行政院原子能委員會

委託研究計畫研究報告

關鍵基礎建設實體防護系統保護效能電腦模擬分析工具建立

A Simulation and Analysis Platform for Evaluating the Effectiveness of Physical Protection System of Critical Infrastructures

計畫編號：992001INER011

受委託機關(構)：清雲科技大學資訊工程系

計畫主持人：易俗

核研所聯絡人員：鄭武岳

聯絡電話：(03)581196 轉 7713

E-mail address：swuyih@cyu.edu.tw

報告日期：99 年 11 月 25 日

目 錄

圖 目 錄

中文摘要

自美國 911 事件發生以來，世界上各國一直積極的在加強重要的關鍵基礎建設保護，關鍵基礎建設即在一個國家中提供人們生活所需，如電力、通訊、交通、日常用水等，當關鍵基礎建設遭到破壞而不能正常運作時，國家安全與民生將會造成重大的威脅。為了要有效保護與維持國家的重要基礎建設正常運作，世界各先進國家已經投入了相當龐大的人力、金錢等資源來發展相關的分析方法與模擬工具，但是對於不同種類的模擬沒有一個共通的平台可以分享其模擬元件。本計畫提供一個關鍵基礎建設模擬平台，針對不同種類之模擬整合到此平台上，並將功能模組化，讓模擬器的功能可以被重複的利用。

關鍵詞: 關鍵(資訊)基礎建設防護，模擬平台。

Abstract

In recent years major developed countries have strengthened the protection of their Critical Infrastructures (CIs) since the 911 terrorist attacks on the USA. Critical Infrastructures refer to the products or services that are needed to maintain national security as well as the economic and social welfare of a nation. Such infrastructures include telecommunication, energy, finance, traffic, water supply, medical treatment etc. Effectively protecting these critical infrastructures is a critical issue in the anti-terrorism war.

To assess the effectiveness of Critical Information Infrastructure Protection (CIIP) activities, most countries are engaging in developing related simulators. Such simulators and environments have confidential and localized features, and thus, each country needs to develop their own simulators. However, there is little relative research or development in Taiwan. Moreover, a common platform for the various CIIP simulators is needed so that components can be reused. Based on these reasons, this research has designed a simulation platform under which prototypes of several CIIP simulators have been constructed to share the common architecture and components. The resulting platform of our research enhances the modularization and reusability of CIIP simulator construction.

Keywords: Critical (Information) Infrastructure Protection (CIIP), a simulation platform.

壹、計畫緣起與目的

一、 背景介紹

自 911 攻擊事件之後，人們注意到關鍵基礎建設所隱藏的脆弱性及相關保護措施的重要性。 因此近年來美國、澳洲等先進國家均加強重要民生基礎建設的保護，所謂重要民生基礎建設是指在一個國家中為維持國民穩定的經濟、民生與政府運作而提供的基本產品或服務，例如電力、交通、供水以及醫療等。由於重要基礎建設攸關國家安全、社會秩序以及人民生命財產安全，一旦關鍵基礎建設無法提供服務，民生、經濟都會受到影響。像是台灣近幾年的 729 停電、921 地震、七二水災等，對電力、用水、交通都造成嚴重的影響，反映出基礎建設的防護對於國計民生有著極為重要的影響。

911 事件顯示恐怖份子的攻擊方式是無所不用其極，因此規劃建置防範恐怖攻擊入侵各項基礎建設已是國防的重點。要如何有效保護重要基礎建設成為當前世界上各國反恐的重要議題。

對於基礎建設或設施的防護，政府需要一個能夠整合的模擬分析工具，能夠事前進行風險分析、人員訓練、措施規劃，事發時提供決策支援，掌握各項關鍵設施的風險重要性，將防護資源作最有效益的佈局，以維持國家、社會的正常運作。

二、 目的與重要性

目前世界各國均正在發展各式方法、工具來模擬可能的攻擊劇情以分析弱點，估本身的重要基礎建設之防護能力。目前在台灣尚缺乏針對國內環境的模擬軟體工具可供應用。此項模

擬工具具有區域性、機密性等特色，因此無法直接採用國外工具。本計畫即針對基礎建設可能遭遇的恐怖威脅，發展一套關鍵基礎建設防護模擬分析平台，以提供基礎設施防護措施規劃、防護成效評估、人員訓練與方法驗證的功能。

基本上關鍵基礎建設安全風險評估平台的工作範圍包含下列三項：

(一)單一關鍵基礎建設之安全評估

(二)兩設施間之重要物資運輸的安全評估

(三)各項基礎建設間之互相依賴性影響

如圖 1 所示，此三方面含蓋點、面、和全盤性之影響。

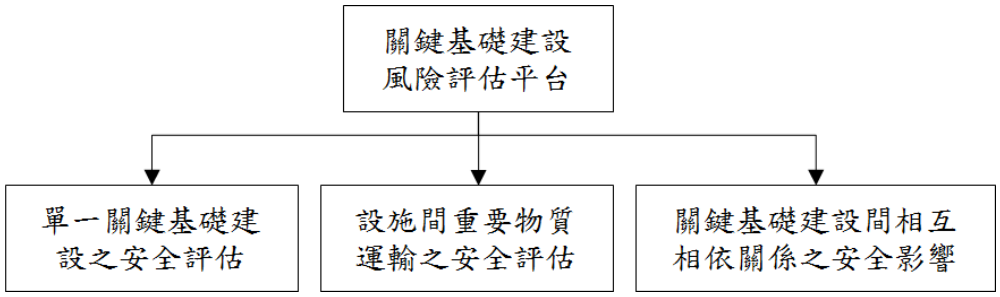

圖 1 關鍵基礎建設防護模擬分析平台

第一部分為，單一關鍵基礎建設面對外部入侵者的實體及網路防護評估。第二部分則用於兩點間關鍵物資（key resource）或危險物質（hazardous material）的運輸保全評估。此部分表達動態受攻擊的可能。第三部分則模擬基礎建設間的相互相依關係（Interdependency），評估一個基礎建設的服務異常或終止，對其他基礎建設之影響。此三項已含蓋關鍵基礎建設的可能遭到的攻擊及後續影響的主要狀況。本計畫提供一個關鍵基礎建設模擬平台，針對不同種類之模擬整合到此平台上，並將功能模組化，讓模擬器的功能可以被重複的利用。

貳、研究方法與過程

美國的國土安全部（Department of Homeland Security， DHS）在 2005 公佈的「國家基礎建設保護計畫」。我國也於 2004 年成立反恐辦公室（現更名為國土安全辦公室），以因應反恐救災的對應單位與程序，並做多種兵棋推演及演習。

