國立臺灣大學電機資訊學院電信工程學研究所

碩士論文

Graduate Institute of Communication Engineering
College of Electrical Engineering and Computer Science
National Taiwan University

Master's Thesis

5G導入智慧電網通訊架構及其資安風險研究

The study on 5G architecture and information security framework for smart power grid

史賀文

Ho-Wen Shih

指導教授：周錫增博士

Advisor: Hsi-Tseng Chou, Ph.D.

中華民國113年6月

June, 2024

doi:10.6342/NTU202401322

國立臺灣大學博士學位論文
口試委員會審定書
DOCTORAL DISSERTATION ACCEPTANCE CERTIFICATE
NATIONAL TAIWAN UNIVERSITY

5G導入智慧電網通訊架構及其資安風險研究

（論文中文題目）(Chinese title of Doctoral Dissertation)

The study on 5G architecture and information security framework for smart power grid

（論文英文題目）(English title of Doctoral Dissertation)

本論文係___史賀文_____(姓名)__P08942A06__（學號）在國立臺灣大學電信工程學研究所完成之博士學位論文，於民國_113_年_4_月 17 日承下列考試委員審查通過及口試及格，特此證明。

The undersigned, appointed by the Graduate Institute of Communication Engineering on _17_(date)_4_(month)_2024_(year) have examined a Doctoral Dissertation entitled above presented by_____史賀文____(name)___P08942A06___(student ID) candidate and hereby certify that it is worthy of acceptance.

口試委員 Oral examination committee:

馮燕麟		
（指導教授 Advisor）		
	郭文光	丁建均
		陳伯重

所長 Director: 馮燕麟

doi:10.6342/NTU202401322

中文摘要

隨著科技演進，未來將會有更多的設備連上網路，加速產業往數位化和智慧化方向推進。而電力系統堪稱是最大的物聯網（Internet of Things, IoT），亦有愈來愈多的分散式能源設施併網，新興智慧巡檢技術、科技工安、智慧變電所興起等，都在加速推動電力系統往智慧電網方向發展。在科技不斷演進的背景下，本論文旨在於深入綜合現有文獻，系統整理5G技術的要點，同時研析有關5G導入智慧電網的關鍵要素及其合適之應用架構，作為未來智慧電網實際導入5G通訊網路時之技術支援和決策參考。

本論文亦透過簡易實驗室資安檢測，發現資安可能導致的高風險問題，並提出未來合適導入智慧電網之資安防護架構之方案和建議，朝多元化資安解決方向部署。

最後，經由本研究結果亦發現，未來的智慧電網通訊網路架構應以電力領域實務應用需求為前提，而任何網路攻擊皆可對智慧電網造成影響。基此，本論文提出5G導入智慧電網架構及其資安風險之防護架構，可強化未來智慧電網網路通訊系統架構，並降低資安風險，同時這也是跨領域專業整合應用，包括：電力專業、通訊技術以及資安解決方案等，希冀經由本研究跨出第一步，提供未來所需之重要研究參考。

關鍵字：5G、智慧電網、資訊安全、時間同步、3GPP

doi:10.6342/NTU202401322

Abstract

With the evolution of technology, more devices are expected to connect to the internet, accelerating the digitization and smartification of industries. The power system, being the largest Internet of Things （IoT）, witnesses an increasing integration of distributed energy facilities. Emerging technologies such as smart inspection, technological safety, and the rise of smart substations are all contributing to the rapid advancement of the power system towards a smart grid. Against the backdrop of continuous technological evolution, this thesis aims to comprehensively review existing literature, systematically organize key points of 5G technology, and concurrently analyze crucial elements related to the integration of 5G into smart grids. This information serves as a technological support and decision reference for the actual implementation of 5G communication networks in future smart grids.

The thesis also conducts a simple laboratory cybersecurity assessment, identifying high-risk issues that could arise from cybersecurity vulnerabilities. It proposes solutions and recommendations for a cybersecurity protection framework suitable for the future implementation of smart grids, emphasizing a diversified approach to cybersecurity solutions.

Finally, through the research findings, it is observed that the future architecture of smart grid communication networks should be based on practical applications in the power domain. It is highlighted that any network attack could potentially impact smart

doi:10.6342/NTU202401322

grids. Consequently, the thesis proposes an architecture for the integration of 5G into smart grids and a corresponding cybersecurity protection framework. This framework aims to strengthen the future smart grid communication system architecture, reduce cybersecurity risks, and represents an interdisciplinary integration of expertise, including power engineering, communication technology, and cybersecurity solutions. The hope is that this research takes a significant step forward, providing essential research references for future needs.

Index Terms — 5G, Smart Grid, 3GPP, Information Security, Time Synchronization

doi:10.6342/NTU202401322

目次

doi:10.6342/NTU202401322

doi:10.6342/NTU202401322

圖次

doi:10.6342/NTU202401322

doi:10.6342/NTU202401322

表次

doi:10.6342/NTU202401322

Chapter 1 緒論

1.1 研究背景

因應國際發展趨勢，電力網路逐漸從以人力操作及類比訊號為主的傳統電網，轉變成為自動且數位化的智慧電網，在這個數位化與智慧化演進的過程中，許多電力公司開始導入新的科技應用，例如：AR巡檢（Augmented Reality, AR）、無人機巡檢、電廠工地CCTV監視（Closed-Circuit Television, CCTV）、AI門禁人臉辨識（Artificial Intelligence, AI）等。而新的科技也意味者新興通訊技術和架構的導入；與此同時，資訊安全的考量及其重要性，亦躍然紙上，成為伴隨而來的重要課題。

此外，隨者5G通訊的興起，國際上也有愈來愈多不同國家的電力公司，開始將5G導入智慧電網中應用。如：5G無人機巡檢，可透過高清晰影像，確認再生能源裝置是否有外觀上的破損或是傾斜等異常狀況發生；又或者是偏遠電廠或是再生能源案場，因地形或是場域特殊的限制，使用5G無線技術進行發電資料即時傳輸。

再者，因應電信業者推出5G專網服務方案，令5G導入智慧電網之相關研究隨之興盛，且陸續有愈來愈多實際應用案例可供參考，衡諸我國政府目前積極推動電網強韌計畫，可以預估未來結合5G導入智慧電網，智慧電網加上無線通訊技術應用的效益，未來將可進一步強化電網的韌性及數位化涵蓋的完整性。

不過，從另個面向來看，智慧電網借重數位化及智慧化技術，雖然提高了電網韌性，但隨之而來的資安風險也逐次提高，國際上各種電力公司遭遇資安攻擊事件層出不窮，即是顯可易見，如2020年6月，巴西電力公司遭到勒索軟體攻擊，勒索1400萬美元[1]；如2019年9月，印度核電公司遭受北韓駭客組織開發的惡意軟體入侵[2]；又如同年美國sPower電力供應商遭受典型的DoS攻擊事件等，均能

doi:10.6342/NTU202401322

造成電力公司鉅大損失[3]。

有鑑於此，本論文除了研究5G導入台灣智慧電網的可行性及其效益，也研究其中可能潛藏的資安風險。智慧電網是國家重要的關鍵基礎建設，關係到民眾的生活日常，也關係到國家整體的安全，是故智慧電網的資訊安全，尤其影響深遠更需要特別加以重視。

doi:10.6342/NTU202401322

1.2 研究動機

隨者國家推行電網強韌政策以及國際趨勢的走向，5G未來有望導入台灣智慧電網系統中，加上電廠有許多實體線路無法到達的場域，因此無線通訊技術的導入，對於電力領域和智慧電網未來的應用來說是可行的選項之一。此外，隨著數位化和智慧化的推動，對智慧電網來說穩定及安全是首要考量，是故未來智慧電網導入 5G 通訊系統前，需先研究5G特性及其傳輸技術，並瞭解智慧電網無線應用，確保5G無線通訊技術可以與智慧電網順利銜接應用。

本研究旨在於針對未來台灣智慧電網導入5G之網路架構進行研析，另根據未來可能出現的資訊安風險亦進一步納入本研究中一併進行相關實驗，最後提出可能資安解決方案和建議，提供相關決策支援，確保5G網路未來導入時，智慧電網可以提升數位化和智慧化的效能，同時亦保有穩定及安全。

doi:10.6342/NTU202401322

1.3 本論文預期效益

本論文首先針對5G技術進行分析，瞭解5G網路整體系統架構，之後分析電網中的通訊以及國際上的案例，檢視電網實際導入和應用之概況，並參照我國電力系統之需，從中構想出未來5G智慧電網的網路架構，同時進一步探討其中可能潛藏的資安風險，並針對資安風險進行評估與測試，最後提出可行的資安解決方案供參考。

