於應變武力的行動有賴於偵測系統的警報，因此，延遲裝置同樣必須在偵測到威脅之後才能視為有效。在本課程中將延遲裝置分成被動型與主動型，概述如下：

a. 被動型屏障（Passive Delay）：又可分為邊界型與結構型屏障，前者設置於設施周界上，例如圍籬、大門、車輛進出屏障等，可將數個屏障結合在一起，發揮極大的延遲效果；結構型則是以設施結構本身作為屏障的一部分，例如設施牆壁、門窗、屋頂、地板等。結構型較易於被入侵，強化卻較為困難，常須涉及到結構本身的改建。

b. 主動型屏障（Active Delay）：需要信號加以啟動，課程中介紹許多容易製造、效果極佳的屏障，例如以黏性極強的黏著劑阻滯行動、以煙霧或泡沫遮蔽視線。

課程練習時，主辦單位特別設計各種練習，使學員親身體驗主動型屏障的效果，例如戴上眼罩後拆除螺絲，即可產生極佳的延遲效果。

(17)應變武力（Response Force）

應變武力在實體防護系統中具有延遲、攔截（Interruption）、弭平（Neutralization）的功能，其本身具有一定的武裝及訓練，可進行一定程度以上的戰鬥，以對應設計基準威脅。雖然應變武力的工作與一般警衛（Guard）所負責的巡邏、監控、檢查等業務不同，然而在面對威脅時，警衛可能位於監控中心進行通報，甚至在第一線面對歹徒，兩者間必須迅速做好溝通協調，因此日常訓練必須盡量將兩者加以結合。

對於應變武力的運用，講師在課程中針對數個要點分別進行解說。首先國家必須制定法律，以授權應變武力在核設施內的運用，並界定清楚使用武力的範圍，例如逮捕、拘束、或使用致命

武器。設施本身亦須依據法律授權，制定明確的規則供應變人員遵守，例如交戰守則等。

在保安應變計畫（Contingency Plan）中，講師強調必須包含幾種不同的作戰策略。首先是圍堵，以防止歹徒做案後成功離開核設施；其次是阻止歹徒接近重要目標進行破壞行動。針對歹徒可能佔領重要據點進行抵抗時，必須有奪回據點的策略。若歹徒成功奪取核物料並離開設施，必須有追蹤並奪回核物料的策略。最後，針對一般民眾的抗議、示威活動，必須有防止破壞的行動計畫。

運用武力進行應變具有一定的危險性，為降低可能導致的傷害，平時的準備必不可少，包括裝備、訓練、指揮與協調，都必須以人員的安全為最優先的考量。

(18)效能測試計畫（Performance Testing Program）

效能測試涵蓋實體保安系統中的偵測、延遲及應變武力三個面向，為簡化測試過程的複雜度，課程建議每個面向應分成四個層級進行測試，即元件、子系統、系統、及全系統測試，其中全系統測試意指整個實體防護系統的測試。在實體保安系統建立前，或有任何改變時都應進行測試，測試地點及環境可依實際需要進行。

測試前應仔細規劃測試程序，並與相關單位預先溝通協調，避免影響設施正常運作；測試中須完整紀錄測試數據，以作為後續效能分析的重要依據。

(19)偵測效能測試（Performance Testing：Detection）

偵測效能測試的目的在於確認元件及系統的運作符合設計要求，其主要指標為 $P_D$，即偵測機率(Probability of Detection)，定義為偵測成功次數除以偵測次數，如下式：

$$P_D = \frac{偵測成功次數}{偵測次數}$$

由於測試過程屬於一種抽樣方法，課程中說明如何利用信心水準(Confidence level)及信賴區間(Confidence interval)，評估測試

結果的準確性。簡單來講，信心水準是指實際的 $P_D$ 落到信賴區間的機率；而要提高信心水準，可經由增加測試次數達成，導致測試成本增加。因此，在測試前必須先決定信心水準以確認所需的測試次數，並謹慎規劃、控制測試過程，避免預期外的因素影響測試結果。

課程中建議，在初次測試或測試新建系統前，可進行先期測試，以了解可能發生的狀況，並減少測試成本。

(20)建立延遲數據資料庫（Building Your Own Delay Database）

每個設施都必須建立自己的延遲數據資料庫，作為評估延遲效果的基礎，課程建議的數據建立方式如下：

a. 由設備的製造商提供測試數據。
b. 實際測量並收集數據。此為最常見的做法，但必須注意測試條件必須一致，例如針對歹徒攀越障礙物所需時間，量測時應確保測試者的狀態一致。
c. 由其他方式蒐集數據。例如參考網路上的影片、到工廠觀察作業情形、或到拆除現場實際量測破壞時間。
d. 由理論或實驗數據推估。