在模擬分析上各國都正在開發相關工具技術。實體建設保護的模擬有 SAVI[14]， EASI[5-6] 等模型。 國內尚缺乏此方面較完整的工具，因此應該發展自己的基礎建設保護措施評估及模擬的技術。

一、 關鍵資訊基礎建設保護

瑞士聯邦理工學院安全研究中心（Center for Security Study）出版名為「國際重要資訊基礎建設保護手冊（CIIP Handbook）」的手冊[1]，目的為對重要基礎建設資訊系統保護主要議題提供整體性與國際性概觀，作為從事本項工作「國際社群之共同參考基礎」。編輯者在整理分析豐富的資料後，提出了許多重要深刻的觀點，對照各國家做法的差異，能夠辨識與解讀差異背後所代表的意義。例如推動 CIIP 不能與 CIP 分離，CIP 與 CIIP 的區別，瞭解各基礎建設關聯關係的重要性，強調分析能力的重要性等。

二、 國家基礎建設保護計畫

美國於 2002 年成立國土安全部（DHS），其主要任務之一為負責規劃整合全國的基礎建設保護工作。為執行此任務，DHS 提出了一系列基礎建設保護計畫文件，供美國政府、民間、地

方政府等執行保護工作的依據其中最重要的文件為 2005 年 11 月公佈的『國家基礎建設保護計畫（National Infrastructure Protection Plan， NIPP）』 [2]。NIPP 的核心部分為風險管理架構，其目的為降低風險，其架構包七個工作步驟（如圖 2）：制訂安全目標、辨識重要資產、評估風險、優先排序、執行保護計畫、測量成效、持續改善。

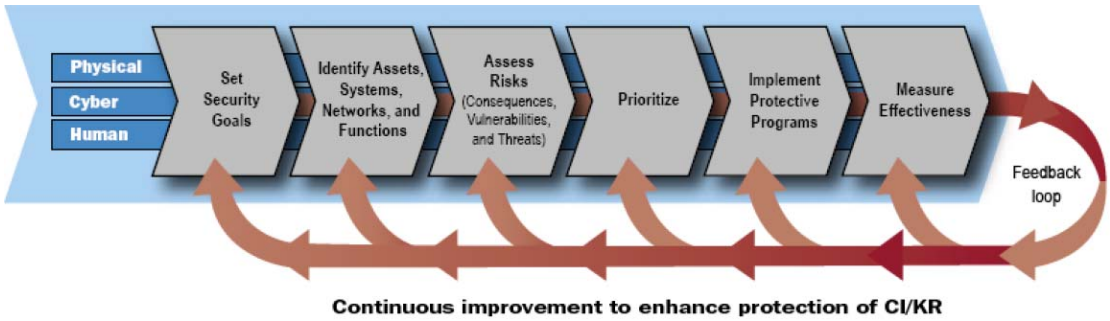

圖 2 NIPP 風險管理架構

三、 設計基準威脅

設計基準威脅（Design Basis Threat，DBT）[3]是由美國核能管制委員會 NRC（U.S. Nuclear Regulatory Commission）所提出，用來描述攻擊威脅的型態、組成方式及攻擊能力。DBT 的重要性在於核電廠防護系統是以 DBT 資訊作為設計的基礎。有關針對核設施惡意破壞之特性描述可以參考 10 CFR 73.1 文件，此文件有完整的分類。

四、 EASI 模型

EASI（Estimate of Adversary Sequence Interruption）是 1970 年由美國聖地亞國家實驗室（Sandia Lab.）所研發，它是一種簡

單、容易瞭解的模型，專門用在實體建設保護的效能評估上[5-6]。到 1985 時已經是架構在微軟 Microsoft 的 Excel®軟體上的一套工具。

此模型的特點是研究一個攻擊路徑包含威脅的相關條件如偵測（Detection）、延遲（Delay）、回應（Response）、通訊（Communication）之間的關係對實體防護系統的影響，經過模型的計算，可以得到有效阻止攻擊發生的機率（Probability of interruption）。偵測及通訊的參數是用功能被有效執行機率來表達，而延遲及回應則是用平均需要的花費時間加上一個正負偏差範圍值表示。

(一) 輸入方式

PD 表示監視感應器成功發現攻擊者的機率，而 PD 等於感測器發現不正常的活動（PS），乘以訊息經過網路或是其他任何管道到達控制點的機率（PT），再乘以警報系統正常的發出警報的機率（PA）。

$$P_D = P_S \times P_T \times P_A$$

回應時間在EASI模型中是從警報系統產生警報信號開始算起到防守方到達能夠阻止及對抗攻擊方的行動的地點為止。

(二) 輸出方式

EASI 運算目的是在評估出在攻擊方完成偷竊或破壞的行為之前，防守方有足夠的能力去中斷攻擊方的行動之可能性，即為中斷攻擊行動的機率值（Probability of Interruption， PI）。PI 的計算方式為：

$$P_I = P_C \times P_D$$

本計畫中在第一部分單一關鍵基礎建設實體防護的模擬器雛型中，將採用 EASI 的攻擊序列圖設計，及入侵者特徵參數組合，來產生攻擊劇情。

五、 形態學分析法

形態學分析法（Morphological Analysis）是由瑞典天文物理學家 Fritz Zwicky 發明的一種分析方法，是一種能夠系統化的組合及發現在多維的（multi-dimensional）、非量化（non-quantifiable）的複雜問題之所有集合之間的關係的方法[7-8]。

一個複雜的問題有幾種特性：

(一)Multi-dimensionality：一個多維度的問題主要因為同時擁有許多不同的觀點。

(二)Uncertainty: 複雜的問題的範圍通常是非可量化，並且是持續的擴張，因此在這種情形下就不適合用因果關係來推論答案。

(三)Subjectivity: 沒有絕對的正確或是錯誤，只能找出有較好或較差的解決方式。

在 1995-1996 年在瑞典的國家防衛研究機構（Swedish National Defence Research Agency in Stockholm）的 Tom Ritchey 發展了一套利用電腦輔助的 Morphological Analysis 軟體：MA/Casper。MA/Casper 是一套根據形態學上的推論模型所建立的一個發展平台，可用來建立各種劇情及策略。本計畫中將採用類似 MA/Casper 軟體的輸入方式，自行開發在輸入恐怖份子的攻擊劇情因子，利用使用者輸入各項參數，接著設定矛盾的