本論文深入研究5G應用發展趨勢，評估5G通訊的可行架構，5G用於智慧電網的可行性探討，及其針對未來可能潛藏資訊安全之影響進行評估，係本論文主要的研究架構。

綜觀本論文之研究旨趣，本論文預期可收穫的效益茲羅列如下：

- 瞭解5G技術以及電網導入5G網路之國際應用趨勢。
- 為台灣電力系統評估分析5G網路導入的可行性。
- 提供一個未來台灣智慧電網導入5G網路之通訊架構合適之參考模式。
- 探討其中潛藏的資安風險並進行實驗室評估與測試，提供參考解決方案與建議。

doi:10.6342/NTU202401322

1.4 論文章節架構安排

本論文首先講述5G技術及系統，同時列舉國際電網導入5G的實踐案例，接著分析台灣現有電網基礎架構與通訊技術，瞭解通訊相關需求及5G帶來效益，並規劃出未來5G通訊的參考架構；在此基礎上，並進一步探討5G通訊可能存在的資安風險，進行測試與實驗。最後，本論文提出未來可能參考的解決方案與建議，並針對後續研究方向提供未來研究展望。

具體而言，本論文第一章為緒論，針對研究背景、研究動機、研究預期效益，提出說明。第二章研析國際電網導入5G之應用案例，包括探討5G技術與5G系統、5G核心網路與封包傳輸，過即上實際應用案例及其所發揮的效益等。第三章提出台灣智慧電網導入5G網路未來可行的應用架構及其未來可能潛藏的資安風險。第四章針對智慧電網導入5G網路可能潛藏的資安風險進行實驗室的檢測與評估，據而提出可能的防護架構和解決方案。第五章結論與建議，並提出未來研究相關展望。

doi:10.6342/NTU202401322

Chapter 2 電網導入 5G 技術國際應用案例

2.1 5G 技術與 5G 系統

因應未來日益複雜的數位轉型和IoT技術之需求，當前全球通信業者刻正積極推動5G技術的應用俾能提供高頻寬、連接和低延遲的無線網路基礎設施。此趨勢不僅賦予過去需依賴大規模人力處理的勞務以各式創新的可能性，同時使得諸多自動化服務應用，諸如自駕車、無人機以及人工智慧等技術，得以逐漸實現。與此同時，傳統電網也在這股潮流中汲取數位化和智慧化的養分，逐次轉變為智慧電網。

在智慧電網下，大量接入智慧裝置支應用以提高電網控制能力，進而提升電網韌性；然而，其所帶來的龐大通訊需求，同時也衍生了對於電網既有通訊方式造成的衝擊和影響。過往，電力系統主要透過光纖等固網方式來滿足通訊系統上的穩定需求，然而，隨著電網數位化與智慧化的需求不斷提升，後加上再生能源案場的推動和分散式能源的興起，傳統固網通訊系統逐漸顯露出其不足之處，而對於無線通訊及新興的5G技術之需求，則是同時大大的提升。

有鑑於此，本節首先深入探討3GPP國際標準[4]所提出的5G通信技術。考量5G在高需求場域的卓越特性，本論文主要著重於分析5G通信技術在電力系統中的具體應用和可行性，期望能為智慧電網的進一步發展提供所需之堅實的通訊網路基礎和實用支持。

在5G通信技術的制定中，國際電信聯盟（ITU）提出了三個主要項目，包括高頻寬大連結與低延遲，茲分述如下：

- 增強型行動寬頻：

  （Enhanced Mobile Broadband, eMBB）

  5G所使用的高頻段相對於4G，使其能夠提供更快的連接速度和更大

doi:10.6342/NTU202401322

的傳輸量。這對未來高頻寬應用，例如AR/VR（Virtual reality, VR）及AI辨識，提供了相當強大的支持。

- 大規模機器類型通訊：

  （Massive Machine Type Communications, mMTC）

  mMTC的特點在於設計針對大量連線，著重於低功率和少量傳輸的通訊方式。在未來人口高密度的城市中，這將扮演關鍵角色，以因應大量設備的連接需求。

- 超可靠低延遲通訊：

  （Ultra-reliable and Low Latency Communications, uRLLC）

  5G通訊的傳送延遲時間約為1毫秒，非常適用於需要實現不間斷資料交換的關鍵任務設備。這項技術將廣泛應用於車聯網和無人機技術，提供毫秒等級的低延遲無線通訊。

相對於其他無線通訊技術，5G以其eMBB、mMTC和uRLLC等特性脫穎而出。因此，國際上已經開始探討如何在電力領域中運用5G技術，包括再生能源和發電廠的各個階段，從輸電電網、配電電網、電塔，一直到用戶端的各種用電設備，如電表等。這些應用領域涉及能源管理、分析、監控、封包傳輸，甚至包括都會城市的監視器、路燈、電動車及充電樁等設備，皆可透過5G無線通訊技術進行連接。5G如何融入電力公司的發、輸、配、售各種服務，亦將是未來強化電網韌性的一項關鍵技術。

基於3GPP的國際標準規範，5G NR（New Radio, NR）技術的研究於2015年啟動，並於2017年底制定首份標準。在3GPP標準化過程進行之際，學界與產業界積極致力於實施遵循標準草案的基礎設施。首個大規模商用的5G NR規範於2018年底正式面世。

5G 目前使用兩個頻率，如下所示：

- 頻率範圍1（FR1），適用於410 MHz ～ 7125 MHz範圍內的頻段

doi:10.6342/NTU202401322

- 頻率範圍2（FR2），適用於24250 MHz ～ 71000 MHz範圍內的頻段

於2018年，3GPP發佈了Release 15，該版本包含了5G NR第一階段的標準化內容。Release 16則被制定為5G的第二階段，釋放日期定於2020年3月，完成日期則為2020年6月。原本，Release 17預計於2021年9月問世，然而，由於COVID-19大流行的影響，Release 17的發布時間被重新安排至2022年6月。

目前，3GPP已啟動了Release 18版本的工作。Release 18被冠以NR Advanced的稱號，象徵著無線通訊系統的又一重要里程碑。NR Advanced將納入擴展實境、人工智慧/機器學習研究以及移動性增強等功能。移動性一直是3GPP技術的核心，迄今為止主要在第3層層面進行處理。然而，在Release 18中，移動性相關的工作將引入更低層的觸發機制。

此外，頻譜可以在 4G LTE和5G NR之間動態共用幾個特點，如下所述：

- 動態頻譜共享

  為了更有效地運用現有資產，電信商會選擇在4G LTE和5G NR之間進行動態頻譜資產共享的策略。隨著時間的推移，頻譜在這兩代行動網路之間實現複用，同時滿足4G LTE網路用戶需求。動態頻譜共享的部署可以在現有的4G LTE設備上實現，它也與5G NR相容。這種靈活的共享模式為運營商提供了更大的彈性，以平衡現有資源的使用和5G技術的逐漸推進。

- 非獨立模式（Non-Standalone, NSA）

  5G NR的NSA是指一種特定的5G NR部署選擇，其特點在於其控制平面的實現於現有4G LTE網路，5G NR僅專注於用戶資料平面。這種模式被是一種過渡性的策略，是為了在現有基礎設施的基礎上引入5G技術，以加速5G網路的部署而設計通訊架構。

- 獨立模式（Standalone, SA）

  5G NR的SA指的是利用僅使用5G進行訊號和訊息的傳輸。這種模式包

doi:10.6342/NTU202401322

括全新的5G分組核心架構，而不在依賴4G的核心網路，使得5G能夠在沒有LTE的情況下獨立運作。此模式預計具有較低的成本、更高的效率，並有助於新應用案例的發展。

doi:10.6342/NTU202401322

2.2 5G 核心網路與封包傳輸

5G技術的關鍵之一在於其採用模組化和雲端架構，徹底改變了核心網路的設計。新一代的網路結構遠離傳統的4G電信架構，而是朝向基於服務的結構（Service Based Architecture, SBA）邁進。SBA透過網路通訊協定實現各組件之間的高效溝通，特別仰賴網際網路協定層（Internet Protocol, IP）確保核心網路實體間的順暢通信，同時促成IP層與更高協議層（傳輸和應用層）之間的協調運作。

為提高網路系統的模組化程度，5G引入了SBA，容許網路功能 （Network Function, NF） 透過服務介面實現相互通信，使得每個NF能夠更細緻且專業化地提供功能。相較於傳統的4G系統架構演進（System Architecture Evolution, SAE），5G SBA更進一步將各項功能進行細分。以用戶伺服器 （Home Subscriber Server, HSS） 為例，被拆分為接取管理功能（Access and Mobility Management Function, AMF）、統一資料管理功能（Unified Data Management, UDM），而行動管理實體 （Mobility Management Entity, MME） 也被拆分加入到AMF和連結管理功能（Session Management Function , SMF）。這樣的改變有助於使得任何第三方應用程式能輕鬆接入5G網路，進一步提升系統的靈活性和擴展性。

