出國報告(出國類別：實習)

參加第 27 屆
國際核子保安訓練(ITC-27)研習

服務機關：台灣電力公司
姓名職稱：蘇拓殷/核能保安專業管理師
派赴國家：美國
出國期間：107.04.28 到 107.05.21
報告日期：107.06.07

行政院及所屬各機關出國報告提要

出國報告名稱：第二十七屆國際核子保安訓練

頁數 23 含附件：□是■否

出國計畫主辦機關/聯絡人/電話

台灣電力公司/陳德隆/23667685

出國人員姓名/服務機關/單位/職稱/電話

蘇拓殷/台灣電力公司/核能發電處/核能保安專業管理師/23667053

出國類別：□1 考察□2 進修□3 研究■4 實習□5 其他 洽公

出國期間：107.04.28~107.05.21　　出國地區：美國

報告日期：107.06.16

分類號/目：保安

關鍵詞：核子保安、ITC

內容摘要：(二百至三百字)

赴美國新墨西哥州聖迪亞國家實驗室參加第27屆「國際核子保安訓練」(ITC) 研習。ITC自1978年11月舉辦以來，每18個月舉辦1次，前26屆累積了來自72個會員國的884位學員，堪稱歷史優久也是目前國際間最完整、深入之核子保安訓練。本次課程以課堂講授、分組討論、現場觀摩、設備展示、專題報告及實地參訪等方式，並輔以電腦程式模擬演練。研習的目的，希望各國的核子保安相關人員(官方、業者與研究機構等)，系透過系統化的訓練，能夠學習並切磋核子實體防護保安系統的建構與評估方法，在自己的崗位上實際應用，以提升各國核子物料貯存設施與核子反應器設施之保安防衛與實體防護能力，降低核子設施被破壞或核子物料失竊之風險，有效抵禦歹徒的暴力攻擊或偷竊行為，保障核子設施與核子物料之安全。

本文電子檔已傳至出國報告資訊網(http：//Report.nat.gov.tw/reportwork)

目　　錄

頁次

壹、 出國目的與過程

一、目的

國際原子能總署(IAEA: International Atomic Energy Agency)為貯備各會員國有足夠的智能與技能、可助於規劃防範核設施遭受蓄意破壞(Sabotage)及核物料失竊(Theft)的人才，委託美國能源部(Department of Energy,簡稱 DOE)「聖迪亞國家實驗室」 (Sandia National Laboratories,簡稱 SNL) 辦理「國際核子保安研習」(The International Training Course on the Physical Protection of Nuclear Facilities and Materials, 簡稱 ITC)，各國依分配名額派員參訓。

「國際核子保安研習」(ITC)歷史優久，自 1978 年 11 月舉辦第一屆以來，平均每 18 個月舉辦 1 次，今年已是第 27 屆(ITC-27)，從 ITC-1 到 ITC-26 共累積了來自 72 個會員國的 884 位學員(如圖 1)，堪稱目前國際間最完整、最深入之核子保安訓練。本屆(ITC-27)有來自 40 個會員國的 51 位學員(如圖 2)，另主辦單位特提供兩位觀察員名額給我國，由原能會派一員參加，另分配一個名額給台電公司，以利本公司在核子保安上與原能會有相同的理念。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、防護技術與設備，以及國際最新指導原則、法規等文件)。

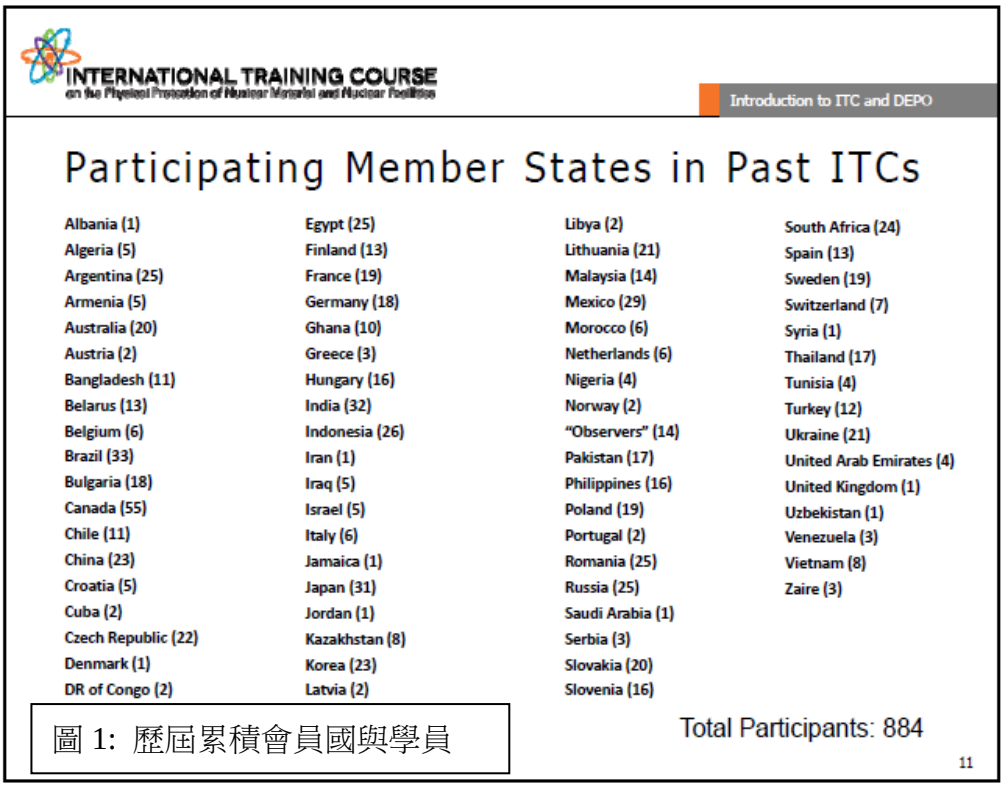

圖 1: 歷屆累積會員國與學員

本研習目標為希望各國的核子保安相關人員(官方、業者與研究機構等)，系透過系統化的訓練，能夠學習並切磋核子實體防護保安系統(Physical Protection System，簡稱 PPS)的建構與評估方法，在自己的崗位上實際應用，以提升各國核子物料貯存設施與核子反應器設施之保安防衛與實體防護能力，降低核子設施被破壞或核子物料失竊之風險，有效抵禦恐怖份子暴力攻擊或偷竊行為造成公眾及環境危害，保障核子設施與核子物料之安全。

