

出國報告（出國類別：訓練）

參加第二十四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：劉德銓 技士

派赴國家：美國

出國期間：102 年 10 月 19 日-11 月 11 日

報告日期：103 年 1 月

摘 要

本次出國目的為參加國際原子能總署主辦之第 24 屆核子保安訓練課程，藉以提升我國核子保安防衛力量。

訓練課程內容為核子保安系統的建構，建構過程分為三個步驟，第一步是先確定待保護目標與欲防禦之威脅並訂定可接受實體防護效能值，第二步是建立核子保安系統三大功能：偵測、延遲與武裝防衛力量，建立同時須考量深層防禦與平衡健全策略，第三步是評估核子保安系統，找出弱點並改良至符合可接受風險值為止，評估過程並應納入各種情境分析與內部破壞份子分析。

目 次

壹、	出國目的.....	1
貳、	出國行程.....	1
參、	課程內容.....	1
肆、	心得及建議.....	16

表 圖 目 次

表一、ITC-24 學員名單	17
表二、核子保安專家專題演講	19
圖一、虛構核子設施保安系統結構圖	20
圖二至圖五、保安防衛武器展示	20
圖六至圖八、歹徒可能使用工具展示	22
圖九、實地測試教學（一）紅外線入侵偵測器	24
圖十、實地測試教學（二）微波型入侵偵測器	24
圖十一、實地測試教學（三）--震動型入侵偵測器	25
圖十二、延遲裝置（Aqueous Foam 泡沫）展示	25
圖十三至十四、汽車防撞設備展示	26
圖十五、保安監控中心展示	27
圖十六、Multipath VEASI程式操作介面	27
圖十七、簡易救平機率 P_N 評估程式操作介面	28
圖十八、ITC-24 團體合照	28

「參加第 24 屆國際核子保安訓練」出國報告

壹、出國目的

本次出國為台美民用核能合作計畫進行中合作項目之一，參加由國際原子能總署（International Atomic Energy Agency, 簡稱 IAEA）主辦、美國 Sandia 國家實驗室（Sandia National Laboratory, 簡稱 SNL）承辦之第 24 屆核子保安（Physical Protection of Nuclear Facilities and Materials）訓練課程，目的是在學習核能電廠實體防護系統建立及評估方法，並藉由電廠實體防護學理之探討，了解如何避免核設施遭暴力破壞或核物料遭失竊之具體可行措施，以防範造成公眾及環境之危害，相信對於核子保安的認識與業務推動將有所助益。

貳、出國行程

本次出國受訓課程為期三週，自 102 年 10 月 19 日出發至 11 月 11 日返國。課程地點在美國新墨西哥州阿布奎基市舉行。詳細行程如下表：

起迄日期	地點	內容
10 月 19 日	台北→洛杉磯→Albuquerque	去程
10 月 20 日	Albuquerque	報到
10 月 21 日~25 日	Albuquerque	訓練課程
10 月 26 日~27 日	Albuquerque	週末
10 月 28 日~11 月 1 日	Albuquerque	訓練課程
11 月 2 日~3 日	Albuquerque	週末
11 月 4 日~8 日	Albuquerque	訓練課程
11 月 9 日~11 日	Albuquerque→洛杉磯→台北	返程

參、課程內容

一、課程簡介

本訓練課程由 IAEA 主辦，美國 SNL 承辦，自 1978 年 11 月開辦第一屆 ITC-1 至今

年已是第 24 屆，平均每一年半舉辦一屆。歷屆參訓國家多達 70 國，學員人數總計達 749 人。授課講員均為 SNL 專家學者，以英語授課。第 24 屆參與學員 43 人分別來自 38 個國家，名單如表一。

我國因不屬 IAEA 正式會員國，故參加人員未註明國籍，而以觀察員 (Observer) 稱之，會場亦不顯示我國國旗與國名。

二、 研習方式

本課程研習方式以課堂講授、分組討論 (Subgroup Exercises)、現場觀摩、設備展示等方式進行，而重點在於課堂講授及分組討論。

主辦單位將 43 位學員分為 7 組，每組 6~7 名學員，每一單元課堂講授後，都隨即安排分組討論，由資深專家擔任分組指導員 (Subgroup Instructor)，協助分組成員進行活動。分組演練進行時，課程講員、主辦單位主管及專家亦分別前往分組演練地點，瞭解演練情形，並作適切指導。

分組討論所使用之教材係虛構一個中歐小國，在其國家核子研究機構中，有兩個核子反應器設施，一為典型之水池式反應器，一為脈衝型中子反應器，各有實體防護設施，如圖一所示。教材中詳細描述兩座設施之規模、尺寸、設備、保安人員數量與日常運作型態，並輔以 3D 電腦動畫模型，幫助學員瞭解這兩座設施之結構。每次分組討論之習題即是針對單元課程主題，就虛構水池式反應器設施進行探討、弱點偵測與設計補強等演練，使學員有類似實體操作的概念。課程最後一週的週三及週四兩天為「期末考」，每一分組運用所學及歷次分組討論獲得的數據，評估並量化脈衝型中子反應器設施的實體防護效能，並提供補強措施。該評估、量化及補強措施的總結報告，於訓練最後一天，各分組依抽籤順序上臺報告，每個人都戰戰兢兢輪流發表了 3 至 5 分鐘不等的簡報，並接受質詢及指正。準備期間除了要消化報告的內容之外，還得克服語言的障礙，真是史無前例的大挑戰。