參數關係，再剔除之間有矛盾關係的參數選項後，組合所有的可能性因素，列出所有可能的劇情。

六、 貝氏信心網路

貝式信心網路（Bayesian Belief Network， BBN）[9-10]為一種有向的非循環圖形。主要由兩個部分所組成，包含了節點與連結線，並結合了一組狀態機率表（Condition Probability Tables）表達節點間的條件機率。在此有向圖中，每一個節點用來表示隨機變數，而連結線用來表示兩個變數之間的關聯或因果關係，每一個節點的機率表則提供了節點中變數的每一個狀態的機率。簡而言之，此有向圖形用狀態機率表來表示變數之間的聯合機率表影響關係。每一節點附有一表達因果之間關係的條件機率表，此表的數值由專家決定或統計得來。一有新的證據，整個網路的節點數值，可由父節點至子節點或由下而上計算，全部更新。

七、 地理資訊系統

地理資訊系統（Geographic Information System， GIS）[11]為一種結合地貌或地圖的圖形化介面及處理地理數據之電腦輔助系統;地理數據包括了空間數據(座標),及屬性數據(氣候)。

地理資訊系統一般應用於科學調查， 資源管理， 財產管理、發展規劃、繪圖和路線規劃。最早開發者為加拿大的 Roger Tomlinson，其系統 Canadian GIS 用於存儲，分析以及處理所收集來的有關加拿大土地存貨清單數據。現今的 GIS 提供者，主要為 ESRI 及 MapInfo，占了 GIS 使用率的八成以上。一些被廣

泛應用的新型網路 GIS 服務，例如：Google Map[13]或 Yahoo Map，這些系統提供了應用程式介面，能讓使用者決定在地圖上顯示的內容。

本計畫在危險物質（hazardous material）的運輸模擬器雛型中，使用 Google Map 及它的 API 來作為地圖上互動顯現，使決策者更能清楚了解問題之所在。

八、 危險物質的運送

險的物質（hazardous materials， HAZMAT），像是核廢料、化學藥劑、生化武器、火藥等具有放射性、污染性、傳染性、爆裂性等高度危險的物質，一但外洩，往往會造成區域或全球性的傷害。而這類物質的運送，就要特別的小心，尤其 911 事件後，恐怖份子無所不用其極，把危險物質搶去做髒彈或直接破壞造成當地污染都是有可能的。關於這部份的研究，大部份的研究者都是研究安全的路徑規劃，想要事先避開可能有危險的地方。或是定一套嚴格的標準來審查相關的任何人、事、物、以及程序。還有模擬外洩後造成的影響[12]。

九、 系統架構

本計畫首先提供一個關鍵基礎建設模擬平台，針對不同種類之模擬整合到此平台上，並將功能模組化；整合在過去的幾年本實驗室已實做的數個 CIIP 模擬器雛型。

整體的架構圖如圖 3 所示，主要的模組敘述如下：

(一) 模擬器（Simulator）

1. 攻擊事件模擬：此模組是用來模擬攻擊劇情，需要考慮到

攻擊者、位置、目標與防禦因素。

2. 實體防護模擬：此模組是用來模擬攻擊者入侵實體防護系統，如核電廠周圍的監視器、外牆或警報器等。
3. 運輸模擬：此模組是用來模擬危險物質的運輸途中可能會遭受到的攻擊，其地理環境可能會影響到攻擊的機率。
4. 相互相依關係模擬：此模組是用來模擬基礎設施受到間接影響時的情形。
5. 支援模擬：此模組是用來模擬部隊防禦方面，如軍隊、警衛、修理專家等，這些因為會影響到修復的機率與時間。

(二) 輸入模組（Input）

1. 場景設定：使用 GIS-base 的方法來設置場景。地圖可以用來配置和連接基礎建設或找尋運輸的路徑。此外，使用者也可以自行定義基礎建設的層次與通道，將基礎建設的每一層互相連接。
2. 資產設定：用來設定像是運輸的核廢料、保護元件（如武器、人力、物力等）、附近可支援的力量（如警衛、軍隊等）。
3. 威脅設定：用來設定攻擊方的交通工具、武器、人員規模、有無受訓或專業人士等等。
4. 劇情連結：目前是使用形態學分析法將所有可能的攻擊做連結，並從中刪除掉矛盾的劇情。這種組合攻擊劇情可以找出一些不可預期的情況。

(三) 運算模組（Computation）

不同的模擬器用來運算出不同的攻擊結果，以下是我們目前所採用的計算方式：

1. EASI：此公式是用於實體關鍵基礎建設模擬。
2. BBN：在運輸的案例裡使用 BBN 來做因果關係的推導。
3. IIM：在相互相依關係中使用 IIM 公式做計算。

在進行模擬後，計算之結果可供分析與統計，透過排序來找出最好與最壞的情況，並提供決策者針對可能的漏洞來做更嚴謹的修改。

(四) 輸出模組（Output）

在模擬完成後，模擬器會做結果的輸出，在這部分我們將輸出模組分為兩類：

1. 輸出顯示：顯是最後的模擬結果與分析比較。
2. 視覺呈現：對於單一劇情模式我們使用動畫來顯示，例如運輸模擬中貨車的行經路徑；而多劇情模式使用長條圖來顯示成功防守的機率。

