智慧電網家庭閘道器資安驗證標準之制定與應用
--資訊安全與實體安全整合評估

林佳瑩[1]　易俗[2]　范金鳳[1]
[1]元智大學資訊工程系　[2]健行科技大學資訊工程系
csfanc@saturn.yzu.edu.tw　swuyih@uch.edu.tw

摘要

智慧電網家庭閘道器不僅需考慮資訊安全（security）議題，亦需考慮到資訊安全漏洞可能引起之實體安全（safety）影響。後者在此類應用上尚未廣被重視。本研究針對此現象，制定以能處理資訊安全及實體安全兩方面需求的智慧電網家庭閘道器資安驗證標準。作法首先延伸德國 BSI 之智慧電網閘道保護剖繪，為其新增及修正了實體安全相關的章節及元件；接著根據此延申之保護剖繪制定了一套對照的驗證準則；最後以一商用之閘道器為個案，顯示我們所提之資安驗證標準之有效性。

關鍵詞：智慧電網、家庭閘道器、實體安全、資訊技術安全評估共同準則、保護剖繪。

Abstract

Smart grid home gateway needs to consider both the information security and the physical safety issues. However, the safety issue has not yet been widely emphasized. This research project developed an information security certification standard for smart grid home gateway, and the standard emphasizes both of the information security and physical safety requirements. First, we extended the newest Gateway Protection Profile (PP) of a Smart Metering System by German BSI [4] to include safety-related information and to develop safety-related CC components. Then we defined a corresponding certification standard for this proposed PP. Finally, a case study was conducted to demonstrate the effectiveness of the proposed certification standard.

Keywords: smart grid, home gateway, safety, common criteria, protection profile.

1. 緒論

智慧電網[1]將傳統的電力系統與現代資通訊技術結合，整合發電、輸電、配電、及用戶端裝設智慧電表，搭配電腦監控、診斷及修復等功能，可提升電力的使用效率。世界各國為因應節能減碳之趨勢，皆積極推動「智慧電網」之研究。

資訊安全（security）為智慧電網的核心議題；若連上電網的用戶端為工業控制系統、智慧家電控制系統等，智慧電網進一步涉及實體安全（safety）議題。傳統資安議題旨在防止攻擊者經由系統漏洞竄改資訊(例如少付電費)、或是竊取用戶之個人隱私資料；實體安全議題（safety）則需考量因資安漏洞導致電力系統遭入侵破壞，以至系統故障(例如不運作、引起不安全後果等)。

資訊技術安全共同評估準則(ISO/IEC 15408, Common Criteria，簡稱 CC）[2-4]，是現今資訊產品資安評估及驗證的通用國際標準。CC 原針對資訊系統（IT）所制定，並未考慮工業控制系統（Industrial Control System, ICS）可能延伸之實體安全問題。近年來先進的電腦病毒事件已影響重大基礎建設的安全:例如，2013 年南韓首爾媒體及銀行遭受 APT (Advanced Persistent Threat)攻擊[5]，損失嚴重。2010 年 6 月伊朗鈾濃縮工廠遭受 Stuxnet 病毒攻擊[6]，損失重大。

消費者可透過網路控制及監測智慧型家電；智慧家電通常具有溫度、濕度等控制系統；若具有獨立的 IP，亦可進行資訊收集、監測，可視為小型的 ICS。然而現今智慧電網家庭閘道器的安全需求(即保護剖繪 Protection Profile， PP[2])，多數尚未考慮實體安全（safety）。本研究針對上述議題，發展了一套智慧電網家庭閘道器保護剖繪標準及其檢測技術規範，能兼顧資訊安全及實體安全，本研究並提出處理 APT 的機制。最後，以一商用智慧電網閘道為例，評估此標準之適用性。本研究成果可提升智慧電網之資訊安全及實體安全等級。

2. 相關背景

2.1 智慧電網家庭閘道器（Smart Grid Gateway）

「閘道器」（Gateway）為連接兩種網路的一種通訊裝置；可連接兩個不同通訊協定的網段，處理通訊協定間的轉換包括：訊息格式轉換、位址轉換、協定轉換。目前國內已有多家廠商正進行智慧電網家庭閘道之開發，包括資策會開發之智慧型能源閘道器（Intelligent Energy Gateway）[7]，此為家庭能源管理控制器之系統核心，透過智慧家電應用層控制通訊協定（SAANET），可即時蒐集各家電設備及電表之資訊，並透過網際網路上傳至資料庫。