此外，主辦單位在每天課程結束前，還會利用 15 分鐘，進行全天課程內容的不記名小考，包含選擇題及是非題，答案由班主任在第二天課程開始之前公布，並統計每題

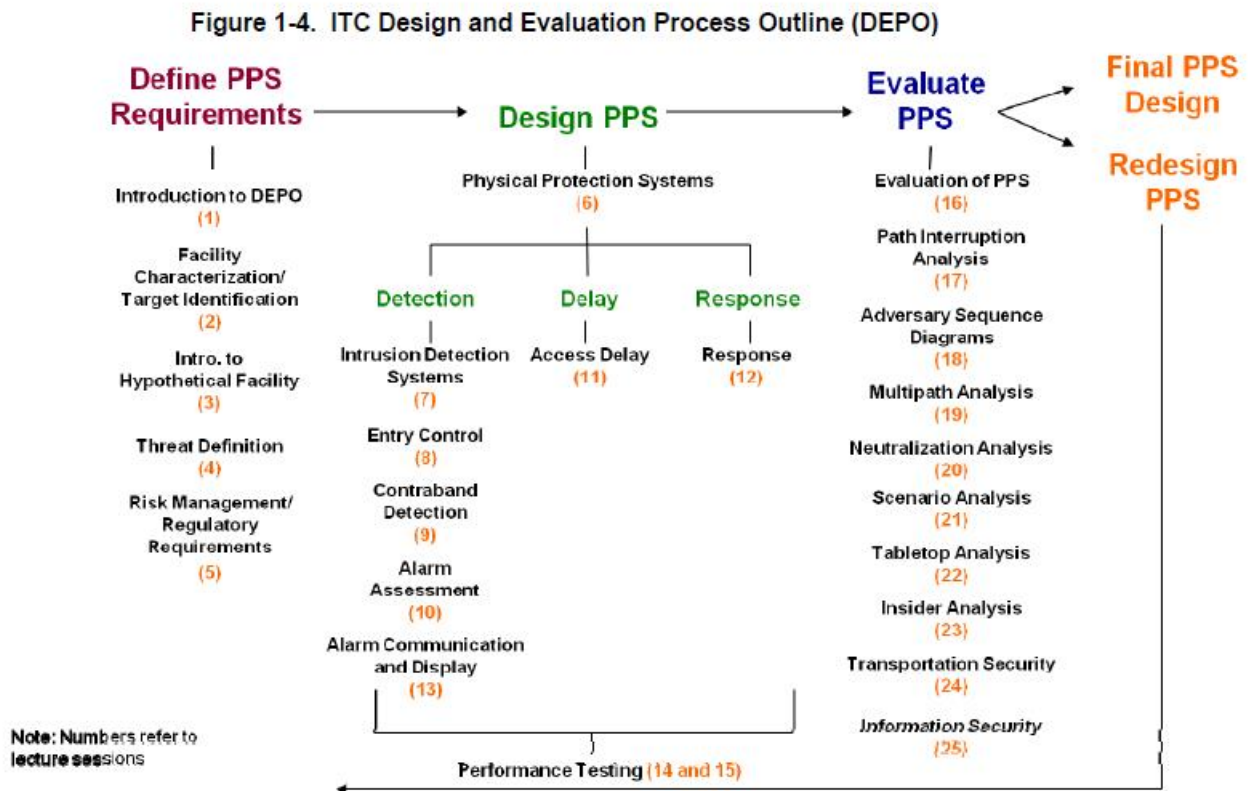
錯誤之人數比例，針對錯誤的地方講解。

課程安排有現場觀摩與設備展示，使用 SNL 的場地舉行，課程相關圖片見圖二至圖十八。

本課程另邀請 IAEA、NRC、MEXICO、FRANCE 及 NETHERLANDS 之實體防護專家就核子保安國際合作、推動及各國執行核子設施、核子物料實體防護經驗發表演講，演講題目列於表二，並邀請上述專家於各分組陳述其「期末考」總結報告時給予指導。

三、 課程介紹

國際核子保安訓練課程主要在介紹核子設施實體防護系統（Physical Protection System，簡稱 PPS）的建構與評估，其過程分為三個步驟：第一是先確立 PPS 的目標，亦即保護什麼標的物與對抗什麼威脅；第二是設計 PPS；第三是以風險觀念評估此一系統是否符合效能之要求，如未符合則回到第二步驟重新修改設計，直到符合要求為止。PPS 的建構與評估流程稱作「實體防護設計與評估流程」（Design and Evaluation Process Outline，簡稱 DEPO）如下：



以下就實體防護保安系統的建立與評估步驟分項簡介如下：

(一) 界定實體防護系統之需求 (Define Physical Protection System Requirements)：

主要是討論保安系統的目的與基準、法規要求等，其最重要的目的在於防止核子物料的偷竊 (Theft) 與破壞 (Sabotage)。實作項目為確定防護目標與預期威脅，研擬設計基準威脅，作為保安系統設計與評估之基準。

(二) 設計實體防護系統 (Design PPS)：

在實際進行 PPS 設計之前，除了確認保護標的物與 DBT (參考 p11) 外，設計者仍須蒐集瞭解核子設施之相關資料，如廠區平面圖、建築物設計圖、各出入口門禁管制、核子設施周界圍籬與廠房入侵偵測、人員組織上下班時間、值勤班表、武裝警衛人數與武器彈藥配備等。

Security risk equation公式如下：

$$R = P_A \cdot (1 - P_E) \cdot C$$

R = 風險值。

P_A = 歹徒攻擊核子設施之機率 (通常以一年為時間單位)。

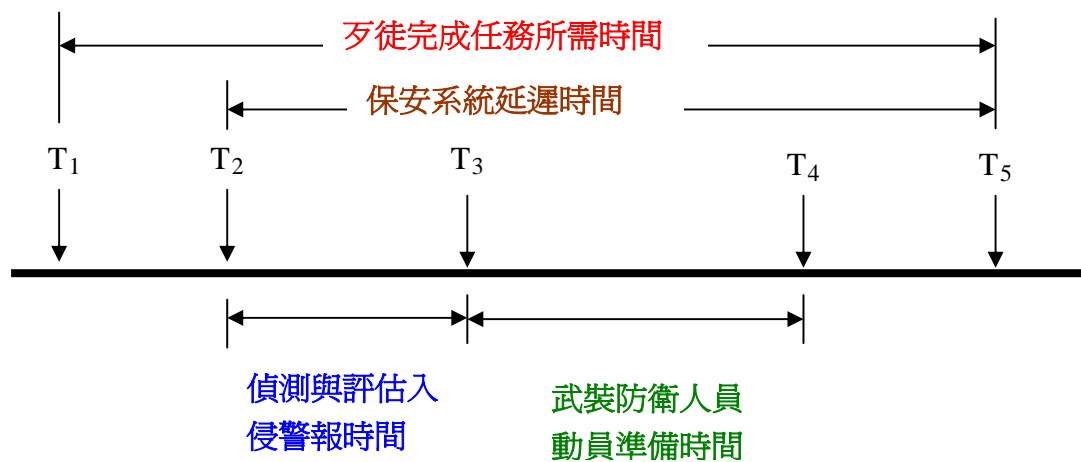
P_E = 實體防護系統之效能 ($P_E = P_I \cdot P_N$ ， P_I = PPS成功攔截 (Interruption) 機率，亦即核子設施武裝防衛人員接獲歹徒入侵警報後，在歹徒完成破壞或偷竊行動前，抵達現場加以攔截的機率。 P_N = PPS成功制服 (Neutralization) 歹徒與救平威脅的機率，亦即武裝防衛人員到達現場後成功擊退歹徒，阻止歹徒執行破壞或偷竊任務之機率。)