圖 2: 本屆會員國與學員

二、行程

本次任務出國期間自中華民國 107 年 04 月 28 日至 107 年 05 月 21 日止，共計 24 天，行程內容如下：

日期	地點	內容
4月28 日	台北→美國新墨西哥州阿布奎基市	去程
4月29 日	阿布奎基市	報到
4月30 日～5 月 4 日	聖迪亞國家實驗室	訓練課程
5 月 5 日～6日	阿布奎基市	週末
5 月 7 日～11日	聖迪亞國家實驗室	訓練課程
5 月 12 日～13日	阿布奎基市	週末
5 月 14 日～18日	聖迪亞國家實驗室	訓練課程
5 月 19 日～21日	美國新墨西哥州阿布奎基市→台北	返程

三、執行過程與內容

I. 出國任務執行過程（研習方式）：

本訓練課程由聖迪亞國家實驗室(SNL) 代表美國能源部(DOE) 所設計：

1 課程目標：研習課程結束時，學員能依教授的方法與學理來設計和評估核子設施被破壞或核子物料失竊之風險，做出適當的實體防護。

2 課程設計：分為課堂講授(Lecture Sessions，含專題演講 Guest Speakers)、分組實作(Subgroup Exercises)及示範觀摩(Equipment Demonstration)等方式進行，本次主辦單位借每位學員一台載有課程的 ipad，以利無紙化，在每一單元結束時會有三題小測驗，於課堂上立即統計每道題的正確率，針對答錯率較高的部份，立即進行討論說明，協助學員觀念釐清，最後則以結訓成果報告(Final Exercise Report)作為總結。

2.1 課程講授：依照 DEPO (Design and Evaluation Process Outline)的原則逐步建構核子設施實體防護系統(PPS)，DEPO 分為三部分：系統需求(Define Requirement)、系統設計(Design)及系統設計評估(Evalution)依序進行，DEPO 課程計有 26 個單元，每一單元均由專業講師擔任課堂講授，課堂後分組實作，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。另外尚有專題演講等課堂講授，目的在強化核保安文化，講師來自 IAEA、核管會(Nuclear Regulatory Commission, NRC)等專家就核子保安相關議題、法規文件等發表專題演講，並請巴西、南非與法國之業界專家(都是前幾期的學長、姐)介紹所屬機構的核子保安現況。

2.2 分組實作期間，各課程講師主辦單位將 53 位學員分為 6 小組，每小組 8～9 名學員，進行分組實作練習。利用一虛構之核子設施以紙上作業做為分組實作時 PPS 建構練習標的，由聖迪亞國家實驗室專家擔任分組指導員(Subgroup Instructor)，指導每位學員對該單元能一起充份討論與演練。最後報告題目設計另外兩個虛擬核設施，3 組以一個研究用反應器(Hypothetical Atomic Research Institute facility, HARI)、另 3 組以一座核電廠(Lone Pine Nuclear Power Plant, LPNPP)，進行整體實體防護系統設計，而學員則需運用受訓教材中所學的經驗，小組一起完成設計、建構及評估與改善上述兩個虛擬核設施之 PPS 系統，結訓前須完成製作成果報告，並於結訓日小組輪流上臺發表，接受講師及其他學員之提問及指教。

2.3 示範觀摩：為使學員更加深印象且有身歷其境的臨場感，主辦單位在 SNL 訓練場，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，並由學員以碼表計時完成破壞時間，藉以瞭解運用不同工具破壞不同遲滯屏障材料的難易程度及所需時間。

圖 3：氣焊槍破壞示範

於 SNL 的「保護區圍籬測試場」(Test Field)，學員們現場觀察包括雷射(Laser)、振動(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，並完成記錄。

此外，主辦單位安排學員於「實彈射擊訓練中心」觀看訓練中心教官進行對徒攻堅示範，及手槍、來福槍、輕機槍及槍榴彈發射器等各類型武器展示與說明其破壞力，及說明如何訓練所屬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。

II. 課程內容

國際核子保安訓練課程設計安排，係以核子設施實體防護系統(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) 三部份為主軸，PPS 整體建構流程稱作「實體防護設計與評估流程」(DEPO)，依據建構流程及其內容計有 26 項專業課程，課程圖示(如圖 4)及各項課程簡介說明如下：

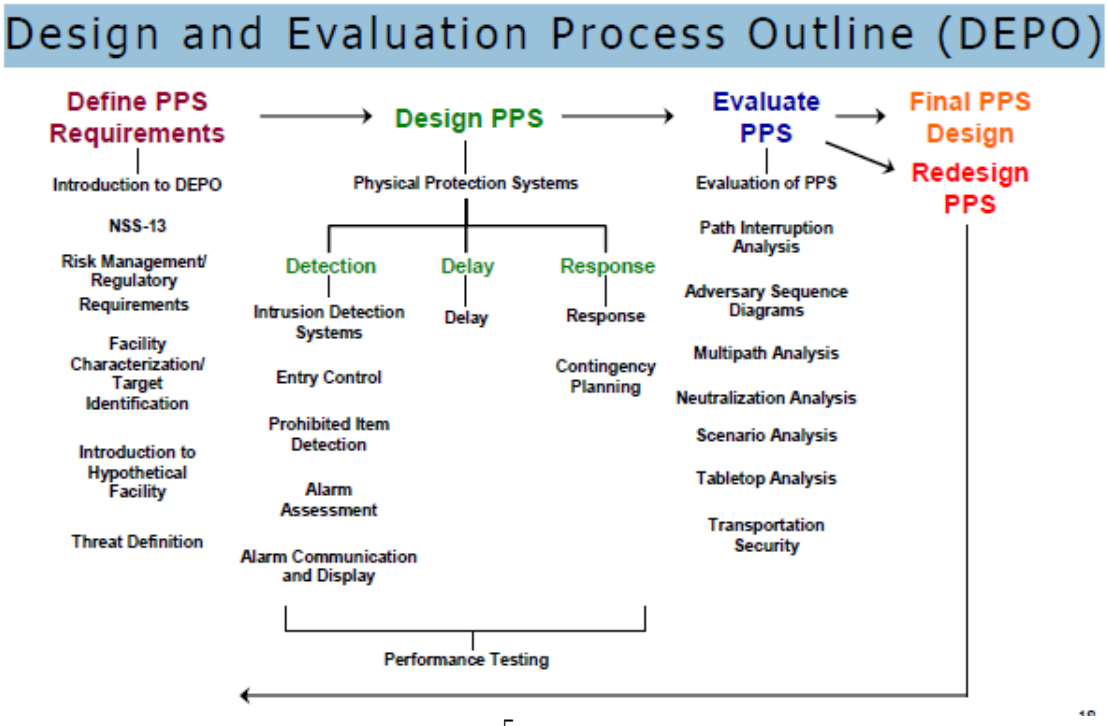

圖 4、DEPO 流程及其 26 項專業課程

1. 確認實體防護系統需求(Define PPS Requirement)