在3GPP標準中，應用程序功能被稱為應用功能（Application Function, AF），任何連線均需以安全的方式與5G NF進行互動通信。網路暴露功能 （Network Exposure Function, NEF） 位於AF與外部通信之間，充當著重要的中介角色。例如，AF並非直接訂閱AMF事件，而是在事件發生時，AMF通知NEF，NEF的訂閱功能再通知AF。此種機制確保了系統中各個模塊之間的有效溝通和資訊傳遞，同時保障通信的安全性。

在5G網路環境下，各功能模組具備以下關鍵功能[5]：

I. 接取管理功能（AMF）：

- UE進入行動網路連線管理：

doi:10.6342/NTU202401322

- 包含對UE的進入管理，以及行動網路連線的建立、修改、和釋放等過程的有效管理。
- 用戶身分驗證註冊管理：
- 負責處理和管理用戶身分的驗證程序，同時管理用戶的註冊相關事宜。
- gNB間移動交遞管理：
- gNB之間的移動交換，以確保無縫的用戶移動體驗。
- 非存取層信令的加密和完整性保護：
- 對於非存取層的通信信令進行加密和完整性保護，以確保通信的隱私和安全性。
- 緊急電話定位服務管理：
- 管理與緊急電話相關的定位服務，確保在緊急情況下能夠精確定位用戶位置。

II. 連結管理功能（SMF）：

- UE連結管理，涵蓋連結的建立、修改和釋放等方面。
- 用戶面安全策略管理，負責管理用戶面的安全性策略。
- 動態主機設定協定

  （Dynamic Host Configuration Protocol, DHCP），處理動態主機設定協定，提供UE所需的IP地址等設定。
- 位址解析協定 （Address Resolution Protocol, ARP），負責處理位址解析，實現IP地址與MAC地址之間的映射。
- UPF的流量控制，有效管理和控制用戶面功能的數據流量。
- 提供連結和服務連續性模式

  （Session and Service Continuity Mode, SSC），確保連結和服務在不同模式下的持續性。

doi:10.6342/NTU202401322

- 支援不同類型連結：支援多樣化的連結類型。
- 收集UPF的計費數據介面資料：蒐集UPF的計費數據，用於計費和監控。

III. 認證服務功能（AUSF）：

- 決定是否進行UE的認證。
- 使用5G認證和密鑰管理的「5G 密鑰機制」（5G-Authentication and Key Agreement, 5G-AKA）或可擴展身分驗證協議、身分驗證和密鑰管理的「可延伸驗證通訊協定」(Extensible Authentication Protocol, EAP）。

IV. 統一資料管理功能（UDM）：

- 承載和管理相關數據。
- 包括身分認證憑證和用戶資料儲存庫。
- 處理功能（ Authentication Credential Repository and Processing Function, ARPF）。

V. 網路切片選擇功能（NSSF）：

- 選擇適用於UE服務的網路切片實例。
- 確定允許的網路切片選擇輔助資訊（NSSAI）。
- 確定用於服務UE的AMF集合。

VI. 策略控制功能（PCF）：

- 支援統一的策略框架，提供給控制平面（CP）功能策略規則。
- UDR中的策略決策的訂閱資訊。

VII. 用戶平面功能 （User plane Function, UPF）：

- 負責UE上網連線。
- 處理資料的路由與轉發。

doi:10.6342/NTU202401322

- 執行資料封包檢查。
- 進行用戶面的流量監控與服務品質（Quality of Service, QoS）管理。
- 管理與外部資料網路的連接。
- 處理用戶面部分的策略規則管理等功能。

以上模組的合作協同確保了5G網路中的安全性、網路切片的適切配置、策略的有效控制，以及用戶面功能的高效執行。這樣的架構不僅提供了更彈性的網路服務，也確保了資料的安全性和用戶體驗的優良品質。

下圖1中N1使用NAS Protocol，N1介面是UE到AMF的透明介面，用於將UE資訊傳輸到AMF，類似於4G中的NAS將資訊從UE傳送到核心網路，而不是專用於無線網路的存取層。

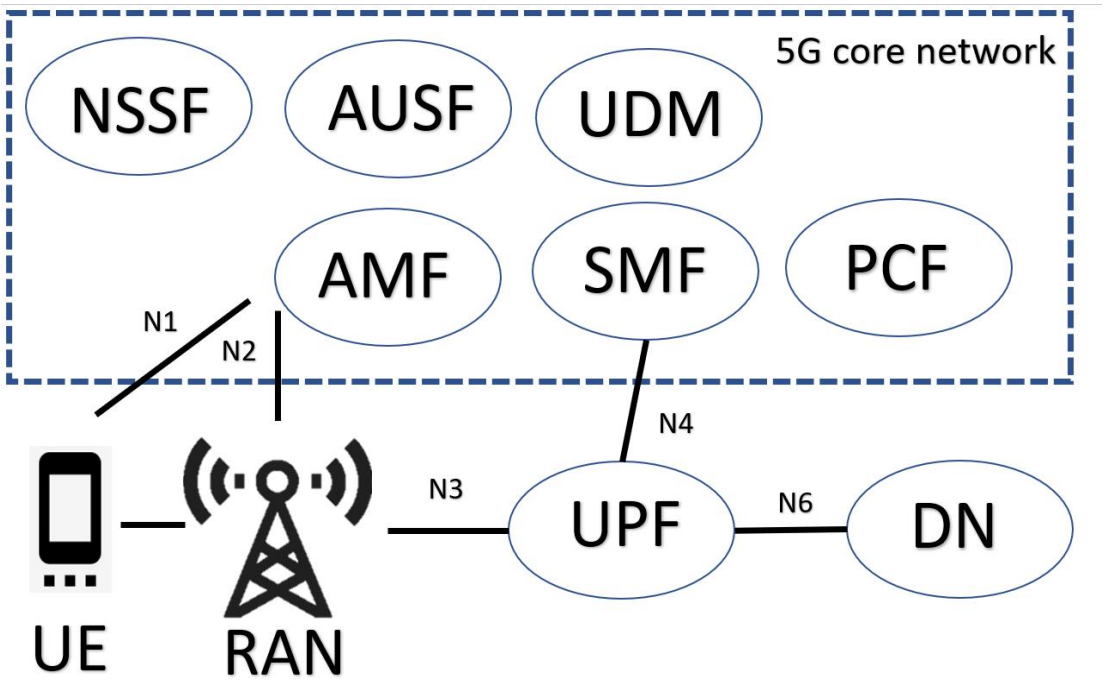

圖 1　5G 核心網路架構

N2使用NGAP Protocol，N2將RAN連接到存取和AMF。控制平面和用戶平面分離，將控制訊號與使用者會話流量解耦，支援邊緣運算和更分散的網路架構的引入。因此，N2至關重要，因為在存取服務之前UE必須連接到網路。雖然會話控制現在由新的會話管理功能處理，但UE上下行流量由AMF負責，故在啟動任

doi:10.6342/NTU202401322

何流量或連線之前，需要考慮UE上下文、位置等。

N3使用GTP-I Protocol，N3是5G RAN與UPF之間的接口，主要用於傳送上下行用戶數據。N4使用 PFCP Protocol，N4是SMF與UPF之間的接口，主要用於傳送SMF和UPF控制訊息。N6是UPF與DN（Data Network）的接口，用於傳送用戶上下行數據接口，是一種基於IP和路由協議的通訊網路。

在5G封包傳輸中，時間被分為一系列的Frames，而每個Frame的時間間隔為10毫秒。每個Frame進一步被切割為多個Slots，而每個slot包含14個Symbol。在1毫秒內，Slot的數量取決於所使用的子載波的頻寬。可以使用以下方式計算：

表 1　Solt 與頻段的關係

SCS	N Slot Symb	N Frame Slot	N Sub Farme Slot
15KHz	14	10	1
30KHz	14	20	2
60KHz	14	40	4
120KHz	14	80	8
240KHz	14	160	16

這種時間分割的方式確保了在不同頻寬條件下，slot的數量能夠被合理且有效地分配。在5G的封包傳輸中，考慮到uRLLC的使用場景，為了追求低延遲，使用配置較大的子載波間隔，以降低每個Slot的時間，進而滿足低延遲的需求。這種靈活的配置提供了對不同應用場景的適應性，尤其是對可靠性和傳輸延遲要求較高的應用來說是不可或缺的技術之一。

在每個slot中，有三種不同的傳輸方式，包括：Downlink、Uplink和Flexible等。這種靈活性使得5G NR相對於4G LTE更加具有適應性，能夠支援上下行傳輸的動態變化，這是一種有力的工具，可以有效地調整傳輸方式，以滿足不同應用的需求。此外，5G NR使用分時雙工（Time Division Duplexing, TDD）技術，這種技術通過時間的分割來實現資料的傳送。對於TDD配置，通常業者會使用7:3的比例，這表示時間被劃分為上行和下行的比例為7:3。然而，這也帶來了對時間

doi:10.6342/NTU202401322

同步的高要求，需要精準到±1.5微秒。如果時間同步的誤差超過這個範圍，可能導致訊號無法正確解析，甚至在極端情況下可能對附近使用相同頻率的基地台產生干擾。因此，確保高精度的時間同步是TDD正常運作的關鍵[6]。