C = 核子設施遭受暴力攻擊或核子物料失竊之後果。

上述風險值計算公式可以簡化成一般所謂風險等於失敗機率與損失之乘積，亦即 $R = P \cdot C$ ，其中 P 等於 PPS 失敗機率，C 為損失；故 $P_A \cdot (1 - P_I \cdot P_N)$ 代表 PPS 失敗機率，其中 $P_I \cdot P_N$ 為 PPS 成功攔截並制服歹徒的機率即 P_E ，而 $(1 - P_I \cdot P_N)$ 即為 PPS 防禦失敗機率，由於歹徒攻擊核子設施之機率無法得知，故僅就實體防護系統之效能 P_E 評估，並由 Competent Authority 指定一可對抗 DBT 之 P_E 值。

對於單一核子設施而言，在核子物料種類與數量固定不變下，所造成的損失或傷害是固定的，歹徒發動攻擊的機率，又非核子設施本身所能掌控，因此核子設施必須加強的就是提高自身 PPS 成功攔截並且救平歹徒攻擊的機率；當核子設施自身防禦力夠堅強，歹徒見無機可趁，自然也可能降低發動攻擊的機率。

確認 PPS 的目標後，即可著手於設計工作。PPS 基本上是一種防禦系統，面對可能的威脅（偷竊或暴力攻擊），必須具備偵測（Detection）、延遲（Delay）與武裝防衛力量（Response Force）等三大功能，亦即當歹徒入侵，核子設施遭受威脅時，必須儘早偵測威脅的存在，由於歹徒多半採取無聲無息入侵方式，因此當其被偵測發現時，可能已越過多層障礙，甚至於已很接近目標物（特殊核子物料或重要核安設備組件），因此 PPS 除了必須在適當的位置裝置合宜且靈敏的偵測設備外，亦必須設置多重的延遲裝置，以爭取 PPS 武裝防衛人員反應時間，以及時阻止歹徒可能造成的破壞。以上所述可以下面時間軸線圖說明：



T₁：歹徒開始執行任務時刻

T₂：PPS偵測入侵後發出警報時刻

T₃：武裝防衛人員開始準備動員時刻

T₄：武裝防衛人員完成佈署準備展開攻擊時刻

T₅：歹徒完成任務時刻

T₁至T₅：歹徒完成任務所需時間

T₂至T₃：PPS於入侵偵測系統發出警報至警報經評估確認所需時間

T₃至T₄：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

T₂至T₅：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，因此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 $T_4 < T_5$ （否則 $P_i = 0$ ），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，要確保 $T_4 < T_5$ ，一則將 T_4 提前（縮短武裝防衛人員動員準備時間），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，以提早發現歹徒入侵)；一則將T₅延後，即藉由核子設施的層層關卡對歹徒入侵行動產生延遲，以爭取武裝防衛人員動員準備時間。

建立了上述 PPS 整體架構觀念後，接下來就是其個別的偵測、延遲與武裝防衛力量等三大功能設計方法的考量：

首先是偵測部分，偵測的功能包括歹徒入侵偵測器(核子設施周界與核子設施建物)、偵測器發出警報信號的傳遞與顯示及評估、門禁管制(Access Control)與違禁品管制(Contraband Detection)等。入侵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)；其中偵測機率愈高愈能確保偵測發現歹徒的入侵，其次誤動作率要儘量低，否則過多的誤動作將造成保安監控人員額外的負擔。最後，弱點亦是愈低愈好，才能確保偵測器不被破壞而能正常執行偵測功能。

入侵偵測器種類繁多，依其工作原理可分為拉力式(Taut Wire)、紅外線(Infrared)、微波(Microwave)、電場式(Electric Field)、光纖(Optical Fiber Cable)與影像移動式(Video Motion Detectors)等。依使用方式可分為主動式或被動式(Active or Passive)、隱藏式或外顯式(Covert or Visible)、線偵式或體偵式(Line or Volumetric Detection)、埋地型(Buried-Line)、圍籬型(Fence-Associated)或立柱型(Freestanding)等。選用時須考量整體 PPS 的均衡(Balance)理念與配合現場的地理條件。

入侵的偵測除了裝置於核子設施周界與建物的入侵偵測器外，門禁的管制亦不可欠缺；門禁管制的目的是限制非授權人員的進入，而允許經授權人員的進出，管制方式有很多種，基本上是依據進出人員：(1)所知道的：如密碼；(2)所擁有的：如識別證、鑰匙；(3)所天生的：如指紋、虹膜等，這幾項檢查方式如合併使用更可提高效率。嚴密的門禁管制具備下列特點：(1)無法被旁通；(2)武裝防衛人員可監視；(3)可提供武裝防衛人員防護；(4)門禁檢查過程中，受檢人員被阻隔進出；(5)針對未通過自動查驗者，執行第二道檢查；(6)受保安監控中心監看。

核子設施除了設置門禁管制限制人員進出以外，還須設置違禁品管制，以管制物品進出，通常是允許授權物品的進出，而限制武器、爆裂物等進入與管制核子物料的流出。管制方式可概分為人工檢查與機器偵檢，後者包括：X光掃瞄、金屬探測、輻射偵測與爆裂物偵測等。