DEPO 的程序首先要確立保護標的物與威脅來源，作為後續系統設計、評估基礎，各項課程內容簡要說明如下:

1.1 實體防護設計與評估流程(DEPO)介紹

保安系統目的在於防止核物料於使用、儲存或運輸過程中失竊(Theft)或核設施遭受恐怖暴力攻擊、破壞(Sabotage) 等被用來製成民眾恐慌的事件發生。本課程在介紹建構核子保安系統 DEPO，使來自不同背景的學員們，能先建立此一概念，以利後續課程之展開。

1.2 INFCIRC/225/Rev.5 核子保安建議(NSS-13)

IAEA 為使成員能有所共同的規範，建立核子保安系統國際標準，1975 年發表第 1 版：INFCIRC/225(核子保安系列第 13 號，NSS-13)，供會員依循，並於 2011 年 1 月發表第 5 版修正。本課程說明 INFCIRC/225 第 5 版修正目的及增訂建議內容，包括「防止非法竊取核物料」、「尋回復原失竊核物料」、「防範破壞核設施」及「減輕核設施破壞後果」等 4 大目標，核物料實體防護公約(CPPNM)修正版 12 條基本原則(包含責任界定、國際運輸、深度防禦、安全文化、品保等)，以及核材料在使用、儲存、及運輸時之相關防護建議等，另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。

1.3 風險管理與法規要求(Risk Management and Regulatory Requirements)

良好的風險管理才能建構好的防護，課程介紹風險和風險管理，教導學員確定風險管理的法規基礎，應用於核子保安，以找出減少風險的方法。核子保防風險管理三因子：核設施威脅的可能性(P_A)、威脅成真的後果、PPS 成功防止威脅的效能(P_E)，考量降低 P_A 與後果、提升 P_E 即可降低核子保防風險。降低 P_A 可藉由偵測與延遲來達成，靠著應變武力阻擋、弭平可降低後果，而偵測、延遲與應變的效能就影響了 P_E。最後，規劃矩陣表(如表 1)在考量成本效益下，定出最佳 P_E 值。

Notional P_E Matrix

TARGET	LOCATION	THREAT	SCENARIO	P_E
Fresh Fuel	Vault	Outsiders (Terrorists)	Overt Attack	0.80
Fresh Fuel	Vault	Outsiders (Terrorists)	Covert Attack	0.90
Fresh Fuel	Vault	Insider	Remove during maintenance	0.90
Fresh Fuel	Vault	Insider	Falsify shipping paperwork	0.95

表 1 矩陣表範例

1.4 核子設施的特性與目標的界定

為了滿足防護系統設計、評估需要，必須對核子設施運轉、環境、安全及法律規及營運特性等，先進行資料收集，並確認可能遭受的威脅(可能直接或間接造成均要列入考量)。依據 INFCIRC/225 之「核物料分類表」(Categorization of Nuclear Material)介紹國際間最主要之核物料防護等級三項分類(I, II, III)之保護要求，界定出所要防護的目標，依不同分類，訂定核設施之保護區(protected area) 、限制區(limited area)與緊要區(Vital Area)。依每個設施所在環境條件不同，應有不同的風險與威脅後果，界定出那些可能造成不可接受的輻射後果(unacceptable radiological consequences, URC)或高輻射後果(high radiological consequences, HRC)的核設施與物料而加以保護。

1.5 虛擬核設施的介紹

介紹虛核子設施，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元素，包含偵知、延遲裝備數量，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顯示廠區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、天花板等防護單位，另同步輔助 3D 電腦動畫模型加強說明，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佈署，俾利進行後續一系列設計改良分組實作課程。

1.6 威脅評估

偷竊(Theft)與蓄意破壞(Sabotage)是 PPS 所要對抗的二大威脅，設計者必須以假想之最大可能威脅來作為實體防護系統設計之基準，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：

(1)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。

(2)調查攻擊動機或意圖，例如：意識形態、謀財、報復等。

(3)評估犯案能力，例如：人數、使用武器類型、爆裂物類型及數量、輔助攻擊工具、運輸、移動、專業技術、是否有內部潛伏破壞份子等。

經彙整、篩選模擬各種對核設施造成威脅的可能，再考量所能接受最大風險，成為可能的設計威脅基準(DBT)。在評估 DBT 時，據以參考的背景情資可靠度是非常重要的，因為若低估風險，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。

而依前述 INFCIRC/225「核子物料與核子設施之實體保護」要求，各國政府須自行訂定設計基準威脅，需考量核設施業者有能力據以擬定保安計畫，而需整體國家防衛力量來防治者(像是 911 之攻擊)不應列為 DBT。

2. 實體防護系統設計(PPS Design)

完成確認實體防護系統需求，DEPO 的下一目標為設計實體防護系統課程，內容計有：PPS 三大功能(偵測、延遲、及應變)設計過程，防護系統工程設計原則(縱深防禦、弱點防護平衡性及可靠度要求)，衡量效能方式(計算偵測機率、延遲時間、反應時間、攔截機率及平亂機率)，以及內部潛伏份子(insider)之防範措施等。說明如下:

2.1 實體防護系統的設計

PPS 必須具備偵測(Detection)、延遲(Delay)與應變武力(Response Force)三大功能的防禦系統。首先，當歹徒入侵，必須儘早偵測威脅的存在，防止歹徒採取隱密的入侵方式，接近目標物(特殊核子物料或重要核安設備組件)，因此 PPS 必須在適當的位置裝置合宜且靈敏的偵測設備，並設置多重延遲裝

