Regular Paper

Communications of the CCISA
Vol. 27 No. 3 Aug. 2021

# 智慧電網之資訊安全標準的研究分析

宋明軒[1]、葉錫勳[2]、郭文中[1]
[1]國立雲林科技大學資訊工程系、[2]財團法人台灣商品檢測驗證中心
[1]{M10817047, simonkuo}@yuntech.edu.tw、[2]ccueacn@gmail.com

## 摘要

智慧電網是利用資訊化以及自動化整合發、輸、配電以及用戶的電網系統，也就是將 IT (Information Technology) 與 OT (Operational Technology) 結合在發、輸、配電以及用戶的電力系統。因為電力系統是國家重要的基礎建設，若貿然將其資訊化及自動化，可能會面臨相當大的風險。因此各國專家學者都積極投入智慧電網之網路安全標準的制定，而這些標準內容繁雜，使得相關人員難以尋找所需的資訊安全標準。因此，在本篇文章中，我們首先研析智慧電網及工業自動化的相關資訊安全標準 (如 IEC 62443、IEC 62351、NISTIR 7628 以及 ISO 27001)，然後針對這些標準的差異、使用的安全技術以及面臨的資安威脅進行分類及比較。最後，我們再利用美國政府制訂的網路安全框架 (Cybersecurity Framework，CSF) 內之五大核心功能來對這些智慧電網標準進行歸類，期望能夠以提供人們在建置或設計智慧電網時，當作資訊安全防護參考指南。

**關鍵詞：智慧電網、安全標準、IEC 62443、IEC 62351、NISTIR 7628、ISO 27001**

Communications of the CCISA
Vol. 27 No. 3 Aug. 2021

# Research of Information Security Standards for Smart Grid

Ming-Xuan Sung[1], Hsi-Hsun Yen[2], Wen-Chung Kuo[1]
[1]National Yunlin University of Science & Technology, Taiwan.
[2]Taiwan Testing and Certification Center.
[1]{M10817047, simonkuo}@yuntech.edu.tw, [2]ccueacn@gmail.com

## Abstract

A smart grid is a grid system that integrates power generation, transmission, distribution, and users through information and automation technology. In other words, it combines IT (Information Technology) and OT (Operational Technology) to be used in the power system which includes the power generation, transmission, distribution and users. However, the power system is an important infrastructure, and it will face considerable risks after informatization and automation. Therefore, many expert groups from various countries are actively involved in the drafting of smart grid-related cyber security standards. The content of these standards is complex, making it difficult for relevant personnel to find the required information security standards. Firstly, we will analyze many related information security standards for smart grids and industrial automation, such as IEC 62443, IEC 62351, NISTIR 7628 and ISO 27001 in this paper. Secondly, we will classify and compare the differences between the security technologies and threats of these standards. Finally, we will use the five core functions of the Cybersecurity Framework (CSF) to category these standards and then provide an information security protection guideline when people want to set up or design the smart grids.

**Keywords: Smart Grid, Security Information Standard, IEC 62443, IEC 62351, NISTIR 7628, ISO 27001**

# 壹、前言

## 1.1 背景

在這個電力能源需求越來越多的時代，如何有效率的產生、使用能源成為了最重要的議題，因此結合了網路資訊科技的智慧電網就能應用在此議題上面。

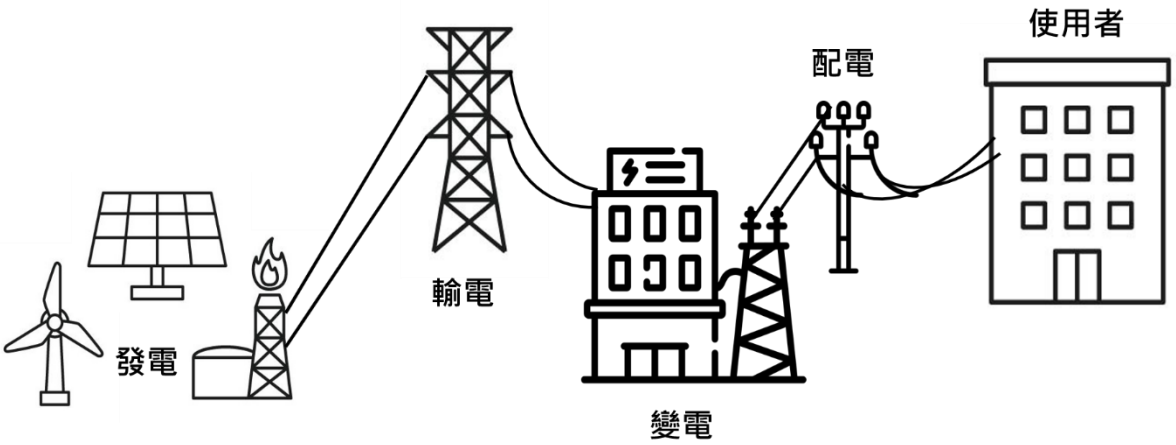


圖 1：電力產業簡單示意圖

發、輸、配電以及用戶是整個電力系統主要部分。如圖 1 所示，由不同類型的能源如風力、太陽能、核能等發電方式發電後，再透過輸配電系統像是變電站、配電站以及電線杆等基礎建設傳送至用戶家中[2]。傳統電網是以集中式發電為主要發電方式，由一個大型電廠發電後，再通過輸配電系統降壓傳送至用戶家中，這種方式能降低發電成本且簡單，但是當主要的發電廠故障時就會造成整個電力網路無法使用[22]，而且近年因為環保綠能等因素，發電方式漸漸朝太陽能，風力等綠色能源的發電方式。因此電力供應方式逐漸往分散式發電為主[23]，分散式發電則是由多個小規模的小型發電站，像是風力發電、太陽能發電等所組成，但由於這類再生能源的不穩定性，需要搭配感測器以及網路去做適時的調度，因此分散式發電所組成的電網系統也逐漸朝智慧電網所邁進。

## 1.2 動機及目的

智慧電網是利用資訊化以及自動化整合了發、輸、配電以及用戶的電網系統，將 IT 與 OT 結合在發、輸、配電以及用戶，電廠透過偵測以及收集電力資訊來提供高品質的電力到用戶端。智慧電網是相當重要的基礎建設，因此需要佈署相當大量的基礎設施，才能達到電力數據化且雙向溝通的效果，而其中一種基礎建設就是智慧型電表基礎建設 (Advanced Metering Infrastructure，AMI) ，AMI 透過智慧電表讓用戶得知自己的用電量，或者是收集更詳細的電力資料來提升用電效率。

綜觀智慧電網，我們發現會有大量用戶用電資料會在此網路中傳輸，甚至於我們可透過智慧網路的自動化及通訊系統去控制發電或者是輸配電。隨著電網大量使用資訊技術進行資料傳輸的同時，也將原本網路中的威脅與風險帶入了需要高安全性的電力系統中，甚至產生新的風險，例如 2020 年 1 月伊朗駭客攻擊美國電網[21]，又或者是駭入智慧型電表偽造帳單[19]，這些威脅與風險會影響電力系統運作，以及要如何管理這些系統的公用事業的運作以及支援這些系統的業務流程等問題，這些問題已經引起許多學者專家的重視。因此各個專家小組都制定了跟智慧電網有關的相關標準。

然而，在各國專家小組的研究下，近年來已經發布了許多的智慧電網相關安全標準，種類繁多，使得想要跨足、研究相關領域的人員難以在眾多文獻中找到自己的方向，甚至忽略了其他可用的標準[1]，因此本篇論文分析智慧電網以及工業自動化的資訊安全相關標準及控制措施如 NIST 7628、IEC 62443 以及 ISO 27001 等標準，並進行比較，以利相關人員及智慧電網建置之參考。