表 2　業者 7:3 上下行傳輸表

Frame	0									
Subframe	0	1	2	3	4	5	6	7	8	9
Slot	slot 0	slot 1	slot 2	slot 3	slot 4	slot 5	slot 6	slot 7	slot 8	slot 9
	D	D	D	F	U	D	D	F	U	U

在探討 5G 的無線通訊方面時，亦須同時考慮到實體封包傳輸部分，而這就是軟體定義網路（Software Defined Networking, SDN）技術發揮作用的地方。5G 和 SDN 之間存在緊密而有機的相互關係，兩者相輔相成，為整個網路架構的革新和優化提供了有力的推動。以下是此二者之間主要的相互影響和關係：

- 網路靈活性和彈性：

  5G和SDN都致力於提高網路的靈活性和彈性。5G通信技術通過支援不同類型的應用和服務，以及提供更高的頻寬和低延遲，實現了網路的高度靈活性。同時，SDN通過將網路控制層和數據傳輸層分離，使網路能夠更靈活地適應不同的需求，提高了整體的網路彈性。

- 智慧網路管理：

  SDN引入了集中式的網路控制，使網路管理更加智慧化和集中化。5G通信網路也採用智慧化的元件，如自適應調制和編碼和智慧天線技術，以提供更好的連接性和性能。

- 網路切片：

  5G引入了網路切片的概念，允許在同一基礎設施上同時支援多種應用和服務。SDN技術可以在不同網路切片之間實現有效的管理和資源分配。

- 資源優化：

  SDN通過動態資源分配和優化網路流量，提高了整體效能。5G同樣透過

doi:10.6342/NTU202401322

智慧的資源管理，使得網路能夠更有效地應對不斷變化的需求。

總體而言，5G和SDN的結合可以實現更靈活、智慧、高效的網路架構，適應各種不同的應用場景和服務需求。这樣的整合有助於提供更好的用戶體驗，同時提高網路的可管理性和效能。在智慧電網系統中，如導入SDN技術，SDN擁有廣泛的應用潛力。它不僅提高了網路使用效率和QoS，還賦予整個網路更大的靈活性。SDN使網路管理員能夠透過GUI和SDN自動化腳本快速配置、管理、保護和優化整個網路資源。

本節深入研究了5G核心網路和封包傳輸，並試圖將其成功整合至智慧電網。然而，為了更全面地瞭解其在電力系統中的應用，有必要進一步探討5G是否已被成功導入與電力系統相關的國際案例。

doi:10.6342/NTU202401322

2.3 電網導入 5G 國際應用案例

根據3GPP-TR22.867技術文件資料顯示，電力系統導入5G網路主要可成就共有24項大項的應用[7]，詳如表3。

表 3　3GPP-TR22.867 應用案例

應用案例	
1	分佈式儲能
2	智慧型電表
3	分佈式饋線自動化
4	配電網線路電流差動保護
5	用於傳輸加密數據的智慧能源差異化 QoS
6	公用事業通信服務部署的服務壽命
7	智慧能源連接的遠程 DSO 管理 （Distribution System Operator, DSO） 配電系統運營商
8	智慧配電變壓器終端
9	能源應用的隔離需求
10	公用事業端到端安全
11	QoS 監控和報告機制
12	配電智慧 –FLISR（故障定位、隔離和服務恢復）
13	5GS 支持廣域智慧電網中的同步相量
14	變電站監控
15	分佈式能源和微電網
16	保護分佈式能源和電網互聯
17	智慧能源中的公用事業服務運營商 M2M 服務管理平台
18	協調能源回收用例
19	IEC 61850-9-2 採樣值的應用 （多了 KPI ）
20	配電網狀態估計服務用例
21	配電網電控服務用例
22	在緊急情況下確保不間斷 MTC 服務可用性的用例
23	邊緣雲驅動數據採集（edgePMU）
24	配電網負荷及發電量預測服務用例

doi:10.6342/NTU202401322

在5G導入電網在國際應用案例中，最顯著的應用，包括：中國電信、南方電網、國家電網和華為，均已啟動3GPP的5G智慧電網項目[8]。自2018年開始，南方電網便開始嘗試導入5G技術至其電網系統，並在實驗網中應用了5G無線切片技術。此外，基於R16標準的時間同步機制也已在電網中得以應用。

另外，挪威智慧電網中心，亦開始將5G切片技術用於智慧電網中，用於控制電網中設備，例如電動車、智慧家電等[9]。

葡萄牙的機電公司則是在5G智慧電網自我修復的使用案例中展現了新的應用，這種應用採用5G行動網路，以支援公用事業管理範圍內的通訊，並且無需修改現有的通訊框架，使得在電力系統中幾乎任何地方都可以進行部署[10]。

在SliceNet專案中，葡萄牙電信創新公司（Altice Labs, ALB）和葡萄牙能源公司EFACEC攜手合作，在葡萄牙共同部署這個5G智慧電網自我修復的實例。ALB的5G SliceNet基礎設施將與EFACEC的智慧電網硬體/軟體組件整合，並完成實務上的展示應用。

而值得注意的是，等待時間在這個應用中變得極為重要。在電力系統保護中，開關設備的管理對通訊提出了嚴格的等待時間和時延要求，但現有的通訊基礎設施難以滿足這些需求。此外，為了在使用公共網路支援電力基礎設施管理通信時獲得系統營運商的信心，必須透過共享網路以交換關鍵數據。

而在印度，對5G技術在智慧電網領域的研究亦日漸受到關注，相關的研究項目包括如下[11]：

- 智慧電網實施：

  研究如何實施智慧電網技術，以提升電網的效能和可靠性。

- 智慧電能計量：

  探討5G技術在電能計量方面的應用，以實現更準確的能源監測和管理。

- 需求響應 場景：

  研究在需求響應場景中，5G如何應用於實現更靈活和高效的能源管理。

doi:10.6342/NTU202401322

- 能源工廠遠端現場檢查：

  探討5G在遠端現場檢查方面的應用，以提高能源工廠的運營效能。

- 5G在能源工廠推送視訊進行服務：

  研究如何利用5G技術實現能源工廠內視訊服務的高效推送。

- 使用5G和人工智慧進行預測維護：

  研究5G結合AI和ML的應用，以實現對電網設備的預測性維護。

- 5G支援延展實境（Extended reality, XR）：

  探討5G如何支援AR、VR和MR應用，以提升電網運營的可視化和操作性。

- 5G低延遲調變解調器用於控制等關鍵任務使用案例：

  研究5G低延遲調變解調器在電網控制等關鍵任務中的應用，以確保高度可靠的通信和控制。

上述這些應用項目旨在於充分發揮5G技術的優勢，並將其應用於智慧電網的各實務領域，以實現更現代化、高效和可持續的能源基礎設施。

doi:10.6342/NTU202401322

2.4 小結

本章節深入解析5G通訊的基本技術原理和關鍵技術，同時闡述了國際上應用5G導入電力系統之趨勢和應用案例，從中亦勾勒出電網對於5G服務之需求所在。 接下來，下一章則進一步研析台灣智慧電網對於導入5G的可行架構和網路應用模式，以確定5G通信技術能夠用在能源領域上發揮關鍵的效用。

台灣電力系統目前逐步轉型成為智慧電網，已經開始採用大量智慧裝置，如智慧電表等，與5G大連結特性相符。智慧電網也導入即時監控系統，未來還會加入AI和ML的應用，其目的是為了實現對電網設備的預測性發電及維護，需要傳輸大量數據，與5G高頻寬特性相符。智慧電網中也使用了大量調器在電網控制等應用，其目的是確保高度可靠的通信和控制，與5G低延遲高可靠特性相符。

從上述資料整理可知，5G可協助智慧電網導入無線通訊端的應用，並符合智慧電網的通訊標準需求。在5G的協助下，可讓未來的智慧電網通訊更完整。

doi:10.6342/NTU202401322

Chapter 3 台灣智慧電網導入 5G 技術可行架構

3.1 台灣智慧電網發展歷程

電力系統內涵蓋多元應用，過往近20年台灣電網推動自動化歷程，主要以發展（Distributed Network Protocol 3, DNP3），搭配PLC（Programmable Logic Controller, PLC）可程式化邏輯控制，和RTU（Remote Terminal Unit, RTU）遠端終端裝置，構成電力系統遠端調控，保護電驛和數據資料蒐集分析等電網自動化控制藍圖。及至2017年始，隨者我國經濟部推動智慧電網新的總體方案，特別羅列「資通訊基礎建設」作為智慧電網線體架構的支撐，其中規範電網的資通訊標準接軌國際電網之發展趨勢，由原來的DNP3.0標準推動國家電網新標準IEC 61850標準。

