架構分析於國家關鍵基礎設施安全防護之應用

Applying Architecture Analysis Methodology to National Critical Infrastructure Protections

鍾健雄[1]、黃俊能[2]
[1]中華科技大學資訊工程系
[2]中央警察大學行政警察學系
[1]Email:jschung@cc.cust.edu.tw

摘要

關鍵基礎設施(Critical Infrastructure, CI)為所有國家經濟的中樞神經系統， CI 本身具有高度的脆弱性，關鍵基礎設施的確保與防護已成為國土安全中重要的一環，行政院國土安全辦公室委託產、官、學界進行「行政院國家關鍵基礎設施防護計畫專業服務委外研究」，擬定台灣的關鍵基礎設施部門，制訂國家基礎設施防護計畫(NIPP)，形成相關政策，並引入風險管理導向之防救災及關鍵基礎設施防護架構。識別資產、系統、網絡和功能為 NIPP 風險管理架構中重要步驟，本文提出一個較為系統化方法論，藉由以活動為基礎的架構分析結果，支持資產辨識，此一方法論是以活動為基礎辨識重要資產，包括領域分析(Domain Analysis)、活動分析、資產關聯、及資產列表等四個步驟。同時，本文將以台灣某高科技園區為研究案例，驗證方法之可執行性。

一、前言

一個現代化的國家運作高度依賴水、電、能源、通訊、網路、金融、交通等基礎設施，這些設施或系統一旦因為天然災害或人為破壞造成中斷，對整體社會的運作和國家安全將會產生極大的衝擊與傷害。以 1999 年發生的 921 大地震為例，當時因南投縣中寮鄉的中寮超高壓變電所遭震損，導致南電北送之線路受到影響，北部都會區供電吃緊，由於電力供給不足，使得新竹科學工業園區損失最為慘重，國家經濟損失難以估計[1]。

這些基礎設施並非獨立運作，甚至彼此勾連、綿密互動、相互影響。針對國家關鍵基礎設施的相互關聯性研究，認知這是一個高度連結的網絡系統，系統間的運作牽涉政策、經濟、技術、資通、資產、使用者...，如此複雜的系統堪稱系統中系統(System of Systems)[2]。針對系統中系統，必須採用系統化的分析方法來釐清組成關鍵基礎建設的系統、次系統、元件，及其相關活動、功能、與能力。本研究採用架構分析方法(Architecture Analysis Methodology)作為有效描述關鍵基礎建設之工具。

為有效防護關鍵基礎設施，我國 NIPP 導入風險管理架構，包括建立安全目標；識別資產、系統、網絡和功能；風險評估；行動優先順序；防護計畫的執行；成效的評量等 6 個步驟[3]。其中確定資源、系統、網絡和功能步驟最為重要。本文的主要目標即提出一個以架構分析為基礎的方法論，協助系統化地辨識資產重要性，建立資產清單，以利後續 CI 防護的執行。

二、相關研究

關鍵基礎設施的確保與防護已成為國土安全中重要的一環，各國近年來紛紛積極推動 CI 的防護工作(Critical Infrastructure Protection, CIP)。歐盟(EC)、美國(US)國土安全部和世界各國持續關注國家基礎設施的安全的工作，並視為新的國際威脅。2005 年歐盟通過「歐洲計畫的關鍵基礎設施防護(EC, 2005)」綠皮書[4]，隨後歐盟的理事會通過指令 114/08/EC，對於歐洲關鍵基礎設施的調查、辨識以及需求

加以評估，提高它們的防護水準，同時發起歐洲關鍵基礎設施防護計畫（EPCIP）[5]。2009年美國發佈並啟動美國國家基礎設施防護計劃（NIPP, 2009）[6]。