前述方法在應用時必須注意數據來源與實際狀況的差異，尤其在應用於設計基準威脅的評估時，必須注意歹徒的能力與數據來源之間的差異，例如網路影片的錄製者，可能比歹徒更熟悉相關作業程序；當歹徒進行破壞行動時，可能不會考慮自身安全，因此行動可能更快速。此外，應將其他可能的影響因素納入考量。例如對於較長時間的破壞行動，應考慮歹徒因體力下降而導致延遲時間增加的可能性。

(21) 應變效能測試（Performance Testing: Response）

如同在效能測試計畫中所說明的，應變效能測試區分成三個層級進行，以下分別就每個層級的執行方法進行說明：

a. 元件：對象為警衛或其他應變武力人員、應變系統設備、以及應變程序，課程中建議於此一層級採取

的測試方法稱為 Time Motion Study，需量測從接收到信號、到完成反應所需的時間，例如應變武力人員從完成著裝到抵達指定地點的時間。

也可測試一連串應變動作完成的時間，例如應變人員從接收到指令、分析狀況、分配任務、著裝到抵達指定地點的時間。這種測試目的主要是針對應變能力及相關技術的熟悉程度。

b. 子系統：使用的測試方法稱為 Alarm Response and Assessment Performance Test (ARAPT)，對象為整個應變系統人員及設備，採取不預警演練方式，測試時必須先與設施經營者制定相關計畫，避免造成設施運轉的安全問題，並且於測試過程量測各重要階段的時間點，例如偵測時間點、評估及通報所需時間、延遲時間、應變完成時間、歹徒破壞完成時間。

c. 系統：課程中稱為 Enhanced Limited Scope Performance Test (ELSPT)測試方法，可視為 LSPT 的進階做法，差異在於納入部分偵測及延遲設施，以評估應變人員對於偵測信號及延遲設施的熟悉程度，並量測其反應時間。

(22)全系統測試（Whole System Testing）

系統測試的最高層級即為全系統測試，將偵測、延遲、以及應變功能同時納入測試程序，並記錄兩個重要的系統效能指標：攔截能力及弭平能力。系統測試的情節設定須依據設計基準威脅，測試結果有助於改善設施的各項應變計畫以及防護措施，此外，可作為訓練時的重要依據。

系統測試的方法為兵棋推演、電腦模擬及實兵演練，前兩者所需費用最低，結果的再現性較高；但實兵演練較貼近實際狀況，相關結果的分析及檢視亦比較容易進行。實際應用時應考量設施防護需求擇一採用。

**步驟三：完成步驟二的設計階段之後，進入實體防護系統評估（Evaluation of Physical Protection Ssystems）階段。**

本階段的目的在於確認設計結果是否達到步驟一所定義之防護需求，並尋找可能的改善機會。以下簡述各節課程內容：

(23)實體防護系統評估簡介（Introduction to the Evaluation of Physical Protection System）

DEPO 方法論係由成功攔截機率（$P_I$）及成功弭平機率（$P_N$）計算系統效能 $P_E$，亦即 $P_E = P_I \times P_N$。其中，成功攔截代表應變武力於歹徒達到目的前完成佈署，使其行動遭到中斷；成功弭平則代表應變武力制服、逮補或殲滅歹徒。

課程中使用「路徑分析」方法計算成功攔截機率，借助 ASD(Adversary Sequence Diagram)及程式工具計算歹徒入侵所需時間，以及應變武力到達所需時間，即可得出 $P_I$ 值。至於成功弭平機率的計算方式，可選擇由情境分析、兵棋推演及實兵演練等方式進行評估。

在課程中曾針對此一系統效能 $P_E$ 的計算方法提出質疑，因理論上 $P_I$ 及 $P_N$ 必須為兩個獨立變數，其計算結果才會呈線性變化，否則任兩次測試的 $P_E$ 無法比較。例如，$P_I$ 及 $P_N$ 都與應變武力有直接相關，其計算結果可能過分偏重應變武力，無法公平看待其他因素的影響。講師認為實務上為線性，但可視情況深入研究。