入侵偵測器發出的警報信號必須送到保安監控中心，並加以顯示才能供保安監控

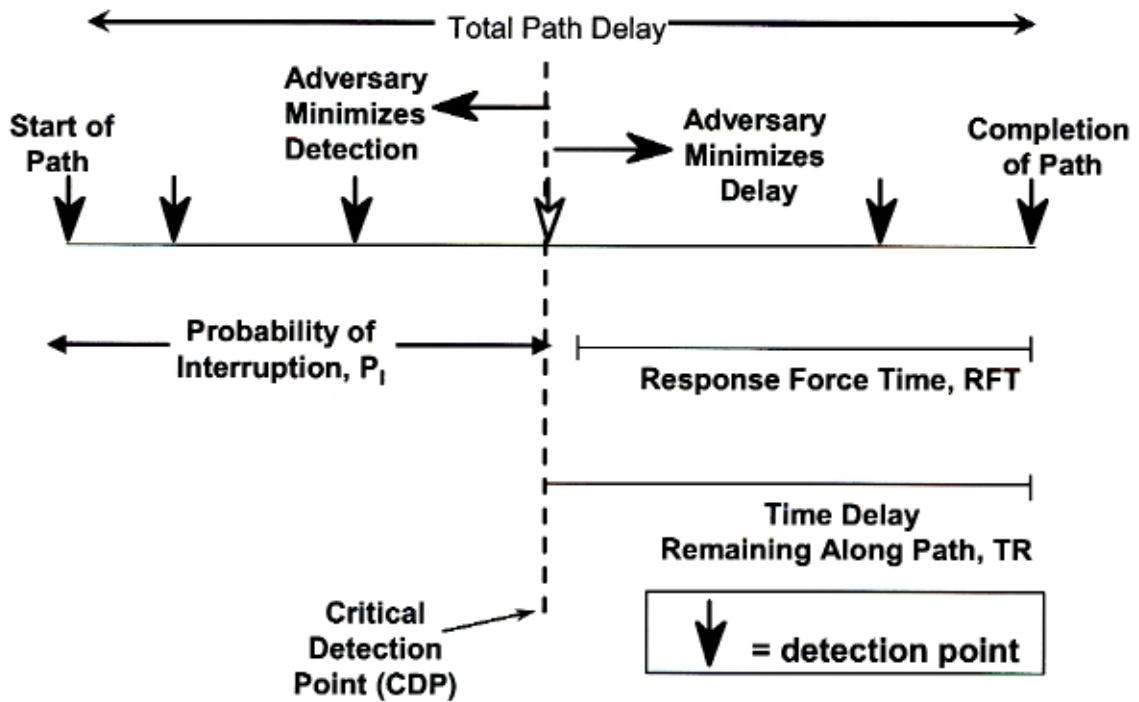
人員進一步評估警報信號的真偽，並據以判定應變作為，通常警報信號的評估是依賴警報現場的閉路電視所拍攝的影像，因此評估的速度與準確性取決於影像的清晰性，為了獲得清晰影像，舉凡燈光照明、相機鏡頭的大小與焦距長短、彩色或黑白或紅外線鏡頭等均須適當搭配以獲得最佳影像解析度。

PPS 一方面藉由偵測系統來偵測發現歹徒入侵，一方面也藉助延遲裝置拖延歹徒行動，以爭取時間讓武裝防衛人員及時出動，阻止歹徒偷竊或破壞，因此延遲裝置應設置在偵測器之後，歹徒被偵測之前的延遲是無效的；延遲裝置形形色色，舉凡任何能阻礙歹徒前進到目標地區的路線上的東西皆是，如蛇籠圍籬、牆壁與屋頂、旋轉門、泡棉膠、泡沫、煙霧等，利用多層次與多樣性的延遲裝置，因相對需要多樣的破壞器具與技巧，故可大幅提高歹徒進行破壞之困難度，進而達到延遲歹徒行動目的。

武裝防衛力量較 PPS 其他二大功能（偵測與延遲）更具決定性角色，因為偵測與延遲的目的均是協助武裝防衛人員達成核子保安的最終作為—制服歹徒與救平威脅，成功的武裝防衛力量應具備下列特性：（1）足夠人力與武裝以救平威脅；（2）適時適地攔截歹徒；（3）平日嚴實的訓練（包括各種情境下戰術演練與外界兵警支援單位之協同演練）；（4）精良配備（包括防護裝具、攻擊武器與其他輔助工具）；（5）保密與清楚的通訊（包括動員前與戰鬥中）。

（三）評估實體防護系統（Evaluate PPS）：

完成PPS設計後，接著就是課程的第三部份—PPS的分析與評估。分析評估的目的在於檢查PPS是否滿足設計目標，即效能是否大於指定值，倘否，則須進行PPS的修正，直到改進到符合目標為止。評估目的即在求出風險值方程式中之 P_T （PPS成功攔截機率）與 P_N （PPS成功制服歹徒與救平威脅的機率），其中 P_T 之評估方法以及時偵測（Timely Detection）觀念說明如下圖：



及時偵測 (Timely Detection) 觀念說明圖

直線代表時間軸，最左邊點是歹徒行動的開始，最右邊點是歹徒完成任務時間 (Completion of Path)，之間各點代表PPS層層關卡 (具有偵測入侵與延遲功能之設置)，為有效攔截歹徒，武裝防衛人員必須在歹徒完成任務前及時趕到現場保護目標物，故由此時間往前推，扣掉警報發生後武裝防衛人員接獲動員通知至完成佈署所需時間 (Response Force Time, RFT)，之前最近的偵測點稱為臨界偵測點 (Critical Detection Point, CDP)，如圖中虛線所示，其意義是如果超過此點後才偵測發現歹徒入侵，武裝防衛人員即使開始動員也來不及攔阻歹徒完成任務，因此為有效攔截歹徒行動，入侵偵測裝置必須於臨界偵測點之前發出警報，亦即PPS的攔截成功機率 P_i (Probability of Interruption) 即等於臨界偵測點之前的成功偵測機率，其值等於 $(1 - \text{臨界偵測點前各點偵測設備失敗機率乘積})$ 。

以上說明是以某一入侵路徑為例，進行PPS分析評估時，必須完備的對每一條可能入侵路徑執行 P_i 計算，以找出最難攔截 (最易入侵) 的路徑，並據以提出改善措施。本課程美國SNL運用及時偵測技術發展了路徑分析軟體 (Multipath VEASI - Version 1.0) 供使用者進行PPS分析評估。

除此之外，PPS是否有效，尚須分析評估武裝防衛人員的戰鬥力量是否足以救平歹徒反擊力量，其成功救平機率 P_N 之評估必須考慮敵我雙方之人數、武器裝備與動員佈署

時間等因素而求出；課程中為教學目的而採用Neutralization簡易軟體，只要輸入歹徒人數、類別（恐怖份子、罪犯、異議份子）、攜帶武器及武裝防衛人員於動員後各階段陸續到達人數、配備武器等，程式即可自動算出成功斃平機率 P_N 。

以上的討論均是針對外來者（Outsider）的威脅，藉由歹徒自核子設施外圍侵入的可能偵測機率與各種阻隔設備造成的延遲等數據，配合及時偵測模式分析計算出成功攔阻機率 P_I ，再配合成功斃平機率 P_N 即可求出效能值，至此亦即完成核子設施PPS的評估。

完成保安系統設計後，須依據系統評估方法，找出系統弱點與量化系統效能。若系統效能無法達成設計目標，須就系統弱點重新設計；若系統效能可達成設計目標，那就以系統弱點進行演練與訓練以發揮系統效能到極致。