有關關鍵基礎設施防護的方法與工具研究，Yusta [7]收集 1999 至 2010 年間有關 CI 防護的方法論、應用程式和軟體等55篇論文，提出一篇綜合性整理評論，極具參考價值。許多學者聚焦於 CI 之各系統間的相互關聯(Interdependency)的複雜性議題，從「架構描述模型」及「效能評估分析」兩個角度提出許多研究成果。Rinaldi[8]提出一篇深入探討 CI 相互關聯性的經典論文，並提出以模式模擬評估 CI 系統間相互關聯性影響。Thissen[9]針對 CI 的實體、作業管理、及產品服務三個面向提出一個參考模型。Sokolowski[10]運用概念建模概念提出 CI 的建模方法，運用功能分解(Functional Decomposition)及影響圖(Influence Diagram)來分析基礎設施。Ligaarden[11]的研究顯示 UML 及 SysUML 可用來建立模型有效地描述 CI 間複雜的相互關聯性。Bagheri[12]藉由模型驅動架構(MDA)觀點，運用 UML 延伸定義能力建立一個可描述 CI 的內部結構與外部連結的參考模型，此模型聚焦基礎設施的服務、管理、資訊、及實體等四個構面。NISAC(The National Infrastructure Simulation and Analysis Center)[13]提出一套分析評估 CI 相互影響的模擬方法論，此方法論是由系統動態學、IDEF0 模型工具、及非線性決策最佳化演算法組成。綜觀國外相關研究，大部分研究都關注在建立適當模型，並運用模擬分析來洞察複雜的 CI 行為及評估相互間的關聯性。

相較於國外對 CI 的研究，行政院國土安全辦公室自 2009 年起積極推動建構關鍵基礎設施防護計畫(NIPP)，委託產、官、學界進行「行政院國家關鍵基礎設施防護計畫專業服務委外研究」[3]，研究參考各國理論與實務運作經驗，結合我國國情需要，經與學者專家及政府官員討論後，初步將台灣的關鍵基礎設施分為「能源」、「水資源」、「資通訊」、「交通」、「銀行與金融」、「緊急救援與醫院」、「中央政府及主要都會」、及「高科技園區」等八個部門，並勾勒出我國 CI 主要防護部門項目(Sectors)、次部門項目(Sub-sectors) 與各重要元件(Critical Elements)。同時，採取以風險導向之國家關鍵基礎設施防護架構。

三、風險導向之關鍵基礎設施防護架構

經文獻探討顯示，各國面對關鍵基礎設施防護時，多數關鍵基礎設施防護計畫(NIPP)是基於風險管理的架構作為標準。美國 NIPP[6]提出一個 6 個步驟的風險管理框架，如圖 1。

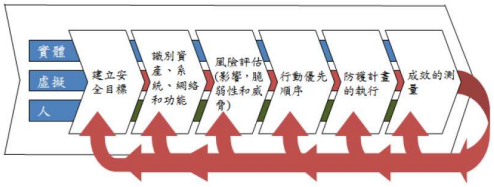

圖 1 關鍵基礎設施防護框架[6]

1. 建立安全目標：安全目標的制定必需考慮如生命損失，國家安全的經濟影響和衝擊。
2. 確定資源、系統、網絡和功能：發展一個完整的清單，包含國家資源、系統和網絡基本資訊，以及物質產品、人員功能和系統資訊。
3. 風險評估：針對影響、脆弱性、與威脅，使用定量方法透過系統化嚴謹的流程提供完整的分析結果。
4. 行動優先順序：國土安全部門與安全合作夥伴進行風險評估，確定行動的先後順序，確保防護措施能夠降低風險。
5. 防護計畫實施：執行防護措施，降低風險。
6. 成效測量：建立相關指標，以確定是否實際達成安全目標的資訊。

上述以風險導向之關鍵基礎設施和關鍵資源的防護框架中，防護的目的是降低 CI 部

門的受損風險，每一個 CI 部門由許多系統、次系統、重要元件、人…等組成，這些組成元件將遭受威脅攻擊(威脅可能是人為攻擊或自然災害損傷)，此處威脅攻擊成功機率定義為脆弱性(Vulnerability)，脆弱性與損害造成的影響相乘形成風險(Risk)，CI 部門(Sector)的風險由部門組成元件的風險所組合而成[14]。結合 CI 的關鍵資產列表及風險可以產生一個關鍵資產的風險排序，此一風險排序表可以提供執行 CI 防護計畫時間優先次序，以使防護資源與投資的運作最佳化。現階段辨識關鍵資產的工作均由第一線工作人員決定，人為決定欠缺客觀性，常因人而異，另關鍵資產認定可能因不同情境或隨時間而有變化。因此，本研究針對資產辨識提出架構觀點之方法論，以活動分析為核心，輔以 IDEF0 模型工具，建立資產辨識流程產生關鍵資產列表。運用關鍵資產可以結合初步危害分析(PHA)快速評估建立關鍵資產之關鍵性(Criticality)排序，或結合風險評估建立關鍵資產之風險排序，以利後續關鍵基礎設施和關鍵資源的防護作業。

