結合軟體工程方法與風險評估機制建構資安威脅模型：以物聯網架構下之智慧電網應用為例

陳宇佐[1*]、黃莊喬[2]、吳建東[3]
[1,2]國立聯合大學資訊管理學系、[3]捷而思股份有限公司
[1]yutso.chen@nuu.edu.tw、[2]a596466@gmail.com、[3]james@jrsys.com.tw

摘要

預防與治療是疾病防治的兩大手段，而對於資訊系統的資訊安全防護，亦不脫事先的預防與事發的處置，尤其是事先的預防往往能降低事發處置的工作負擔。本研究引用軟體工程的成熟技術與資安威脅的風險評估機制，提出一套資安威脅塑模方法 TMER，使得資訊系統在設計過程，即得以系統化、模組化地辨認資訊安全威脅，並確保應用程式的設計可靠性與日後系統運作的理論可用性。而為能實際演練 TMER 的運作過程，本文以智慧電網的資訊系統應用為例，展示建構智慧電網應用之資安威脅模型，內容涵蓋傳統電力系統、資料採集與監控系統 supervisory control and data acquisition (SCADA)、先進測量基礎設施 advanced metering infrastructure (AMI)的功能元件剖析；接著針對擬分析的智慧電網應用，在確認關鍵功能元件之後，透過使用案例圖、資料流程圖、威脅分類表 STRIDE+p 以及風險評估分析，逐步篩選關鍵資安威脅以完成威脅模型的建立。本文所提出的 TMER 資安威脅塑模方法，考慮功能元件的框架內容建立、引入軟體工程的分析與設計工具，再援引資安威脅類型與風險評估理論，為系統化的資安威脅塑模指出了一條足資參考的學術研究方向；而所展示的資安威脅塑模案例演練，亦可為智慧電網的資安設計在實務研究上提供有價值的參考。

關鍵詞：威脅模型、軟體工程、風險評估、智慧電網

Build Information Security Threat Model by Integrating Software Engineering Method and Risk Assessment Mechanism: Application of IoT Based Smart Grid as an Example

Yu-Tso Chen[1*], Chuang-Chiao Huang[2], James Wu[3*]
[1,2]Dept. of Information Management, National United University, [3]Jrsys International Corp.
[1]yutso.chen@nuu.edu.tw, [2]a596466@gmail.com, [3]james@jrsys.com.tw

Abstract

Prevention and treatment are the two major ways of disease handling; the security protection of information system is also the same. In particular, prior prevention can reduce the workload

of protecting the system against the happening attacks. This study proposes a novel threat modeling method, named TMER, by leveraging the features of software engineering method and risk assessment mechanism. The TMER can help identify information security threats in a systematical and modularized fashion in the progress of system design; accordingly, to ensure the reliability of system design and the theoretical availability of system operations. In order to introduce the operation process of the proposed TMER, this paper takes an application of smart grid (SG) as an example to demonstrate the works of TMER. Firstly, to confirm the functional components of SG that covers the traditional power system, supervisory control and data acquisition (SCADA), and advanced metering infrastructure (AMI). And then, a selected SG application is analyzed through the tools of use case diagram, data flow diagram, the proposed STRIDE+p threat classification table, and risk assessment mechanism to build a probabilistic threat model. The proposed TMER considers the functional components of system, adopts software engineering methods, as well as invokes the security threat types and risk assessment mechanism, so that indicates a considerable research direction of systematic threat modeling. Besides, the demonstrated practice towards application of SG also provides a valuable and practical reference for information security design on SG applications.

Keywords: Threat Model, Software Engineering, Risk Assessment, Smart Grid

壹、前言

隨著資通訊技術的發展，資訊系統的使用已經與人類生活、商業活動緊緊相繫，而資訊系統因遭受攻擊而致的後果，往往也會直接影響與之相關的人類活動，且影響層面通常廣泛。資訊系統的資訊安全防護，與人體防禦外來病毒的狀況類似；人體也是一種系統，人體遭受病毒攻擊的後果就是嚴重狀況各異的疾病。除了染病時針對攻擊病因的即時診治，預防醫學提前針對可能的致病威脅施以作為，如：增強免疫力、注射疫苗…等，無疑展現另一種有效的處置方法。而從整體醫療資源支出的角度來看，事實確如常言所道：預防勝於治療，預防性處置或先天性改善的投入成本，通常較問題排除所需投入的成本為少。

同理，資訊系統的資訊安全防護，除了即時處理或抵禦當下所受之攻擊，如能提前確認資安威脅以為系統設計的「體質」強化，則其效益當可更佳。然而，攻擊與威脅實有本質特性上的差異，攻擊之發生就是一起明確事件，但威脅卻是不確定的風險，如何辨識威脅項目、評估威脅風險、確認關鍵威脅，正是能否有效建構威脅模型的成敗所在。尤其以大型資訊系統為設計標的時，所涉元件之多、功能範圍之廣，使得建構資安威脅模型的複雜度大增，如何能有系統地對資安風險抽絲剝繭、有效地確認資安威脅，是一項既需理論基礎又需考慮務實效益的重要議題。

近數十年來，軟體工程方法的成熟發展使得軟體系統在質與量的成長，亦似摩爾定律(Moore's Law)的呈現曲線，軟體工程方法對於系統分析、設計乃至於實作與測試的操作，提供穩固有效卻又不失彈性的好處。如能引入軟體工程方法的優點，讓同樣屬於軟體範疇的資安威脅模型建立，能夠透過系統化的歷程作步進式演成，將有助於資安威脅模型在學理研究與實務運用上的發展。此外，針對威脅的不確定性的檢驗與處置，學術研究與產業實務上常用的風險評估方法，提供了合理建構威脅模型的線索。尤其是針對如智慧電網一般的大型複雜系統，在涉及多種重要設備運作以及廣大使用者的資訊存取的應用中，更需要全面且能扼要點出關鍵威脅的重要優先順序的建模方法。

智慧電網(smart grid, SG)的推動是全球議題[36]，它以傳統電力系統為基礎，透過聯網裝置與資通訊技術的運作，以及先進測量基礎設施 advanced metering infrastructure (AMI)的導入，執行範圍涵蓋電力生產者至消費者端之間的即時資料收集[19]，帶來更勝於傳統電力系統的資料存取即時性與資訊分析可用性。也因此，在電力系統相關設備與聯網相關設備，需即時提供電力生產、管理與交易相關資訊的功能需求下，就必須加入資料採集與監控系統 supervisory control and data acquisition (SCADA)的功能。然而，在受益於導入 SCADA、AMI 而有資料存取即時性與資訊分析可用性的同時，SG 也面臨了許多不同於傳統封閉式電力系統的資安威脅。

來自開放性網路的威脅具有能夠癱瘓整個系統的潛力[10]，2015 年烏克蘭電網遭到惡意軟體破壞，導致大範圍停電[37]；2016 年以色列電力局遭受網路攻擊，被迫將電力設施中被感染的電腦進行關閉。由此可知，針對智慧電網的資安威脅具有造成巨大損失的潛力，也因此，建立智慧電網應用的資安威脅模型，將有助於識別系統中需要被保護的軟硬體資產[30]，也能在資訊系統設計階段確認關鍵的潛在威脅，有機會針對可能遭受的攻擊手段，事先制定相對應的安全防範措施，以確保智慧電網的資訊安全。

因此，本研究引用軟體工程的成熟技術與資安威脅的風險評估機制，提出一套具備預防概念的資安威脅塑模方法 TMER，TMER 的設計以確認標的系統的功能架構為始，再於確認關鍵功能元件之後，針對擬分析的系統應用，透過使用案例圖、資料流程圖、威脅分類對應表與風險評估分析，逐步計算風險機率、篩選關鍵威脅項目，以完成威脅模型的建立。而為展示 TMER 的操作，本文以一項智慧電網的資訊系統應用為例。