置，爭取應變武力的反應時間，得以及時阻止歹徒可能造成的破壞。以上所述可用時間軸線圖(圖 5)說明：

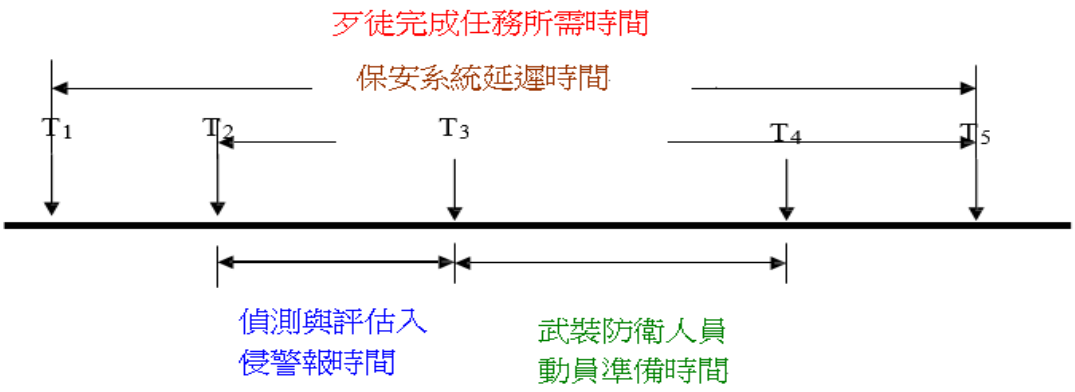

圖 5、PPS 系統時間軸線圖

T_1：歹徒開始執行任務時刻

T_2：PPS 偵測入侵後發出警報時刻

T_3：武裝防衛人員開始準備動員時刻

T_4：武裝防衛人員完成佈署準備展開攻擊時刻

T_5：歹徒完成任務時刻

T_1 至 T_5：歹徒完成任務所需時間

T_2 至 T_3：PPS 於入侵偵測系統發出警報至警報經評估確認所需時間

T_3 至 T_4：武裝防衛人員從接獲動員命令到現場就戰鬥位置所需時間

T_2 至 T_5：歹徒入侵被發現後至完成任務所剩時間。由於此段時間亦是 PPS 設計時希望藉由種種延遲裝置來爭取武裝防衛人員動員時間，故此段亦稱為延遲時間。

由以上可知，PPS 要能成功防禦的先決條件是 $T_4 < T_5$，即武裝防衛人員必須在歹徒完成任務前完成佈署並展開攻擊行動，若要確保 $T_4 < T_5$，一可將 T_4 提前(縮短應變武力動員準備時間)，或 T_3 提前(縮短警報確認時間)，或 T_2 提前(提高及時偵測能力，便於提早發現歹徒入侵)；另一方式則是延長 T_5，即藉由核子設施的層層關卡對歹徒入侵行動產生延遲，以爭取應變武力動員準備時間。

2.2　入侵偵測感測系統(Intrusion Detection System, IDS)介紹

偵測為 PPS 的最前線，IDS 可偵測異常狀況發出警報信號，包括：周界入侵偵測及評估系統(PIDAS - Perimeter Intrusion Detection and Assessment System)、室內偵測系統。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)。其中，偵測率愈高愈能發現非法侵入，另外，誤動作率要盡量低，否則將增加了保安人員的負擔，最後，因不同的偵測器有不同的限制(弱點)及適用環境，因此，在選用偵測器種類時，必須對環境、氣候條件、偵測目標、偵測效率作通盤考量；不同形式偵測器間亦可互補搭配使用，建立完整連續的偵測系統，以增加偵測成功機率。

2.3　門禁管制

門禁管制為延遲設計之一，此系統可允許授權人物的進入，監控並防止非授權人物的進入及經授權者的離廠。本課程介紹不同類型門禁管制系統的原理，包含依據進出人員的(1)所知道的(Something you know)：如密碼(PIN)；(2)所擁有的(Something you have)：如識別證、鑰匙；(3)天生的生物識別特徵(Something you are)：如指紋、虹膜及語音辨識等等特性加以設計。

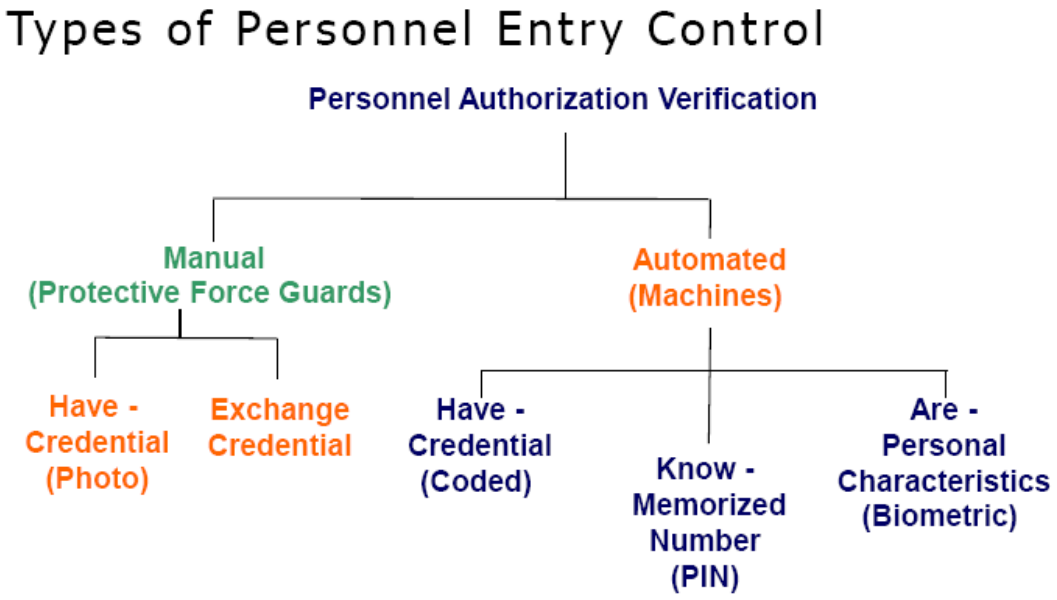

圖 6：門禁管制類型

不同門禁管制系統各有其優點及限制，例如偵測速度快的系統，可能排錯率會較低；反之，則較高，所以，在選擇門禁管制系統時，也需通盤考量環境的適用性，不同特性的檢查方式若能搭配使用，可提升管制的完整性。

若要設立良好的門禁管制系統，須考量下列因素：(1)無法被旁通；(2)人員可監視；(3)可提供武裝人員防護；(4)檢查過程中隔離受檢者；(5)針對未通過自動查驗者執行人工檢查；(6)受保安監控中心監看。