ITC 針對實體防護系統的開發與訓練，以邏輯流程圖來做整體性的介紹，此流程與架構稱為 Design and Evaluation Process Outline (DEPO)，從流程圖來看，以上所述三大部分為主體，各包含若干單元主題課程，共有 25 個課堂講授，課程主題為：

1. 國際訓練課程（ITC）的介紹。
2. 核子設施的特性與目標的界定。
3. 虛構核子設施的介紹。
4. 威脅的定義。
5. 風險管理。
6. 實體防護系統的設計。
7. 入侵偵測感測器（Intrusion Detection Sensors）介紹。
8. 門禁管制（Entry Control）。
9. 違禁品（Contraband）偵測。
10. 警報評估（Alarm Assessment）。
11. 入侵行動延遲（Access Delay）。
12. 應變（Response）武力。
13. 警報通訊與顯示（Alarm Communication and Display）。
14. 性能測試（Performance Testing- Detection and Delay）。
15. 性能測試（Performance Testing- Guard and Response Forces）。

16. 實體防護系統評估。
17. 單一路徑分析。
18. 侵入者滲透入侵路徑圖模型 (Adversary Sequence Diagram (ASD) Model)。
19. 多路徑分析。
20. 救平能力分析 (Neutralization Analysis)。
21. 情境分析 (Scenario Analysis)。
22. 沙盤分析 (Tabletop Analysis)。
23. 內部破壞份子 (Insider) 分析。
24. 核子物料運送之保安。
25. 期末考 (Final Exercise) 介紹。

以下將就這 25 項單元主題課程依序摘要敘述，這些單元構成了整個 ITC 課程，也是實體防護系統建構與評估的實質內容。

1. 國際訓練課程 (ITC) 的介紹

主辦單位對於三週 ITC 課程、演練及預期目標的整體介紹，此外還包括 ITC 沿革、生活環境、課外活動、應配合事項與急難救助等相關資訊之介紹。

2. 核子設施的特性與目標的界定

防護目標包括核設施重要的組件設備與核物料，本課程的核物料分類係依據 IAEA 文件 INFCIRC/225 之「核物料分類表」(Categorization of Nuclear Material)。核子設施特性尚包括廠界、廠房、樓板平面圖及出入通道等相關資料，應確認保安設施布置與核設施運轉間之關聯及介面、警衛佈署、警衛應變與應戰程序等。

3. 虛構核子設施的介紹

虛構一個中歐小國，在其國家核子研究機構中，有兩個核子反應器設施，一為典型之水池式反應器，一為脈衝型中子反應器，各有實體防護設施。詳細描述兩座設施之規模、尺寸、設備及其數量、人員、組織與日常運作型態，並輔以 3D 電腦動畫模型，幫助學員瞭解這兩座設施之結構。

4. 威脅的定義

偷竊 (Theft) 與暴力攻擊 (Sabotage) 是 PPS 對抗的二十大威脅，設計者必須以假想之可能最大威脅來作為系統設計之基準，此一威脅定義為設計基準威脅 (Design Basis Threat, 簡稱 DBT)。依國際原子能總署的 INFCIRC/225 「核子物料與核子設施之實體保護」要求，各國須開發一個設計基準威脅，而核子設施與核子物料等須置於一個實體防護系統能將該威脅加以防禦的場所。建立 DBT 之困難在於是否可靠 (credible)，如果 DBT 不可靠，則依其設置之實體防護系統可能會功能太強或不足，功能太強是一種資源浪費，功能不足則增加威脅風險。

5. 風險管理與管制要求

介紹以機率量化風險的觀念，並討論管制法規之要求。

6. 實體防護系統的設計

介紹有效的實體防護系統設計，包括偵測、門禁管制、通道管制、通訊聯絡及應變等，以及防護系統的安裝、維護及操作。

7. 入侵偵測感測器 (Intrusion Detection Sensors) 介紹

為了準確探知侵入者隱蔽或公開行為目的，偵測系統應具備入侵感應之功能，在異常狀況下，探測器也應可發出警報信號。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)。入侵偵測器種類繁多，依其工作原理可分為拉力式、紅外線、微波、電場式、光纖與影像移動式 (Video Motion Detectors) 等。依使用方式可分為主動式或被動式、隱藏式或外顯式、線偵式或體偵式、埋地型、圍籬型或立柱型等。選用時須考量整體 PPS 的平衡理念與配合現場地理條件，以免造成防禦弱點，重點涵蓋外圍及內圈。

8. 門禁管制 (Entry Control)

門禁管制及進出人員的查核措施，為偵測系統中主要功能之一。一方面允許經確認身份無誤之人員進入電廠，另一方面則監控並排除未經授權而企圖闖入防護區域的人員或物料。目前較被廣泛使用的系統：鎖鑰、識別證、指紋掃描機、手掌掃描機、視網膜掃描器及語音辨識系統等，其他如人力驗證、崗哨亦具有偵測功能。

9. 違禁品 (Contraband) 偵測

人員、行李、車輛進出特定區域時，應加強對違禁品的管制。偵檢設備包括 X 光掃瞄、金屬探測門、輻射偵測器與爆裂物粉末偵測等。

10. 警報評估(Alarm Assessment)

當人員接收資訊之同時，應即進行評估判斷警報是否正確、是否為雜訊或異物（如動物或天候影響）誤觸，如警報無評估判斷內容，形同沒有偵測。警報評估最主要是透過影像系統的使用，例如閉路電視系統（Closed Circuit Television，簡稱 CCTV）。必須快速、正確判定狀況，才能獲得實效。

11. 入侵行動延遲 (Access Delay)

對入侵者之進出及路徑應設法延遲其行動力。實體防護系統的主要目標，乃在確認具有充足之應變人力可及時到達現場並阻止侵入者進行其不法目的。而屏障

(Barrier) 即為在偵測侵入者位置後，沿入侵者可能選擇之途徑，預先或臨時設置障礙物以延遲入侵者遂行其惡意行為之時間，並提供應變人力抵達現場並展開行動所需之時間。核子設施中典型之兩種屏障系統為：(1)「結構屏障」(Structural Barrier)：指實體防護系統最外面防護層，包括廠界圍牆、大門出入口、車輛進出通道、牆壁、門窗、屋頂、樓地板等；(2) 調劑材料屏障 (Dispensable Barrier)：運用煙霧、泡沫、黏結等方式延緩敵人行進。