## 貳、相關研究

### 2.1 安全標準

目前許多國家針對智慧電網制定許多相關標準，像是美國國家技術標準局 (National Institute of Standards and Technology，NIST) 所制定的 NISTIR 7628，是為智慧電網網路安全所制定的標準。而 NISTSP800-82 是基於 NISTSP800-53 針對工業控制系統所額外訂製的補充，以提供適用於工業控制系統的安全標準。國際電工委員會 (International Electrotechnical Commission，IEC) 也制定了許多資安標準，IEC 62351 的主要範疇為能源領域的資料交換與傳輸協定的安全規範，IEC 62443 則是工業控制系統相關的資安技術議題。

### 2.2 NISTIR 7628[16]

傳統上，IT 網路安全著重於確保電子資訊通信系統之機密性、完整性和可用性所需的保護。電力網路安全則需要適當組合電力系統和 IT 通訊系統領域，以保持智慧電網的可靠性和消費者資訊的隱私。因此智慧電網中的網路安全應包括在 IT 和電力系統營運和治理中實現電力和網路系統技術及流程的平衡。也就是，從一個領域應用不當的做法到另一領域時，可能會降低可靠性。因此，安全性和可靠性在電力系統中至關重要。與傳統的 IT 強調的網路安全是有所不同的。而目前 NISTIR 7628 總共有三大部分。

在 NISTIR 7628 第一部分文件資料為智慧電網提出了七大領域:傳輸、配電、營運、發電、市場、客戶和服務提供者，如圖 2 所示。發電、傳輸、配電是將產生的電力透過電力線傳送至客戶家中，而控制領域則是透過通訊流向客戶、服務提供者、或是電力市場提供自動化，或者是資訊雙向傳輸的服務。

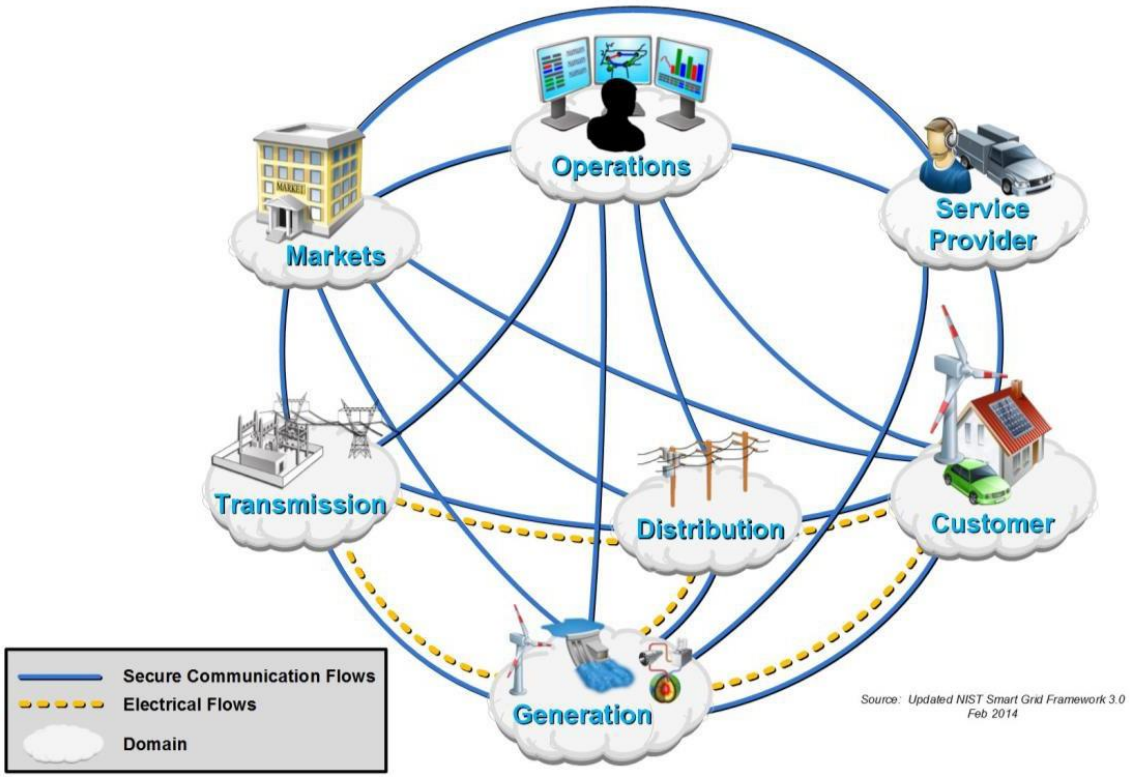


圖 2：智慧電網7大領域[16]

NISTIR 7628 也為了這 7 大領域提供了邏輯介面以及 19 項資訊安全控制項，19 項資訊安全控制項請參照表 2-1，為智慧電網相關人員提供電網資訊系統建置使用。

表 2-1：硬體規格

| 編號 | 資訊安全需求 | 編號 | 資訊安全需求 |
|---|---|---|---|
| SG.AC | 存取控制 | SG.MP | 媒體保護 |
| SG.AT | 認知和培訓 | SG.PE | 實體和環境安全 |
| SG.AU | 審核和責任制 | SG.PL | 規劃 |
| SG.CA | 安全評估和授權 | SG.PM | 安全計劃管理 |
| SG.CM | 配置管理 | SG.PS | 人員安全 |
| SG.CP | 操作持續性 | SG.RA | 風險管理與評估 |
| SG.IA | 身分驗證和授權 | SG.SA | 智慧電網資訊系統和服務的採購 |

| | | | |
|---|---|---|---|
| SG.ID | 訊息和文件管理 | SG.SC | 智慧電網資訊系統和通訊保護 |
| SG.IR | 突發事件回應 | SG.SI | 智慧電網資訊系統和資訊完整性 |
| SG.MA | 資訊系統的開發與維護 | | |

### 2.3 ISO 27001[14]

ISO 27001 是由國際標準組織 (International Organization for Standardization) 以及國際電工委員會一起發佈的資安管理標準，此標準提醒在建構及管理整個資安管理系統時，必須注意且不可忽略的層面，並藉由 PDCA 循環機制來持續進行規劃 (Plan) 、執行 (Do) 、審查 (Check) 及改善 (Act) 等方式來確保系統持續運作並且預防資安事件的發生或是降低遭受損失的風險。這項標準已在國際上被廣泛的使用。回顧 ISO27001:2013 規範內，除本文要求之外，還包括 14 個控制目標。

然後在依據不同控制目標需求下，區分為 114 控制措施。這些控制目標是用於建立資訊安全管理系統並且進行審核，已確保組織的資訊安全管理系統有持續性的運作，當審核通過，就代表獲得 ISO27001 認證。目前台灣資通安全責任等級分級辦法內已要求等級 A 及等級 B 之公務單位在「初次受核定或等級變更後之二年內，全部核心資通系統導入 CNA27001 或 ISO27001 等資訊安全管理系統標準、其他去有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，於三年內完成公正第三方驗證，並持續維持其驗證有效性」。

### 2.4 NIST SP 800-82[17]

此標準的目的是為確保工業控制系統 (Industrial control system, ICS) 的資訊安全提供指導包括監測控制和資料收集 (Supervisory Control and Data Acquisition, SCADA) 系統、分散式控制系統 (Distributed Control System, DCS) 以及執行控制功能的其他系統。提供 ICS 的名義概述，審查典型的系統拓撲和體系結構，識別這些系統的已知威脅和漏洞,並提供了降低相關風險的建議安全對策。另外，此篇標準基於 NIST SP 800-53 Rev. 4 針對 ICS 領域提供了適用於 ICS 領域獨特性的安全需求。ICS 存在於許多行業如電力、水、石油和天然氣、化工、製藥、造紙、食品和飲料以及製造 (如汽車、航空航太和耐用品) 。由於存在許多不同類型的 ICS，其潛在風險和影響程度各不相同，因此此篇標準提供了保護 ICS 的許多不同的方法和技術的清單。此篇標準不是純粹用作保護特定系統。建議對各個不同的 ICS 進行風險評估，並訂製建議的解決方案，以滿足其特定的安全、業務和營運要求。