貳、文獻探討

2.1 威脅模型（Threat Model）

Olivoa *et al.* [22]認為威脅模型的內涵是攻擊策略組合的最小特徵集，威脅模型應該將所能測定的威脅作風險形式化，以「風險發生的可能性」與「風險發生而致的後果」作表示。而根據 Cardenas *et al.* [5]的觀點，威脅模型應描述威脅的潛在破壞力，並根據

預期的後果設定相對應的安全需求。對於威脅模型的描述，至今仍少有公認的標準，Opdahl and Sindre[23]針對兩種描述威脅的方法：惡意濫用案例圖(misuse case)以及攻擊樹(attack tree)作比較，從其研究分析之結果推斷攻擊樹模型較能描述更多、更完整的威脅項目。最早由 Schneier[41]提出的攻擊樹技術，是以樹狀結構描述攻擊項目與潛在受攻擊目標之間的關係[7]，以表示攻擊發生的各種途徑[1]。

然而，諸如攻擊樹之類的威脅模型，其內容之產生多仰賴參與建模之研究人員或領域專家對標的系統以及資安威脅種類之專業知識，以內容推論、假設、歸納…等方式演繹而來，少有系統化、甚至模組化的建模方法。Wuyts *et al.* [32]提出一種名為 LINDDUN 的隱私威脅塑模方法，在其建模的六大步驟[40]中，即善用了傳統軟體工程的資料流程圖 (data flow diagram, DFD)，以及其自訂之 LINDDUN 威脅類別表(Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance)，並將威脅項目繪製成威脅樹(threat tree)，再以風險矩陣對風險項目的影響性(impact)與可能性(likelihood)衡量，決定威脅關注的優先順序，以及後續的應對策略擬定。

LINDDUN 隱私威脅塑模方法是以 LINDDUN 威脅分類表為運作核心而命名，另一種知名的 STRIDE 資安威脅塑模方法[35][26]也是以一種 STRIDE 資安威脅分類表為基礎，以 9 個步驟完成資安威脅模型的方法。STRIDE 所代表的資安威脅包括：欺騙(Spoofing)、竄改(Tampering)、否認(Repudiation)、資訊洩漏(Information disclosure)、阻斷服務(Denial of service)與權限提升(Elevation of privilege)[14][17][29][21]，而依循安全開發生命週期(Secure Development Lifecycle, SDL)[11]所設計而成的過程步驟也是以 DFD 為工具、以威脅樹呈現威脅項目[40]。但是，LINDDUN 或 STRIDE 威脅塑模方法在面對大型且複雜的資訊系統(如：智慧電網)時，如何從種類繁多的功能元件推導出 DFD？如何針對威脅種類作更為客觀的風險評估？是值得進一步分析與討論的重要議題。

2.2 智慧電網(Smart Grid, SG)

從應用功能面來說，智慧電網是一種能夠智慧化地收集從發電、輸電、配電至消費者端的所有電力資訊的電力系統，提供消費者電力相關(如：電力交易…等)資訊服務以及交易運作平台[33][8][6]，Rahman[24]認為智慧電網能提供創新、高效能以及高可靠性的能源管理服務。從技術架構面來說，Güngör *et al.* [9]指出智慧電網結合自動控制與通訊技術的長處，是兼具高效率、可靠性及電力運作安全性的現代化電力網路基礎建設，尤其是能整合可再生能源打造永續能源系統。Mohassel *et al.* [19]認為智慧電網是將傳統電力系統透過資通訊技術作加值，達到從電力生產到消費者用電的資料管理之最佳化。

綜上描述可知，智慧電網以傳統電力系統(electric power system)為基礎。傳統電力系統架構依其功能可分為電力生產、傳輸及配送三個部分[38]，以最基本的組成機件來說，生產部分包括發電廠及可再生能源，配電部分主要為變電所及變壓器，傳輸部分則是分

佈綿密的電力線網路[20]。而如前段所述，智慧電網的功能在於實現創新、高效能以及高可靠性的能源管理，因此，針對各式設備的有效監控與狀況評估，就需要仰賴 SCADA 的運作[3]。

SCADA 以監督控制與資料蒐集為其名，常用於民生基礎建設及工業系統，如：水力系統、發電系統…等，是以資訊科技作為核心運作架構的工業化控制系統[42]。當 SCADA 被納入智慧電網成為其重要組件時，就負有監控[2]和管理發電、輸電及配電資訊的功能[12]。根據 Keith *et al.* [13]的定義，SCADA 可區分成控制中心(control center)、廣域網路(wide area network)及現場設備(field site)。控制中心主要由人機介面(human machine interface, HMI)、工程工作站(engineering workstation)、控制伺服器(control server)、歷史資料庫(data historian)及路由通訊設備(communication router)所構成，具有監督設備狀態、控管執行程序以及擷取裝置資訊的功能；而接受監控的設備主要有：遠程終端設備(remote terminal unit, RTU)、可編成邏輯控制器(programmable logic controller, PLC)[43]與智慧型電子裝置(Intelligent electronic device, IED)[42]。廣域網路如其字面意義，負責 SCADA 中跨區網的資料通訊。而現場設備的主要任務就是將現場資料經收集、彙整後回傳至控制中心。

除了傳統電力系統的產、送、配電，以及奠基於 SCADA 的設備自動化監控運作，智慧電網的特點包括提供與終端使用者端直接相關的資訊應用與管理，那麼，AMI 就是關鍵角色。根據 Electric Power Research Institute [39]對 AMI 的介紹，裝設有 AMI 的電力終端用戶可以有效率地收集以時間為導向的電力相關資料，並存入電表資料管理系統（Meter Data Management System, MDMS），作為後續資料分析與管理之用。AMI 的運作除了能讓電力終端使用者透過網路向 MDMS 查詢用電情形[24]外，也能執行使用者端(需求端)的需求管理，有助於智慧化地掌握用電峰值、調整輸配電規劃以避免異常的負載壓力[25]。AMI 是實施更先進的能源管理服務(如：時間電價、電力負載平衡…等)所需的關鍵角色[18]，也是併入來自散戶端的可再生能源，以提高智慧電網的電力來源可靠度的必要系統[34]。

2.3 智慧電網的資安威脅模型

智慧電網的運作涵蓋對傳統電力系統、SCADA 的設備監控以及 AMI 的能源管理應用，在近來對智慧電網設計與產業推動的趨勢發展下，智慧電網所涉及的資安威脅是一項重要研究議題。Li *et al.* [16]列出智慧電網可能遭遇的四大資安攻擊類型，包括：對裝置的攻擊(device attack)、對資料的攻擊(data attack)、對使用者隱私的攻擊(privacy attack)、對通訊網路的可用性攻擊(network availability attack)。此外，Skopik and Ma[27]將智慧電網資安威脅模型劃分為三層式的攻擊發生區域，是以區段式的威脅模型探討智慧電網資安架構的重要參考。第一層屬區網內部攻擊，共有 7 種可能的攻擊；第二層屬骨幹網路攻擊，包括 6 種可能的攻擊；第三層涵蓋 6 種可能來自骨幹網路之外的資安攻擊。除了