(五) 資料管理模組（Data Management）

資料除了顯示在界面上之外也需要輸出至檔案中儲存，如純文字檔或 XML 檔。而且，把資料存檔也可以用來當作輸入使用。

1. 資料檔案：在模擬的過程中用來儲存劇情，以利日後用來做脆弱分析或視覺化。
2. XML 檔案：XML 儲存了資產設定與威脅設定，用來讓不同元件共享資料。

圖 4 為我們實做實體防護系統模擬器與運輸模擬器中擷取出來的部分函數。

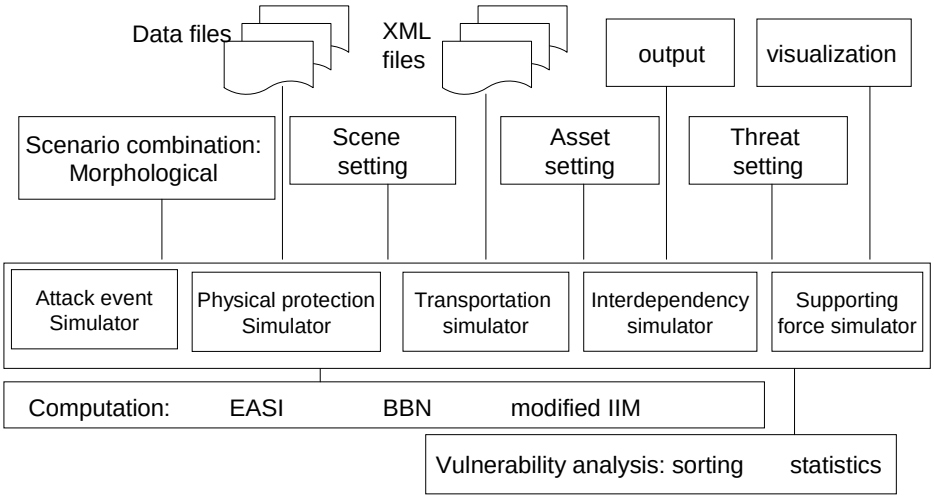

圖 3 CIIP 模擬器之架構圖

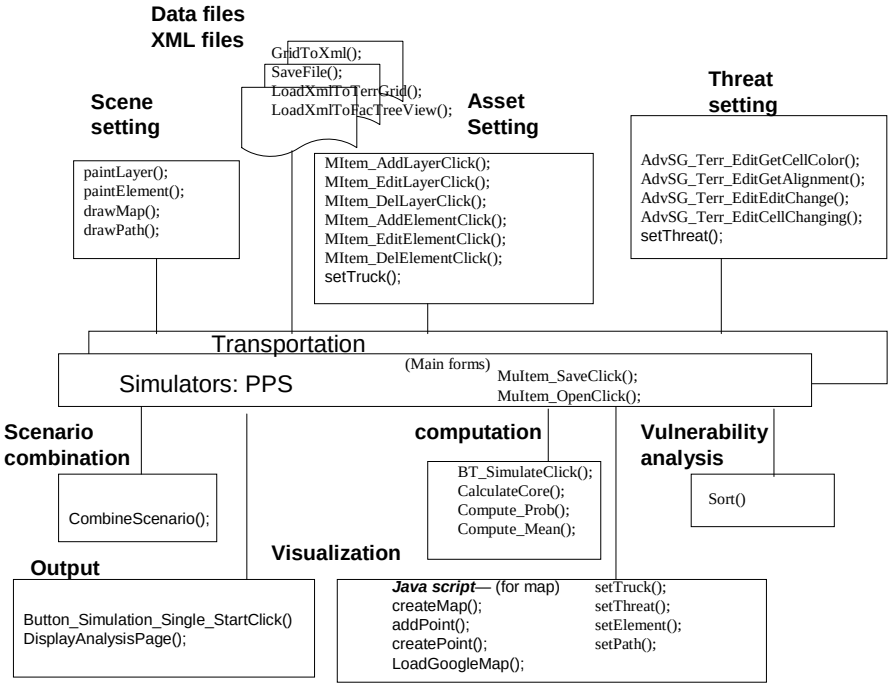

圖 4 函數範例

十、 系統流程

在此節中我們介紹模擬平台的方法流程；此模擬平台的主要流程有八個步驟：場景設定、資產設定、威脅設定、劇情連結、計算模擬、視覺呈現、脆弱分析與輸出，如圖 5 所示。以下是各步驟的詳細介紹：

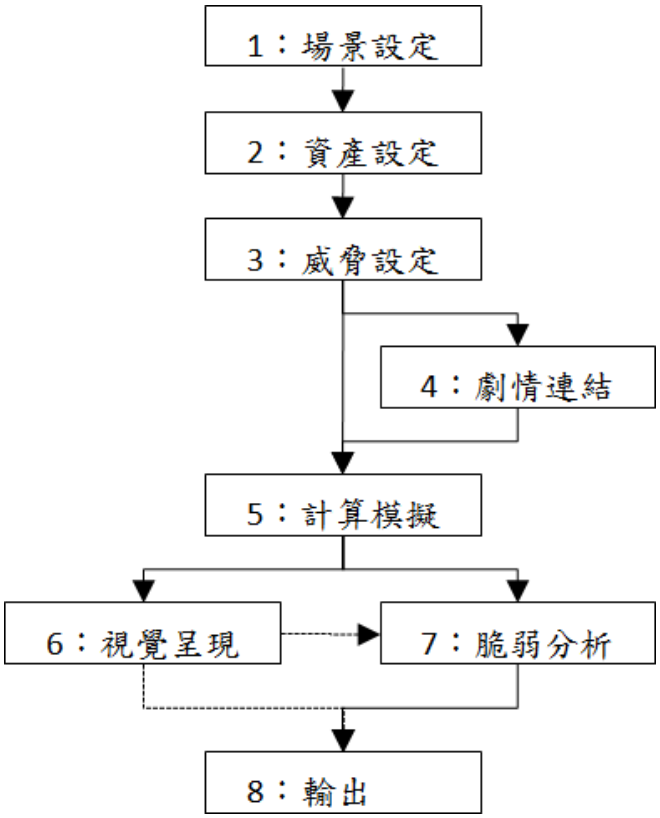

圖 5 模擬平台之流程

(一) 步驟一：場景設定

首先，使用者要先設定模擬的背景、場景，例如設定實體關鍵基礎建設的每個層次（如外牆、關卡、目標建築物等），與連接每層的通道（如汽車通道、人員走道等）；或是運輸模擬中的 Google Map 設定。

(二) 步驟二：資產設定

此步驟須先設定被保護的資產與其特性，因為對於不同的資產所因應的保護措施與面對的風險皆不一樣。而資產的特性則包括了是否會爆炸、危險程度、放射性與遭到人為破壞後的結果等。防護則包括了圍牆、監視器、警報器、保全人員與軍隊警力等。

(三) 步驟三：威脅設定

威脅來源主要是鎖定在人為的攻擊破壞上，例如恐怖份子或有內部惡意的員工。決策者可根據攻擊方的武力強弱來增減其攻擊元素，每個攻擊元素都會各自有權重，因此對於計算模擬則會有不同的結果。威脅設定主要是從過去的案例中取得，也可參考設計基準威脅。

(四) 步驟四：劇情連結

在設定好威脅設定後，形態學分析法可用以剔除會產生矛盾的劇情，例如汽車與飛行兩個屬性是矛盾的，因為目前的汽車是行走在道路上，所以要剔除此種組合。如此一來可以減少掉不合常理的部分，最後再將所有的劇情給組合起來，劇情連結架構如圖 6 所示。

(五) 步驟五：計算模擬

在此步驟將會把上述幾個步驟設定完成的屬性導入現有的公式中做計算，而我們目前有三種公式用於不同的模擬雛型上：EASI、BBN 與 IIM，EASI 主要是用在實體防護系統；BBN 是用在運輸模擬；而 IIM 則是用在相互相依關係。經由這幾個公式的模擬與運算後會產生出成功防守的機率與最好最壞的

劇情。例如圖 7 為貝氏網路因果示意圖。

(六) 步驟六：視覺呈現

在模擬過程中圖形化的介面可用於呈現結果。對於多劇情的模擬，使用長條圖來顯示，圖上會標註防守機率；而對於運輸模擬，可在 Google Map 上顯示貨車的移動路徑，並以動畫的方式呈現。