## 2.5 IEC 62351[9]

隨著智慧電網的發展與普及，電力系統的管理、資料的傳輸都是智慧電網的核心，而這些都仰賴著網路通訊技術，因此網路通訊的安全是智慧電網非常需要探討的議題[8]，因此 IEC 制定了與電網通訊相關的安全標準 IEC 62351。IEC 62351 是基於 IEC 61850、IEC 60870-5、IEC 60870-6、DNP 3.0 四項通訊自動化標準所建立的，它透過現有的安全機制、加密技術、數位認證的方法來進行機密性與完整性的保護，以確保電力系統的管理、資料的傳輸交換能受到保護。

IEC62351 目前共有 13 部份，一以及二部分為概述，三到七為通訊標準的安全技術，八為電力系統中的存取控制，使用基於角色的存取控制方法來實現 (Role-based access control，RBAC) ，九為密碼學，裡面規定了加密密鑰管理，即如何生成，分發，吊銷和處理公共密鑰證書和加密密鑰，以保護數據及其通訊。第十部份為電力系統中與安全相關的元件、功能及其安全控制與架構指引的技術報告。十一部分為電力系統中 XML 文件的保護，十二部分則是討論了分散式能源系統面臨的威脅，以及相關的保護措施。十三部分提供了有關在電力行業中使用的標準和規範 (IEC 或其他) 應涵蓋哪些安全主題的指南。

## 2.6 IEC 62443[4]

是對於工業自動化與控制系統的安全規範，原本被命名為 ISA 99，由國際自動化學會 (International Society for Automation, ISA) 所創立的，後經審核再透過美國國家標準協會 (American National Standards Institute, ANSI) 發布，之後被 IEC 納入並以 IEC 內部委員會修訂並發布，因此會有 ISA/IEC 62443 兩種名稱。

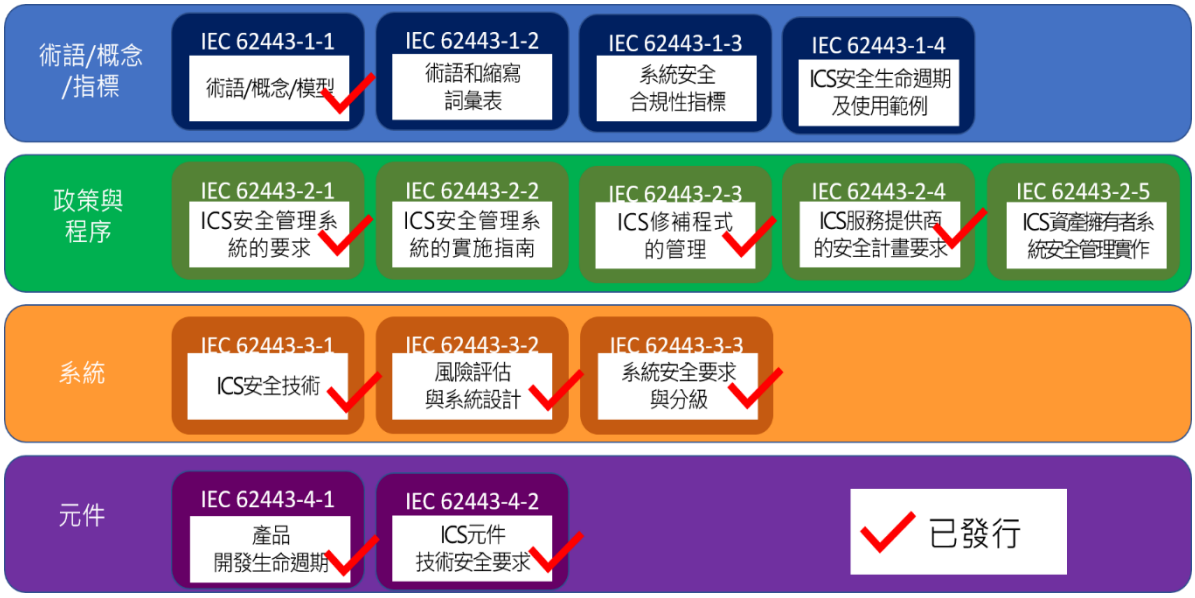


圖 3：IEC62351系列

如圖 3 所示，IEC 62443 總共分為 4 個部分，分別為概述、政策與程序、系統以及元件，而 IEC 62443 有一些部份目前為尚未發布，因此本篇論文會以已經公開發布的標準來進行分析：

IEC 62443 由上至下分別為：

- 第一部分是概述，裡面包含了一般或基本的概念、模組及專有名詞，也包括 ICS 的安全規律。
- 第二部分則是透過組織內有效的 ICS 安全計畫，來解決並維護 ICS 安全問題。
- 第三部分為系統設計概述與安全要求。
- 第四部份則是製造商的產品開發與系統控制，以達到產品的安全技術要求。

## 2.7 Framework for Improving Critical Infrastructure Cybersecurity[18]

又被稱作網路安全框架 (Cybersecurity Framework，CSF) ，由於關鍵基礎設施日益增加的複雜性，以及越來越倚靠網際網路進行設施的運作，因此網路安全的威脅也逐漸影響到關鍵基礎設施的運作。美國 NIST 提出了這套 CSF 框架用來維持 IT 以及關鍵基礎設施的網路安全。關鍵基礎設施即為公有或私有，實體或虛擬的資產，生產系統，會因為人為破壞或自然災害受損進而影響國家及社會功能運作者[24]，要管理網路安全的風險，需要清楚了解組織的業務以及其技術所需要的安全注意事項，每個組織的風險，優先順序和系統都是獨一無二的，因此所評估的風險以及所使用的標準都會有所不同。

此框架的主要核心有五大功能，

- 識別 (Identify) ：組織理解並管理系統、人員、資產、數據和能力的網路安全風險。
- 保護 (Protect) ：制定和實施適當的保障措施，確保提供關鍵服務。
- 偵測 (Detect) ：檢測功能能夠及時的發現安全事件。
- 回應 (Respond) ：對檢測到的網路安全事件採取行動，控制潛在的網路安全風險。
- 復原 (Recover) ：及時恢復關鍵服務的運作，減少網路安全事件的影響。

這五個功能底下還有類別以及子類別，如圖 4 所示，而類別與子類別就是為了達成這些核心功能，組織所需要做到的事項。

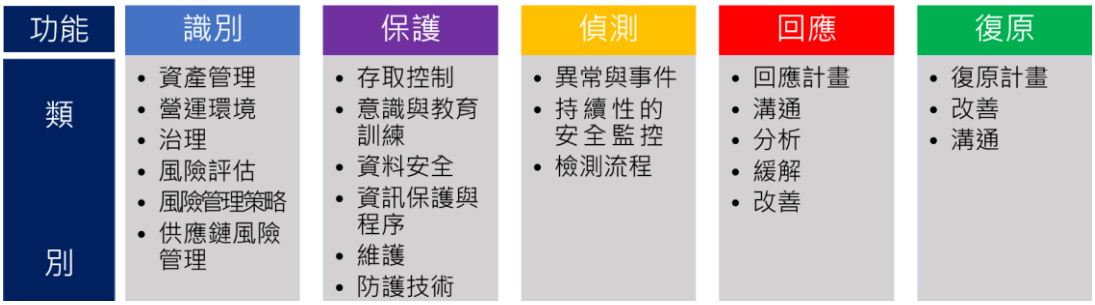


圖 4：核心功能與類別

在評估完這五大功能後，組織將根據組織現況依照此框架所定義 4 個層級去確認組織在哪一層級，這 4 個層級請見圖 5，在確認組織位在哪一層級後，並盡力往成熟度高的層級 4 實現組織的風險管理計畫。