2.4 違禁品(Contraband)偵測

防止內部破壞，先阻絕使用跟器材，違禁品可能包括:武器、爆裂物、工具及放射性物料等，當人員、行李、車輛進出保安區域時，須執行違禁品偵測，通常是允許授權物品的進出，而限制違禁品進入，及核物料的流出。偵測方式有以下幾種類型，包含人工檢查、金屬偵測(武器工具爆裂物)、X 光掃描(行李、背包有無夾帶違禁品)及輻射偵測器(高放射性核物料)等。其中，以人工(含緝毒犬)具備高機動性及敏感度，且能應用於任何爆裂物的偵測，但時間效益差，且起始成本雖低，而維護成本高；若以儀器偵測雖成本較高，但相對節省檢查時間。因此，若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靈敏度。

2.5 警報評估(Alarm Assessment)

警報評估是警報偵測系統的最重要的一環，當完成偵測後若發現異常，系統應立即發出警報示警，判斷是否為雜訊干擾(如天候)或異物(如動物)誤觸，及評估警報內容，以協助提供應變人員正確資訊以迅速弭平入侵。如僅有警報而無法評估及判斷狀況，則偵測無法發揮效益。評估可分為人力及科技產品兩類，人力評估包括警衛、應變武力或當地員警，科技產品則包括影像應用。人力評估優點為機動性較強，可適用於特殊狀況，但缺點則是費用較高；而科技產品評估優點是可長時間連續性的監測，並可記錄相關影像，缺點是儀器後續維護費用高。科技產品最主要是透過影像系統的使用，而影響一個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，必須針對不同環境、天候(雨、雪、霾、霧)等狀況，搭配不同的組合，架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形成視線死角，產生偵測漏洞。常見的影像系統

包括：閉路電視系統(Closed Circuit Television，簡稱 CCTV)，熱成像攝像機(Thermal Cameras)及影像動作感測器(Video motion detection)等。

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

AC&D 主要功能是提供人機介面，將從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)、經過通訊傳遞，到中央處理器整理與展示偵測數據，將數據展現成監控室操作員易於讀取的警報與即時資訊，以利相關應變人員(例如:緊急應變人員、應變警力等)，在不法份子入侵時能有效應變；此外通訊系統應考慮其保密及不易受干擾，顯示方式則須考量人因工程，依重要性分層次加以顯示，以便監看人員掌控全盤狀況，並立即處理緊急情況。

2.7　延遲入侵行動 (Delay)

運用屏障(Barrier)沿入侵者可能選擇之途徑，以預先或臨時部屬障礙物以遲滯歹徒行動，讓歹徒抵達目標物的時間延長，為應變武力爭取更多的時間，能及時阻止歹徒行動。核設施中典型之兩種屏障系統為：

(1) 被動型屏障：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。

(2) 主動型屏障：需要電力啟動，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；或是彈出式交通屏障(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：偵測後立即發揮延遲作用、平衡設計且不形成連續弱點，以及縱深防禦佈署等特性。

2.8　應變(Response)

應變為 PPS 的最後一道設計，分為一般警衛(Guard)：負責檢查、監視、通報功能及防止未獲授權人事物的進出等例行勤務，與應變武力：具特種戰鬥能力的快速打擊部隊，本國為國家級的保安警察擔任。應變武力主要職責有二：其一為當接獲歹徒入侵偵測警報後，必須及時趕往歹徒所在地或欲破壞的目標，以執行攔截並阻止敵意行為；其二為狙殺或逮捕歹徒以防止其達成破壞目的。而要進行一成功的攔截，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或目標地點等眾多環節。而一個完整的 PPS 時間計算則是從第一次警報偵測至應變武力趕往目標地點的時間，其間包含應變部隊通訊、準備、集合、佈署及行動等，並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，故需精確評估反應時間能否及時制止歹徒不法活動。而建置應變武力亦需有周詳計劃、合格人員、精實訓練及確實評估過程，並需經常進行實兵對抗演練，以保持任務執行效率及能力。

2.9 偵測與延遲的效能測試(Performance Testing Detection and Delay)

為驗證 PPS 的設計是否能達到所要求的目標，必需執行效能測試，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)及整體系統測試(Whole System Performance Tests)之評估程序。整個程序，首先要規劃一個測試、執行該測試、蒐集資料、分析蒐集的資料與記錄結果。其目的在於評估 PPS 之人、程序書與設備/技術之效能，找出可能弱項與驗證 PPS 的能力，以確保足夠的防護。

分析蒐集的資料與記錄結果，可以數學式表示：

$$P_D \text{estimate} = \frac{\text{Number of Successful Detections}}{\text{Number of Trials}}$$

P_D 表示能功偵測率，愈高當然愈好，但在考量經濟成本，可以調整在 85%~99%之間，P_D 要配合廠家所保證的信心值(confidence level)、測試次數與成功次數查表得之。

2.10 應變的效能測試(Performance Testing Response)

為整體測試項目之一，設計理念與上項同，驗證應變實力，針對可能的偵、阻與應變的情境逐步演練，整體測試之成功可能是中斷歹徒進攻或成功弭平事件。整體測試可以兵棋推演(Tabletop exercise)、模擬推演(Computer simulation)與實兵演練(Force-on-Force)方式進行，目的在找出 PPS 的有效性(P_E)。

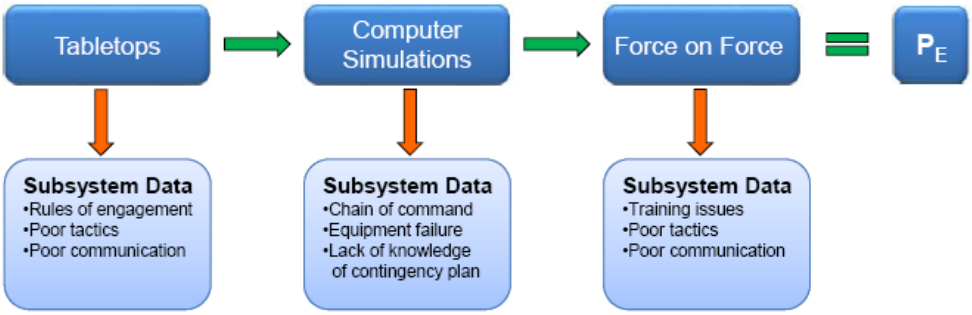

圖 7：各種演練方式

3. 實體防護系統設計評估（Evaluate the PPS Design）

為 DEPO 的第三環，在運用效能基礎（Performanc-based）方法，量化評估分析實體防護系統及其效益，以找出防護系統的弱點並加以改良。

3.1 實體防護系統評估

實體防護系統的有效性(P_E)可藉由量測到的 P_I 值及 P_N 值來確認，即能將其系統的有效性能使用量化數值來呈現，（$P_E = P_I * P_N$ ，P_I＝PPS 成功偵測（Interruption）機率，P_N＝PPS 成功弭平（Neutralization）威脅的機率），P_I 值評估值可由「情境分析」及「路徑分析」計算分析得出在防護目標與歹徒入侵路線確認後，輸入相關參數後，即可由電腦軟體程式計算結果。P_N 值評估值除可由「情境分析」得出外，亦可由兵棋推演電腦模擬及實兵對抗等方式得出。