四、基於架構分析之資產辨識方法論

1. 資產辨識

資產辨識是在關鍵基礎建設防護中最首要的工作，資產辨識的最終目的在於找出關鍵資產，資產的形式並無具體限制，可能是一個實體設施、空間、軟體所提供的功能等，甚至用來維護社會秩序的法律條文都可視為國家的必要資產。因此資產的定義並不在於其形式，而是其所提供的功能，在 NIPP 的架構下，主要目的為國家安全，相關公共設施依其設立之原意正常運作，而主要探討之公共設施則以實體設施為主。基於不同單位的權限範圍以及其所要達成的不同目的，所涵蓋的資產為數可能甚多，因此確認資產的必要性為資產辨識的第一步。

除了資產本身的重要性之外，當特定資產對其他資產可能造成影響時，則可能進一步對整體系統造成連鎖影響，從而提升此一資產的重要性，因此資產的相依性亦是評估關鍵資產的指標之一。為了清楚描述資產相依性，必須更進一步了解資產之間互動的情形，亦即必須對所有必要資產之間的關聯性有完整的描述，方能完整評估特定資產的重要性。資產相依性應包含以下三種類型，(1) 供需關係：資產進行的任務之間有供需關係，例如各項電子設備需依賴電力設備、電力的輸送須依賴電力線路、輸配電系統等，任一部分的設備的滅損皆會直接造成最終的功能喪失。(2) 屬性共通：資產在特性上有共通處須加以留意，例如資產在地理空間上置於一處，或同一流域或山脈走向的影響關係，當發生洪水或土石流等情事時對下游地域的連帶影響等。(3) 備援關係：資產之間具有相互支援或取代性，當其中一個設施損害時，可立即由其他設施替補。

2. 架構分析方法

關鍵基礎建設防護不僅必須考量單一部門(sector)中複雜的系統組成與功能運作，同時也要考慮不同部門間相互影響，故可將關鍵基礎建設防護視為一系統中系統 (System of Systems)。面對複雜系統，必須採用系統化的分析方法來釐清組成關鍵基礎建設的系統、次系統、元件，及其相關活動、功能、與能力。為有效描述關鍵基礎建設，架構分析方法是一種系統化的分析工具。

CI 是一個複雜的相互影響的網絡系統，其複雜性源於不同類型的基礎設施所構成，且單一的基礎設施具有高度的複雜性，系統複雜性實際地表現於系統元件、工作流程、系統能力、系統節點、及作業組織。架構分析方法論植基於系統架構學，以不同觀點來描述系統，當架構一個系統時，可以由系統功能(Functional)、系統運作(Operational)、及實作技術(Technical)等三個觀點來考量。系統架構化的終極目標則是期望建立一個可執行架構(Executable Architecture)，可用於分析系統行

為及評估系統效能。圖 2 說明系統架構模型概念，系統架構建模起始於任務(Mission)授領，根據任務，產生作業構想。依據作業構想分析與實作概念，建立系統功能、實體裝備、及作業組織等需求。其中將系統功能分解，產生功能架構(Functional Architecture)，包括資料字典、流程模型、資料模型、規則模型，另實體裝備及作業組織亦演化成實體架構(Physical Architecture)及組織模型(Organization Model)。同時，亦觀察系統動態行為，建立動態模型(Dynamic Model)。最後整合上述相關模型建立可執行模型(executable model)。