(七) 步驟七：脆弱分析

在算出所有防守成功機率後，程式會透過排序的演算法將所有的防守成功機率做排序，找出最好與最壞的劇情，並且將兩個結果顯示出來可供比較。這部分可以幫助決策者來找出脆弱的地方，加以改進之後可再重新模擬，直至滿足決策者所希望達到的防禦程度。

(八) 步驟八：輸出

最後，程式會將先前所輸入的攻擊方設定與資產設定寫入 XML 檔。存入 XML 檔案中之設定也可供做輸入使用，使用者就不需要再重新設定一次，直接由程式讀檔即可。

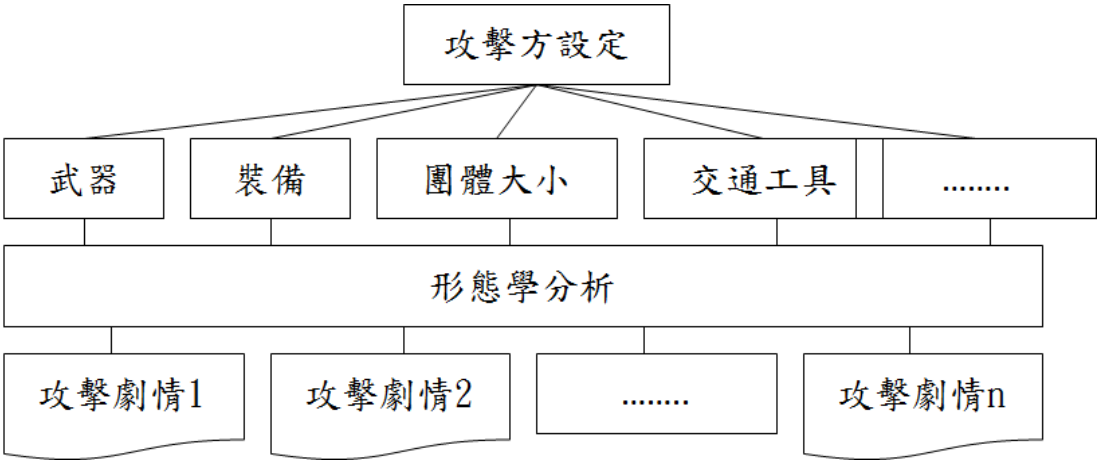

圖 6 劇情連結之架構圖

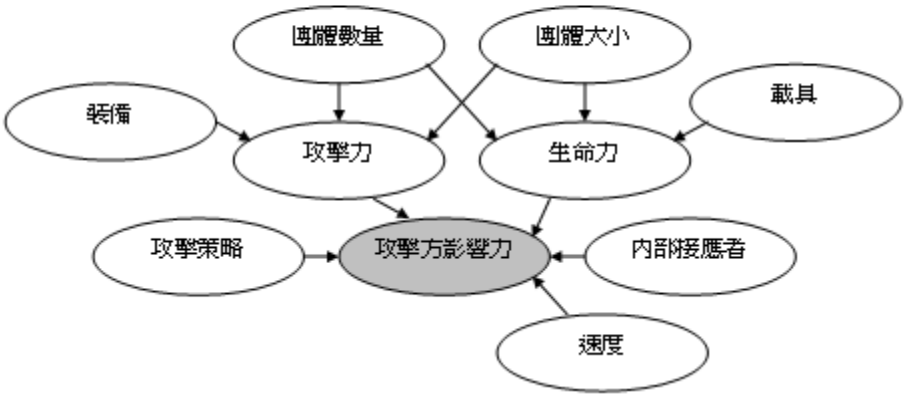

圖 7 攻擊方因果關係圖

參、 主要發現與結論

一、 案例一：關鍵建設實體防護之安全評估

上述模擬平台架構、模擬流程步驟、及相關元件可運用在不同的 CIIP 模擬器上。首先介紹關鍵建設實體防護之模擬器建構。

此案例按照上述八個步驟來做設定與模擬如下：

(一) 步驟一：場景設定

先設定關鍵基礎建設場景，將建築物以層次的表示方法呈現，層與層之前會有連接的通道，例如車輛通道或員工走道等，設定畫面如圖 8 所示。

圖 8 防護配置示意圖

(二) 步驟二：資產防禦設定

實體建設在層與層之間的連接通道上或是外牆，需要增加

監視器、警報器或保全人員，用來提高發現入侵人員的機率。

(三) 步驟三：威脅設定

此步驟為攻擊方的輸入設定，攻擊方的攻擊要素包括了武器、裝備、團體大小、交通工具等，每個要素皆可指定權重，權重則會影響到公式計算防守成功的機率。

(四) 步驟四：劇情連結

當前面三個步驟都設定完成後，程式會將所有的劇情做組合，但在組合之前，這些劇情裡面可能會存在著不合常理的劇情，我們藉由形態學分析把矛盾的劇情剔除掉，介面如如圖 9 所示，完成後再將所有可能的劇情做組合連結。