(24)路徑分析簡介（Introduction to Path Analysis）

本課程中對於入侵路徑(Path)的定義，除了歹徒入侵的途徑，還包括過程中的時序，因此，經由路徑分析的結果可決定應變武力阻止歹徒入侵成功的機率，即為成功攔截機率（$P_I$）。

路徑分析作業需使用步驟一及步驟二所建立的實體防護系統模型及相關數據，針對可能的入侵途徑模擬入侵時序（Adversary Timeline）及應變時序（Response Timeline），將兩者合併後呈現如圖 4。在實體防護系統中，應變的起始點來自於入侵途徑上的偵測裝置，從裝置發出警報到歹徒行動完成為止，若應變武力及時抵達即為攔截成功，因此，攔截成功機率受到偵測

成功機率、延遲時間、應變武力反應時間的影響。由圖 4 可知，在某個偵測時間點之後應變武力即無法及時抵達，稱為關鍵偵測點（Critical Detection Point, CDP）。

綜上所述，只要關鍵偵測點前任一設備成功偵測並發出警報，即可達成攔截任務，因此，可將攔截成功機率 $P_I$ 定義為 CDP 前偵測設備偵測成功機率。由於關鍵偵測點決定攔截成功與否，因此在設計偵測設備與延遲裝置時，必須依據分析結果謹慎考量。

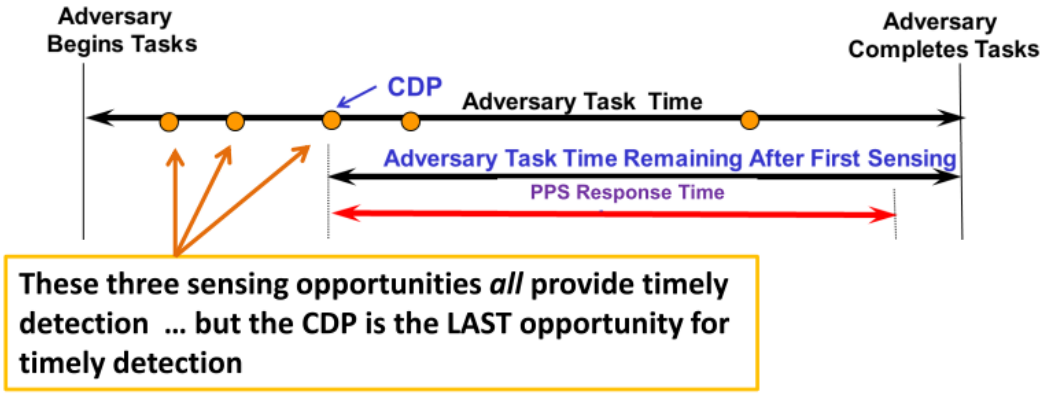


圖 4 關鍵偵測點概念示意圖

(25)威脅時序圖（Adversary Sequence Diagrams, ASD）

任何設施皆具有多種可能的入侵路徑，本節課程的目的在於決定其中最脆弱的路徑以進行後續分析，所使用工具稱為威脅時序圖（Adversary Sequence Diagrams, ASD），如圖 5 所示。其基本概念為，將實體防護設施由外而內簡化為數個層級，在圖上以由上而下的方式呈現，包括圍籬(Facility Fence)、通道、建築物及標的物，並加上各設施的偵測機率($P_D$)及延遲時間(T)，即為設施的威脅時序圖模型。

該模型假想歹徒由最上方的廠區外界展開入侵行動，每個層級皆有一個到數個不等的入侵路徑可供選擇，最後得出在特定威脅情境及目標下，每個可能入侵路徑的總偵測機率及總延遲時間。由於模型本身的特性，不同的威脅情境必須加以分類，例如偷竊與破壞必須分別建立模型以進行評估，以了解設施面對不同威脅的防護效能是否足夠。