以上所列對 SG 資安威脅分析的較早期研究，另有作綜整性的研究檢索與挑戰論述的文章[31]，但多著墨在一般觀點下之網路與資安攻擊的探討。

直到近年來，針對 SG 特性的資安威脅研究逐漸增加，Suleiman *et al.* [28]在同時考慮 SCADA 與 AMI 的前提下，提出一個以 SG 為標的的資安威脅模型 SG Systems Security Threat Model (SSTM)，此 SSTM 列舉了 76 種資安威脅，不過，如何建構如此大架構的威脅模型以及是否需確認此些資安威脅的被關注優先順序？是值得進一步探討的問題。Langer *et al.* [15]同樣在考慮 SCADA 與 AMI 的 SG 架構下探討 SG 的資訊安全，尤其是以一套兼顧風險評估(risk assessment)在概念面(conceptual level)與實施面(implementation level)的流程模型(process model)，試圖以系統化觀點建立 SG 資安模型；然而，此篇研究只點到 SG 的資安功能需求，尚缺乏對資安威脅的進一步評估。

2.4 發現與探討

從以上文獻內容，本文歸納幾點值得探討的項目：

1. 資安威脅模型的建構，如採以系統化的流程步驟(如：[15][26][32])，將有助於威脅模型建構過程的內容信效度與操作穩定性。
2. DFD 是普遍用來描述系統資料及其相互關係的設計工具，然而，DFD 的演成應可慮其它先導工具，尤其是針對大型資訊系統作分析時，可能涉入的系統外部實體數量可能龐雜，如果沒有先作確認與篩選，則後續展開的資安威脅項目將過於發散而不易聚焦。
3. 常用的資安威脅類別表，無論是 LINDDUN 或 STRIDE，都是對應 DFD 元件以列舉資安威脅類型的有利工具，但是，兩張類別表的威脅種類涵蓋範圍或有差異或有雷同，是否有機會整併使用？
4. 儘管 DFD 元件得以對應出資安威脅類型，但是，仍無法確定更精細的資安威脅項目。威脅項目的展開，除了引入專家意見(多以德菲法)進行討論確認外，可以考慮建立風險分解結構(risk breakdown structure, RBS)作為討論與對應威脅項目的客觀依據[4]。
5. 在標的系統的功能元件眾多且應用程式數量龐大的情形下，所演成的資安威脅項目必然也是為數可觀。而相對地，倘若可用於資安威脅處理的資源，在實務上不可能同步倍增的話，那麼，如何評估與篩選關鍵資安項目以為後續處置的標的，是實際上必須關注的議題，而在評估資安威脅項目的過程中，如何兼顧專業知識的引入及避免專家意見的偏誤，是一項重要議題。

參、TMER 資安威脅塑模方法

根據 2.4 節所列的探討項目，本研究提出一套引用軟體工程(Engineering)的成熟技術與資安威脅的風險(Risk)評估機制的資安威脅塑模(Threat Modeling)方法，按重要詞彙字母簡稱 TMER。TMER 採用產出流程圖(product flow diagram, PFD)作為展開系統功能元件的工具，採用使用案例圖(use case diagram, UCD)確認標的應用的功能關係，作為繪製 DFD 的先導產出；而在資安威脅類別對應部份，本文參考 STRIDE 與 LINDDUN 的內容意義，提出一個新的 STRIDE+p 威脅類別對應表；至於威脅項目的展開與關鍵項目的篩選，則是分別以風險分解結構(RBS)概念與德菲法引入專家意見來進行；最後再以資安威脅樹建構資安威脅模型。TMER 的流程步驟(如圖一)與重要的操作方法說明如后小節。

3.1 TMER 的流程步驟

步驟 1. 建立系統之產出流程圖(PFD)：針對標的系統元件進行文獻檢索，以 PFD 確認元件的產出前後相對位置，必要時，表列各元件名稱及註記其相關定義。

步驟 2. 建立功能應用之使用案例圖(UCD)：選定欲進行資安威脅分析之功能應用，並依應用所需從 PFD 中選取應用相關之系統元件，再將涵蓋功能元件或操作觸發者(如：系統管理人員或終端使用者)的應用功能，以主動賓語序(主詞+動詞+受詞，S+V+O)原則，清楚描述標的系統於所選定功能應用之功能需求，並據以描繪 UCD。

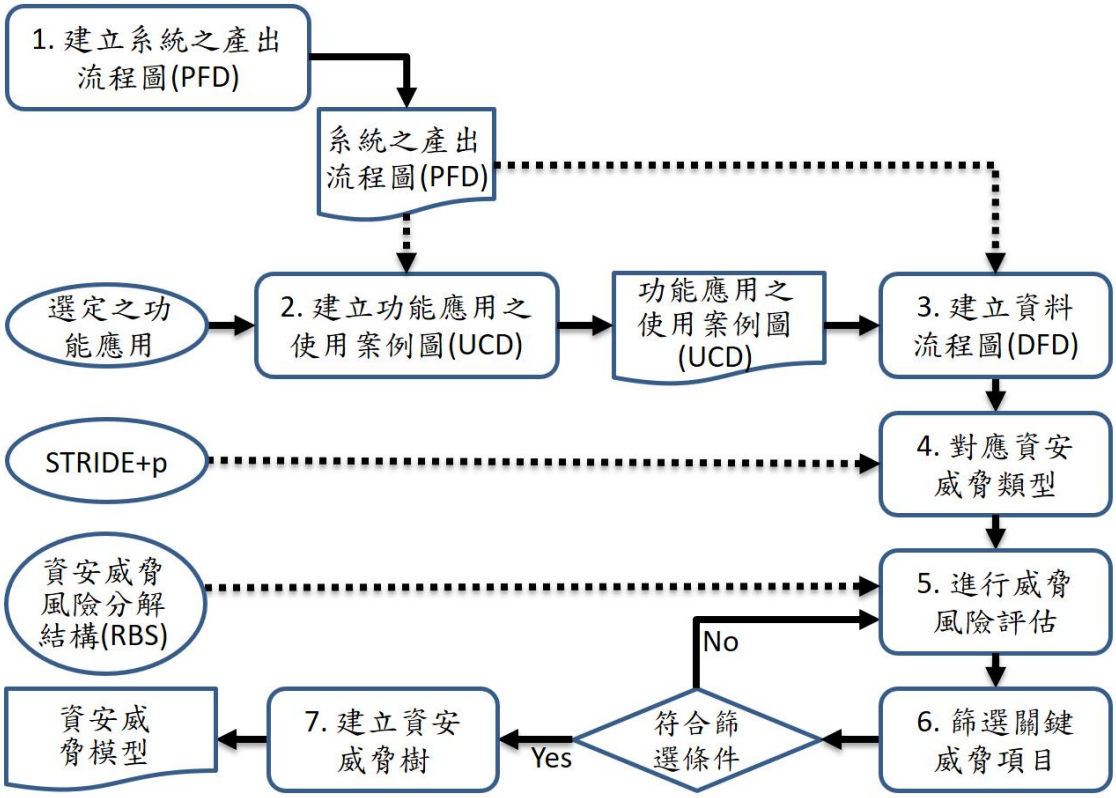
步驟 3. 建立資料流程圖(DFD)：針對 UCD 中的各個功能，以情節描述方式作操作流程展開(含例外路徑)與介面藍圖設計，再依細部操作流程與資料詞彙，以向上整併與向下功能展開方式，建立各階 DFD。

步驟 4. 對應資安威脅類型：運用本研究提出之 STRIDE+p 威脅類型對應表(如后 3.2 節之說明)，針對 DFD 中之各類型元件(外部實體、資料流、資料儲存、處理)對應其資安威脅類型。

步驟 5. 進行威脅風險評估：以 RBS 內容為參考，依序對各 DFD 元件對應出的威脅種類作威脅項目探討，並就各項目評估其「風險發生的可能性(likelihood)」與「風險發生而致的後果(impact)」。

步驟 6. 篩選關鍵威脅項目：在考慮可投入威脅應對之資源狀況的前提下，以德菲法引領專家意見進行關鍵威脅項目之篩選(如后 3.3 節之說明)，過程以秘密評分、開放討論、公開確認結果作反覆式(iteratively)操作，直到滿足事先設定的停止條件為止。