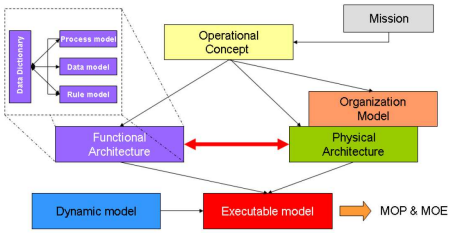

圖 2 系統架構概念模型

架構分析的方法是由不同的觀點下對系統進行了解，具體的分析結果為各種觀點下的塑模產品。這些產品可以用來描述系統，也可轉換為可執行模式進行模擬[15]。架構分析方法已用於許多複雜系統分析，如美國國防部發展出的 DoDAF (DoD Architecture Framework)，DoDAF 以作戰、系統、及技術標準的觀點針對國防部各項任務進行塑模，建立作業流程、組織架構、資訊分享、決策規則模型、及事件互動等作戰觀點塑模產品，以及針對任務遂行，建立系統功能、元件、介面、資料通訊、及裝備部屬等系統觀點塑模產品。同時，亦根據系統開發可行性，探討技術標準以支持系統建構。以活動為基礎分析法(Activity-Based Methodology，ABM[16])是執行 DoDAF 的一個方法。ABM 以作戰時所執行的相關任務活動為分析時的重點，透過執行任務活動的需求面，分析出作戰觀點上組織架構、作戰節點、資訊傳遞內容等資料，以及系統觀點中支援做活動的系統功能律定、系統與介面定義、資料流內容等，進行相關架構產品的開發。從 ABM 分析的結果中，可以釐清(作業節點、作業行動、角色)，(系統節點、系統功能、系統)，及(角色、系統、組織)之間關係。ABM 方法可以幫助我們以活動分析為核心，分析出與活動相關的流程、功能、設備、執行者、單位組織、及作業節點等資訊。這些資訊在關鍵基礎架構防護作業中同樣扮演重要角色，可做為資產辨識的依據。

3. 架構分析工具

考量以活動分析為關鍵資產辨識的核心工作，本研究採用整合性定義方法論(IDEF)作為塑模工具。IDEF 源自美國空軍的整合型電腦輔助製計畫，藉由圖形剖析複雜的製造流程以提供共通運用的介面提高製程效率。其理論基礎是建構於結構化系統分析概念上，由上而下局部細分活動內容，逐步將實體系統分解。由於 IDEF0 主要是針對系統活動運作的過程，提供順序性的分解排列呈現，此種呈現方式對於架構分析之活動流程分析，可獲得相當清楚的表示。故本研究以 IDEF0 的方法呈現相關活動流程。

IDEF0 在系統運作過程描述中，不僅可協助系統功能模組的分解，並提供階層化系統運作流程的表示。IDEF0 模型中，活動以方塊圖表示(如圖 3)，每個活動都必須命名與定義，且活動名稱以動詞為宜。另整合與每項活動有關的四項資訊，表示與該活動相關的對象。四項輸入資訊說明如下：

(1) 輸入(Input)：為進入活動方塊的對象，例如所傳遞的資訊、原料等；

(2) 輸出(Output)：為該活動處理過後的結果，並可傳遞給下一活動使用。

(3) 控制(Control)：控制活動執行的項目，例如操作手冊或某項控制訊號。

(4) 機制(Mechanism)：執行該項活動所需要的資源，例如人員或系統。

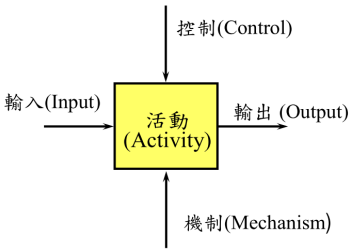

圖 3 IDEF0 塑模表示示意圖

IDEF0 圖像的呈現，可明確表達系統的活動與資料流程，以及兩者之間的關係，而此種以活動順序為導向的思維基礎，對於本研究應用於資產辨識來說，提供相當明確的表示。

4. 可操作性資產辨識流程

資產辨識是以風險為基礎的關鍵設施評估方法論中的首要工作，本研究所提出之以活動為基礎的資產辨識方法是一個可操作性的流程，包括四個步驟：(1) 領域分析、(2) 活動分析、(3) 資產關聯、及(5) 資產列表。

(1) 領域分析：領域分析(Domain Analysis)的主要目的是對問題領域背景知識進行全面性的瞭解。以 CIP 而言，相關知識應包括 CI 設置目的、系統組成(包括任何支援及影響其運作得系統、次系統、裝備、重要設施、作業組織…等)、運作流程、影響運作歷史事件、管理政策與規定、災害管控與應變處理計畫、…等。領域分析應由基層單位做起，所搜集的資料逐級匯整，以應付各種災害及支援各層級運用。各級單位的領域分析資料可經由資料庫儲存及運算應用。