此框架也引用各種相關標準的安全控制來跟五大功能的子類別做對映，如 ISO 27001、IEC 62443、NIST SP 800-53 等，作為組織進行網路安全需求、風險管理的參考。

## 參、標準分析

### 3.1 概述

在本章節，將會針對 NIST 7628、NIST 800-82、IEC 62443、IEC 62351 以及 ISO 27001 等與智慧電網有關的安全標準做全面性的分析，像是智慧電網所面臨的網路威脅，這些威脅會影響到智慧電網的哪些方面，而智慧電網的相關安全標準是在運用在電網的哪些方面，這些標準又用了哪些技術來解決威脅。

### 3.2 智慧電網相關威脅

這節將要介紹智慧電網有哪些相關威脅，如圖 5 所示，智慧電網的相關威脅以機密性、可用性、完整性來做分類。可用性遭到威脅的情況下為系統或設備無法使用的情況，在此情況會遭到的攻擊有蠕蟲，以及阻斷攻擊；機密性遭受威脅的原因則是未經授權取得機敏資料，木馬病毒、竊聽攻擊以及中間人攻擊等會破壞智慧電網的機密性[1,2]；完整性則是未經授權修改資料，木馬病毒，中間人攻擊，重送攻擊等都會破壞智慧電網的完整性[1,2]。

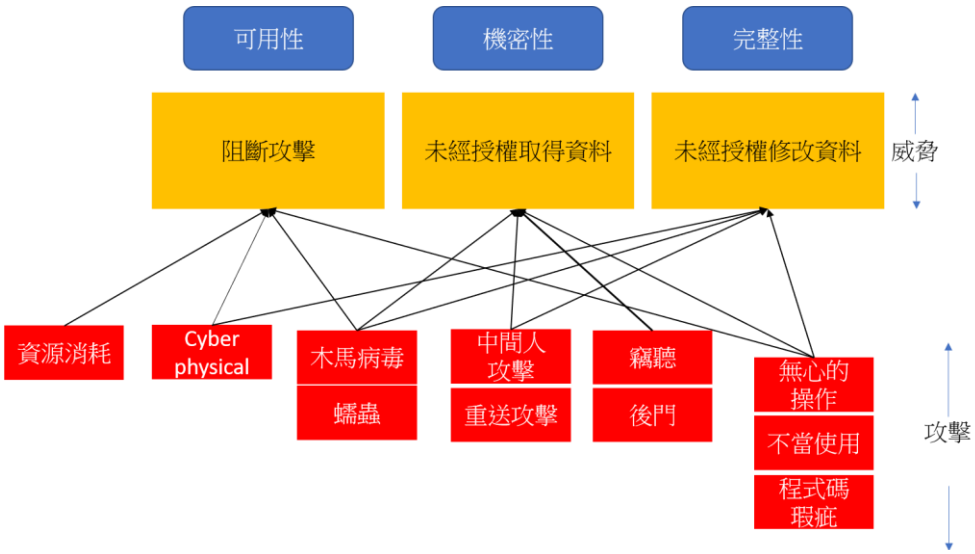


圖 5：智慧電網的威脅與可能的攻擊[12]

網路實體攻擊 (Cyber physical attack) 是 ICS 系統以及智慧電網上出現的新興的攻擊，由於智能電網包含複雜的電力、能源、控制、感應、計算和通訊系統。這種架構的複雜性凸顯了其安全性和彈性面臨的潛在威脅[3]，智慧電網的實體設備之間利用網路相互連結，因此攻擊者可以竄改發送給設備的指令，進而讓設備超載毀壞[16]，此類型的攻擊影響到了可用性以及完整性。

無心的操作、不當使用以及程式碼瑕疵雖然屬於人員上的疏失，卻會在智慧電網上造成相當巨大的影響，例如：2021 年 5 月 13 日所發生的興達電廠跳機事故，即為工作人員在驗收時的操作不當所引起的[20]。而程式碼瑕疵也會造成攻擊者在系統找到漏洞，進而發動零日攻擊[1]。

### 3.3 智慧電網威脅與智慧電網領域與智慧電網標準

在本節，智慧電網的威脅分別威脅至不同的智慧電網領域中，而在不同領域也各自有不同的安全標準做對映。

圖 6 中顯示了智慧電網的領域與標準的對映，首先智慧電網的組織管理所對應到威脅為人為疏失的無心的操作、不當使用以及程式碼瑕疵所造成的，因為組織的培訓政策與流程錯誤才會造成此問題，而 NIST 7628、NIST 800-53、IEC 62443 以及 ISO 27001 都有明確的控制項目來推定組織各項安全管理政策。

電網系統控制，是智慧電網自動化與調度的核心，人為疏失的部分會造成電網系統相當大的隱憂，而資源消耗與蠕蟲則是會造成整個電網運作系統的癱瘓，網路實體攻擊則是會利用中間人攻擊、木馬、重送攻擊等方式傳送惡意指令到電網的各個設備中造成莫大的損傷，在電網系統控制上 NIST 7628 有通訊保護 SG.SC 與資訊完整性 SG.SI 這兩項控制項確保系統的機密性與完整性不受威脅[16]，而 NIST 800-82 則是網路分隔與存取控制的詳細指導[11]，IEC 62443-3-1 是安全技術相關詳細指導[5]，IEC 62351 則是有智慧電網系統建議使用的加密技術指南，來保護通訊的機密性與完整性[10]。

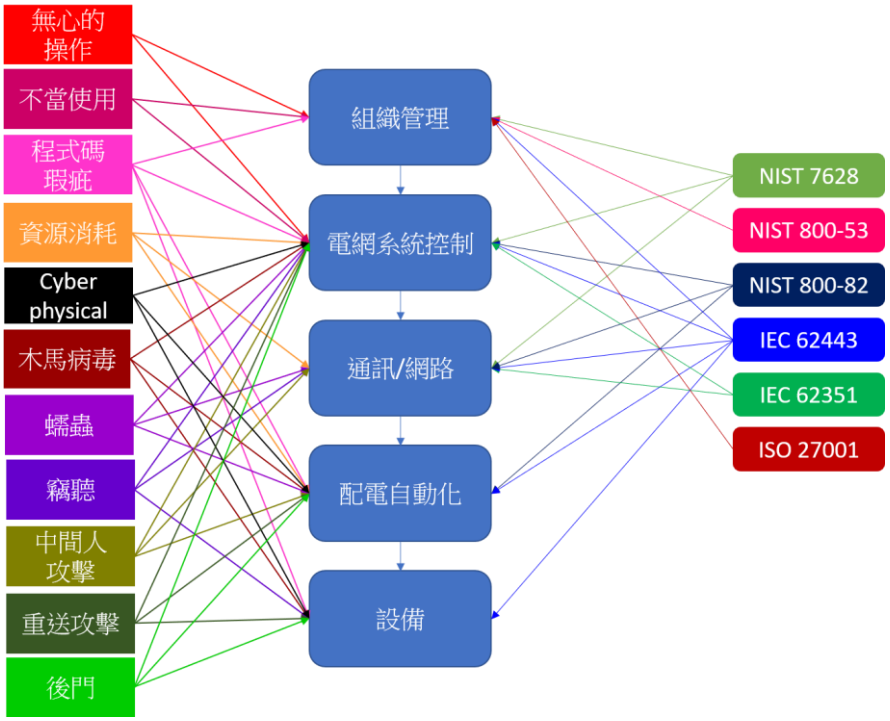


圖 6：智慧電網領域與標準對映圖

在智慧電網的通訊/網路的部分，蠕蟲與阻斷攻擊會癱瘓智慧電網的通訊與網路，造成智慧電網可用性的威脅，竊聽與中間人攻擊攔截機敏資訊造成機密性的威脅。在 NIST 7628 與 IEC 62351-9 有對於金鑰管理系統詳細指導[13,16]，IEC 62351 的第三至第五部則是規範了金鑰的加密方式與網路協議的使用[10,11,12]，NIST 800-82 與 IEC 62443-3-1 中，都有對網路使用網路分隔，架設入侵檢測系統等等的使用[5,19]。