家庭網閘道器可連接並控制許多家電用品，因

此若有心人士利用惡意程式碼入侵或攻擊閘道，讓電暖爐或是烤麵包機等家電運轉不停，可能產生溫度過高引發火災等問題。因此，未來智慧電網閘道器在避免及偵測惡意攻擊上應扮演一重要角色，需具備防火牆、存取控制及監控等功能外，還需包含以下功能：收集、處理電表資料、保護區域網路中的裝置、提供其通訊、加密等功能。

2.2 資訊技術安全評估共同準則及保護剖繪

資訊技術安全評估共同準則(ISO/IEC 15408，即 Common Criteria，簡稱 CC）[2-4]，是現今各國為資通安全產品評估及驗證時所遵循的一個國際標準。此標準包含三個部分：第一部分：介紹和一般模型[2]、第二部分：安全功能需求[3]、第三部分：安全認證需求[4]。CC 定義了七個評估保證等級（EAL1-EAL7）用以判斷產品的安全等級。CC 將資訊科技產品之安全功能需求（Security Functional Requirement）分成十一大類，除此之外，尚還介紹保護剖繪（Protection Profile, PP）、安全標的（Security Target, ST）以及九大類安全保證需求（Security Assurance Requirement）。

十一大類型（class）之安全功能需求分別為: 安全稽核(FAU: Security Audit)、通訊(FCO: Communication)、密碼學支援(FCS: Cryptographic Support)、使用者資料保護(FDP: User Data Protection)、識別及認證(FIA: Identification and Authentication)、安全管理(FMT: Security Management)、隱私(FPR: Privacy)等。每一個類別(Class)皆可以再細分為幾個家族(Family)，每個家族又可以分為幾個元件(Component)，每一個元件也可以分為幾個元素(Element)。

保護剖繪（Protection Profile, PP）[2,8]是根據 CC 為資通產品類型所撰寫的基本安全需求文件，主要包含以下部分(見圖一)：

- PP 介紹
- TOE（Target of Evaluation）描述
- TOE 資訊安全環境
- 資訊安全目標（Security Objective）
- 資訊科技產品（IT）資訊安全需求
- 理由闡述

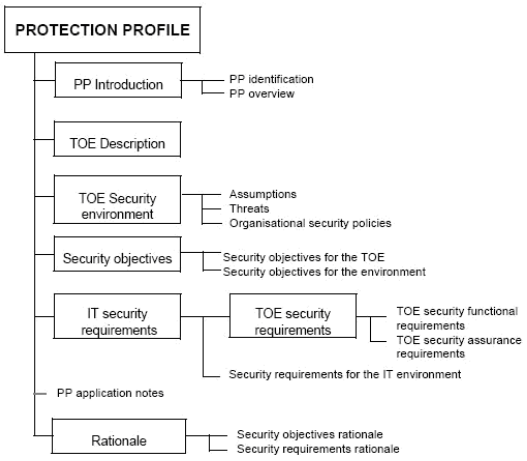

圖 1 保護剖繪內容

2.3 德國 BSI 智慧電網閘道保護剖繪

德國聯邦信息安全辦公室（BSI）於 2011 年根據 CC 製作了智慧電網閘道保護剖繪[9]。本研究已將其第六章之安全需求翻譯為中文，並延伸此 PP 作為智慧電網之家庭閘道器之資安驗證標準；延伸部份將在第三節章中介紹。

在 BSI 之 PP 中所用到的安全功能需求類別包含了安全稽查（FAU）、加密支援（FCS）、用戶資料保護（FDP）、身分識別及認證（FIA）、安全管理（FMT）、隱私（FPR）、保護評估標的安全功能（FPT）以及可信任之路徑／頻道（FTP）類別。以 FAU 為例，FAU 為安全稽查及產生稽查日誌類別，其下有數個元件，例如：FAU_ARP/SYS.1，為「系統日誌的安全警報」，指 TOE 的之安全功能應偵測潛在的違規行為並通知已授權之閘道管理員。

3. 家庭閘道器保護剖繪特殊需求分析

本研究進行步驟如下:

(1) 比較工業控制系統(ICS)與 IT 系統之差異性
(2) 翻譯並分析德 BSI 之 PP 主要技術章節
(3) 制定新的、符合控制系統之安全(safety)元件
(4) 綜合 BSI 原有的以及我們新制定的元件以撰寫更完整之智慧電網家庭閘道器保護剖繪
(5) 制定此保護剖繪之資通安全檢測技術規範
(6) 用一實際商用閘道器作為個案以評估所制定之保護剖繪績效

首先，資訊(IT)系統與工業/智慧家電控制系統(ICS)不同在於前者主要保護的是邏輯性（logical）資訊資產，而後者關注的則是實體（physical）資產，因此，攻擊此兩者的機制與損害亦不相同。例如，IT 系統遭攻擊可能不會立即發生作用，且可利用系統備份還原，因此較注重攻擊來源的分析、預防、偵測與回復。然而針對控制系統的攻擊(例如 APT 等)通常具有破壞性，若遭攻擊可能引起實體安全上之後果，如何控制損失規模則是 ICS 所要關注的[10]。

我們建議智慧電網家庭閘道器保護剖繪應如圖 2 所示，新增和延伸部分以紅字標註並加註編號。新增和延伸部分為 TOE Security and Safety environment (圖 2 編號 1)、Safety and security objective(編號 2) 及 IT security and safety requirements(編號 3)；原來資訊安全相關章節皆延伸為 資訊安全與實體安全(safety)，包含實體安全相關資訊、需求、及其下的子項目。

針對圖 2 編號 1, 我們建議在 PP 組織安全策略（OSP）內新增 OSP.System 策略，意旨 TOE 設

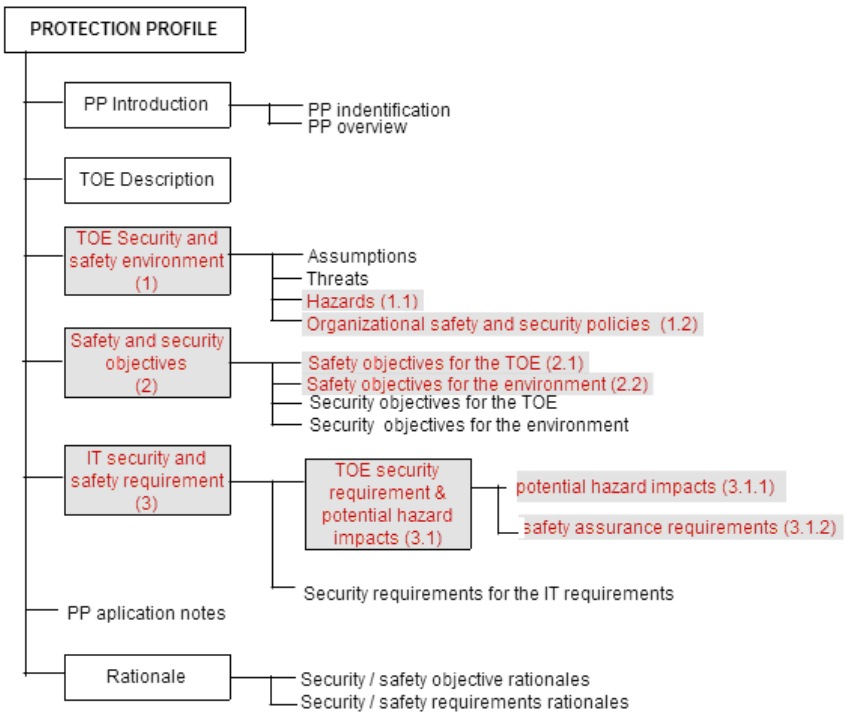

圖 2 建議之保護剖繪結構（修正及新增部分有加註編號）

計需要考慮安全因素；包含多套（N-version）設計，避免單一元件失誤造成全系統失效（single failure criteria）、深層/多層防禦等，以避免後續之實體安全影響（Hazard impact）(見表 1)。 另外，針對 APT、Stuxnet 等進階潛伏病毒，我們並建議修正原 BSI PP 中之 OSP.Log 內容為如下：TOE 應將正常使用的行為模式（patterns）和正常工作區間（envelope）儲存於另一同步監控處理器（co-processor）中(見表 2)。Co-processor 可動態對封包比對及偵測可能有的進階持續性滲透攻擊或 Stuxnet 等病毒。