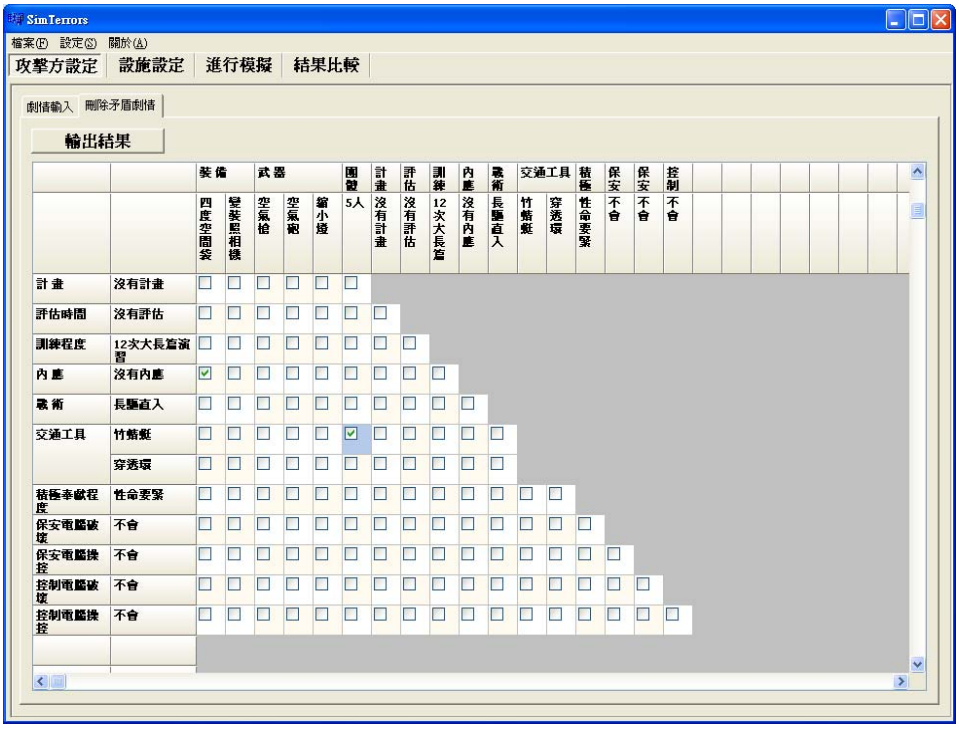

圖 9 形態學分析法組合劇情之示意圖

(五) 步驟五：計算模擬

此步驟為計算模擬所有的劇情，並且算出每個劇情的防守成功機率，我們在此步驟使用 EASI 模型來做計算。但其模型只會考慮到通過每層所花費的平均時間、偏差時間、偵測機率、及位置；所以攻擊方的要素設定必須先經過計算處理，算出攻擊方所設定的要素對這四個值的影響，然後再帶入 EASI 公式裡做計算。最後會得到一個防守成功的機率，如此反覆計算，直至所有劇情皆運算完成。

(六) 步驟六：視覺呈現

在模擬完成後，針對每個劇情程式都會算出其成功防守之機率，在模擬的過程中，使用長條圖來顯示其過程，每一條長條代表一個劇情的機率，並會在每個長條頂端標上其機率值，讓決策者一目了然。

(七) 步驟七：脆弱分析

在此步驟我們會將每個劇情的成功防守機率透過排序演算法做排序，找出最好與最壞的劇情，然後將這兩個劇情擺在一起，提供給決策者來做比較與脆弱分析，並找出其脆弱點進一步的做改善，介面如圖 10 所示。

(八) 步驟八：輸出

在最後此步驟中，決策者可以將先前所設定的背景設定、資產設定與威脅設定等，藉由存檔把這些設定存到 XML 檔中。而且存好的這些檔案也可拿來當作日後的輸入使用。

圖 10 脆弱分析之畫面

二、 案例二：危險物質運輸之模擬

上述模擬平台架構、模擬流程步驟、及相關元件應用在模擬兩基礎建設間以貨車運送危險物質的過程。同樣地，上述的八個步驟使用如下：

(一) 步驟一：背景設定

首先，我們要設定 Google Map 的路徑，這裡我們會使用到 Google Map API 來設定在地圖上的點。在地圖上我們必須設定起點、終點與必須經過的點。

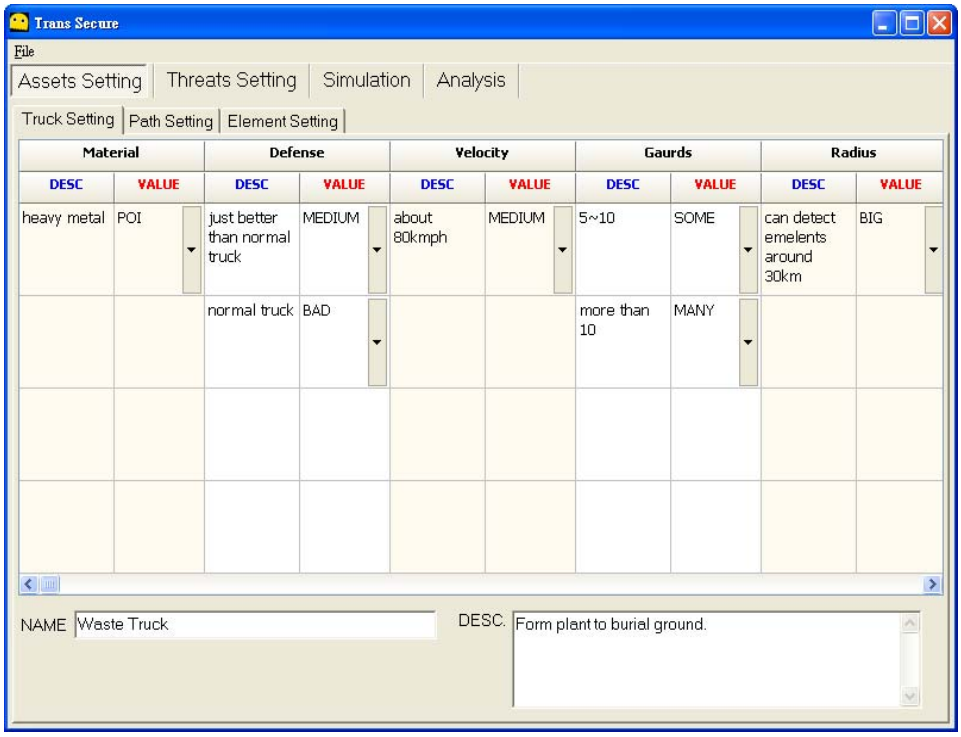

圖 11 貨車設定之畫面

(二) 步驟二：資產設定

貨車為運送危險物質的交通工具，此步驟設定貨車與物質的一些相關屬性，如物質的特性、防禦能力、車速、支援範圍、保全人數等屬性，如圖 11 所示。除此之外，使用者也可在地圖上新增不同的設施，我們設定的類型有：橋樑、隧道、加油站、警局、軍營，對於不同類型有不同的防禦率及救援性等對應。