配電自動化是智慧電網的核心概念之一，利用感測器判斷使用者使用多少電力而透過變電站自動化及時調度電力，但因電網其複雜的特性有著相當大的安全隱憂，利用中間人攻擊、木馬、重送攻擊等方式導致設備接收到錯誤指令的網路實體攻擊造成電網的實際損害，利用阻斷服務攻擊與蠕蟲造成電廠停擺都是對於智慧電網來說有著相當大的風險。IEC 62443 與 NIST 800-82 都是工業自動化系統的安全標準，IEC 62443-3-1 與 NIST 800-82 說明了 ICS 系統的安全技術與解決的漏洞，IEC 62443-3-3 則是 ICS 的安全控制措施[7]。

智慧電網的終端設備，如智慧電表會接收到相當大量的使用者隱私資料 ：像是帳單資訊、用電資訊等等[8]，這些都會是攻擊者容易下手的目標，IEC 62443-4 是第三方設備的安全控制措施與指南。它定義了一個安全的開發生命週期，用於開發和維護安全的產品。此生命週期包括安全需求定義、安全設計、安全實施、驗證和確認、缺陷管理、修補程式管理和產品壽命。

### 3.4 智慧電網安全標準與 CSF 核心功能對映

在本節，將會以智慧電網的相關安全標準與 CSF 核心功能做主要的對映，並且以技術跟管理方面分析與比較出相關標準會對映到那些核心功能，如圖 7 所示，實線為該標準有可以與核心功能對映的相關安全技術指南，而虛線則表示該標準與對映到的核心功能僅有管理政策。

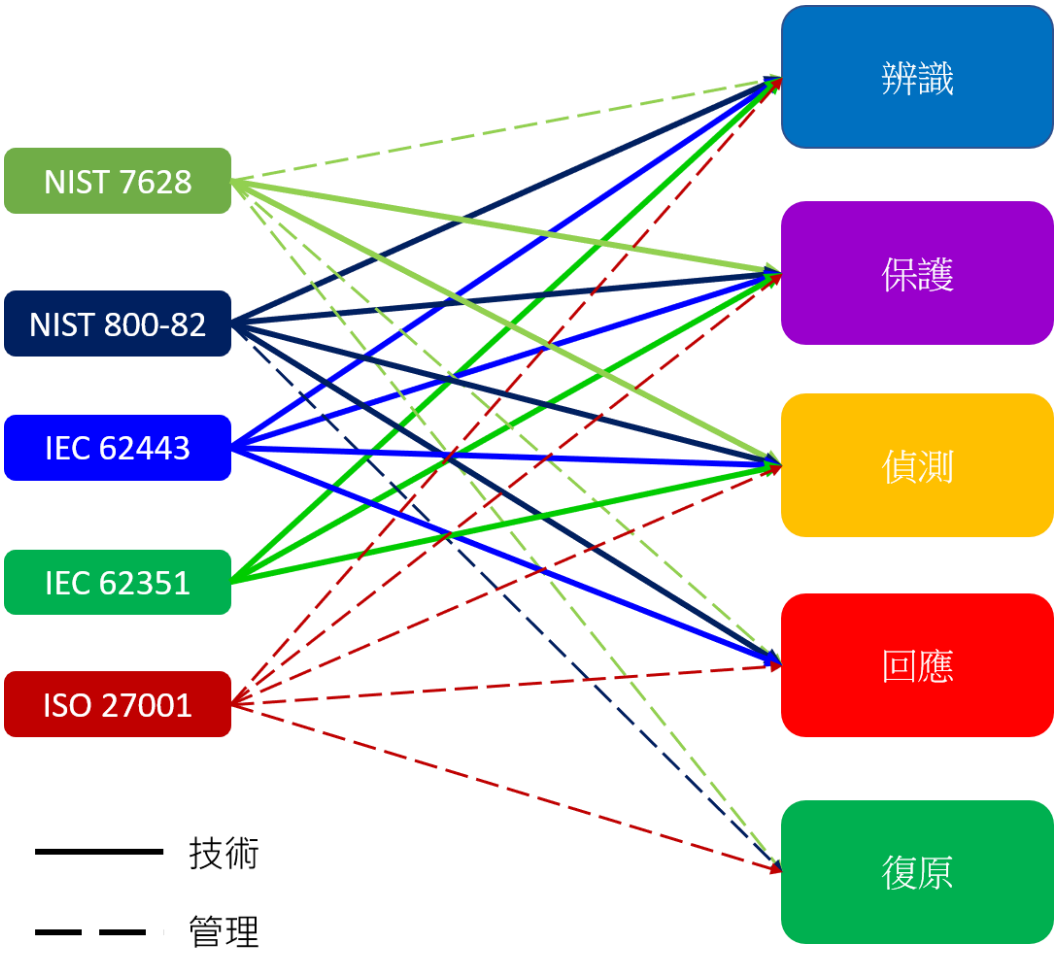


圖 7：智慧電網標準與CSF核心功能對映圖

- **辨識**

辨識的核心功能是有效使用該框架的基礎。組織了解業務背景、使用關鍵功能的資源以及相關的網路安全風險，使組織能夠根據其風險管理戰略和業務需求，集中精力並確定其優先次序。

在 NIST 7628 中，辨識為安全控制項的管理像是 SG.RA 風險管理與評估、SG.PL 規劃、SG.CA 安全計畫管理等等。但是卻沒有對風險評估的具體實作指引。

NIST 800-82 有對於風險評估的詳細方法解說，這是基於 NIST 800-39 管理訊息安全風險這項標準裡的方法而來的，並且也有辨識功能的安全管理控制項，這是基於 NIST

800-53 所制定的。

IEC 62443 系列的 IEC 62443-3-2 是針對自 ICS 網路安全提供網路安全風險評估的詳細說明。

IEC 62351 在第 12 部分中，針對分佈式能源系統 (DER) 進行了風險緩解的建議，將風險分為幾種方式處理：

- ✓ 可接受的風險：不採取任何緩解措施，因為事件的預期影響似乎不值得實施緩解措施。
- ✓ 可分擔風險：例如通過向保險公司付款來承擔風險。此方法通常用於防止實體資產 (例如建築物和 DER 設備) 的損失。
- ✓ 轉移風險：通過與第三方簽約負責操作和維護 DER 系統的責任。
- ✓ 可以將風險降低到不同的階級：例如，某些 DER 系統可能只需要使用帳號密碼來進行存取控制保護，而其他 DER 系統可能需要進行多因子身份驗證和密碼證書驗證才能進行存取。

ISO 27001 中與辨識功能的對映中，也是僅有相關控制項來達到辨識功能如 A.8.2 資訊分級、A.12.6.1 脆弱性管理以及 A.6 資訊安全組織等等，而風險管理評估的詳細措施在 ISO 27005 中有詳細說明。