針對圖 2 編號 2，我們建議 BSI PP 中 TOE 之資訊安全與實體安全目標中 O.Protectd 可移至編號 2.1 安全目標；而操作環境目標中之 OE.PhysicalProtection 移至編號 2.2，因其內容都考慮到實體安全（例如 fail-safe）及資訊安全失效後續影響。

針對圖 2 編號 3，我們制定了一新的安全功能需求類別 FSP，主要內容為避免系統失效。此新增的類別可進一步分為家族名為 FSP_SYP(system protection)，其下包含數個元件以對照上述組織安全策略 OSP.System（見表 3），包含不同設計之多套系統（N-diverse version）、置於不同地點、電源之多套系統及多層次的防禦機制等。

此外，針對編號 3，我們亦建議於原 BSI PP 之安全稽核 FAU 類別中新增一家族 FAU_APT（Advanced Persistent Threat），內容即是偵測或阻止 APT 或 Stuxnet 之類病毒的攻擊威脅方法。其下包含三個元件：設定正常時間之家電使用之溫度、壓力、通風等正常範圍；利用同步處理器做分析與監控；如發生異常狀況，需有警示或是能夠立即切斷電源 （見表 4）。

原 BSI PP 安全保證需求下（圖 2 編號 3.1.2）中，包含了一 ADV 類別，為 TOE 開發時每一項安全功能皆須提供安全評估所需的資訊。本研究建議 ADV 下新增家族 Safety functional specification (ADV_SF) 和 Safety design (ADV_SAF)。ADV_SF 加強實體安全功能，例如故障亦安全（fail-safe）[11],及監控（monitoring）等。即時監控可分析可疑行為如 APT 攻擊，以立即偵測並隔離，此家族與 FAU_APT 相關。ADV_SAF 家族則說明產品在設計時是否使用不同設計之多套系統（N-diverse version）、置於不同地點、電源之多套系統及多層次的防禦等安全機制；其下的元件見表 5。

針對圖 2 編號 3.1.2 下之 ATE，我們建議新增一安全分析家族 Safety analysis(ATE_SAF)。此家族之可利用錯誤植入（fault injection）方法進行側試，亦可採用故障樹分析（fault tree analysis）[12]方法，以驗證產品之安全性（safety），並進一步了解可能的不安全事件的過程及因果。

其中安全分析元件 ATE_SAF.1 可採用故障樹分析。故障樹採取由意外事件往前推導其可能之原因（backward）方法。舉一電器走火故障樹為例 (見圖 3):電器走火基本原因含電壓異常、溫度過高、或軟硬體故障；溫度過高則可能起因於電器過熱、短路等；電器過熱則可能因為不當使用、或被駭客端控制；駭客則可能非法取得密碼、或竄改訊息等。駭客可入侵的原因又可進一步推導，因網路釣

表 1 新增之組織安全策略

組織安全策略	描述
OSP.System	TOE 在系統的設計上需包含以下方法以降低系統故障所造成之後續安全影響： • 多套備份系統（Multiple version system） • 避免單點失效（single failure） • 避免共同失效模式（common mode failure） • 深層防禦（defense-in-depth）

表 2 修正 OSP.LOG 之內容

組織安全策略	描述
OSP.Log	TOE 應該要有下列四種記錄檔（log）：1～3 （同原始 BSI 智慧電網閘道保護剖繪） 4. 儲存正常使用型式（patterns）或正常工作區間（envelope）於 co-processor，包括時間、範圍、數值狀況等。

表 3 新增 FSP_SYP 家族之元件內容

元件名稱	內容描述
FSP_SYP.1	不同方式設計的多套系統(N-diverse version)，可用不同邏輯、平台、感應器及輸出等，以避免單點失效（single point of failure, SPOF）的發生，提高可用性及可靠性。
FSP_SYP.2	一多套系統置於不同地點、電源及基礎建設等，以避免共同失效之故障模式（common mode failure）。
FSP_SYP.3	多層次的防禦機（defense -in-depth）以增加安全性。

表 4 新增 FAU_APT 家族之元件內容

元件名稱	內容描述
FAU_APT.1	設定正常時間之溫度、壓力、通風等家電正常使用之範圍（即正常工作範圍）。
FAU_APT.2	利用 co-processor 做分析及監控－偵測器偵測並回傳值。
FAU_APT.3	異常警示、切斷電源