步驟 7. 建立資安威脅樹：依關鍵威脅項目，繪製資安威脅樹，完成資安威脅模型之建立。



圖一：TMER 資安威脅塑模流程示意圖

3.2 STRIDE+p 威脅類型對應表與風險分解結構

使用資安威脅類別表的目的是要自 DFD 找到威脅類型，是塑模過程中相當重要的一步。STRIDE 是已知的類別表中，最常被提及與使用的，它的對應範圍可適用於一般類型的資安威脅。此外，同樣是供 DFD 對應用的 LINDDUN 威脅類別表則是著重在隱私權的對應範圍，雖不似 STRIDE 的普遍性，但仍有其參考價值。只是，這兩張類別表的威脅種類涵蓋範圍或有差異或有雷同，因此，本研究試圖將其整併後提出一個 STRIDE+p 威脅類型對應表(如表一內容)。

STRIDE+p 的生成原則是以 STRIDE 為基礎，再將具有隱私(privacy)威脅意義的 LINDDUN 內容加入 STRIDE 中，故取 STRIDE+p 為名。就 LINDDUN 的內涵來說，「違反 Linkability 或 Identifiability」都與 Spoofing 相關，但應該不會發生在資料流上；「違反 Non-repudiation」與 Repudiation 同義，作聯集合併；「違反 Detectability」與 Denial of service 相關；「違反 Disclosure of information」與 Information disclosure 同義；「違反 Content Unawareness」指使用者未察覺，未察覺的結果可能是上述資安問題的發生，故略之；「違反 Policy and consent non-compliance」與 Elevation of privilege 有關，但應該不會發生在資料流上。所以，作兩相內容的部份整併調整後得 STRIDE+p。

然而，即使採用了 STRIDE+p，也只能對應出 DFD 元件的一致性資安威脅種類，而

實際可能發生的威脅項目，還是會依應用情境與威脅類別而異。因此，本研究在對應完資安威脅類型的步驟後，加入 RBS 的概念[4]來輔助提醒應關注的威脅項目。所謂的輔助提醒是指在進行確認威脅項目的過程中，多會引入專家意見進行項目分析與內容討論，RBS 的價值在於善用可類比的過去經驗與紀錄，提高該項步驟的執行效率以及增加內容討論的客觀基礎。

表一：STRIDE、LINDDUN、STRIDE+p 威脅類型之對應比較表

威脅分類 / DFD 元件	STRIDE						LINDDUN							STRIDE+p					
	S	T	R	I	D	E	L	I	N	D	D	U	N	S	T	R	I	D	E
Process	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x
Data flow		x		x	x		x	x	x	x	x		x		x	x	x	x	
Data store		x	x	x	x		x	x	x	x	x		x	x	x	x	x	x	x
External entity	x		x				x	x				x		x		x			

3.3 風險評估機制

風險評估以影響性(impact)與可能性(likelihood 或 probability)為評估因素，影響性是指一旦標的風險發生，其對標的主題所造成的衝擊程度。本研究建議以加權平均法計算影響性的得分，計算方式如公式 1，在總共有 m 個待評項目、n 個專家的情況下，I_i 代表第 i 個項目的影響性得分，IS_{ij} 代表第 j 個專家對第 i 個項目的影響性給分，IE_{ij} 代表第 j 個專家對第 i 個項目的影響性給分之專業程度自評分數，分數皆以 0~10 為值域。

$$I_i = \frac{\sum_{j=1}^{n} IS_{ij} \times IE_{ij}}{\sum_{j=1}^{n} IE_{ij}} \quad , i = 1,2,\dots,m; j = 1,2,\dots,n \quad \text{(公式1)}$$

風險同時具有影響性與可能性，故除了影響性的評分外，也要給予每個風險項目在可能性的評分。P_i 代表第 i 個項目的可能性得分，以公式 2 計算之，PS_{ij} 代表第 j 個專家對第 i 個項目的可能性給分，PE_{ij} 代表第 j 個專家對第 i 個項目的可能性給分之專業程度自評分數，分數皆以 0~10 為值域。

$$P_i = \frac{\sum_{j=1}^{n} PS_{ij} \times PE_{ij}}{\sum_{j=1}^{n} PE_{ij}} \quad , i = 1,2,\dots,m; j = 1,2,\dots,n \quad \text{(公式2)}$$

3.4 篩選關鍵風險

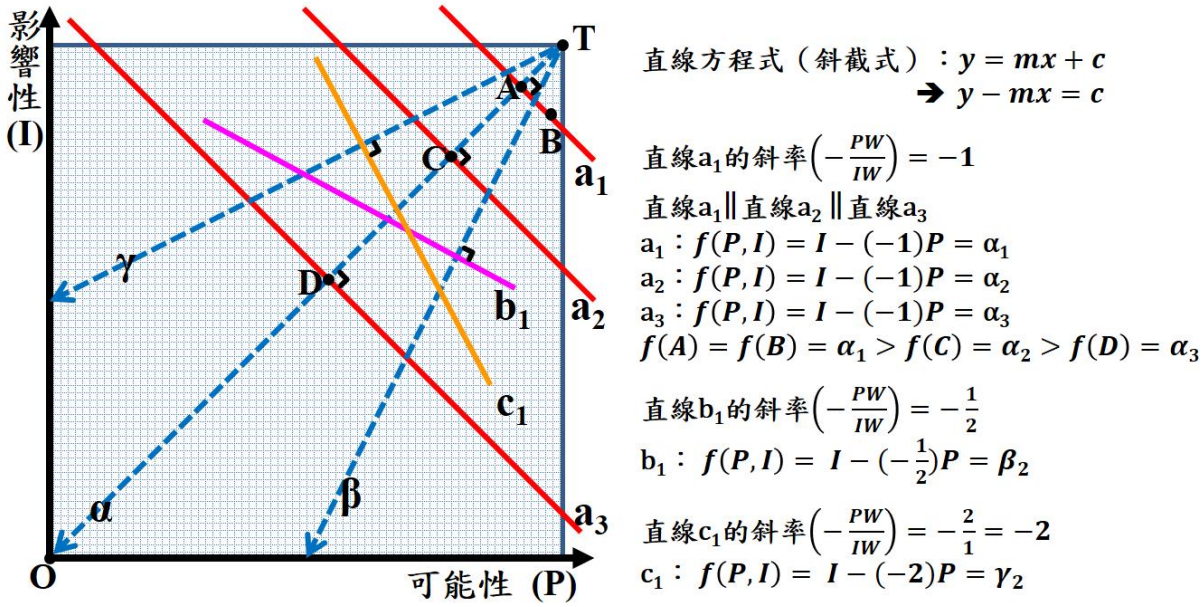
關鍵風險的篩選建議以常見的德菲法進行，德菲法篩選的停止條件是：「篩選所依恃的分數≥門檻值」且「滿足預先設定之項目數」。設定篩選風險項目所依恃的分數，必須同時考慮影響性得分與可能性得分，再如果影響性與可能性的重要程度並不相等時，就必須納入影響性與可能性的權重關係；也就是說，當以 IW 代表影響性的權重，PW 代

表可能性的權重，進行德菲法篩選關鍵風險項目時必須同時考慮 I_i、P_i、IW 與 PW 四項數字，而不是單一項目的數值。關鍵風險(S^R)的篩選以風險綜合得分(R_i)作為篩選所依恃的分數，R_i 是各風險項目的影響性得分乘上影響性權重與可能性得分乘上可能性權重的總和，如公式 3 之二元一次多項式。

$$R_i = (PW \times P_i + IW \times I_i) \ , i = 1,2, \dots, \mathrm{m} \quad \text{(公式3)}$$