- **保護**

保護核心功能為制定和實施適當的保障措施，確保關鍵服務的提供以及限制或遏制潛在網路安全事件影響的能力。

在 NIST 7628 裡，保護功能的相關技術主要是密碼學，NIST 7628 第一部分的第四章主要是講解密碼學和金鑰管理問題，像是密碼學在智慧電網系統中，因為部分智慧電網設備的因素會有計算限制，或是智慧電網設備的壽命過長而產生的憑證管理問題。

NIST 800-82，主要講解的安全技術為網路隔離的相關技術，像是使用防火牆並且也詳細說明了防火牆的制定規則如 ICS 防火牆的出站流量應僅限於基本通訊、ICS 網路到 IT 網路的出站流量都必須受到來源端和目的地的限制等等，或是使用 ICS 系統專用的網路協定等等。

IEC 62443-3-1 講解了各種網路安全相關的技術與工具，像是認證與授權技術、存取控制技術以及加密與資料驗證等等。在保護核心功能中，資料的保護佔了相當大的一部份，IEC 62443-3-1 也提供了加密技術的選擇與建議，也列出了使用虛擬私人網路 (Virtual Private Network，VPN) 來對資料做完整性及機密性的保護。

IEC 62351 透過現有的安全機制和加密技術來確保資料機密性與完整性，並且讓電力系統的管理、資料的傳輸交換能受到保護，IEC 62351 的第三部份到第五部分規範了金鑰的加密方式與網路安全協議的建議，IEC 62351 的第八部分也詳細說明了如何在電力系統中實施基於角色的存取控制 (Role-based access control，RBAC) 的指引。

- **偵測**

偵測功能制定和實施適當的安全政策或技術，能夠及時發現、確定網路安全事件的

發生。

NIST 7628 在第六章中有對智慧電網系統內常見的漏洞進行分類並對組織會造成影響的部分進行描述，在第七章中也有建議對電力設備使用入侵檢測系統檢測安全事件。

NIST 800-82 有在 ICS 中對於病毒和惡意程式碼檢測的建議與指引，也建議 ICS 系統佈署入侵檢測系統應佈署在 ICS 網路與 IT 網路的防火牆上等建議。

IEC 62443-3-1 對於偵測功能與保護功能都有詳盡的技術與工具的指引，像是入侵檢測系統、網路監控以及日誌稽核等等。

IEC 62351 在第七部份網路系統管理中 (Network and System Management，NSM) 提出了 NSM 概念，這個概念包含了監測軟體應用程式、監測系統與通訊的性能、入侵檢測以及配置管理，規範了 IDS 系統的監控項目如設備路徑、存取控制清單網路配置資訊等等。

- **回應**

回應功能制定和實施適當的安全政策，對偵測到的網路安全事件採取行動並控制潛在網路安全事件的影響的能力。

NIST 800-82 對於回應的建議和指引為當有異常繁重的網路流量、嘗試或實際使用管理員帳戶、防病毒或 IDS 警報等事件徵狀發生時，可能表示 ICS 受到攻擊，必須實施回應計畫，事件回應也可以包括以下方法：

- ✓ 事件分類：應查明各類 ICS 事件,並對潛在影響做分類，以便針對每一潛在事件制定適當的對策。
- ✓ 回應操作：在發生事件時，可以採取多種回應。所採取的回應將取決於事件的類型以及對 ICS 系統的影響。應準備書面計劃，記錄事件類型和每種類型的回應，這可以在事件可能造成混亂或壓力時提供指引。該計劃應包括各組織應採取的分步行動。
- ✓ 恢復操作：事件的影響可能很小，也可能事件導致 ICS 發生許多問題。應進行風險分析，在各種事件情境下，都應該把恢復操作步驟記錄下來，以便系統能夠盡可能快速安全地恢復正常操作。恢復操作將與系統的災難恢復計畫緊密一致。

IEC 62443 對於回應功能的相關技術為使用數位件事和分析工具，數位鑑識在回應計畫是相當重要的，在事件發生時，使用數位鑑識工具快速分析安全事件類型，提供了事件回應所需的重要資訊。

- **復原**

恢復功能制定和實施適當的安全政策，以保持彈性的計劃，並恢復由於網路安全事件而受損的任何能力或服務到正常運作，以減少網路安全事件的影響。

復原在這幾項安全標準中都是以安全管理政策為主並沒有出現技術相關或者是更詳細的建議跟指導，但災難後的復原計畫的制定以及組織名譽的恢復等恢復計畫也是在網路安全管理中重要的一環。