表 5 新增 ADV_SAF 家族之元件內容

元件名稱	內容描述
ADV_SAF.1	不同方式設計的多套系統(N-diverse version)，可用不同邏輯、平台、偵測器及輸出等，以避免單點失效（single point of failure, SPOF）的發生，提高可用性及可靠性。
ADV_SAF.2	一多套系統置於不同地點、電源及基礎建設等，以避免共同失效之故障模式（common mode failure）。

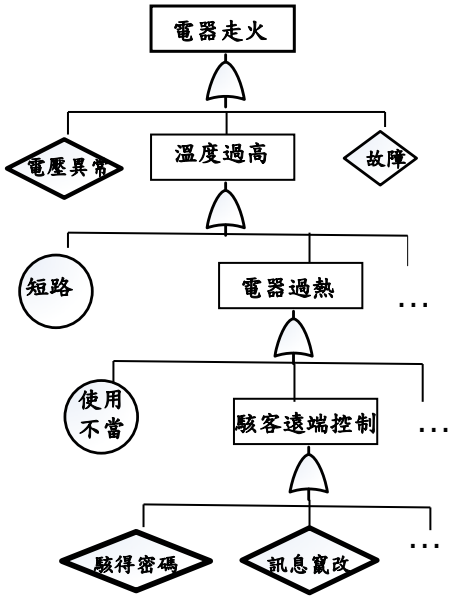

圖 3 電器走火部份故障樹

表 6 新增及修正的元件

編號（依照圖 2 之分類編號）			新增或修正內容
1：TOE 之資訊安全與實體安全環境	1.1：Hazards		T.Infrastructure
	1.2：組織資訊安全與實體安全策略		OSP.System
			OSP.Log
2：資訊安全與實體安全目標	2.1：TOE 實體安全目標		O.Protect
	2.2：環境之實體安全目標		OE.PhysicalProtection
3：資訊安全與實體安全需求	3.1 TOE 資訊安全需求及潛在實體安全影響	3.1.1：TOE 資訊安全與實體安全功能需求	FSP_SYP.1 FSP_SYP.2 FSP_SYP.3
			FAU_APT.1 FAU_APT.2 FAU_APT.3
		3.1.2：TOE 資訊安全與實體安全保證需求	ADV_SF.1 ADV_SF.2 ADV_SF.3
			ADV_SAF.1 ADV_SAF.2
			ATE_SAF.1

魚、訊息未加密簽章、網路設備安性不足等等。故障樹圖中長方形為事件，菱形為未進一步展開的事件，圓形為基礎肇因，不需再展開。從故障樹之一縱向分支可組成一因資訊安全問題導至實體安全效應的一情境。表 6 彙整本研究所增修之元件。

4. 制定家庭閘道器驗證標準及個案評估

本研究進一步根據上述智慧電網家庭閘道器 PP 制定驗證標準。方法為修改並延伸國內最新的相近驗證標準:電信技術中心（TTC）之「防毒閘道設備資通安全檢測技術規範」 [13]。其安全功能需求之審查內容包括稽核紀錄、使用者身分關

表 7 部份安全功能需求之書面審查內容[13]

項目	審查標準
1. 稽核紀錄	安全功能應具備以下稽核紀錄： (1)依下列事件類型產生其稽核紀錄並存於資料庫中： A. 啟閉稽核功能。 B. 存取稽核資料。 C. 使用者登錄成功或失敗、登錄權限變更及恢復。 D. 變更安全屬性。 E. 變更系統時間。 (2) 每筆稽核紀錄至少包含下列資訊：A. 事件識別碼。 B. 事件日期及時間。 C. 事件類型 D. 事件成功或失敗
…	…
8 防毒措施	(資訊)安全功能應具備以下防毒措施： (1) 清除病毒 (2) 隔離病毒 (3) 監控企圖透過遠端 TCP、UDP 或 SMTP 協定進行非授權之程序
9 防毒告警	(資訊)安全功能應具備以下防毒告警： (1) 偵測到病毒時，應發出警示訊息，內容應包含病毒資訊與處置措施 (2) 應持續提供警示訊息，直到使用者與管理者有所回應
10 密碼操作….	…
12 安全功能資料管理….	提供管理者設定查詢、更改或刪除下列事項： (1)病毒被偵測後所需行的動作 (2)病毒特徵檔 (3)稽核紀錄
14 ….	