(2) 活動分析：活動分析是資產辨識的核心作業。為達成資產辨識的目標，首先將針對 CI 所要執行的任務(或功能)進行分析。所執行的任務可以是主任務下並行的次任務，或是具階層性的次任務。因此每一項任務都可進行拆解或整合，以達成 CI 功能。任務執行可以由數個活動所組成，任務可視為活動流程，活動可以獨立個別進行或彼此間存在邏輯連結關係。有些活動可視為主要活動，有些則視為支援活動。有些活動具關鍵性(如活動無法進行則任務無法完成)。依照 ABM 架構分析概念，每一個活動具有執行者或單位，以及執行活動所需資源，此處資源可能是人力、資訊、設施或是裝備機具…等。因此，關鍵基礎設施中所有的資源可視為資產。決定關鍵性活動能否正常進行的資源被考量為關鍵性資產。活動分析的目的將 CI 的任務、活動、資產串連起來。

本研究中運用 IDEF0 塑模工具支援關鍵設施活動分析。根據 IDEF0 的定義，每一個活動的表示可以由輸入、控制、輸出、機制等四個部分組成，其中控制是指執行此一活動所需之政策方向、法規辦法、操作規定…等，機制則是指執行活動所需資源(如圖 4)。

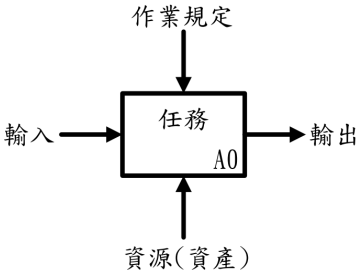

圖 4 IDEF0 資產活動分析元件

圖 5 表示系統遂行任務需要執行三個相關聯的活動，活動間存在循序與回饋之複雜關係，每個活動具備個別獨立的資產以支援活動進行。假設其中一個資產遭毀損，則其相關活動無法進行，此一結果甚至影響任務執行，故可將此資產視為關鍵資產。

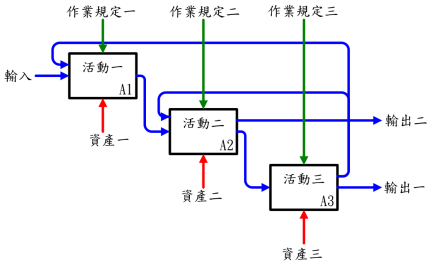

圖 5 IDEF0 資產活動分析示意圖

(3) 資產關聯：根據活動分析結果，可以找出支援任務執行的各項活動所需的關鍵資產。進一步須釐清任務、活動、資產間關聯性。此處可以運用階層整體性模型 (Hierarchical Holographic Modeling，以下簡稱 HHM)描述關聯性。首先運用 HHM 可以探討任務間的階層性(如圖 6)，其次表現單一任務、活動、資產間關係，如圖 7。

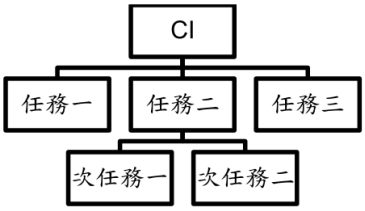

圖 6 任務階層圖

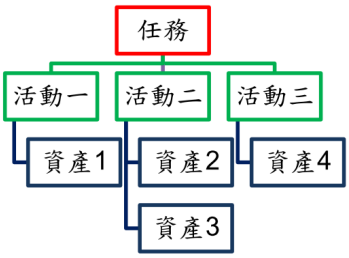

圖 7 任務、活動、資產圖

根據任務階層圖及活動資產圖之彙整，可以找出所有支援 CI 運作所需資產。分析中發現有些資產可能為多個活動所共用(如圖 8)，如資產二支援二個任務中不同活動，表示資產間有爭奪資源的可能性，將增加分析複雜度，但也更加證實資產的關鍵性。

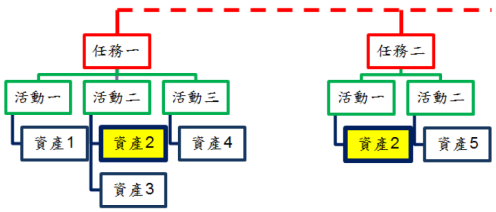

圖 8 資產共用示意圖

(4) 資產列表：依據活動分析與資產關聯分析之結果建立資產列表。表列資產項目可以根據任務分類及關鍵基礎設施分類，或可根據領域專家討論，以及支援任務執行的程度進行重要性排序，亦可支持風險評估排序。