在分數值域相同(座標值等量)的前題下，每一個風險項目(同時具備影響性得分與可能性得分)可以被視為相對應在平面座標(如圖二直角座標系統)上的點，在關鍵風險的選擇以高影響性與高可能性為優先的原則下，圖二中的點 T 是具有最高影響性與最高可能性的第一優先項，原點 O 是最低影響性與最低可能性的最末項。從平面邏輯意義上來看，自點 T 出發沿著 α 方向往點 O 前進，代表選項的優先順序從最高位往最低位方向遞減，即經過的點 A、點 C 和點 D，依序是選擇優先順位上的較高至較低。從數值內容上來看，平面座標系統上的任兩點可以決定一條直線，直線 TO 穿過點 T、點 A 與點 O，是一條$\mathrm{PW} = -\mathrm{IW}(|PW| : |IW| = 1 : 1)$所構成的直線，其斜率為$-\left(\frac{PW}{IW}\right) = 1$；而與點 A 具有相同二元一次多項式值 R_i 的點 B，可以與點 A 共同決定出一條 R_i 值皆相同的直線 a_1，a_1 也是一條$|PW| : |IW| = 1 : 1(\mathrm{PW} = \mathrm{IW})$的直線，但 a_1 與直線 TO 垂直，其斜率為$-\left(\frac{PW}{IW}\right) = -1$，以斜截式來表示 a_1 的二元一次方程式為$f(P,I) = I - (-1)P = \alpha_1$。同理，點 C 落在直線 a_2 上，點 D 落在直線 a_3 上，a_1、a_2 與 a_3 相互平行，a_2 的二元一次方程式為$f(P,I) = I - (-1)P = \alpha_2$，$a_3$ 的二元一次方程式為$f(P,I) = I - (-1)P = \alpha_3$，$f(A) = f(B) = \alpha_1 > f(C) = \alpha_2 > f(D) = \alpha_3$。若 PW、IW 的權重關係改變，直線的斜率就會跟著變動，直線方程式也就隨之不同。當圖二中的點 T 沿著 β 方向往 P 軸的中點延伸出一條$|PW| : |IW| = 2 : 1(\mathrm{PW} = -2 * \mathrm{IW})$的直線，其斜率為$-\left(\frac{PW}{IW}\right) = 2$，與之垂直的 b1 是$|PW| : |IW| = 1 : 2(2 * \mathrm{PW} = \mathrm{IW})$的直線，其斜率$-\left(\frac{PW}{IW}\right) = -\frac{1}{2}$，二元一次方程式為$f(P,I) = I - (-\frac{1}{2})P$；同理，當圖二中的點 T 沿著 γ 方向往 I 軸的中點延伸出一條代表$|PW| : |IW| = 1 : 2(-2 * \mathrm{PW} = \mathrm{IW})$的直線，其斜率為$-\left(\frac{PW}{IW}\right) = \frac{1}{2}$，與之垂直的 c1 是$|PW| : |IW| = 2 : 1(\mathrm{PW} = 2 * \mathrm{IW})$的直線，其斜率$-\left(\frac{PW}{IW}\right) = -2$，二元一次方程式為$f(P,I) = I - (-2)P$。因此，設定關鍵變因($S^R$)的篩選以$f(P_i, I_i)$作為篩選所依恃的分數，門檻值為$\mathcal{L}^R$，如公式 4 之二元一次不等式。

$$S^R = \left\{ i \middle| f(P_i, I_i) = I_i - (-\frac{PW}{IW})P_i \geq \mathcal{L}^R, i = 1,2,\dots,\mathrm{m} \right\} \text{.....(公式4)}$$



圖二：以二元一次直線方程式觀念作關鍵風險篩選之示意說明圖

肆、案例演練

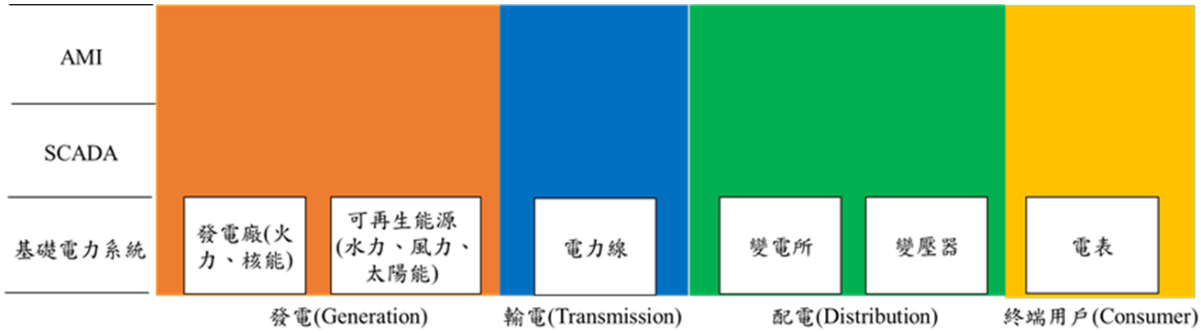
本節以智慧電網為例，簡要展示 TMER 在各步驟的執行過程與產出。

4.1 建立系統之產出流程圖(PFD)

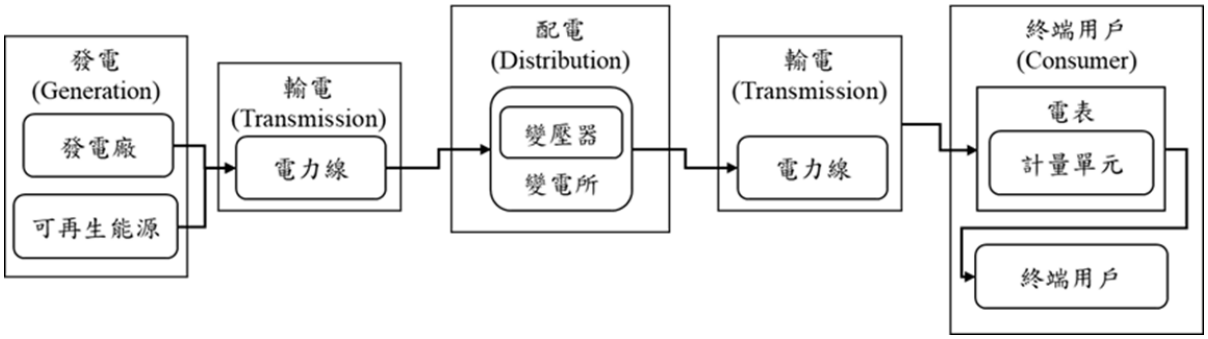
此階段步驟針對傳統(基礎)電力系統進行功能元件檢索，發電廠以及可再生能源負責生產電力，電力線負責電力的傳輸，電力在供給用戶使用前必須先送至變電所，由變電所內的變壓器進行電壓的轉換。同時，針對傳統電力系統的元件功能進行運作分區，分為生產電力的發電(generation)、傳輸電力的輸電(transmission)、調整電壓及配送電力的配電(distribution)及使用電力的終端用戶(consumer)，如圖三所示。再據以繪製傳統電力系統的產出流程圖 PFD，如圖四所示。

依此方式，再逐步加入 SCADA 與 AMI 的功能元件分區與 PFD。SCADA 主要透過控制中心、通訊網路以及現場設備進行監控和收集發電、輸電、配電相關資訊，RTU、PLC 與 IED 歸屬於配電分區，其它如：儲存資料庫、控制伺服器、通訊路由器、工程工作站、人機介面…等則屬控制中心的功能元件。AMI 的主要功能分為資料收集、網路通訊及資料分析管理；負責透過聯網功能作現場資料收集的智慧電表，可將用電資訊傳送至後端 MDMS 系統，MDMS 是控制中心內負責電力相關資料記錄，以及掌控電力資料