聯、稽核審查等項目。此份技術規範可涵蓋大部分 BSI 之智慧電網閘道保護剖繪之項目且有具體檢查細項 (見表 7)，共 14 大項。例如第一項稽核紀錄之技術規範標準包含開啟關閉稽核功能、存取稽核資料等以產生稽核紀錄，且每筆紀錄需包含資訊如事件識別碼、日期時間等。

此一技術規範僅考慮一般防毒閘道器所需具備之功能，但未考慮智慧電網之實體安全或資安漏洞之後續危害效應。根據上述第三節之延伸實體安全功能需求、實體安全保證需求元件，我們新增了下面 15-18 項(見表 7)：

- 第 15 項－實體安全功能保護：
  (1)平時並在開機時執行安全功能測試，且應定期執行自我測試或由已授權使用者執行測試，以確認所有安全功能皆可正常運作。
  (2)當系統運作期間，應偵測本機之外盒是否被拆開，以確保不會遭受實體竄改。
  (3)當有任何故障發生時，評估標的應保持實體安全狀態。
- 第 16 項－可信任之通訊頻道：TOE 之安全功能應在自己與另一可信任之 IT 產品間提供可信任之通訊頻道，保護本身及頻道之資料不被修改或公開。
- 第 17 項－避免系統失效：為避免因系統失效而導致後續之實體安全影響，因此需事先準備多套系統便不時之需。
- 第 18 項－APT 攻擊偵測：預先設定家電正常使用時，溫度、溼度等的範圍，並利用一同步處理器（co-processor）動態監測並分析網路傳入之封包是否符合正常範圍，如未在正常範圍，則應發出警示，或是切斷其電源。

表 8 上表新增項目

項目 (元件)	審查標準
15 實體安全功能保護 (FPT_TST.1 FPT_PHP.1 FPT_FLS.1)	(1) 實體安全功能應在以下情況執行自我測試已確認安全功能之正常運作： A 開機初始化時 B.已授權之使用者要求時 C.正常操作期間定時做自我檢測 (2)實體攻擊之被動偵測 (3) 當故障發生時亦保持安全（safe）狀態
16 可信任之通訊頻道 (FTP_ITC/WAN.1 FTP_ITC/MTR.1 FTP_ITC/USR.1)	評估標的之安全功能應在自己與另一可信任之 IT 產品間提供可信任之通訊頻道，保護本身之端點及頻道之資料不被修改或公開。
17 避免系統失效 (FSP_SYP.1 FSP_SYP.2)	(1) 具有 redundant version 或 N-version programming，如偵測到有模組錯誤，方可以另一功能相同之模組做替換 (2)避免共同失效模式
18. APT 攻擊偵測 (FAU_APT.1 FAU_APT.2 FAU_APT.3)	(1)設定正常時間之溫度、壓力、通風等家電正常使用範圍。 (2)利用 co-processor 做分析及監控－偵測器偵測並回傳值。 (3)異常警示、切斷電源

本研究向合勤科技借了一項產品－整合式安全閘道器（ZyWALL USG 200）[14]，用以作為評估標的（TOE） 用上述驗證標準家以評估。此閘道器主要可應用於中小企業（25～50 個 PC 使用者），具有入侵偵測防禦系統，除了可防範來自外部的威脅，亦可防範內部之威脅。其主要優點並包含安全連線、主動防禦、容易管理、網路恢復力等。

評估結論為此台閘道器幾乎皆符合上述智慧電網家庭閘道器驗證標準，僅有少數項目未符合審查標準，包含：

- 第八項防毒措施之（3）監控企圖透過遠端

TCP、UDP 或 SMTP 協定進行非授權之程序：此閘道器主要支援 HTTP/FTP/SMTP/POP3/IMAP4 協定，因此並無支援審查標準中之 TCP 與 UDP。

- 第十五項安全功能保護之（2）實體攻擊之被動偵測：因此閘道器之最初目的為設計給中小企業使用，因而並未考慮到其實體可能遭受竄改。
- 第十八項 APT 攻擊偵測，目前較少閘道能夠偵測 APT 之攻擊，因其潛伏期長且難發現。