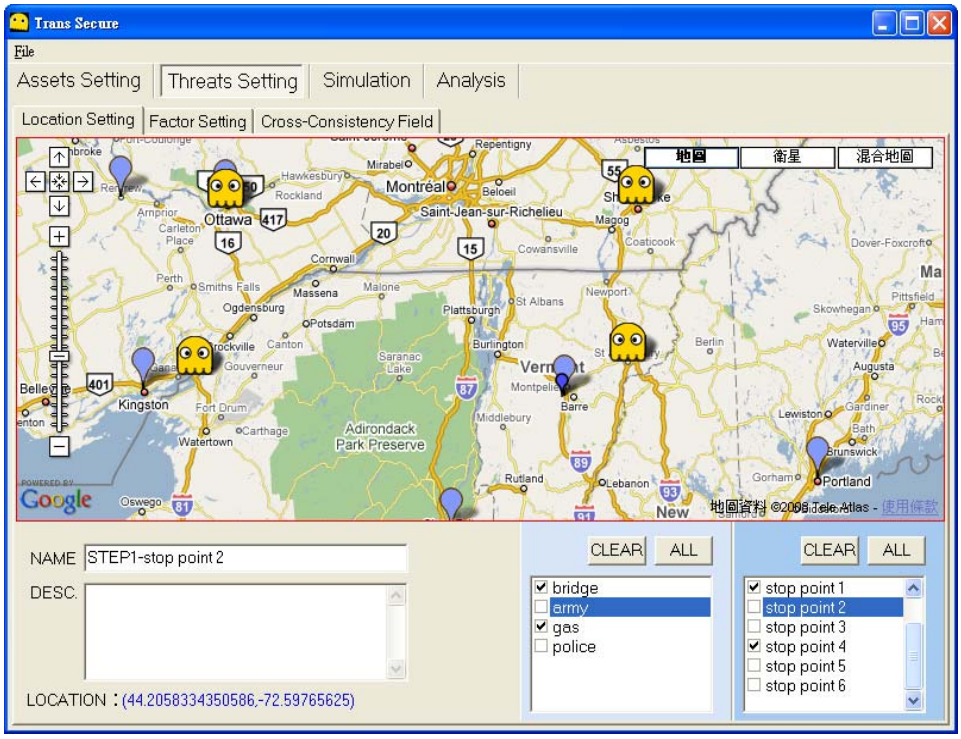

圖 12 威脅地點設定之畫面

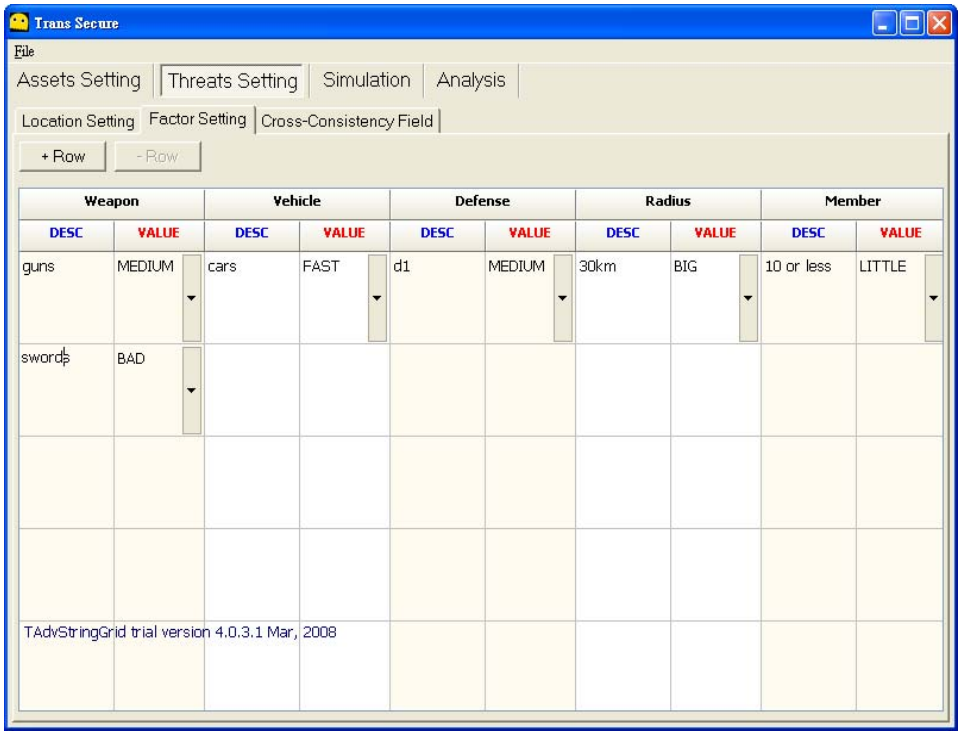

圖 13 威脅要素設定之畫面

(三) 步驟三：威脅設定

此步驟主要是要加入攻擊者的攻擊地點，如圖 12 所示。每個威脅埋伏的地點可以從設施及路線清單中勾選，地點的位置決定了貨車會不會遇到、在哪裡遇到；模擬時只有在貨車進入該威脅集團的攻擊範圍內，才會對貨車的運輸成功機率發生影響。除此之外，我們也要設定攻擊者的特性，如圖 13 所示。

(四) 步驟四：劇情連結

上述三個步驟都完成後，一樣可透過形態學分析法將矛盾的劇情剔除，之後再把所有可能的劇情組織起來。

(五) 步驟五：計算模擬

用貝氏網路被用來計算成功通過攻擊點的機率；將每個被攻擊地點的運送成功機率算出來之後做乘積，最後就得到整個運送過程的成功機率。

(六) 步驟六：視覺呈現

計算模擬完成後，我們對其結果使用視覺化的方式呈現。對於單一劇情，我們使用 Google Map 並且會在模擬過程中運用動態的方式模擬，如圖 14 所示；而對於多劇情，我們使用長條圖來呈現。