3.2 路徑攔截分析

沿著所有歹徒可能入侵的途徑，分析實體防護系統之偵測和延遲是否能提供有效的 P_I（P_I＝PPS 成功攔截（Interruption）威脅機率），該值等於臨界偵測點（Critical Detection Point, CDP）之前的成功偵測機率，其值等於（1－臨界偵測點前各點偵測設備失敗機率乘積）(如圖 8)，臨界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 9，入侵偵測系統必須早於臨界偵測點之前發出警報，才能有效攔截歹徒行動。

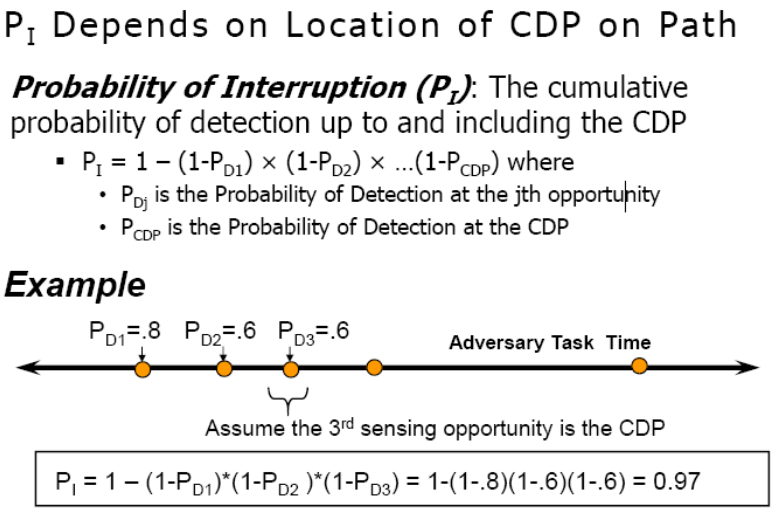

圖 8、侵入者滲透入侵路徑圖之成功偵測機率 P_I

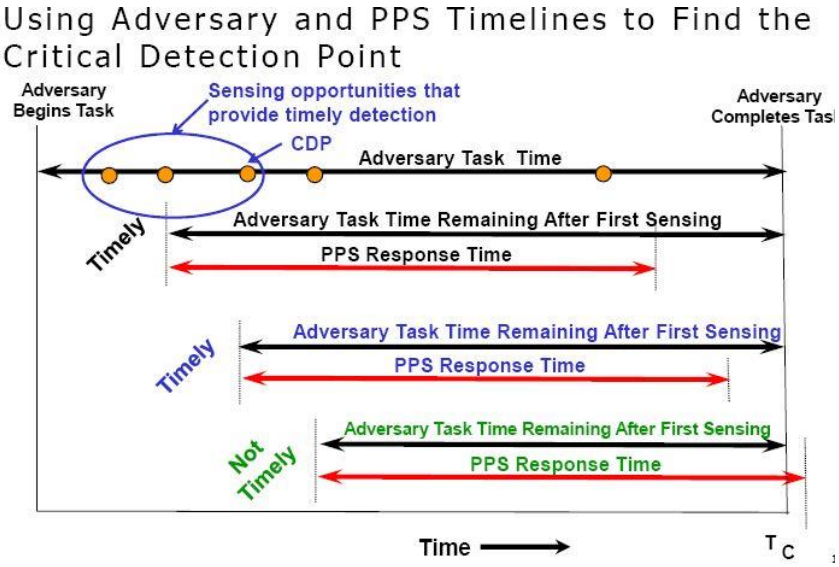

圖 9、歹徒完成任務時間軸（Adversary Timeline）與實體防護系統應變時間軸（Response Timeline）之圖

3.3 侵入者滲透入侵路徑圖（Adversary Sequence Diagram, ASD）

依據現場實況，設定保安目標物及敵方所有可能滲透入侵路徑，繪出詳細的路徑順序，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(ASD)，藉此實際評估實體防護系統在防護上的優弱點，建立基本防護概念。

3.4 路徑分析軟體

路徑分析是利用 Sandia 國家實驗室開發之 MPVEASI 軟體（Multi- Path Very- simplified Estimate of Aversary Sequence Interruption）來算出歹徒最可能入侵到目標物的途徑，即算出最脆弱之路徑，共分三步驟，首先需輸入侵入者滲透入侵路徑圖（ASD）數據，包括每一區域或標的物之偵測機率(P_D)及其延遲時間，接著輸入應變時間數據：包括實體防護系統的應變時間、應變策略（針對直接武力、祕密行動或欺騙三種情形採取的策略）等等，最後按下分析功能鍵得到輸出結果，該結果即最脆弱的途徑(P_I)，並可計算出 CDP，看應變行動是否能成功，若無法成功，就必須針對 PPS 之偵測、延遲與應變 3 項因素加調整。

3.5 弭平能力分析（Neutralization Analysis）

當威脅入侵時，分析應變武力是否具有足夠的能力來阻止歹徒完成惡意攻擊行為，若敵我雙方之武器裝備、人員素質等客觀條件一致情況下，可透過查詢表 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）。

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

3.6 情境分析

藉由情境分析，是以對手的條件來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、歹徒可能採取的路徑、歹徒擁有的專業知識水準及可能掌握的資源等，分析得出實體防護系統整體防禦能力、保安應變計畫、保安政策及程式及跨單位支援協調等各方面弱點，作為後續改進之參考。

3.7　兵棋推演分析

兵棋推演可將人員分成對手組（Adversary Team）、防衛組（Guard and Response Force Team）、評估組（Evaluation Team）及裁判組（Exercise Moderator）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，結束之後評估實體防護系統之防禦弱點，進而提出改善防禦功能建議。

3.8　STAGE(Simulation Toolkit and Generation Environment)工具介紹

是 Sandia 國家實驗室開發之 3D 虛擬實境軟體,可以提供 PPS 之模擬環境。

3.9　簡介核物料帳控 (Nuclear Material Accounting and Control, NMAC)