12. 應變 (Response) 武力

應變武力並非一般警衛 (Guard)，而是指具有武器、採小組編組、不執行一般警衛勤務的特種戰鬥能力編組人員。應變武力需有計劃、人員、武力配置、交通、通訊等能力，並經常演練，以阻斷入侵者。在核子設施中，對於各項危及實體安全防護事件之應變計畫，主要分成下列四部分：緊急應變規劃整備、通訊、阻斷、救平歹徒惡意行動。應變部隊反應時間需確實評估，以評估能否於不法活動進行中加以制止。

13. 警報通訊與顯示 (AC&D)

偵測器和信號評估輔助系統獲得之資料應可相互傳遞。警報須透過可靠的通訊系統快速通知相關人員，並以適當的方式顯示，其間應考慮通訊系統之保密及不易被破

壞，顯示方式也應考量人因工程，使相關人員更易瞭解全盤狀況，或注意到有狀況發生可立即處理。

14. 偵測及延遲性能測試(Performance Testing- Detection and Delay)

性能試驗 (Performance Tests)、局部與全部系統試驗 (Limited Scope and Whole System Tests) 及評估試驗 (Evaluation Tests) 的目的與重點，在於描述偵測及延遲的機率及信心度。

15. 應變武力性能測試(Performance Testing- Guard and Response forces)

性能試驗 (Performance Tests)、局部與全部系統試驗 (Limited Scope and Whole System Tests) 及評估試驗 (Evaluation Tests) 的目的與重點，在於描述應變武力成功達到目的之機率及信心度。

16. 實體防護系統評估

對於實體防護系統評估的整體概述。系統評估依據實體防護三部曲（偵測、遲滯和應變）對實體防護系統及其效益，進行量化評估分析。大部分分析模式均在可能目標與侵入者入侵路線確認清楚以後，輸入相關資料進入各該模式中予以分析。雖然模式簡易，但是計算程序複雜，有賴電腦程式之輔助。情境分析及路徑分析可同時使用，主要在求 P_E ，即為PPS成功攔截並制服歹徒的機率 $P_i \cdot P_N$ 。

17. 單一路徑分析

「單一路徑」分析模式為一種簡化的數學分析程式，依入侵路徑分析所經入侵偵測器、保安區域、目標物之延遲時間、偵測機率及應變時間等，只須輸入每一偵測器可感應侵入者活動之偵測成功機率、延遲時間、應變時間，而輸出結果則為在單一侵入途徑上可以成功阻斷侵入者之機率。只選擇一條侵入者最有可能進行滲透破壞的路線分析，由結果觀察這條路徑之弱點所在，並調節輸入參數值，作靈敏度分析。

18. 侵入者滲透入侵路徑圖模型 (Adversary Sequence Diagram (ASD) Model)

依據現場實況，先設定保安目標物（如反應器廠房、核原料或用過核燃料）及防禦層次，再設定敵方所有可能滲透入侵路徑，繪出詳細的路徑順序。

19. 多路徑分析

「多路徑」分析模式為依據路徑分析軟體 (Multipath VEASI - Version 1.0) 計算 PPS 成功攔截 (Interruption) 機率，操作畫面如圖十六。分析程序為：(1) 確認可能目標 (如反應器廠房、核原料或用過核燃料廠房等)；(2) 進入目標物詳細的 ASDs；(3) 輸入入侵者特性—交通工具及裝備；(4) 列出每一入侵路徑的入侵策略；(5) 界定 PPS 的組件及其功能；(6) 界定 VEASI 每一策略功能—偵測機率、總延遲時間及偵測位置；(7) 界定應變武力特性—應變策略及完成佈署所需時間 (Response Force Time, RFT)；(8) 分析審查 VEASI 結果；(9) 改換應變時間進行靈敏度分析 (Sensitivity Analysis)；(10) 進行升級分析 (Upgrade Analysis)。

20. 救平能力分析 (Neutralization Analysis)

實體防護系統是否有效，不僅要評估實體防護三部曲是否能及時讓應變武力到達現場，尚須分析評估武裝人員的戰鬥力量是否足以救平歹徒反擊力量，其成功救平機率 P_N 之評估必須考慮敵我雙方之人數、武器裝備與動員佈署時間等因素而求出。使用簡易 Neutralization 軟體如圖十七，輸入歹徒人數、類別 (恐怖份子、罪犯、異議份子)、攜帶武器及武裝人員於動員後各階段陸續到達人數、配備武器等，程式即可自動算出成功救平機率 P_N 。

21. 情境分析 (Scenario Analysis)

情境分析為近年來常用的保安反恐分析模式。分析者站在企圖入侵者的立場，考量其動機、欲訴求之目的、專業知識水準、可能掌握的資源、可能尋求之外援與內應、更重要的是可能採取的步驟與路徑，判斷行為模式，採取對應之防範措施，也以此測試實體防護系統之效能。這套方法採取類似「兵棋推演」的對抗模式，因此評估團隊的專業與經驗愈完整，系統評估可以做得更好。

22. 沙盤分析 (Tabletop Analysis)

透過資訊蒐集，模擬測試實體防護系統防禦入侵者武力攻擊下之功能，並改善實體防護系統的防禦性。

23. 內部破壞份子 (Insider) 分析

內部破壞者為具備專業知識，有通行權，獲得授權處理事務的人員，其破壞力很

大，防範困難，因此如何防範內部破壞者，在實體防護系統是一重要課題。首先須確定內部破壞者之威脅與特性，探討加強警衛之效率，再配合單位內工作人員之互相關懷、實行二人一組工作策略（Two-Person Rule），以有效防範內部破壞者行動。另加強門禁管制系統保持人員行蹤紀錄，儘可能限制、減少出入人數；在特定地點裝監視器等，對防範內部破壞者都有幫助。

24. 核子物料運送的安全

核子物料運送的保安，比較固定式核子設施之保安，增加了「移動」的因素，其餘三部曲（偵測、遲滯和應變）的原則依然適用。運輸車輛上裝置入侵偵測設備與入侵行動遲滯裝置，有門禁管制，有警報評估（更容易），而應變武力可能是隨行護衛部隊。核子物料運送時，通訊更顯得重要。情境分析必須大大地改變，而不需要路徑分析。在評估方法上，通常假設應變武力及時到達的的機率為 1.0，所以防護成功機率取決於救平機率 P_N 。