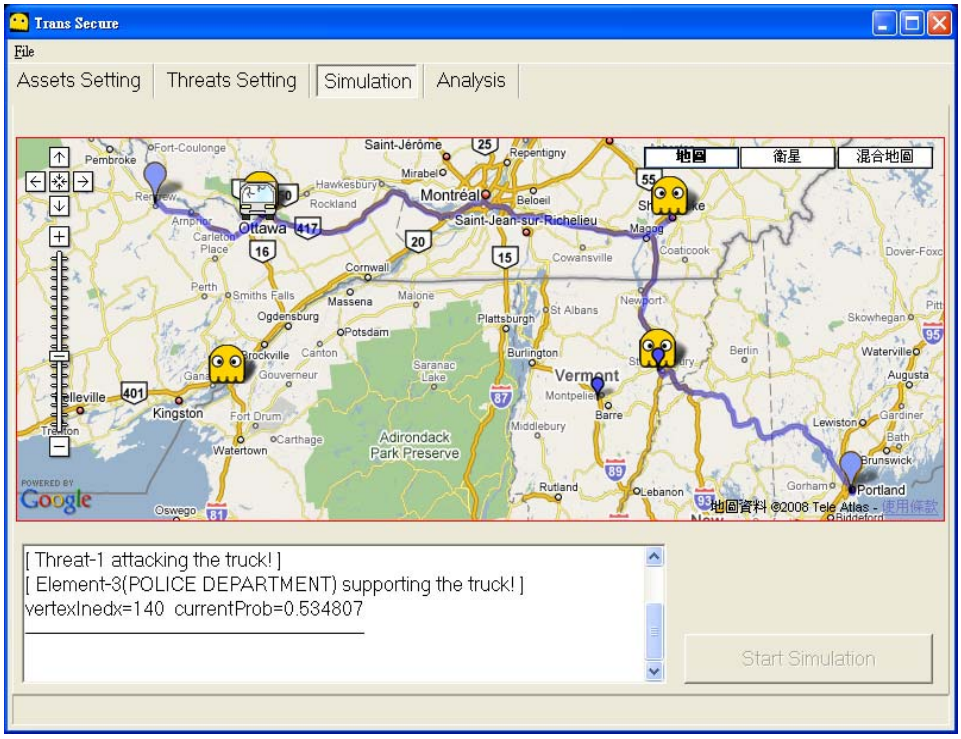

圖 14 單一劇情模擬

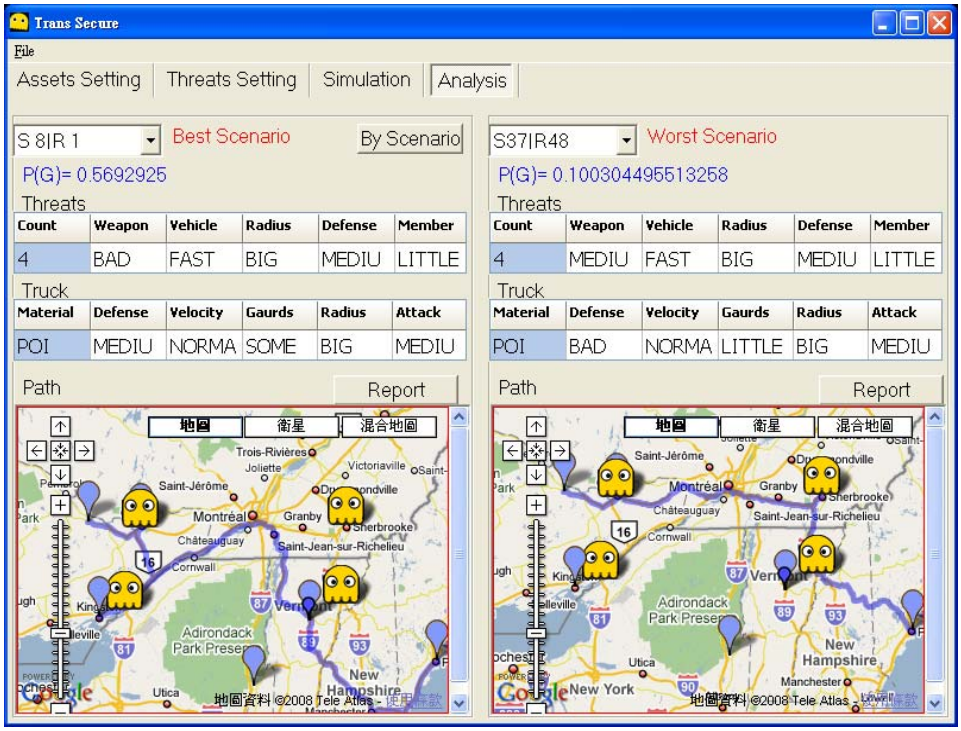

圖 15 結果分析之畫面

(七) 步驟七：脆弱分析

模擬完成後，我們會將所有劇情的機率做排序，找出最好及最壞的劇情，產生報表給決策者，可供決策者做參考，如圖 15 所示。

(八) 步驟八：輸出

最後，我們可以將所有的設定存檔至 XML 檔，供決策者保存。也可當成日後的檔案輸入。

這一套模擬程式是利用 Borland C++ Builder 6 加上 TMS 的元件，以及 Google Maps API 開發完成。開發以及操作的平台皆為微軟視窗作業系統，並無法在其他作業系統上執行。

以上兩個案例顯示，本研究所開發之平台結構、流程、及元件可成功的使用在不同的 CIIP 模擬器上，加速模擬器的開發，提供了一個共通的介面及元件，使輸入輸出資料可以在不同模擬器作分享，提供進一步的分析整合；有助於提升基礎建設防護決策之品質。

三、 結論

關鍵基礎建設之模擬是屬於事前的模擬，目的在於輔助決策者對反恐、國土安全做決策。本計畫開發了一個關鍵基礎建設模擬平台，不同種類之模擬可整合到此平台上。模擬平台具模組化，包括了模擬器、輸入、運算、輸出與資料管理等模組，提供了一個可再利用的環境，加速 CIIP 模擬器的開發。

本研究所開發之平台結構、流程、及元件成功地使用在以下模擬器：

(一)　實體關鍵基礎建設之保護模擬

(二)　危險物質運輸模擬

這些模擬器可輔助決策者辨識關鍵基礎建設防護之弱點，有助於決策者來做進一步的改善防護措施。

在未來我們也希望可以依據這個架構在此平台上創造更多的模組或有更好的架構可以遵循，讓關鍵基礎建設之相關模擬可以更加的完備。此外，模擬畫面我們使用了二維的 Google Map 來呈現，我們也希望可以對這方面加以擴充，使用三維的畫面來呈現，而且可以增加聲音進模擬環境，使決策者更有臨場感，也會讓決策者對模擬可以更有區域性的了解。

肆、參考文獻

[1] International CIIP Handbook 2006, http://www.isn.ethz.ch/crn/_docs/CIIP_Handbook_06_Vol.1.pdf#search='CIIP%202006.

[2] DHS-NIPP 2006, http://www.dhs.gov/interweb/assetlibrary/NIPP_Plan.pdf.

[3] U.S. Nuclear Regulatory Commission**, "**NRC Approves changes to the design basis threat and issues orders for nuclear power plants to further enhance security," April 29, 2003

[4] Matter, J.C., SAVI: A PC-Based Vulnerability Assessment Program, SAND88-1279, July 1988.

[5] Bennett, H.A. "The EASI approach to physical security evaluation." SAND Report 760500 1977; 1-35.

[6] Chapman, L.D., and Harlan, C.P. "EASI estimate of adversary sequence interruption on an IBM PC." SAND Report 851105 1985; 1-63.

[7] Ritchey, T. "General Morphological Analysis A general method for non-quantified modeling, " http://www.swemorph.com/pdf/gma.pdf

[8] Ritchey, T. "Modeling Complex Socio-Technical Systems Using Morphological Analysis, " Adapted from an address to the Swedish Parliamentary IT Commission, Stockholm, December 2002, http://www.swemorph.com/pdf/it-webart.pdf.

[9] Heckerman, D. and Wellman, M. P., "*Bayesian Networks*," *Communication of ACM*, Vol.38, No.3, pp. 27-30, March 1995.

[10] Jensen, F. V. , *An Introduction to Bayesian Networks*, Springer, 1996.

[11] Wikipedia-GIS, 2007,

http://zh.wikipedia.org/w/index.php?title=GIS&variant=zh-tw

[12] NCDR 國家災害科技防救中心,“人為災害研發”, 國家災害科技防救中心 95 年報第二章, January, 2007.

[13] Google Maps API, 2010. http://code.google.com/apis/maps/