此單元在介紹核物料帳控之重要性，經適當的管控與立帳，可防止內部之偷竊或非法移轉，我國核電廠已行之多年，在 IAEA 監管下，管控良好。

3.10 內部潛伏份子（Insider）之防制手法

內部潛伏份子的可能擁有三項主要不利防護因素：1.門禁 2.授權 3.知識，可分為主動型與被動型，其動機方面需考量意識形態（可能有政治或宗教狂熱）、財務問題、身心狀態異常、遭人脅迫等。為了降低風險，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，並建立制度使關鍵操作不得單人為之、違禁品檢查、監控系統與 NMAC 等措施。課堂並以世界真實發生案例講解會發生的弱點與防範措施，嚴密的管理與監控可降低 Insider 犯案機會。

4. 其他：專題演講與期未報告

4.1　資訊安全

資訊攻擊是逐步漸進的(如圖 10)，所以資訊安全也要建立類似實體防護系統的防禦概念，建立深度防禦的防護，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）給予最嚴密的防護、次重要的系統給予嚴

密的防護、較不重要的系統則給予原則性的防護。另外確保資訊安全作法可分為以下 3 方面：

A. 行政控制：資安訓練、政策程式（如密碼管理），以及在不影響運作情況下，應實施最小授權原則（POLA，Principle Of Least Authority）。

B. 實體防護：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。

C. 復原減損：做好備援管理，定期製作備份資料、測試備援系統，並提供備援系統與原系統同等級之防護能力。

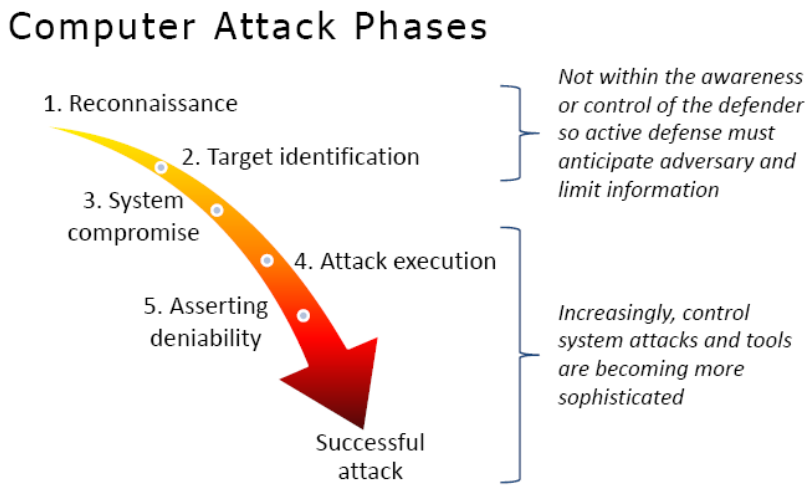

圖 10：資訊攻擊概念圖

4.2 核設施應建立的計畫

為保障核設施之關鍵設備與物料的安全，確保民眾安居樂業，必要建立核設施保安計畫、應變計畫與核子事故緊急計畫，這三項計畫於本國核電廠均實施多年，且在原能會監督指導下日益精進。

4.3 反應器原理

介紹壓水式反應器之燃料五道完整性保護與反應器保護設備，輔以三哩島事件與 Stationery Low Power No. 1 (SL-1) Reactor 實驗式反應器超臨界事件說明為何謂安全系統，以利實作時界定防護目標。

4.4 運送安全

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、破壞等，關於核物料運送之安全防護系統設計，仍依 DEPO 流程設計，最大不同處為運輸是以動態方式進行，故無法設立保護區且路徑會隨環境連續變化等，所以評估過程是以「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，亦須全由押運應變武裝人員負責處理。

4.5 期末報告

訓練倒數第 2、3 天安排專題演講與學員分組準備結訓報告，每一學員集合於分組研究室，相互討論、腦力激盪，合作完成「結訓成果報告」並上台簡報，成果報告須充分運用訓練所學及分組實作時計算、討論之結論及經驗數據等，依組別題目分別設計虛擬核設施：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）設施的實體防護系統，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。

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 30 分鐘，所有學員皆須上臺報告，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。