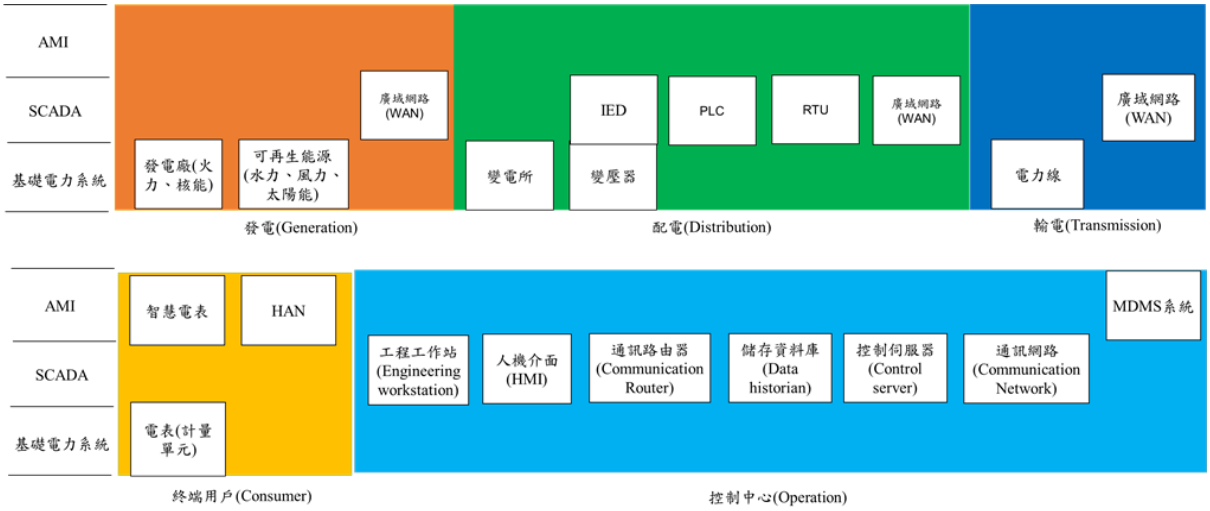
分析、管理與應用的核心元件。整合基礎電力系統、SCADA、AMI 而成的智慧電網元件分區以及 PFD，分別如圖五、圖六所示。



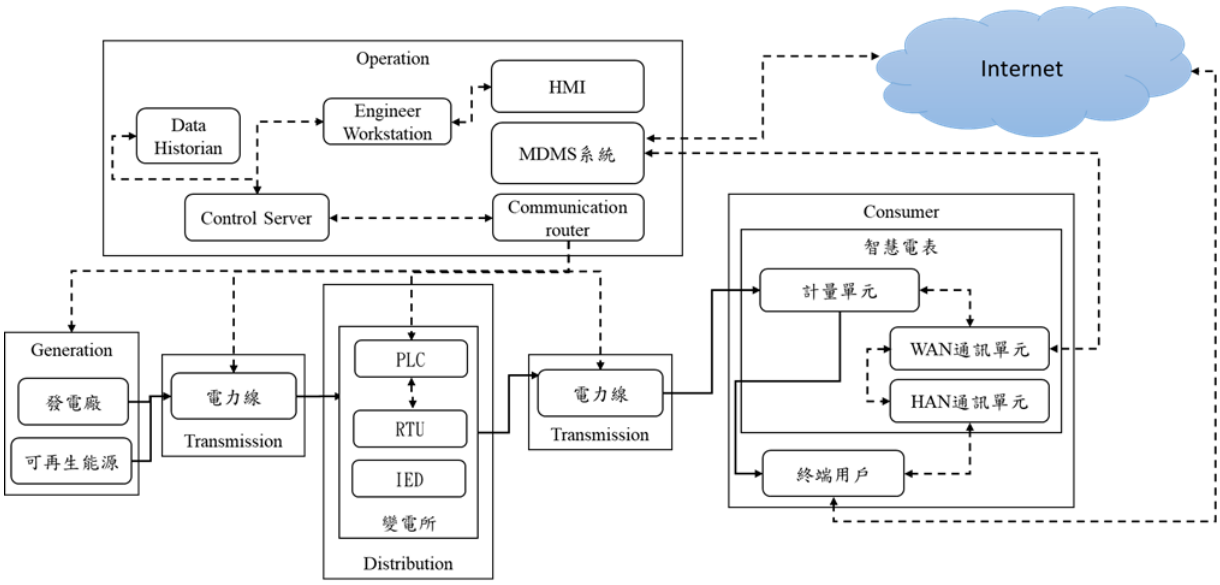
圖三：基礎電力系統元件分區示意圖



圖四：基礎電力系統之產出流程圖



圖五：智慧電網元件分區示意圖



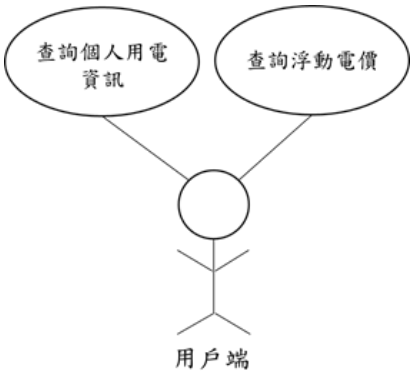
圖六：智慧電網之產出流程圖

4.2 建立功能應用之使用案例圖(UCD)

如 Abdrabou[2]的見解，智慧電網須具有主動監測及控制(主動管理)裝置的動態特性，諸如：控制中心需對多點通信通道的 RTU 進行輪詢，使 RTU 回報斷路器數字狀態；在已搭配資料紀錄以及可遠端控制裝置的功能前提下，智慧電網可執行負載平衡/峰值平衡的功能，在用電高峰時，藉由調整或關閉設備以降低功耗，防止電力系統過載。本演練案例以終端用戶應用為選定之功能應用範圍，再將應用範圍內之需求功能以主動賓語序整理如表二內容，並繪製 UCD(如圖七所示)。

表二：案例應用範圍內之需求功能主動賓語序表

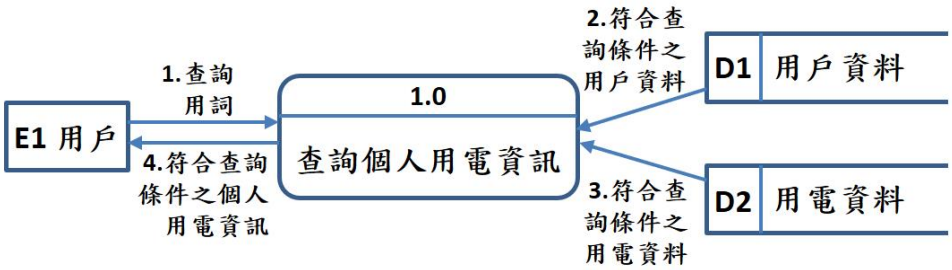
區域	選定之功能應用	主動賓語序(S+V+O)
終端用戶	上傳用電資訊	智慧電表定時傳送用電資訊
	查詢浮動(時間)電價	用戶查詢浮動(時間)電價
	查詢個人用電資訊	用戶查詢個人用電資訊



圖七：應用案例之使用案例圖

4.3 建立資料流程圖(DFD)