至此，IEC 61850標準在標檢局的主政下，逐年按照我國電網發展之需求，建立國家的標準，由台電在新舊交替的過程中，逐年推動應用。電網中IEC 61850涵蓋範圍相當廣泛如下圖2所示。

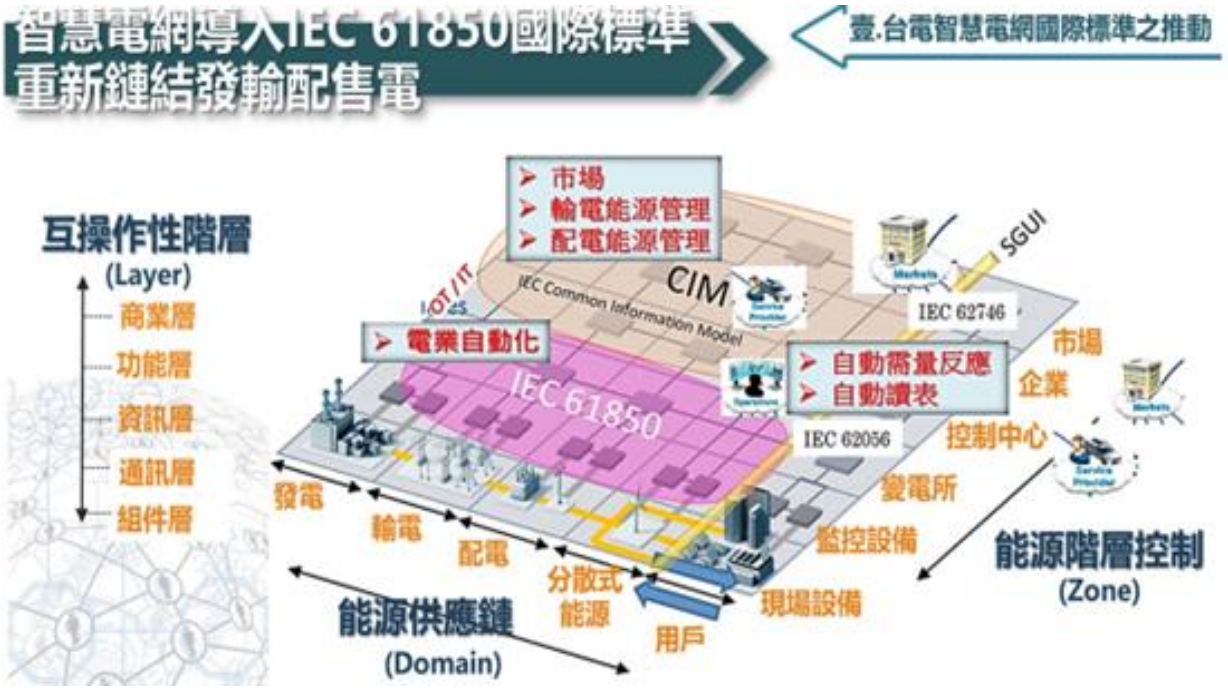

圖 2　智慧電網導入IEC 61850 [12]

doi:10.6342/NTU202401322

其包括原有的能源供應鏈，如發電、輸電、配電、分散式能源、一般用戶，也包括了能源階層控制，如市場、企業、控制中心、變電所、監控設備、現場設備。還有護操作性階層，如商業層、功能層、資訊層、通訊層、組件層。

而標檢局凱定的IEC 61850智慧電網架構，範圍更細緻規畫涵蓋16個區域，詳如圖3所示。

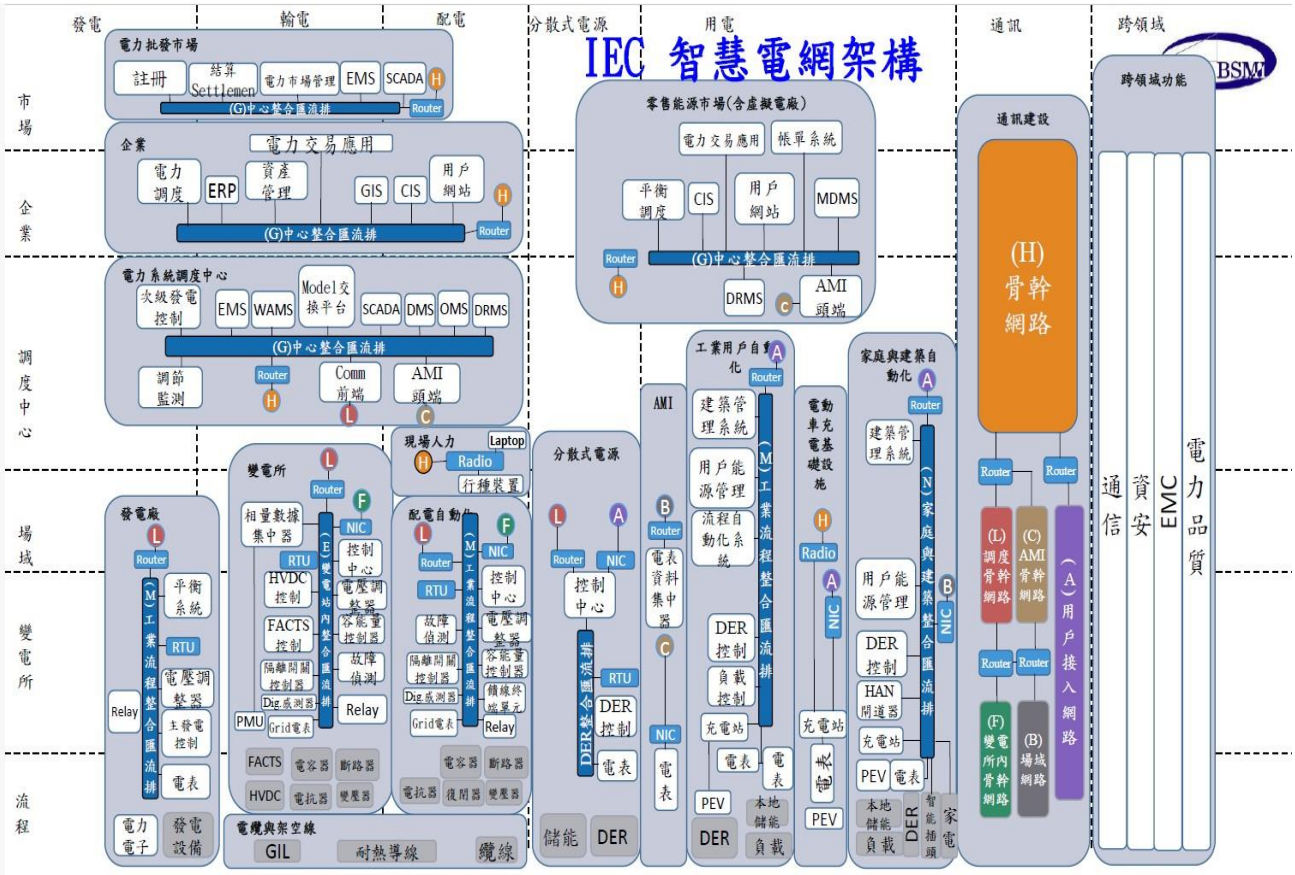

圖 3　IEC 智慧電網架構[13]

此16個區塊其中包括：電力批發市場、企業、電力系統調度中心、發電廠、變電所、電纜與架空線、現場人力、配電自動化、分散式電元、零售能源市場（含虛擬電廠）、AMI（Advanced Metering Infrastructure, AMI）、工業用戶自動化、電動車充電基礎設施、家庭與建築自動化、通訊建設、跨領域功能。

未來整體電網透過IEC 61850標準之導入，除與國際電網之數位化、智慧化發展趨勢接軌之外，透過IEC 61850資料格式統一建模的方式，將使得端到端的資料互通達成一致。傳輸延遲的規定相當細緻，範疇適用於保護電驛自最低小於1毫秒，或適用於變電站間通信至最高1000毫秒以上，反映不同應用等級對通信

doi:10.6342/NTU202401322

性能之多元需求。

然而，雖然不同應用展現出特殊需求，由於對電力品質與電網強韌性的嚴格考慮，目前仍普遍傾向於光纖傳輸技術為主。此種選擇係基於光纖技術所具備之高度穩定性與可靠性。伴隨時代推移、各領域需求的動態演變以及科技持續進步，眾多業者與學術研究者積極投入對電力系統無線通訊技術的深入研究。這種趨勢不僅體現對更具彈性通信方案的迫切需求，同時旨在因應多變的場域需求，並提升整體系統效能。

根據國際研究，目前新型變電所有使用GOOSE （Generic Object Oriented Substation Event, Goose）、SV（Sampled Values, SV）、PTP（Precision Time Protocol, PTP）、MMS（Manufacturing Message Specification, MMS）等封包，台灣則還有使用DNP3.0及XMPP（Extensible Messaging and Presence Protocol）等封包[14]。其標準對應需求表格整理如下：