此個案之 15-18 項評估結論見表 9

表 9 合勤安全閘道器部份評估結果

項目	PP 相對應元件	TOE 符合否
15	FPT_TST.1 FPT_PHP.1 FPT_FLS.1	(1) V (2) X (3) V
16	FTP_ITC/WAN.1 FTP_ITC/MTR.1 FTP_ITC/USR.1	V
17	FSP_SYP.1 FSP_SYP.2	V
18	FAU_APT.1 FAU_APT.2 FAU_APT.3	X

5. 結論

智慧電網為未來之趨勢，藉由與智慧家電與家庭閘道器之結合，使用者可遠端遙控智慧家電之操作。因為電網所連結的多為工業或家電控制系統，此類系統具有對實體環境運作能力，一旦遭惡意攻擊，可能產生實體上的破壞。故此領域衍生了一新議題:如何預防與處理資訊安全(information security)漏洞可能引發之後續實體安全(physical safety) 問題。然而，目前智慧電網閘道相關標準多數尚未考慮實體安全新議題;並且多數未能處理 APT(或 Stuxnet)等進階病毒攻擊及其後對實體安全影響。

本研究針對此問題，將德國 BSI 的智慧電網閘道器 PP 第六章節翻譯為中文，並進一步修正及新增其內容，增加處理實體安全及 APT 之相關元件。本研究建議以此增定版為智慧電網家庭閘道保護剖繪標準；並依此標準，擴充了國內相關之安全檢測規範以做為智慧電網家庭閘道器檢測規範;最後再以一商用閘道器做為個案，評估本研究所制定標準之有效性。

本研究為智慧電網中結合資訊安全與實體安全之初步研究，希望能有拋磚引玉效果，日後能有更多研究人員投入相關技術開發。未來物聯網（Internet of Things）的興起，更需要資訊安全與實體安全之整合。本研究未來方向將擴充實體安全相關元件以達到完整性，亦將此類元件通用化(generalized)，用以修訂資訊技術安全評估共同準則（Common Criteria）內容。

誌謝

本研究部份接受國科會編號 NSC 101-3113-P-033-003，NSC 102-2221-E-155-030 計畫經費補助。

參考文獻

[1] 台灣智慧型電網產業協會，http://www.smart-grid.org.tw/index.aspx.

[2] ISO/IEC 15408-1, “Common criteria for information technology security evaluation, Part 1: Introduction and general model, ” Version 3.1, Release 4, September 2012, http://www.commoncriteriaportal.org.

[3] ISO/IEC 15408-2, “Common criteria for information technology security evaluation, Part 2: Security functional components, ” Version 3.1, Release 4, September 2012, http://www.commoncriteriaportal.org

[4] ISO/IEC 15408-3, “Common criteria for information technology security evaluation, Part 3: Security assurance components, ” Version 3.1, Release 4, September 2012, http://www.commoncriteriaportal.org

[5] 南韓大顆首爾(DarkSeoul) 大規模 APT 攻擊事件，http://blog.xecure-lab.com/2013/03/darkseoul-apt.html.

[6] 惡意程式－Stuxnet 簡介，http://www.cert.org.tw/docfile/Stuxnet.pdf.

[7] 資策會，In-Snergy 雲端智慧綠能管理系統，http://www.insnergy.com/html/home.jsp.

[8] SANS Institute, “Protection Profile, A key concept in the Common Criteria”, 2003 http://www.sans.org/reading_room/whitepapers/standards/protection-profile-key-concept-common-criteria_1007.

[9] Germany Federal Office for Information Security (BSI), “Protection Profile for the Gateway of a Smart Metering System,” 2012, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP-SmartMeter.pdf?__blob=publicationFile.

[10] 易俗、陳振楠、范金鳳、曾婉惠、陳明輝、鄭宗杰， 工業控制系統資訊安全問題及特性初步分析，資訊安全會議，2005。

[11] “Fail-safe,” http:// en.wikipedia.org/wiki/Fail-safe.

[12] Nancy Leveson, Safeware: system safety and computers, Addison Wesley, 1995.

[13] 財團法人電信技術中心，防毒閘道設備資通安全檢測技術規範，http://www.ttc.org.tw/index.html.

[14] 合勤科技，http://www.zyxel.com/tw/zh/homepage.shtml.