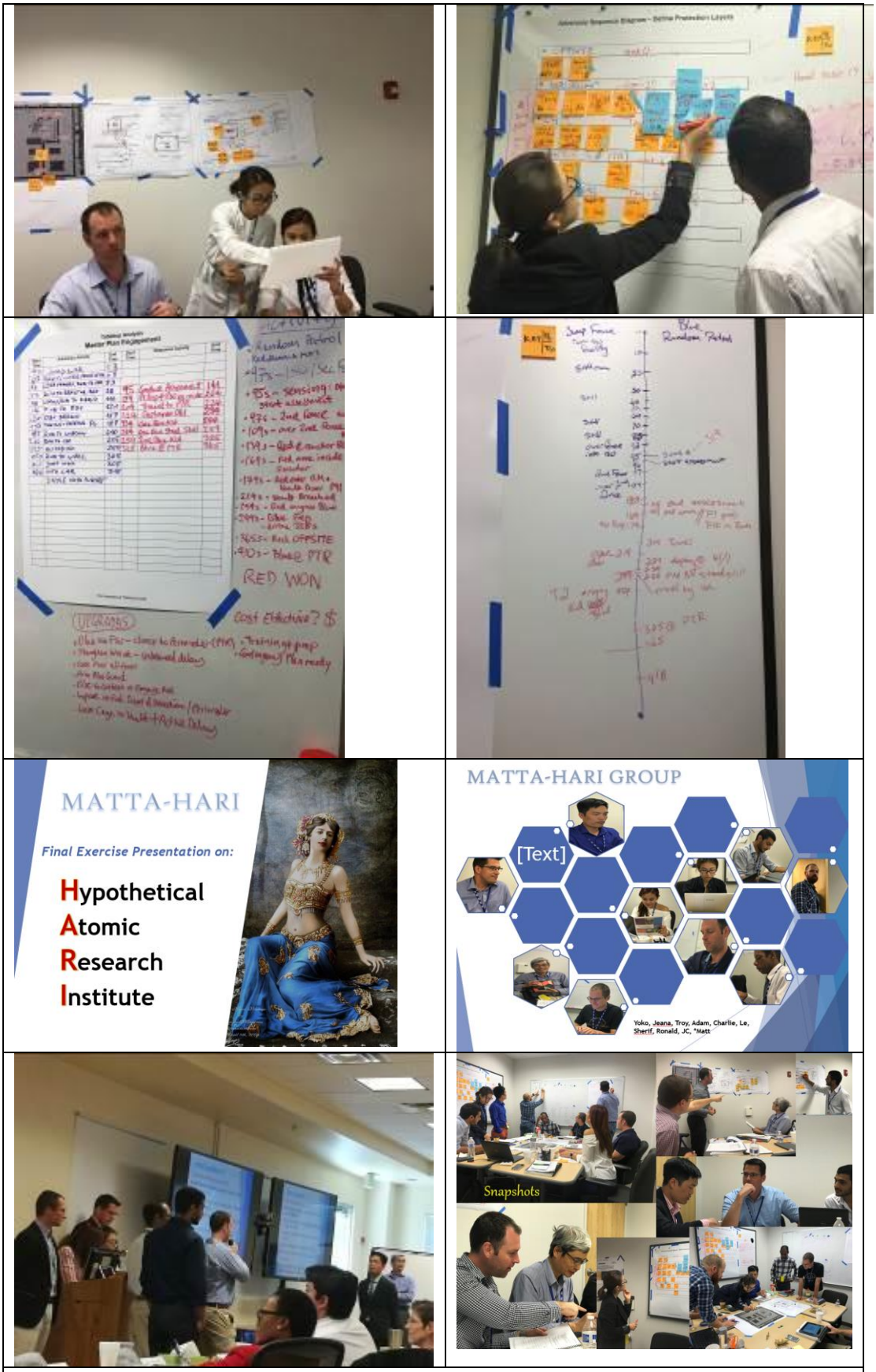

圖 11：本組學員準備分組報告之過程與成果發表

貳、 出國心得與感想

一、本次研習成員來自 40 國計 51 位正式學員參訓，因台灣非 IAEA 會員國，故台灣學員以觀察員身分參加。台灣的參訓者積極參與活動，獲得各國學員與主辦單位的認同，台灣學員均能主動與 IAEA 及美國國務院的官員握手寒暄。在期末分組報告時大家都有默契的不放國旗，任何的照相均要求將寫有國藉的名牌掩藏，特感主辦單位的細心。

圖 12：團体照(箭頭指出本國 2 位參訓者

二、分組方式考量語言、專業領域等來安排，各組成員來自不同領域與國家，並安排一位 SNL 具實務經驗之專家擔任指導員(Instructor)。指導員於分組演練前先行複習課堂講授重點，然後進行習題演練與問題解決。鼓勵學員提出自己的見解，問題沒有固定答案，訓練學員思考深度。經過幾次的討論，小組成員有了革命感情，也會聊天談自己的背景，本組成員 9 位中有政府官員、研究機構與核能業界的代表，並有 3 位擁有博士學位，在熱烈討論中，更可觀察到各個是人才，可見各國對核子保安都極為重視。

三、因 18 個月才可能受訓機會，且由美方以觀察員身份核給後，再由原能會主導分配，因此不易編列本出國預算，但公司長官多予以支持，對本公司核電廠之保安極為重視，讓此次出國任務非常順利。

四、SNL 訓練場，經過多年訓練回饋的改良，視其為珍貴的智慧財產，因此從課堂

要移至該場地前，會再三叮嚀不可帶電子器材，就連智慧手錶也不可帶入。在大門口，接受證件的逐一核對。所有參觀者嚴禁自行照相，若需照相留念，須由專門人員拍攝。

五、相較於他國近來所經歷的恐攻事件與美國槍擊事件頻傳及其他近年遭逢戰亂波及、國內族群嚴重對立國家而言，我國長期以來政經情勢穩定、社會平和，對恐怖攻擊威脅力道較小，但我們仍依美國電廠為範本，建立核電廠之保安防護系統，民眾應可安心於我們所擁有的實體防護專業能力。

六、保安系統並非無限上綱，過多的防護措施除了增加預算負擔外，還可能造成應變反應的靈活度降低。另外，對於大型的恐攻，需藉由國家的防護力量來達成，故建立縱向與橫向的通報非常重要。

七、核子設施實體防護重點在偵測、遲滯與應變武力。有效的防護必須在歹徒未破壞核子設施前阻止或弭平。要達成目標可由及早偵測、延遲歹徒入侵時間以及有效之應變武力。設計上考量全方位與平衡(Balance)，不能有弱點與死角，必須注意保防邊界完整性與考量各種歹徒入侵路徑來加以防範多重偵測(Multiple Detection)與深度防禦(Defense in Depth)一定要列入考量。

參、 建議事項

一、 我國核子保安的市場太小，不可能建置如 SNL 之訓練場，為堅強本公司核子保安之實力，一定要把握此類受訓機會，更要加強與原能會溝通，持續給予本公司實習名額。

二、 ITC 是屬國際型訓練，有來自許多國家的學員，含許多新興小國，能在此場合以台灣學員身份出席，是以可貴機會，雖 18 個月才舉辦一次，但保安人才不能中斷，宜儘早規劃下屆參訓人選，給予儘早準備，更能在 ITC 此國際舞台有亮麗表現。

肆、 附件：

I. 英文縮寫查詢：

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

ASD-滲透入侵路徑圖模型(Adversary Sequence Diagram)

CCTV-閉路電視系統(Closed Circuit Television)

CDP-臨界偵測點（Critical Detection Point）

DBT-設計基準威脅(Design Basis Threat)

DEPO-實體防護設計與評估流程(Design and Evaluation Process Outline)

DOE-美國能源部(Department of Energy)

HARI-虛擬研究用反應器(Hypothetical Atomic Research Institute facility)

HRC-高輻射後果(high radiological consequences)

IAEA-國際原子能總署(International Atomic Energy Agency)

IDS-入侵偵測感測系統(Intrusion Detection System)

ITC-國際核子保安研習(The International Training Course on the Physical Protection of Nuclear Facilities and Materials)

LPNPP-虛擬核電廠(Lone Pine Nuclear Power Plant)

MPVEASI-多路徑入侵估算軟體（Multi-Path Very-simplified Estimate of Adversary Sequence Interruption）

NMAC-核物料帳控 (Nuclear Material Accounting and Control)

PIDAS-周界入侵偵測及評估系統(Perimeter Intrusion Detection and Assessment System)

PPS-核子實體防護保安系統(Physical Protection System)

SNL-聖迪亞國家實驗室(Sandia National Laboratories)

URC-不可接受的輻射後果(unacceptable radiological consequences)