表 4　IEC 61850 標準通訊傳輸要求

協定	通訊架構	優先度	應用	傳輸時間等級	封包大小	封包/秒	吞吐量
GOOSE	ETH（multicast）	High	保護電驛	TT5* 10ms	100-200 bytes	random	3Mbps
SV			一般測量	TT5* 10ms	140 bytes	4800	6Mbps
			質量和計量精度	TT5* 10ms	-	15360	12Mbps
PTP	ETH or UDP/IP/ETH	Medium - high	時間同步事件和命令	-	-	-	3Mbps
MMS	TCP/IP/ETH	Medium - Low	事件、警報	TT1* 1000ms	100-200 bytes	20	32Kbps
		Low	文件、日誌內容	TT0* >1000 ms	50000 bytes >	random	1Mbps

doi:10.6342/NTU202401322

表 5　IEC 61850 傳輸等級需求表

傳輸時間等級	傳輸時間（ms）	應用
TT0	>1000	檔案、事件
TT1	1000	告警
TT2	500	動作指令
TT3	100	低等的自動動作
TT4	20	快速的自動動作
TT5	10	電路改變
TT6	3	保護電驛

為了驗證5G是否可以導入電力系統，本文架設一台Iperf Server 於N6 port，之後使用讓手機連入5G系統，確保系統本身運作正常。考量現實環境，並非所有設備都有5G模組，故架設三種不同架構進行測試。