25. 期末考 (Final Exercise) 介紹

最後一週的週三及週四兩天為「期末考」，每一分組運用所有所學及電腦工具，整體評估並量化脈衝型中子反應器設施的實體防護架構之效能，並提供補強措施。

肆、心得及建議

- (一) 核子保安訓練課程是由國際原子能總署主導的訓練課程，其核子設施實體防護課程架構十分完整，師資經驗極其豐富，行政支援工作人員熱心，並隨科技發展迅速，各種入侵偵測設備及 CCTV 監控設備日新月異，建議持續推薦人員參與學習，不僅可強化保安專業知能，更可增進國際文化交流。
- (二) 對於設計基準威脅 (DBT) 之界定，指導員強調不包括空中飛行器之攻擊，其制定可協調相關機關提供恐怖份子、異議人士等資訊，使得實體防護系統的功能符合實際需求，不至於功能太強或不足，功能太強造成資源浪費，功能不足則增加可能之風險。
- (三) 本次出國前已彙整相關保安工作上所遇到之問題，如緊要海水泵室位於何種保安區域？等，在出國訓練過程中曾詢問指導員，指導員回答須以效能評估實體防護系統是否足以應變，在 SNL 實地測試的各種數據，如各種 PPS 之延遲時間及機率等，因僅作為學理上之研究，不可直接引用作為管制核能電廠之標準；另緊要海水泵室位於何種保安區域，指導員未提供解決方法及答案，且不屬本次訓練課程範圍，因屬法規面之問題，仍須 NRC 同意給予相關資訊，才有可能獲得解決。
- (四) 對於 INSIDER 之防範之問題，指導員也坦承對於 INSIDER 之防範是最困難，防範方法以 TWO PERSON RULE、適職方案、門禁管制及授權、CCTV 監視等措施為主，目前我國也針對 INSIDER 之防範要求核電廠於核子保安作業指引中，增加 TWO PERSON RULE 之規定並配合門禁管制及授權、CCTV 等措施，防範內部破壞者行動。

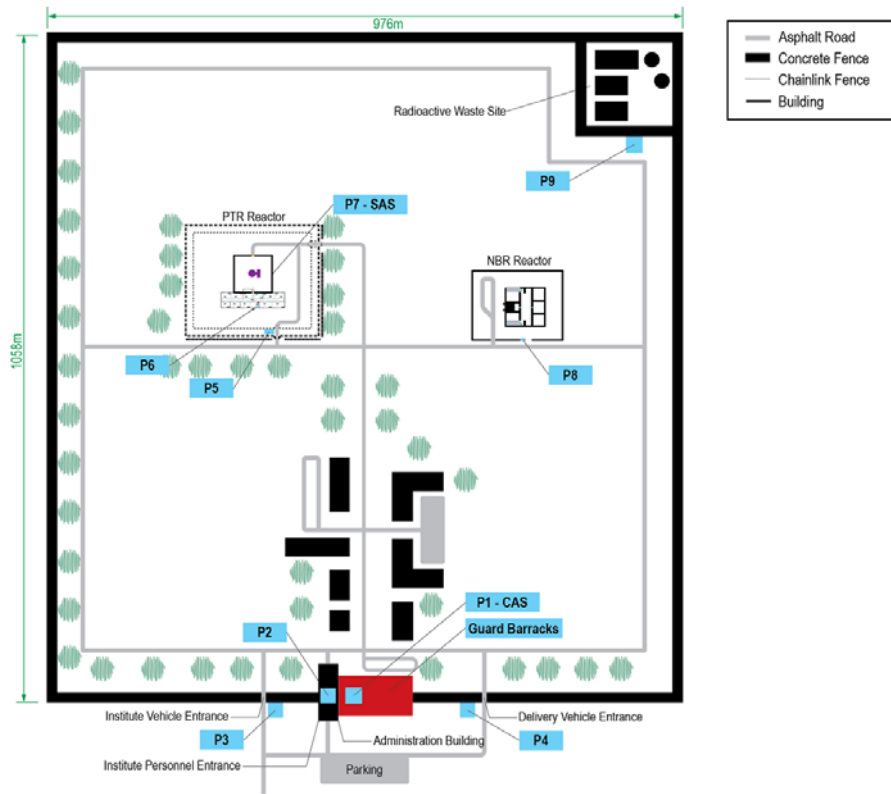
表一、ITC-24 學員名單

國家	姓名	單位
<i>Armenia</i>	Karen Sahakyan	National Security Service; Ministry of National Security
<i>Australia</i>	Tony Rami Haddad	Australian Nuclear Science and Technology Organisation (ANSTO)
<i>Bangladesh</i>	A.K.M. Fazle Kibria	Bangladesh Atomic Energy Commission (BAEC) ; Nuclear Safeguard & Security Division
<i>Belarus</i>	Gleb Drobychev	Department for Nuclear and Radiation Safety (Gosatomnadzor); Ministry for Emergencies of the Republic of Belarus
<i>Belgium</i>	Walid M'Rad Dali	Federal Agency for Nuclear Control (FANC)
<i>Brazil</i>	Marco Aurelio Monteiro Dutra	National Nuclear Energy Commission (CNEN)
<i>Bulgaria</i>	Plamen Yankov	Nuclear Regulatory Agency
<i>Canada</i>	Tanya Charmaine Gorr	Atomic Energy of Canada Ltd.
<i>Canada</i>	Laura Elizabeth Joyce Ouellette	Canadian Nuclear Safety Commission (CNSC)
<i>China</i>	Chun Li	State Nuclear Security Technology Center (SNSTC)
<i>Czech Republic</i>	Marek Kvasnicka	CEZ, a.s., Nuclear Power Plant Temelin
<i>Egypt</i>	Sameh Saber Hussein Mohamed	Egyptian Atomic Energy Authority (EAEA); Nuclear Research Centre (NRC);Engineering Department
<i>France</i>	Jonathan Peterschmitt	French Alternative Energies and Atomic Energy Commission
<i>Germany</i>	Marita Dohler	Gesellschaft fuer Anlagen u. Reaktorsicherheit (GRS), Schwertnergasse
<i>Ghana</i>	Felix Ameyaw	Ghana Atomic Energy Commission (GAEC); National Nuclear Research Institute, Nuclear Reactors Research Centre
<i>Hungary</i>	Hedvig Eva Nagy	Hungarian Atomic Energy Authority (HAEA)
<i>India</i>	Charivukalayil Samuel Varghese	Atomic Energy Regulatory Board (AERB); Department of Atomic Energy (DAE)
<i>India</i>	Maheshkumar Kamble	Bhabha Atomic Research Center (BARC), Reactor Engineering Division
<i>Indonesia</i>	Ferry Ferry	National Nuclear Energy Agency (BATAN)
<i>Japan</i>	Reina Matsuzawa	Japan Atomic Energy Agency (JAEA)
<i>Japan</i>	Masahiro Imase	Japan Nuclear Energy Safety Organization(JNES)
<i>Republic of Korea</i>	Young Wook Lee	Korea Institute of Nuclear Non-proliferation and Control (KINAC)