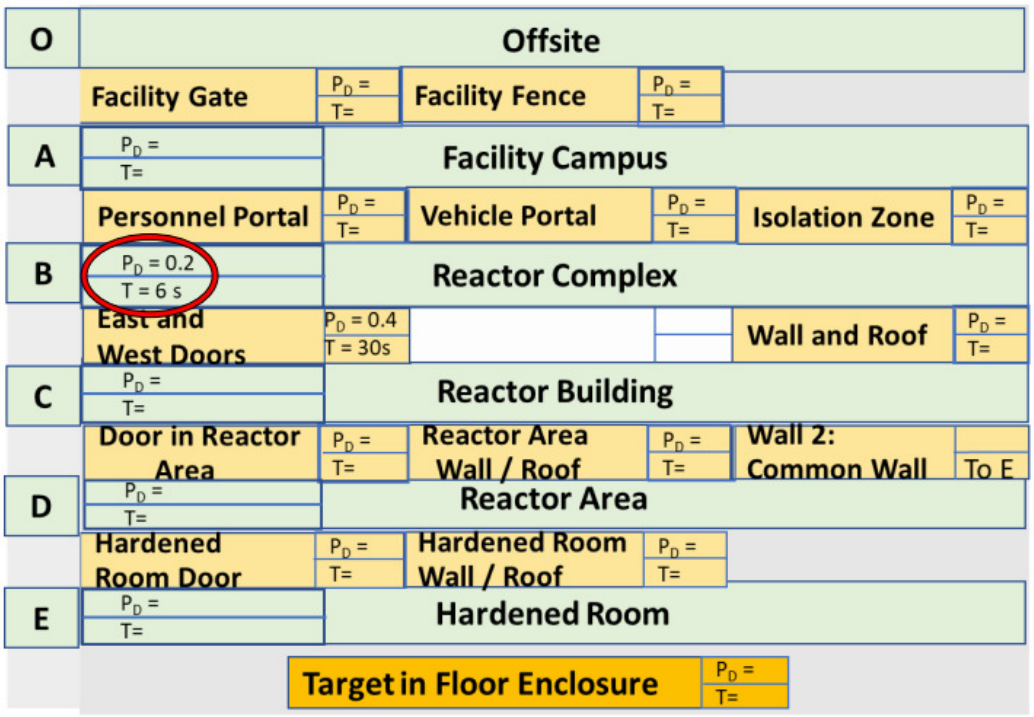


圖 5 威脅時序圖

(26)多重路徑分析（Miltipath Analyis）

在建立 ASD 模型之後，為評估各種威脅情境下最脆弱的路徑，本課程使用由聖迪亞國家實驗室開發的 MPVEASI（Multi-Path Very-simplified Estimate of Aversary Sequence Interruption）軟體進行分析作業。該軟體所需的輸入參數包括：1. ASD 模型；2.偵測機率及延遲時間；3.應變數據，包括實體防護系統的應變時間及應變策略，在軟體中可使用的策略為拒止(Denial)及包圍(Containment)。

完成輸入作業後，MPVEASI 軟體即可決定各路徑的 CDP，並由此計算出 $P_I$ 值以決定最脆弱路徑。

(27)弭平分析（Neutralization Analysis）

課程中計算成功弭平機率（$P_N$）的方式為：

$$P_N = \frac{成功弭平次數}{遭遇次數}$$

由於 $P_N$ 受到許多因素的影響，包括雙方人數、武器、戰術、訓練等等，實際上並無統一且精確的方式可供依循。課程中所建議的計算方式包括：專家判斷、程式模擬、參考實際案例、或實兵演練。以教材中所提供之弭平機率表為例，係以其設施為基礎，以其應變武力為對象蒐集資料後編輯而成，僅能做為參考範本，不能直接套用在我國的核設施實體防護系統設計。此外，針對實兵演練的替代方案，講師以歹徒越獄為例，說明可蒐集類似案例以統計成功弭平機率，做為系統設計時的參考。

(28)情境分析（Scenario Analysis）

比較情境分析與前述的路徑分析，後者偏重以防護系統的構成為出發點，找出其可能存在的弱點以進行補強；前者則從歹徒的視角出發，以各種可能的手段嘗試破壞或滲透實體防護系統，以搜尋路徑分析時存在的盲點，其做法與資安防護中常見的「白帽駭客」類似。

課程中建議在進行情境分析時可採取系統化與結構化的方式進行。首先應確認假想情境的類別與範圍，可依據法規要求、設施特性、設計基準威脅等進行考量。第二步需進行情境細節設計，可分成應變人員與歹徒的劇本，內容可參考路徑分析的結果，納入設施最脆弱路徑進行設計，以確認最嚴重(但不超過設計基準威脅)情況下所可能發生的事故。第三步進行情境確認，確認所有測試目的已被納入情境中、設施條件是否正確、情境是否合理可行。第四步依據情境進行模擬，方法包括程式模擬、兵棋推演或實兵演練，以確認防護系統效能，並從模擬結果尋求改善之道。