測試架構一：終端直連5G通訊系統。使用終端ping N6，記錄延遲時間，架構如圖4所示。

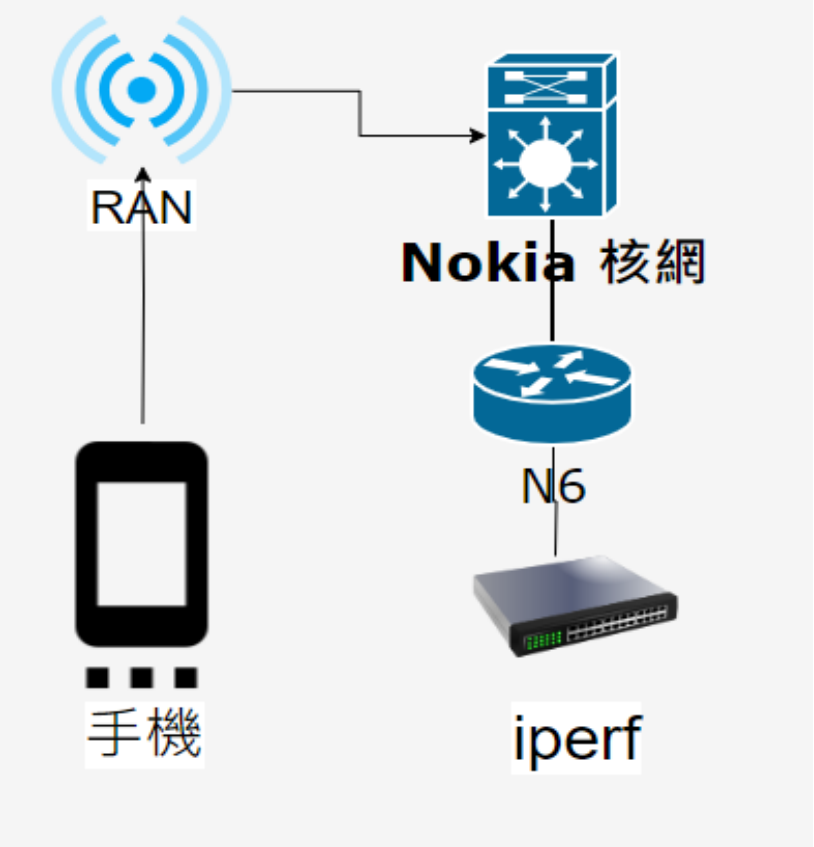

圖 4　手機直連通訊架構

doi:10.6342/NTU202401322

測試架構二：終端透過wifi連到CPE再透過5G連到5G通訊系統。使用終端ping N6，記錄延遲時間，架構如圖5所示。

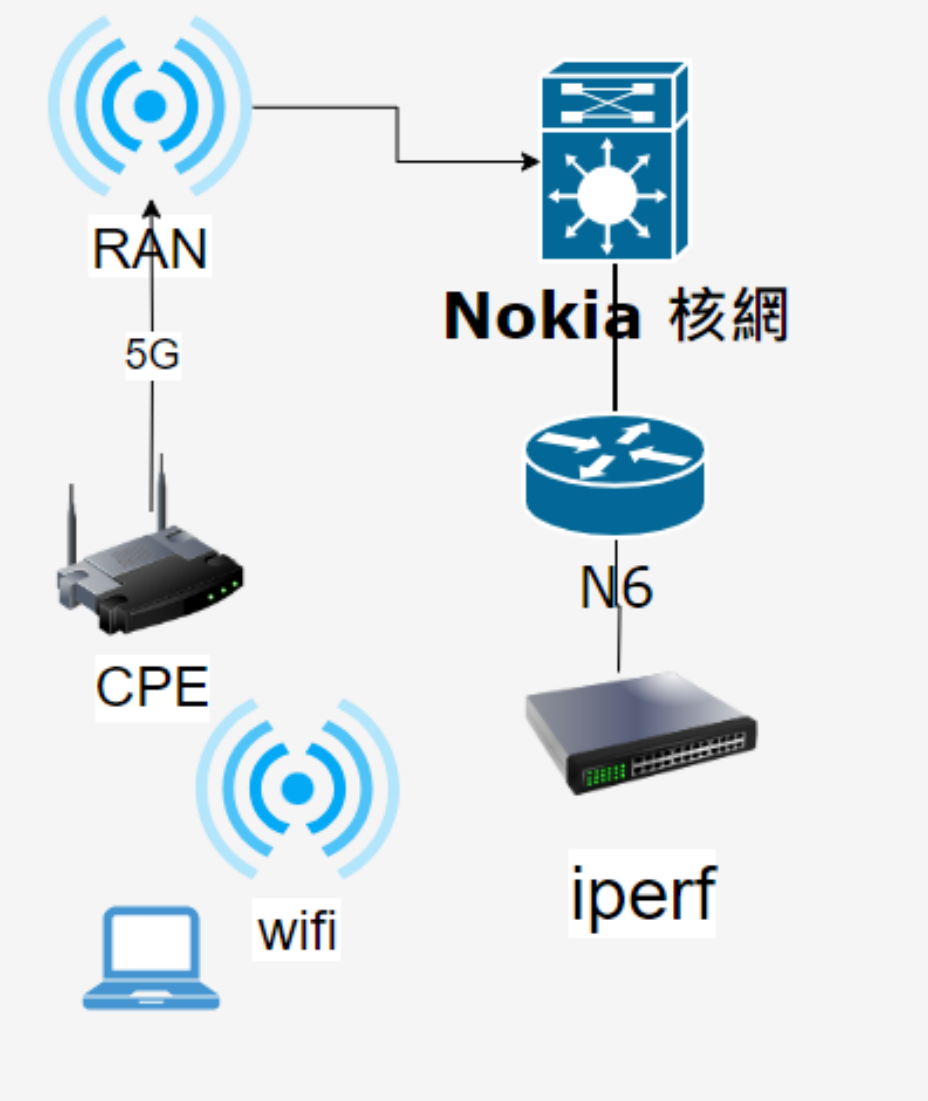

圖 5　終端透過wifi連到5G通訊架構

doi:10.6342/NTU202401322

測試架構三：終端透過網路線連到CPE再透過5G連到5G通訊系統。。使用終端 ping N6，記錄延遲時間，架構如圖6所示。

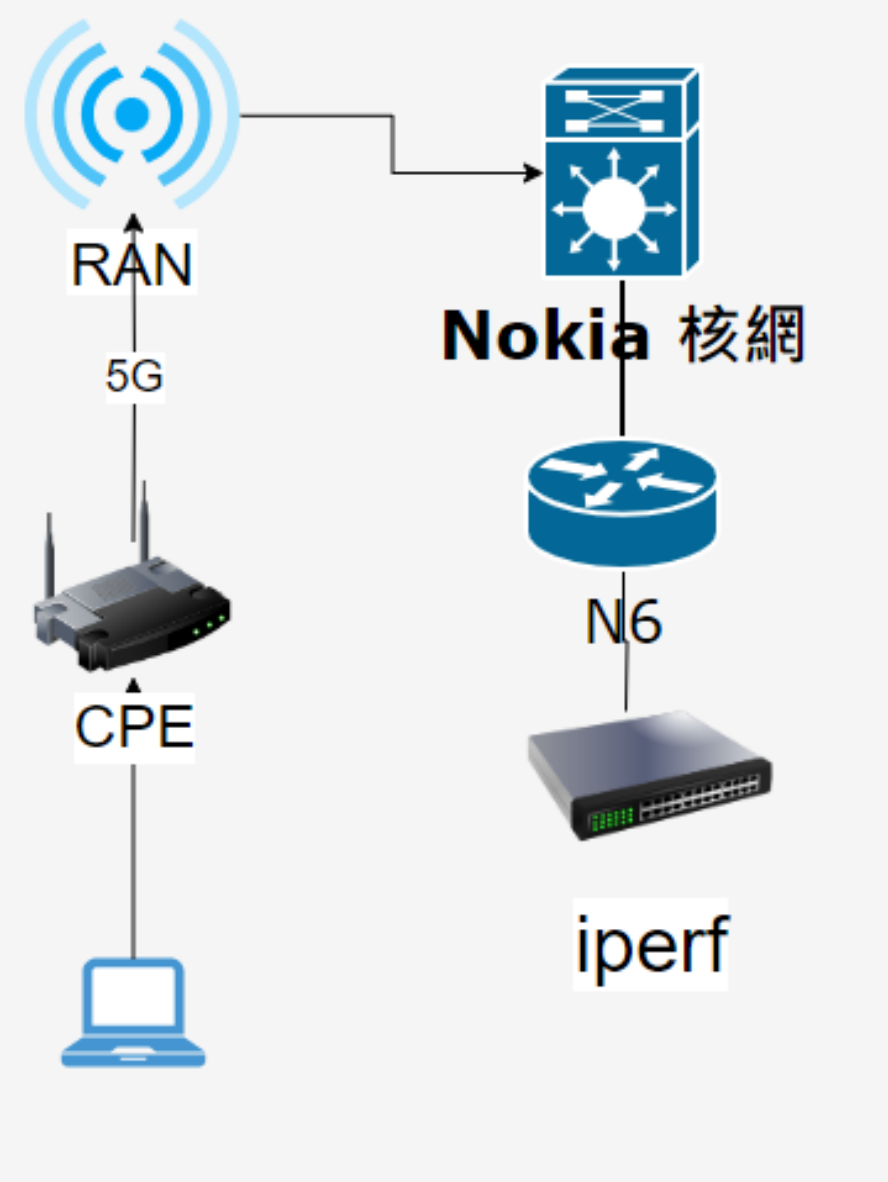

圖 6　終端透過網路線連到CPE再透過5G通訊架構

doi:10.6342/NTU202401322

本次量測結果如表6所示。

表 6　5G 延遲測試

次數	直連的延遲時間（單位:ms）	透過 wifi 連到 CPE，之後轉成 5G 的延遲時間(單位:ms)	將 CPE 當成 5G 網卡的延遲時間(單位:ms)
1	6	20	19
2	15	15	18
3	14	14	18
4	15	14	17
5	17	17	18
6	9	15	13
7	18	11	10
8	17	13	16
9	16	16	17
平均延遲	14.11111	15	16.22222222

從表6的結果來看，三種延遲時間差距似乎不大，雖然封包雖然透過各種設備進行轉換，但延遲的時間沒有因為不同設備轉換，導致延遲有很大的增加。

5G封包傳輸延遲經實驗測試約15ms，故除了Goose應用中的保護電驛 TT6及TT6 需求是無法符合之外，其他應用都可以符合規範。

doi:10.6342/NTU202401322

3.2 5G 技術導入效益

5G通訊已於本文2.2節中有詳細敘述，除了5G本身的特性，如大連結、低延遲、高頻寬的特性，在5G相關技術演進下，2022年制定XR與AI相關標準，為了未來電力系統導入XR工安、AI辨識等應用導入鋪路。這些應用的導入，提升人員安全、供電效率提高、減少故障復原時間、增加通訊備援機制等效益，將大幅強化電網系統韌性。相關標準制訂日期可參考圖7。

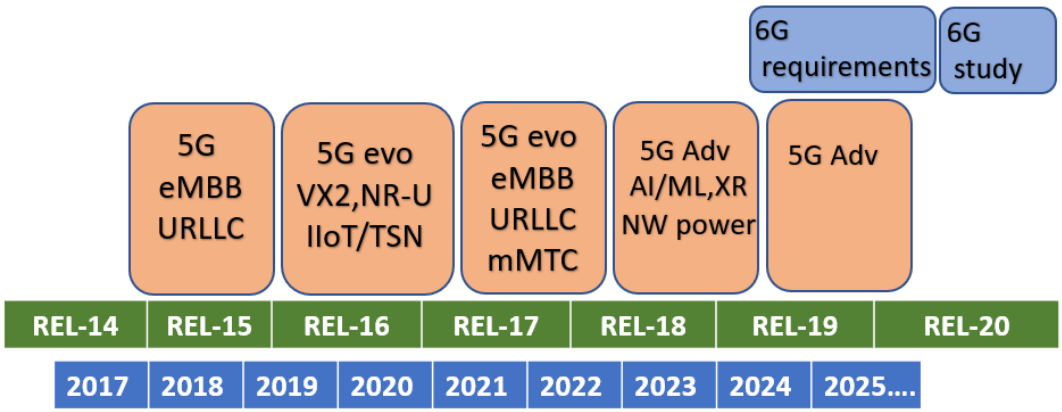

圖 7 3GPP 5G 標準制定日期

5G技術的導入不僅帶來高度的通信效能，同時對電網產生了諸多影響，除了無線應用導入之外，其中之益處之一是節能方面的潛在優勢。每一代通訊技術的演進均伴隨著對電網的連動影響，包括通訊應用耗能的增加、民眾用電習慣的轉變，以及再生能源和分散式能源整合致電網中之通訊議題等。在這樣的科技轉變下，透過文獻整理，可協助瞭解5G通信設備的效能改善、智慧化管理的推動，以及可能的本身所見能源效益的優勢等。透過上述的文獻基礎深入理解5G技術對電網帶來數位化和智慧化的助益及提升能源利用效率的實際影響。

doi:10.6342/NTU202401322

下圖8可以看到，傳統電網從左邊的發電系統到右邊的配電系統，從各種發電廠透過許多變電所發送電力給各用戶，是一個熟悉的直線串連架構電力系統架構，傳統電網是一個具有穩定、持續、可擴展性的系統。

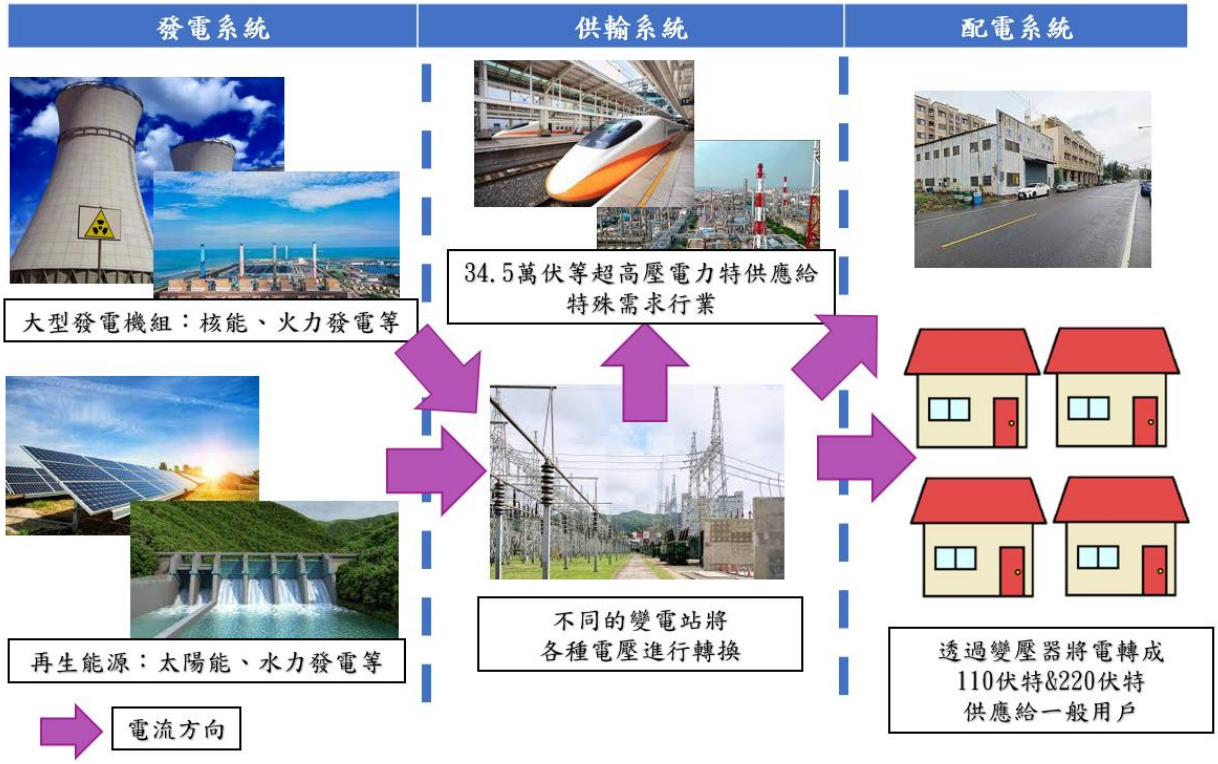

圖 8　傳統電網

doi:10.6342/NTU202401322

而智慧電網架構如下圖9，讓整個電力系統多了互操作、靈活、安全性等，加上大量數位裝置導入，透過數據分析與通訊技術，提升電力系統的可用、有效、準確、可控性，進而帶來鉅大的經濟效益。