### 3.5 智慧電網的安全標準與網路安全技術

含有五個合約，分別為以 ERC20 代幣標準所發行的代幣合約、提供代幣閃電貸服務的借在本節，將會介紹有哪些智慧電網相關的安全標準是有對這些與 CSF 核心功能

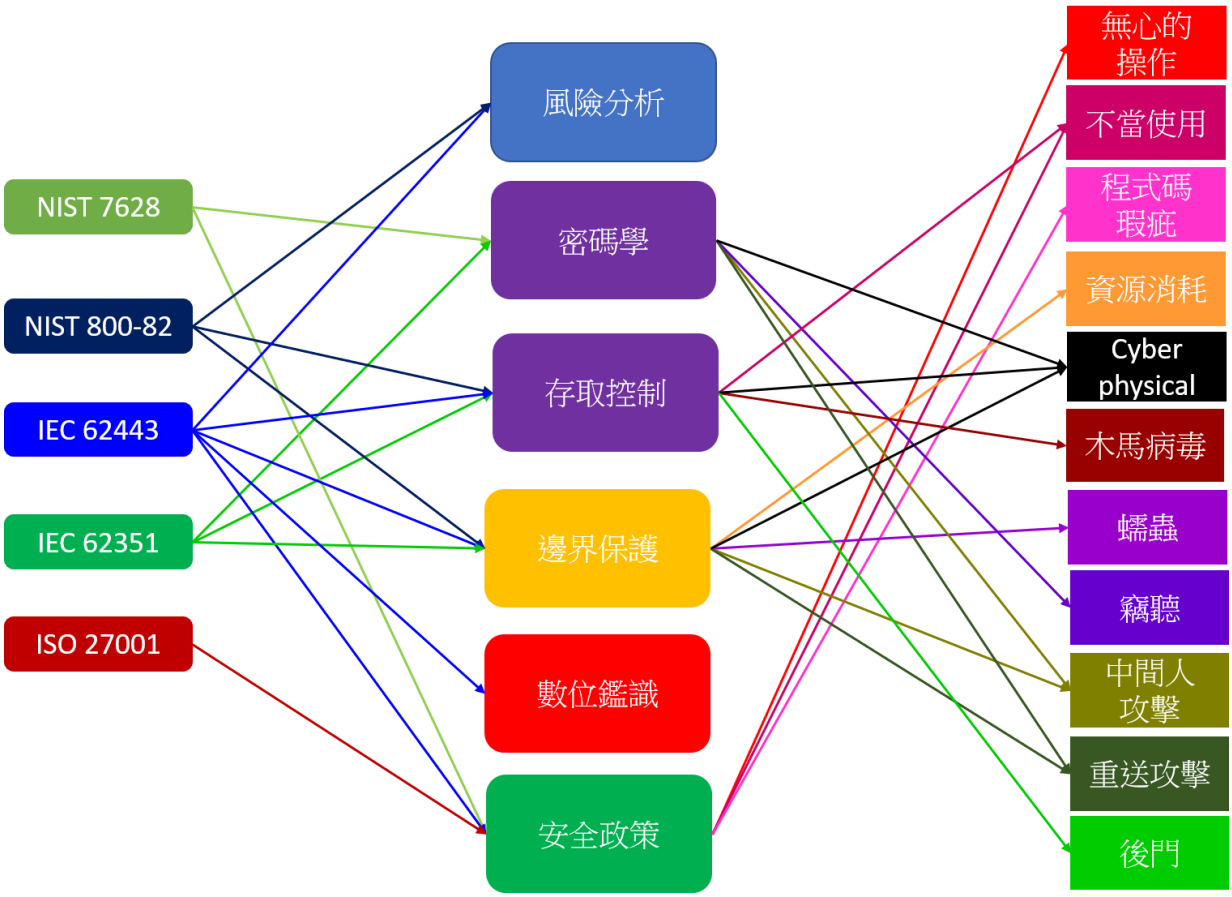


圖 8：智慧電網安全標準與安全技術

對映的技術做詳細的建議及指導以及這些安全技術抵禦了哪些網路攻擊，如圖 8 所示。

- **風險分析**

風險分析是組織建立資訊安全相關政策前，需要做的重要項目之一，透過風險分析的手法降低智慧電網系統的風險。NIST 7628 雖然有風險分析的相關安全控制，但是並無風險分析的詳細說明，但是在 NIST 800-82 中，說明了基於 NIST 800-39 的風險分析方法。首先，組織為了解決如何評估風險、應對風險和監控風險的問題，會先建立風險環境以及風險管理策略，同時也為管理風險制定了風險框架。風險框架建立完成後，就會進行風險分析的步驟，風險分析將會識別對組織的威脅、組織的潛在威脅及發生損害的可能性，接著風險分析所輸出結果是確定風險。接著就是回應風險，根據組織風險框架的資訊來進行風險回應，像是制定相對應的風險替代方案、確定組織的風險承認能力及依據選定的方案實施風險處理措施，監督風險指的是組織監督風險管理流程，並根據風險回應結果假以改善。

IEC 62443-3-2 中，提及了 ICS 系統風險分析的詳細流程[6,25]，風險分析流程在一開始會先識別尚未考慮系統 (System under consideration, SUC) ，所有可以自動化的 ICS 系統，都是屬於 SUC 的範圍，在識別完 SUC 後會進行下一步的網路安全風險分析，藉此識別出風險等級較高的 SUC。進行風險分析後，匯兌 SUC 進行區域的分類，並區分風險高與低的區域，區分後會利用先前風險分析的結果與組織的可容忍風險進行比對，確認該區域是否要繼續進行更詳細的風險分析。比對風險分析的結果後，超過組織風險容忍度的區域將會進行詳細的網路安全風險分析，並在識別其威脅、脆弱性、後果及衝擊之後，透過以上四個要件決定為減緩風險發生的可能性，並為每個區域及管道決定目標的安全等級，以清楚傳達資訊給負責設計、實施、操作和維護網路安全的人員。

- **密碼學**

使用加密的訊息防止了竊聽、中間人攻擊以及重送攻擊等攻擊手段。NIST 7628 與 IEC62351-9 有對於金鑰管理系統詳細指導，IEC 62351 的第三部與第五部則是智慧電網系統加密的詳細指導。

- **存取控制**

存取控制不管是一般的資訊管理系統，或者是工業控制系統，都會有的安全技術，在 NIST 7628 與 IEC 62443-3-1 中有詳細解說存取控制的實施，像是使用 RBAC 方法等，而在 IEC 62351 第八部分則有完整的技術指導，包括在存取控制所使用的 token，以及各個角色的制定。

- **網路隔離**

這裡還包括了對網路相關的安全技術，像是入侵偵測系統與防火牆，這些網路安全技術可以減輕阻斷服務攻擊與蠕蟲等，也可以避免中間人攻擊，重送攻擊等攻擊。

NIST 800-82、IEC 62443-3-1 以及 IEC 62351 中建議將 ICS 與 IT 網路區隔，並設置入侵偵測系統、防火牆等以防止網路安全威脅的發生。IEC62351 第四部份更是規範了網路協定的使用。

- **數位鑑識**

在 IEC62443-3-1 裡，介紹了取證與分析工具，這些工具用來收集網路數據，分析異常的網路流量，數位鑑識工具的功能類似於網路監控工具，因為它們提供企業網路的監控、集中式網路安全管理功能和廣泛的報告能力。不同於網路監控和封包分析工具，因為數位鑑識工具被設計為防禦措施而不是網路管理工具。在數位鑑識應用程式監控流量的同時，它們還從網路安全角度對正常流量進行基準測試，並且可以提供事件回應所需要的關鍵訊息。

- **安全政策**

是組織的重要管理方式之一，透過管理減少人為風險的產生。NIST 7628、IEC 62443 以及 ISO 27001 都有安全控制的方式來制定組織內部的網路安全政策。

### 3.6 總結

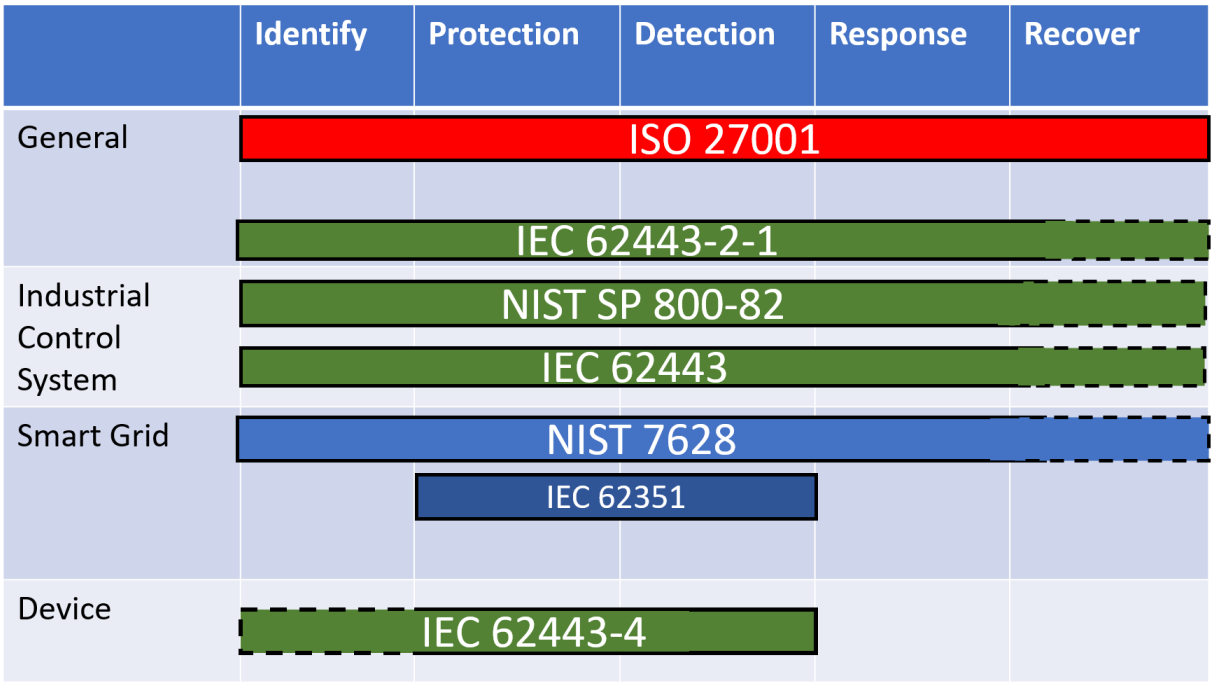


圖 9：智慧電網領域與CSF框架的對映

圖 9 是各項智慧電網與 CSF 框架的對映，部分沒有安全控制措施的標準則是以標準裡的內容來判斷，實線表示該標準內容與該核心項目完全對映，虛線則表示該標準內容與該核心項目部分相符。