(29)兵棋推演分析（Tabletop Analysis）

本節課程說明使用兵棋推演進行情境模擬的方法，實作情形如圖 6 所示。課程中建議將人員分成進攻組（Adversary Team）、防守組（Guard and Response Force）、評估組（Evaluation Team）及仲裁者（Exercise Moderator）。推演時由攻守雙方依據假想情境進行推演，設施起始狀態及人員位置分別由攻守雙方決定，若發

生爭議則進行協調，協調失敗則由評估組負責裁判。推演結果則由仲裁者負責裁定。

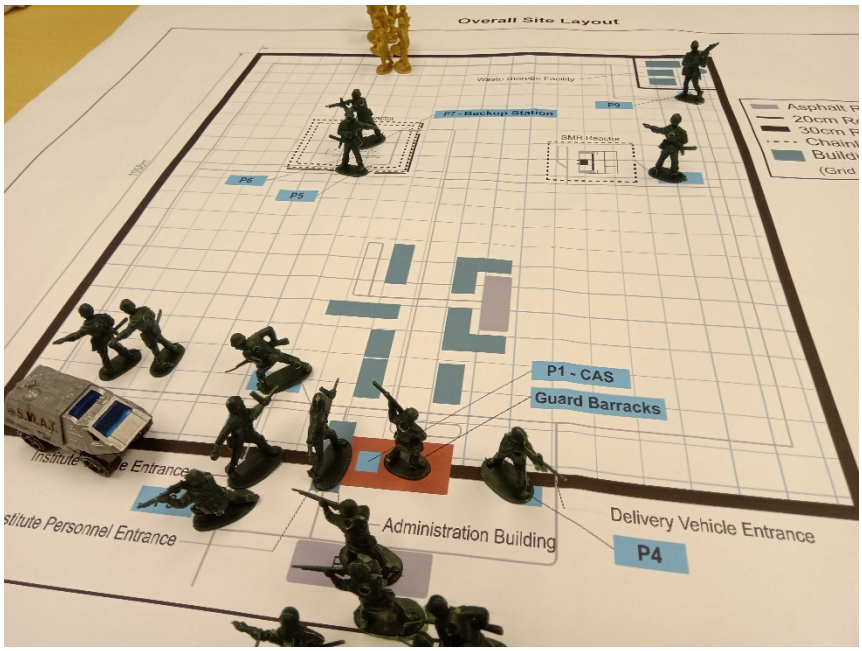


圖 6 兵棋推演

推演時對於重要事件發生點及結果、攻守雙方的重要決定都應加以記錄，包括歹徒穿越重要設施、應變武力評估作業、攻守雙方遭遇時間及地點、對抗過程等。至於推演過程參考的數據，亦應一併紀錄其來源。

實際推演時發現，各崗哨的視野對推演結果有重大影響。即使在日間，位於崗哨內的應變人員並不一定能及時觀察到翻越圍牆或穿越廠區的歹徒，而須仰賴入侵偵測設備(例如 CCTV)的輔助。因此在推演時，本分組即針對該情境使用模擬軟體確認，以保證結果的合理性。

(30)資訊安全（Information and Computer Security）

由於實體保安系統對於資訊系統的依賴，歹徒已將資安攻擊作為入侵核設施的重要手段，包含門禁管制系統、入侵偵測系統、辦公室資訊系統、反應爐相關安全系統等，皆可能成為資安威脅的目標。

針對資安攻擊不易被查覺的特性，課程中建議採用深度防禦的概念，將系統依重要性分級並採取相應的保護措施。除以行政

管制避免資安漏洞，在資訊技術方面，課程建議應注重網路的分區與隔離，避免因單一漏洞造成大範圍的損害，各網路區域之間應有適當的防護措施，例如以防火牆隔離；同時應定期進行系統掃描與檢測，並限期完成漏洞修補，避免遭致駭客利用。

在課程中講師示範以偽造的磁條門禁卡欺騙門禁管制系統，並可順利通過驗證。經實際示範顯示，磁條卡的偽造難度較低，建議在重要設施應採取多重驗證措施加強管制，例如增加密碼鎖等。

(31)運送安全（Transportation Security）

在運送過程中，核物料就離開實體防護系統的範圍，處於公開的環境之中，其安全考量與核設施有許多差異。舉例而言，運送過程所處的位置持續改變，除了歹徒可隨意選擇攻擊位置，沿路的監管規則也可能有所差異。上述這些因素都必須納入運送計畫的考量範圍。