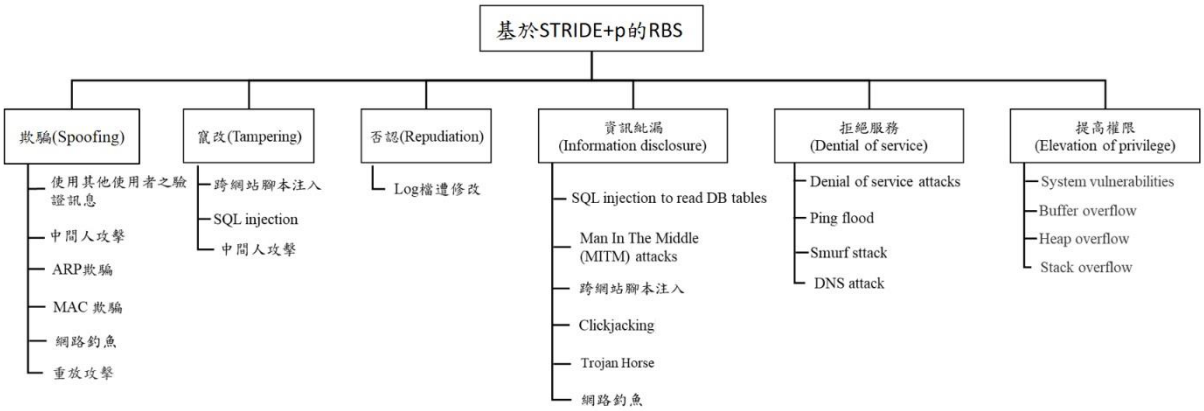
針對 UCD 中的各個功能，以情節描述方式作操作流程展開(含例外路徑)與介面藍圖設計，再依細部操作流程與資料詞彙，以向上整併與向下功能展開方式，建立各階 DFD，本節以圖八之「查詢個人用電資訊」DFD 為展示。



圖八：應用案例之資料流程圖

4.4 對應資安威脅類型與進行威脅風險評估

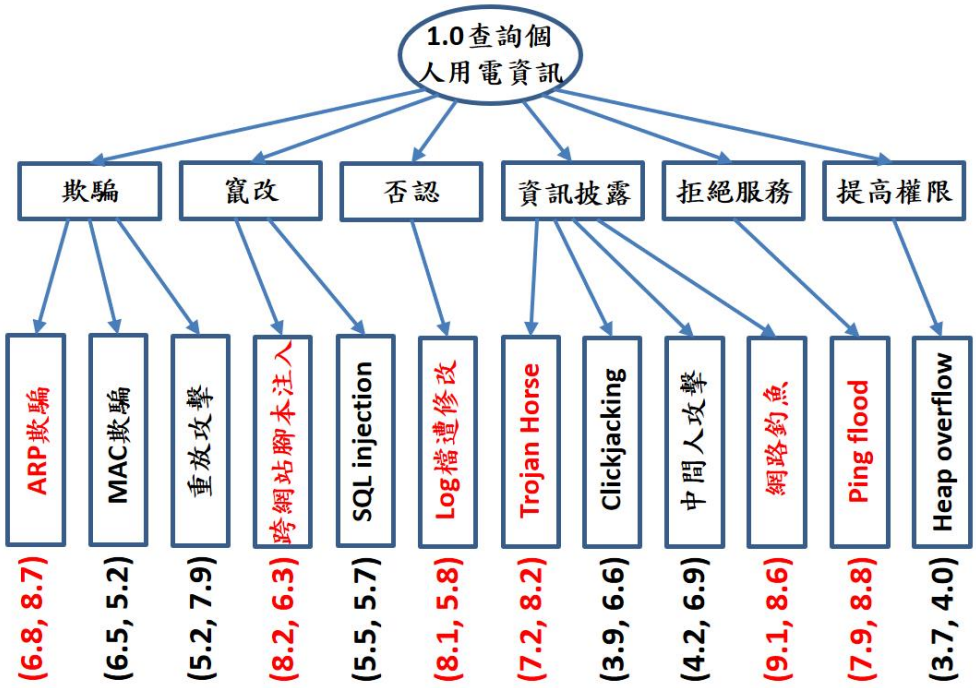
先運用本研究提出之 STRIDE+p 威脅類型對應表，將應用案例 DFD 中之各類型元件所對應的資安威脅類型確定出來。再參照本研究建議之基於 STRIDE+p 的風險分解結構識別風險項目。因本案例為試作例，故略以參與研究之人員代為資安領域專家，以內部進行之德菲法進行威脅風險評估，將各風險項目之「風險發生的可能性(probability)」與「風險發生而致的後果(impact)」得分計算出來。



圖九：本研究建議之基於 STRIDE+p 的風險分解結構示意圖

4.5 篩選關鍵威脅項目與建立資安威脅樹

在試作篩選關鍵威脅項目部份，取$|PW|:|IW|=1:1$(PW = IW)為權重關係，以取5~9 個威脅項目為德菲法反覆操作的停止條件。最後篩選而定的資安威脅樹如圖十所示，樹節點下方之數對為(I_i, P_i)，是篩選時計算 R_i 的依據，所篩選出的關鍵資安威脅項目共有 6 項，分別是 ARP 欺騙(6.8, 8.7)、跨網站腳本注入(8.2, 6.3)、Log 檔遭修改(8.1, 5.8)、Trojan Horse(7.2, 8.2)、網路釣魚(9.1, 8.6)、Ping flood(7.9, 8.8)。



圖十：應用案例之資安威脅樹

肆、結論

解決問題就像治病，都需要正確的藥方與有效的藥材。本研究提出的 TMER 資安威脅塑模方法，結合軟體工程方法與風險評估機制，使得資訊系統在設計階段，就得以系統化、模組化地辨認資訊安全威脅，為確保應用程式的設計可靠性與日後系統運作的理論可用性開立可信賴的藥方。

隨著資通訊設備小型化、資訊應用高度網路化，以及資料處理智慧化的趨勢發展，以物物相聯為導向的資通訊系統種類愈來愈多，智慧電網即是一例。因此，以資安威脅模型的建立，來分析資通訊系統運作時可能遭遇的重大威脅，在系統功能的設計過程，即針對關鍵型資安威脅提早引入必要且合適的因應功能，將能在兼顧運算效能與防護效果的雙重考量下強化系統的整體資安能力，是強化系統的先天防禦能力，達到預防勝於治療的理想作法。

結合既有設備與資通訊技術，強調智慧化發展的物聯網應用，是全球重視的關鍵議題與推動要項之一，而我國產官學研各界也多重視物聯網創新應用所需要的基礎研究與人才培養，尤其是憑藉台灣過去以來所累積的資通訊技術與應用能量，倘能盡早投入物聯網資安領域值得研究的議題，未來台灣在全球物聯網產業競爭中將能有卓越的貢獻。物聯網產業的推動，概以智慧化服務之達成為大方向，它需要得到普遍民眾的信任與使用，而致透過市場力量作成效的擴散，如此才能獲得最大的應用與經濟效益。一般來說，民眾不盡然知道物聯網的運作細節，它有什麼功能？能帶來什麼好處？對於物聯網何以能做到智慧化運作？又能如何同時保護提供安全的資訊存取？往往難有通盤的了解，民眾所能仰賴的，無非就是符合需求的應用以及合理的資訊安全保護。事實上，一套好的物聯網應用系統與資安支援管理平台能夠勾勒出可行、可被信賴的智慧化應用情境，並進一步型塑利基商業模式，更能夠在明確可見的應用示範宣導規劃下，提供足夠的誘因而使民眾願意接受相關服務與產品，促成物聯網產業的推動。而這一切的物聯網應用推廣，資安健全的重要性實不言而喻。

[誌謝]

本文所述之研究承『行政院科技部 106 年資訊安全實務應用專案計畫：物聯網的資安架構及其裝置管理機制之研究（MOST 106-2221-E-239-003）』之補助。

參考文獻

[1] H. Abdo, M. Kaouk, J. M. Flaus and F. Masse, “A safety/security risk analysis approach

of Industrial Control Systems: A cyber bowtie – combining new version of attack tree with bowtie analysis," *Computer & Security*, vol. 72, pp.175-195, 2018.