<i>Lithuania</i>	Asta Jostaite	Ilgnalina Nuclear Power Plant
<i>Malaysia</i>	Nur Shazwani Zainal Abidin	Atomic Energy Licensing Board (AELB); Ministry of Science, Technology and Innovation
<i>Mexico</i>	Garza Victor Manuel Duarte	Instituto Nacional De Investigaciones Nucleares (ININ)
<i>Norway</i>	Tonje Sekse	Norwegian Radiation Protection Authority (NRPA)
<i>Poland</i>	Andrzej Glowacki	National Atomic Energy Agency (PAA)
<i>Romania</i>	Laurentiu Moroca	Romanian Intelligence Service
<i>Russian Federation</i>	Alexander Alexandrovich Egorov	Scientific and Engineering Centre for Nuclear and Radiation Safety (SEC NRS)
<i>Serbia</i>	Vladimir Janjic	Serbian Radiation Protection and Nuclear Safety Agency
<i>Slovakia</i>	Zuzana Bernátová	Slovenske Elektrarne-ENEL
<i>South Africa</i>	Mafihla Johannes Maleka	South African Nuclear Energy Corp. (NECSA)
<i>South Africa</i>	Tumelo Faith Mogamisi	Department of Energy
<i>Sweden</i>	Carl-Gustav Axel Renmarker	Ringhals AB
<i>Sweden</i>	Peter Annoegaard	Forsmark Kraftgrupp AB
<i>Switzerland</i>	Jorge Dejoz	Swiss Federal Nuclear Safety Inspectorate ENSI
<i>Thailand</i>	Boonchawee Srimok	Office of Atoms for Peace (OAP); Ministry of Science and Technology (MOST)
<i>Turkey</i>	Levent Özdemir	Cekmece Nuclear Research and Training Centre (CNAEM); Turkish Atomic Energy Authority (TAEK)
<i>Ukraine</i>	Arkadii Borysenko	State Enterprise the National Power Company ""UKRENEGRO"" of the Ministry of Energy and Coal Industry of Ukraine
<i>Ukraine</i>	Viktor Shulyak	State Nuclear Regulatory Inspectorate of Ukraine, State Nuclear Safety Inspectorate at SNUNPP Site Yuzhnoukrainsk, Nikolaev region
<i>United Arab Emirates</i>	Mohamed Alharbi	Federal Authority for Nuclear Regulation (FANR)
<i>United Arab Emirates</i>	Omar Saad Ahmed Al Shehhi	CICPA
<i>United Kingdom</i>	Alan Bacon	International Nuclear Services
<i>Vietnam</i>	Hanh Bui Dang	Vietnam Atomic Energy Institute
<i>Taiwan</i>	Te-Chuan Liu	Atomic Energy Council, Taiwan, R.O.C.

表二、核子保安專家專題演講

單位	題目	演講者
IAEA	International Physical Protection Advisory Service (IPPAS)	Arvydas Stadalnikas Office of Nuclear Security Department of Nuclear Safety and Security
US NRC	IPPAS Missions - The NRC Experience	Nancy Fragoyannis U.S. Nuclear Regulatory Commission
MEXICO	EXPERIENCE WITH THE IPPAS MISSION IN MEXICO	RUBÉN RAMÍREZ GUERRERO NATIONAL COMMISSION ON NUCLEAR SAFETY AND SAFEGUARDS
France	Implementing INFCIRC 225 rev 5 Experience feedback on IPPAS mission	Géraldine Dandrieux
Netherlands	The Netherlands experience with IPPAS Missions	Bart Dal , Ministry of Foreign Affairs of the Netherlands



圖一、虛構核子設施保安系統結構圖



圖二、保安防衛武器展示（一）



圖三、保安防衛武器展示（二）



圖四、保安防衛武器展示（三）



圖五、保安防衛武器展示（四）



圖六、歹徒可能破壞工具展示（一）



圖七、歹徒可能破壞工具展示（二）



圖八、歹徒可能破壞工具展示（三）



圖九、實地測試教學（一）紅外線入侵偵測器



圖十、實地測試教學（二）微波型入侵偵測器



圖十一、實地測試教學（三）--震動型入侵偵測器



圖十二、延遲裝置（Aqueous Foam泡沫）展示



圖十三、汽車防撞設備展示（一）



圖十四、汽車防撞設備（二）



圖十五、保安監控中心展示



圖十六、Multipath VEASI程式操作介面

Neutralization

Threats				
Type	Number	Weapons	Delay (min:sec)	
terrorist	3	pistol	4	50

Threat Help
 Type: identifies Threat type; has no influence on Pn
 Number: number of adversaries
 Weapon: type of weapon used by adversaries
 Delay: path delay in minutes and seconds
 Use only combo-box buttons and scroll buttons; text area used to input data

Guards				
Type	Number	Weapons	Delay (min:sec)	
<input checked="" type="checkbox"/> 1st patrol	1	pistol	1	0
<input checked="" type="checkbox"/> 2nd Special Response Team	4	pistol	3	0
<input checked="" type="checkbox"/> 3rd Special Response Team	4	automatic rifle	5	0
<input type="checkbox"/> 4th Special Response Team	5	automatic rifle	8	20
<input type="checkbox"/> 5th Offsite	5	automatic rifle	30	

Guard Help
 Check boxes: selects guard groups to be included in calcul.
 If guard group response delay is greater than adversary guard group will not engage, will have no effect on Pn, group text boxes will remain shaded
 Type: identifies Guard type; has no influence on Pn
 Number: number of guards in each response group
 Weapon: type of weapon used by each guard group
 Delay: group response delay in minutes and seconds
 Use only combo-box buttons and scroll buttons; text area used to input data

Results		
Probability of Neutralization:	Total Guards engaging:	Total Threats engaging:
0.753	5	3

Results Help
 The probability of neutralization is only for those selected guard groups who have delay times shorter than the threat delay
 Number of guards engaging is the total number of selected guards who can actually engage the threat

Languages
 English French Spanish Portuguese

圖十七、簡易救平機率 P_N 評估程式操作介面



圖十八、ITC-24團體合照