五、科學園區案例研究

藉由上述之資產分析方法論，實際以某一科學園區為研究案例，探討此一方法之可執行性，由於其中細節牽涉科學園區防護作為，本節僅究重點展示分析結果，並將實際地名、道路名稱、變電所名稱予以代號表示。

首先，以 UML 類別圖表示科學園區之 CI 上層關聯性(如圖 9)。

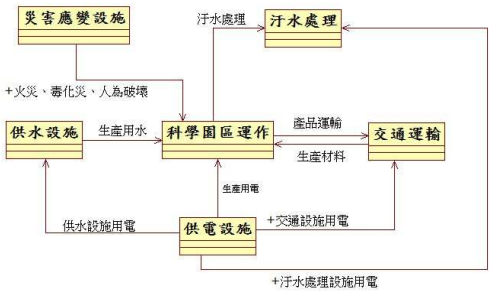

圖 9 科學園區 CI 關聯

針對科學園區運作進行活動分析，為要獲得支持科學園區運作之關鍵資產。依據科學園區運作與基礎建設間關聯性建立第一層 IDEF0 圖(如圖 10)。

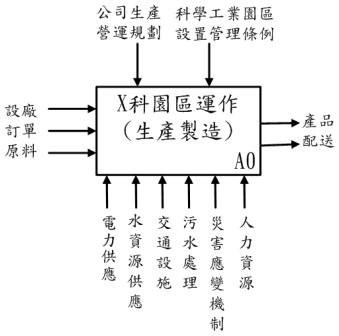

圖 10 X 科園區運作關聯

根據科學園區災害事件蒐集與分析，影響供電設施造成的危害事件比例最高(38%)，最為科學園區所關注，圖 11 表示供電設施之活動分析，包括電力流向、重要變電所、及高壓電塔。

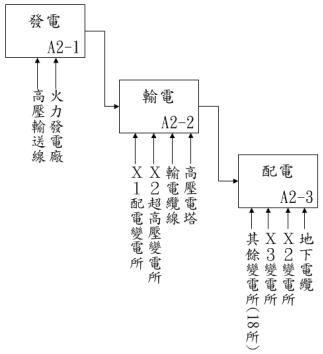

圖 11 科學園區供電分析圖

水為高科技生產過程中的重要資源，故此園區內設有大型蓄水池以供不實之需，且因園區部分生產基地的地勢較高必須設立高架水塔及相關抽水設施，以利水資源供應。園區供水之活動分析如圖 12。

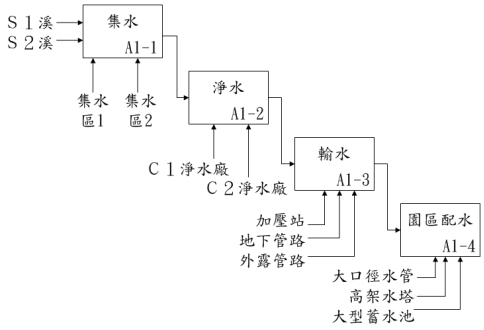

圖 12 園區供水之活動分析圖

交通運輸為科學園區設置時重要考慮因素，針對貨物運輸目的，高速公路及快速道路為其主要運輸管道，故連結高速及快速道路之閘道可視為重要設施。而針對人員及商務旅運目的，則有台鐵、高鐵、機場的支援。園區內道路以 R1 道路縱貫南北最為重要。根據交通功能所作之分析如圖 13。

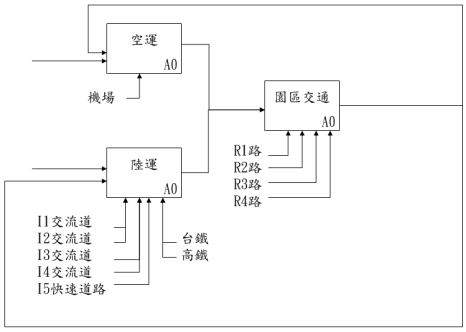

圖 13 園區交通活動分析圖

根據危害事件分析，科學園區操作上可能發生的災害有火災及毒化災，有時亦考量人為因素造成的園區運作上的影響，如居民抗爭、竊盜、破壞、及恐佈份子攻擊…等，園區應規劃災害反應機制，此一機制運作可能需要特殊單位參與，如消防單位、毒化災防護、聯防機制…等，有關災害反應機制活動分析並不在本研究範圍內。