課程中建議，可參考實體防護系統設計運送過程保安計畫。在運送過程中，偵測功能以人員的目視觀察為主，偵測設備為輔，例如在運輸路線上派遣先遣人員進行偵查。運送車及核物料容器本身可加裝防護設備，增強對歹徒入侵的延遲效果，例如裝設被動型或主動型屏障。另外，為預防運送車遭歹徒劫持後駛離，可在車輛動力系統加裝各種開關，以強制關閉油門或鎖死煞車等，達到阻止歹徒的目的。

應變武力為運送過程保安計畫的重點，講師建議須加強其使用的通訊設備及武器，同時在訓練中加入對運送過程的演練，以提高其應變能力。

(32)核子方案計畫（Nuclear Program Plans）

課程中將核子保安計畫（Nuclear Security Plan）、應變計畫（Contingency Plan）、緊急應變計畫(Emergency Plan)，統稱為核子方案計畫，並說明各計畫的關聯及相關重點。

應變計畫屬於核子保安計畫的一部分，主要針對核物料遭竊或遭破壞的緊急狀況，提供應變人員指引以找回失竊的核物料。

由於緊急狀況的發生難以預知，課程中建議採取系統化、結構化的計畫建構方式，事先指定成員的職責與角色，建立確實可用的通信方式，並準備應變所需的裝備及器材。應變措施應結合相關單位定期演練並檢視計畫內容，以提高應變效能。講師特別於課堂上以 1993 年美國德州韋科慘案為例，強調事前協調、詳細計畫與溝通聯繫的重要性。

緊急應變計畫則處理事件造成的放射性物質外釋，其事件成因包括天災、人為疏失、安全設備失效等。在事件發生後，應變人員須依據計畫進行緊急處置，減少放射性物質所造成的危害，並保障民眾生命財產安全。由於緊急應變計畫與核子保安計畫皆與核物料有關，在計畫及執行階段須注意兩者間的指揮、協調、分工及聯繫，同時確認各相關單位在事件處理的角色，避免產生衝突或三不管地帶，造成歹徒有機可乘。

完成上述 32 項課程後，本分組依主辦單位指定，以虛擬核電廠 LPNPP（Lone Pine Nuclear Power Plant）為對象，運用「實體防護設計與評估流程」，進行實體防護系統評估(分組研討情形如圖 7)。LPNPP 位於虛擬國家拉卡錫的東南方，建於 1972 年，廠內有一座雙迴路壓水式反應器。依據主辦單位提供的資料為基礎，本分組建立 LPNPP 的設計基準威脅，並界定兩個可能的受威脅目標，分別為用過燃料池及主控制室。在為期一週的結訓報告研討期間，本分組假定歹徒以上述兩個目標進行攻擊，並採取路徑分析與兵棋推演分析防護系統效能。最後經由分析結果檢討防護系統的弱點，並提出改善建議。

主辦單位安排全部分組於課程最後一天，對講師及全體學員簡報研討成果（簡報過程如圖 8），簡報內容包括分析方法、結論及心得分享，最後並由講師講評各組簡報內容作為課程的總結。

圖 7 分組成員研討情形


圖 8 結訓成果上臺報告

# 肆、 心得及建議

一、 在恐怖主義猖獗的現代局勢中，核設施經常被視為可能的攻擊目標之一。為應付各種可能的攻擊情境，實體防護系統的設計日趨複雜，各應變組織的分工亦日趨精細，因此，如何確實依據應變計畫執行相關步驟，有賴核設施經營者落實整備要求、確實執行應變演練。

二、 實體防護系統的效能來自於設計良好的偵測與延遲設備，加上訓練有素的應變人員共同合作，以應對各種保安威脅。其中偵測設備為應變作業的第一線，若能於第一時間偵測到惡意威脅，則可提供充足的應變時間，以順利阻止歹徒行動。因此，設施經營者應模擬可能的入侵行動，以測試偵測系統效能，確保核設施安全。

三、 本次課程中與各國學員經驗交流，除能獲得國際間最新保安知識，更促進各國從業人員的互相了解。尤其在分組研討期間腦力激盪，共同模擬歹徒與應變武力的計畫與行動，充分應用課堂講授內容與對核設施的專業知識，互相切磋，實為一難得的經驗。鑒於我國目前非 IAEA 會員國，更應藉此機會促進交流，不論在增強管制作為或設施保安技術方面都有正面助益，建議持續派員參訓。