在一般的 IT 領域中，通常都是以 ISO 27001 作為標準建立資訊安全管理系統的，因此在建立智慧電網內部 IT 的資訊安全管理系統時，而在 ICS 系統的 IEC 62443-2-1 中，介紹了智慧電網內的資訊安全管理系統的相關安全控制項，但是卻沒有回覆功能相關的安全控制。

IEC 62351 則是為智慧電網通訊安全所制定的相關標準，其內容大部份都與保護功能以及辨識功能有關，像是通訊協定的使用、通訊加密的方法以及存取控制的方法等等。

在智慧電網設備的領域中，IEC 62443-4-1 定義了產品開發的生命週期，IEC 62443-4-2 是制定了製造 ICS 系統相關設備安全要求。

NIST SP 800-82、IEC 62443 以及 NIST 7628 在 CSF 的五大功能中的前面四大功能大致可以從智慧電網的相關標準找到可以使用的安全控制以及相關技術，像是辨識功能內部的風險分析可以在 IEC 62443 以及 NIST SP 800-82 中找到，而在保護功能的加密部分在 NIST 7628 中也有相關說明，辨識及回應功能內 NIST 7628 及 IEC 62443 有相關的詳細的安全控制，IEC 62443 中也有辨識以及回應相關的安全技術。但在復原功能，NIST 800-53、NIST 7628 以及 IEC 62443 都只做到網路安全政策改善相關的控制措施，對於事件發生後的聲譽，公共關係管理，NIST 800-53、NIST 7628 與 IEC 62443 只有少數甚至是沒有相關的控制措施去應對。若是從技術面考量，NIST 7628、IEC 62443 在相關控

制措施都有相當完善的指引甚至有相關技術的指導，但是在事件發生後的復原程序只有 ISO 27001 資安管理標準有較詳盡的控制項。

以建立太陽能發電這種小型分散式發電廠為例，在建造時可以使用 NIST 7628、IEC 62443 以及 NIST 800-82 等標準建立相關安全控制項，就可以達成辨識、保護、偵測以及回應這四項核心功能而在風險分析階段，NIST 800-82 以及 IEC 62443 有風險分析的詳細說明；太陽能發電的相關設備除了有太陽能發電專屬的安全標準之外，IEC 62443-4 也可以作為清點設備時的參考；在發電後即時傳輸發電資訊時需要加密傳輸，此部分在 IEC 62351 中有通訊協定的使用、加密技術以及金鑰管理等等的保護技術；偵測網路威脅時所使用的相關技術在 IEC 62443 以及 NIST 800-82 中有邊界保護、防火牆以及 IPS 等相關技術的指引；事件發生時的回應 NIST 7628、IEC 62443 以及 NIST 800-82 中有回應相關的安全控制項，IEC 62443-3-1 中也有說明可以使用鑑識工具做網路安全事件分析；在事件後的復原部分，NIST 7628 有說明電網及時回復的安全控制，但在組織管理的回復程序上，ISO 27001 反而有比較詳盡的復原政策。

## 肆、結論

智慧電網的發展迅速，但因為智慧電網為國家重要基礎設施，其複雜性與特殊性，帶來了許多資安隱憂，遭受到攻擊所帶來的影響非同小可，因此需要加強智慧電網的安全性，而透過國際制定的安全標準，來加強智慧電網的安全，本篇論文分析了以智慧電網資訊系統為主的資訊安全標準，並利用 NIST CSF 安全框架做安全控制的對映，讓智慧電網相關安全標準可以多方比較，制定一個因地制宜的智慧電網資訊系統。

智慧電網領域相當廣泛，不同領域有著不同的標準，像是發電領域中也有分太陽能發電所使用的安全標準、風力發電所使用的安全標準等，因此未來也可以分析以及比較其他智慧電網領域的安全標準。

## 參考文獻

[1] M.Z. Gunduz and R. Das, “Analysis of cyber-attacks on smart grid applications”, *International Conference on Artificial Intelligence and Data Processing (IDAP)*, pp. 1-5,2018.

[2] M.Z. Gunduz and R. Das , “Cyber-security on smart grid: Threats and potential solutions,” *Computer Networks 169*,2020.

[3] H.He, and J. Yan. “Cyber-Physical Attacks and Defences in the Smart Grid: A Survey,” *IET Cyber-Physical Systems: Theory & Applications, vol. 1*, pp. 13-27,2016.

[4] IEC, *IEC 62443-1-1:Industrial communication networks – Network and system security –Part 1-1: Terminology, concepts and models.* 2009.

[5] IEC , *IEC 62443-3-1:Industrial communication networks – Network and system security –Part 3-1: Security technologies for industrial automation and control systems*. 2009.

[6] IEC, *IEC 62443-3-2:Security for industrial automation and control systems –Part 3-2: Security risk assessment for system design*. 2020.

[7] IEC, *IEC 62443-3-3: Industrial communication networks – Network and system security –Part 3-3: System security requirements and security levels*. 2013.

[8] IEC, *IEC 62443-4-1:Security for industrial automation and control systems –Part 4-1: Secure product development lifecycle requirements*. 2018.

[9] IEC, *Power systems management and associated information exchange –Data and communications security Part 1:Communication network and system security – Introduction to security issues*.2007.

[10] IEC, *Industrial communication networks – Network and system security –Part 3: Security technologies for industrial automation and control systems*.2014.

[11] IEC, *Industrial communication networks – Network and system security–Part 4: Profiles including MMS*.2007.

[12] IEC, *Industrial communication networks – Network and system security–Part 5: Security for IEC 60870-5 and derivatives* .2013.

[13] IEC, *Industrial communication networks – Network and system security–Part 9: Cyber security key management for power system equipment* .2017.

[14] ISO, *ISO27001:Information Security Management*.2013.

[15] R. Leszczyna, "A review of standards with cybersecurity requirements for smart grid," *Comput. Secur*, pp. 22-73.2018.

[16] NIST, *Guidelines for Smart Grid Cybersecurity Vol 1:Smart Grid Cyber Security Strategy, Architecture,and High-Level Requirements* . 2014.

[17] NIST, *Guide to Industrial Control Systems (ICS) Security* .2015.

[18] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*. 2018.

[19] S. -C. Yip, C. Tan, W. -N. Tan, M. -T. Gan, K. Wong and R. C. -W. Phan, "Detection of Energy Theft and Metering Defects in Advanced Metering Infrastructure Using Analytics," *2018 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE)*, pp. 15-22 ,2018.

[20] 台灣電力公司，"513 停電事故初步調查出爐 台電今提出用戶減免 4.7 億元電費方案"，*新聞稿*，台灣電力公司，www.taipower.com.tw/tc/news_info.aspx?id=4520&chk=d7173b40-7289-46ac-82a3-3e46e400c41d&mid=17&param=pn%3d1%26mid%3d17%26key%3d(2021/05/14)。

[21] 林妍溱，”伊朗駭客惡意程式已駭入美國電網、油氣公司”，https://www.ithome.com.tw/news/135276(2020/01/10)。
[22] 行政院原子能委員會委託研究計畫研究報告，“智慧電網總體規劃方案”，2016。
[23] 行政院原子能委員會，“分散式電力系統相關經濟與產業效益分析”，https://www.aec.gov.tw/share/file/information/pb1pdb33lZ3KWBhkxIeP8g__.pdf(2010/11/30)。
[24] 行政院國土安全政策會報，“國家關鍵基礎設施安全防護指導綱要”，2016。
[25] 魏銪志等，“資訊與工控資通安全風險管理機制評估”，Communications_of_the_CCISA，2020，頁 17-33。