依據前述各項活動架構分析方法論，以活動為基礎之分析步驟，針對支援園區生產單位之基礎設施進行 IDEF0 分析及分析結果回饋給園區決策單位腦力激盪討論其關鍵性，將可獲得資產辨識結果包括供水、供電、交通、汙水處理等重要設施。

六、結論

關鍵基礎設施的確保與防護已成為國土安全中重要的一環，行政院所制訂國家基礎設施防護計畫(NIPP)引入風險管理導向之防救災及關鍵基礎設施防護架構，其中識別資產、系統、網絡和功能為風險管理架構中首要，本文所提出以活動為基礎的架構分析結果，支持資產辨識，此一方法論包括領域分析(Domain Analysis)、活動分析、資產關聯、及資產列表等四個步驟，藉此可以協助辨識關鍵資產。本

方法論已經由台灣某高科技園區為案例，驗證方法論之可執行性。

後續研究工作將持續精進方法論細節，同時聚焦於 CI 系統間相互關聯性之研究，特別是運用代理人模型進行模擬，以了解及評估 CI 之複雜行為，用以確實達成關鍵基礎設施及關鍵資源之防護成效。

參考文獻

1. 李宛蓉, *中察變電所震壞 全台 650 萬戶停電*, *中時電子報*. 1999: 台北市.
2. Tolone, W.J., et al., *Enabling system of systems analysis of critical infrastructure behaviors*, in *Critical Information Infrastructure Security*. 2009, Springer. p. 24-35.
3. 黃俊能, *NIPP 推動及安全評估研究報告*, *行政院國家關鍵基礎設施安全防護專業服務委外研究案（第三階段）*. 2012, 行政院國土安全辦公室.
4. *Green Paper on A European Programme for Critical Infrastructure Protection*. 2005, Commission of the European Communities: Brussels.
5. *European Programme for Critical Infrastructure Protection*. 2006, COMMISSION OF THE EUROPEAN COMMUNITIES.
6. *National Infrastructure Protection Plan*, Dept. of Homeland Security, Editor. 2009.
7. Yusta, J.M., G.J. Correa, and R. Lacal-Arantegui, *Methodologies and applications for critical infrastructure protection: State-of-the-art.* Energy Policy. **39**(10): p. 6100-6119.
8. Rinaldi, S.M., J.P. Peerenboom, and T.K. Kelly, *Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies*, in *IEEE Control Systems Magazine*. 2001. p. 11-25.
9. Thissen, W.A. and P.M. Herder, *Critical Infrastructures: Challenges for Systems Engineering*, in *Systems Man and Cybernetics IEEE International Conference on*. 2003. p. 2042-2047.
10. Sokolowski, J., C. Turnitsa, and S. Diallo. *A Conceptual Modeling Method for Critical Infrastructure Modeling*. 2008: IEEE.
11. Ligaarden, O.S. *Using UML to model dependencies in systems of systems*. in *Fourth International Conference on Critical Infrastructures Crisis*. 2009.
12. Bagheri, E. and A.A. Ghorbani. *Towards an MDA-oriented UML profile for critical infrastructure modeling*. in *Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services*. 2006. Markham, Ontario, Canada: ACM.
13. Min, H.-S.J., et al., *Toward modeling and simulation of critical national infrastructure interdependencies.* IIE Transactions, 2007. **39**(1): p. 57-71.
14. Lewis, T.G., *Critical infrastructure protection in homeland security: defending a networked nation*. 2006, Hoboken, N.J.: Wiley-Interscience.
15. 鍾健雄, 田孟峰, and 謝應言, *基於架構產品之可執行模式研究, 企業架構與資訊科技研討會*. 2009: 台北市.
16. Ring, S.J., et al., *An Activity-Based Methodology for Development and Analysis of Integrated DoD Architectures*, in *Command and Control Research and Technology Symposium*. 2004.