[2] A. Abdrabou, "A Wireless Communication Architecture for Smart Grid Distribution Networks," *IEEE Systems Journal*, vol. 10, issue 1, pp. 251-261, 2016.

[3] F. Ahmad, A. Rasool, E. Ozsoy, S. Rajasekar, A. Sabanovic and M. Elitas, "Distribution system state estimation-A step towards smart grid," *Renewable and Sustainable Energy Reviews*, vol. 81, no. 2, pp. 2659-2671, 2018.

[4] J. Cadle and D. Yeates, *Project Management for Information System, 5th ed.* Upper Saddle River, NJ: Pearson/Prentice Hall, 2008, pp.259-272.

[5] A. A. Cardenas, T. Roosta and S. Sastry, "Rethinking security properties, threat models, and the design space in sensor networks: A case study in SCADA systems," *Ad Hoc Network*, vol. 7, issue 8, pp. 1434-1447, 2009.

[6] V. Delgado-Gomes, J. F. Martins, C. Lima and P. N. Borza, "Smart Grid Security Issues," *The 9th International Conference on Compatibility and Power Electronics*, pp. 534-538, 2015.

[7] I. N. Fovino and M. Masera, "Through the description of attacks: A multidimensional view," *International Conference on Computer Safety, Reliability, and Security. Springer*, pp. 15-28, 2006.

[8] H. Gharavi and R. Ghafurian, "Smart Grid: The Electric Energy System of the Future," *IEEE Proceedings*, vol. 99, no. 6, pp. 917-921, 2011.

[9] V. C. Güngör, C. Buccella and G. P. Hancke, "Smart Grid Technologies: Communication Technologies and Standards," *IEEE Transactions on Industrial Informatics*, vol. 7, no. 4, pp. 529-539, 2011.

[10] M. Henrie, "Cyber Security Risk Management in the SCADA Critical Infrastructure Environment," *Engineering Management Journal*, vol. 25, no. 2, pp. 38-45, 2013.

[11] M. Howard and S. Lipner, *The Security Development Lifecycle*, Redmond, WA, USA: Microsoft Press, 2006.

[12] R. Jiang, R. Lu, C. Lai, J. Luo and X. Shen, "Robust group key management with revocation and collusion resistance for SCADA in smart grid," *2013 IEEE Global Communications Conference (GLOBECOM)*, 2013.

[13] S. Keith, P. Victoria, L. Suzanne, A. Marshall and H. Adam, "Guide to Industry Control Systems (ICS) Security," *NIST Special Publication 800-82 Revision 2*, 2015.

[14] R. Khan, K. McLaughlin, D. Laverty and S. Sezer, "STRIDE-based threat modeling for cyber-physical systems," *Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), 2017 IEEE PES*, 2017.

[15] L. Langer, F. Skopik, P. Smith and M. Kammerstetter, "From old to new: Assessing

cybersecurity risks for an evolving smart grid," *Computers & Security*, vol. 62, pp. 165-176, 2016.

[16] X. Li, I. Lille, X. Liang, R. Lu, X. Shen, X. Lin and H. Zhu, "Securing Smart Grid：Cyber Attacks, Countermeasures, and Challenges," *IEEE Communications Magazine*, vol. 50, issue 8, pp. 38-45, 2012.

[17] S. Madan, "Shielding against SQL injection stacks using admire model," *First International Conference of Computational Intelligence, Communication Systems and Networks*, pp. 314-320, 2009.

[18] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," *IEEE Security & Privacy*, vol. 7, issue 3, pp. 75-77, 2009.

[19] R. R. Mohassel, A. Fung, F. Mohammadi and K. Raahemifar, "A survey on Advanced Metering Infrastructure," *Electrical Power and Energy Systems*, vol. 63, pp. 473-484, 2014.

[20] N. S. Nafi, K. Ahmed, M. A. Gregory and M. Datta, "A survey of smart grid architectures, applications, benefits and standardization," *Journal of Network and Computer Applications*, vol.26, pp23-36, 2016.

[21] S. Noponen and K. Karppinen, "Information security of remote file transfers with mobile devices," *Computer Software and Applications 32nd Annual IEEE International*, vol. 1, pp. 973-978, 2008.

[22] C. K. Olivoa, A. O. Santina and L. S. Oliveira, "Obtaining the threat model for e-mail phishing," *Applied Soft Computing*, vol. 13, issue 12, pp. 4841-4848, 2013.

[23] A. L. Opdahl and G. Sindre, "Experimental comparison of attack trees and misuse cases for security threat identification," *Information and Software Technology*, vol. 51, issue 5, pp. 916-932, 2009.

[24] M. A. Rahman, "A Noninvasive Threat Analyzer for Advanced Metering Infrastructure in Smart Grid," *IEEE Transactions on Smart Grid*. vol. 4, no. 1, pp. 273-287, 2013.

[25] N. Shaukata, S. M. Alia, C. A. Mehmooda, B. Khana, M. Jawadb, U. Farida, Z. Ullaha, S. M. Anwarc and M. Majid, "A survey on consumers empowerment, communication technologies, and renewable generation penetration within Smart Grid," *Renewable and Sustainable Energy Reviews*, vol. 81, no. 1, pp. 1453-1475, 2018.

[26] A. Shostack, *Threat Modeling: Designing for Security*, Wiley, 2014.

[27] F. Skopik and Z. Ma, "Attack Vectors to Metering Data in Smart Grids under Security Constraints," *2012 IEEE 36th Annual Computer Software and Applications Conference Workshops*, pp. 134-139, 2012.

[28] H. Suleiman, I. Alqassem, A. Diabat, E. Arnautovic and D. Svetinovic, "Integrated smart grid systems security threat model," *Information Systems*, vol. 53, pp. 147-160, 2015.

[29] P. Torr, "Demystifying the threat modeling process," *IEEE Security & Privacy*, vol. 3, issue 5, pp. 66-70, 2005.
[30] R. M. Venkatesan and S. Bhattacharya, "Threat-adaptive security policy," *Performance, Computing, and Communications Conference*, 1997.
[31] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," *Computer Networks*, vol. 57, issue 5, pp. 1344-1371, 2013.
[32] K. Wyuts, R. Scandariato and W. Joosen, "Empirical evaluation of a privacy-focused threat modeling methodology," *The Journal of Systems and Software*, vol. 96, pp. 122-138, 2014.
[33] http://www.globalsmartgridfederation.org/smart-grids/ (2018/03/31).
[34] https://en.wikipedia.org/wiki/Smart_grid (2018/03/31).
[35] https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx (2018/03/31).
[36] https://smartgrid.ieee.org/about-ieee-smart-grid (2018/03/31).
[37] https://udn.com/news/story/11254/2520696 (2018/03/31).
[38] https://www.emersonprocessxperts.com/2015/01/ultra-high-voltage-transmission-uhv-a-new-way-to-move-power/ (2018/03/31).
[39] https://www.ferc.gov/CalendarFiles/20070423091846-EPRI%20-%20Advanced%20Metering.pdf (2018/03/31).
[40] https://www.linddun.org/linddun.php (2018/03/31).
[41] https://www.schneier.com/academic/archives/1999/12/attack_trees.html (2018/03/31).
[42] 徐翊城，"SCADA 系統安全調查"，*碩士論文*，國立中正大學通訊資訊數位學習碩士在職專班，2012。
[43] 陳雙源，*機電整合導論(下冊)*，東華書局，1999。