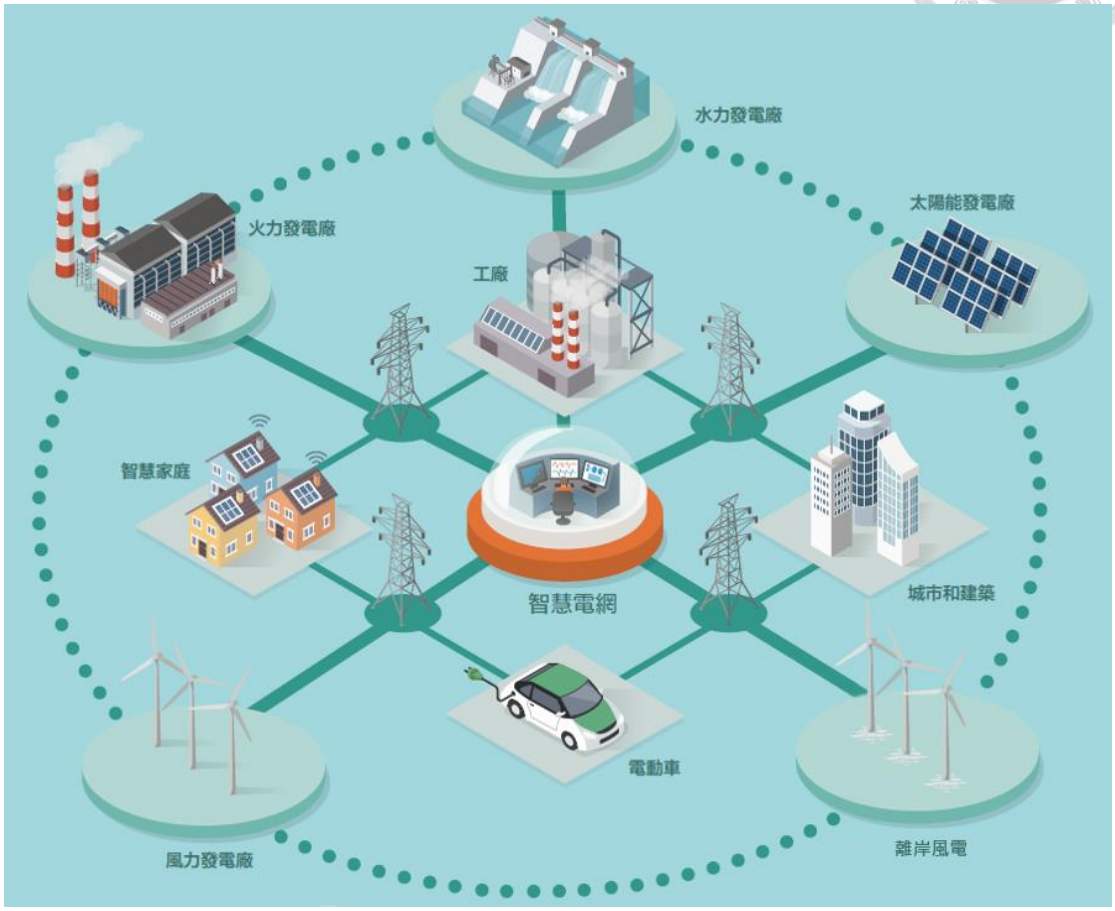

圖 9　智慧電網架構[15]

智慧電網是將傳統電力系統與信息和通信技術結合成的新系統，通訊技術是智慧電網的基石，5G導入智慧電網未來可實現的效益，如XR 維護巡檢修、配電自動化開關、遠程無人巡檢、分散式能源控制與監控等。

5G優點總括前述內容，進一步深入瞭解5G技術及其對電力需求的影響後，可以得知，相較於其他無線通訊技術，5G更能夠滿足智慧電網的需求。它不僅具有優越的安全性，同時也符合電網低延遲的特性。

doi:10.6342/NTU202401322

表 7　5G與其他無線通訊比較表

應用	DL	延遲	可靠性	距離
5G	1000Mbps	10ms	>99.999%	500-1000m
4G	100Mbps	30~70ms	>99.9	1000-1500m
NB-IoT	50Kbps	-	-	20km
LoRa	500Kbps	-	-	20km
WIFI	300Mbps	10ms	>99.9%	100m

以表7來看，如未來導入智慧公安的環境下，需要即時傳輸的高畫質的畫面，並且通訊也需要保持在高穩定的狀態下，且不可以有過多的延遲，因延遲的特性會影響人員的反應，是一個關於性命的特點。

台電現場場域中，因環境特殊，並非所有點都佈有光纖，現場單位常常受限於地理環境，電磁干擾等情況，無法拉光纖到指定地點，故在現在台灣電力系統這樣的環境中，仍需要有無線通訊的輔助。5G無線通訊技術將可改善實體網路無法到達的特殊區域的同時，符合IEC 61850通訊需求的標準。

關於5G 基地台耗能，對於瞭解5G通訊系統對能耗所帶來的影響，首先需要深入探討5G基地台的使用耗能情形以及5G通訊所需基地台的數量。這些資訊未來亦是評估5G通訊導入及電能供應的重要參考。

從通訊技術演進的角度觀察，5G技術將隨時間持續優化，未來預期提供更穩定且通訊範圍更廣的服務，同時伴隨著能耗的持續降低。根據MWC 2022 Ericsson世界行動通訊大會的報告指出，中頻段TDD技術可使覆蓋範圍提升60%。在能源效能方面，華為2020年的資料顯示5G基地台耗電量約為4G的兩倍，然而，根據Ericsson[16][17]與Nokia[18]於2022年的報告，新一代的5G基地台預計可實現約25%到40%的節能效益。另外，Ericsson的報告亦顯示，新技術的應用使得每日平均耗能減少了43%，在離峰時間更可達到55%的節能效果，同時確保辦公大樓的流量需求。對於未來節能應用而言，5G休眠技術也被視為一項關鍵性的節能手

doi:10.6342/NTU202401322

段。

未來在產業環境智慧化及無線化趨勢下，各類IoT設備逐漸透過無線網路連接，這同時也產生了龐大的封包數據流動，顯著提高了人們對網路的需求。根據Ericsson的報告，與十年前相比，現今每月流量增加約300倍。若持續使用4G通信技術，則需要增設更多基站並耗用更多能源。然而，若採用5G技術進行通信，其相對較低的耗能將成為一項鉅大的優勢，對於台灣電力系統的長遠規畫而言，帶來顯著的節能利益。

伴隨每一代通訊技術的推陳出新，5G基地台亦會不斷朝向更加節能的方向進行研發。隨著5G技術逐漸成熟，預計未來其所帶來的耗能將進一步降低。這意味著5G的部署不僅在當前對節能產生積極影響，同時亦在未來展現出更為更高的能源利用效率。

doi:10.6342/NTU202401322

3.3 導入 5G 網路架構

未來，智慧電網導入5G的情境，首要原則應是不干擾現有網路架構，甚且能與現有網路架構同存共榮。換言之，5G無線通訊技術不是為了取代現有智慧電網通訊網路，5G無線通訊技術導入是補足智慧電網在數位化轉型過程中通訊不足的地方，讓智慧電網的通訊可以更完善，引入更多無線應用，進而提升智慧電網整體效益。目前台灣智慧電網的通訊骨幹仍是以光纖為主，而未來5G無線技術則被規劃為備援傳輸系統的結構性元素，是串接終端入網的最後一哩。電力系統未來將納入各種無線應用，包括導入XR技術工安輔助眼鏡系統、無人機巡檢、再生能源通訊系統等，同時進一步融入手機、平板等移動裝置以進行限電使用與教育訓練。

對電力系統顯著不同之處，首先值得注意的是多邊邊緣運算（Multi-access edge computing, MEC）應用。5G技術具備即時處理現場資料的能力，可在現場進行資料處理並迅速回傳，避免透過網際網路將資料傳送至遠端機房進行處理，這對於對低延遲要求極高的電力系統至為重要。其次，5G技術支持大規模裝置連接，這對電力系統數位轉型的發展而言，具有關鍵性意義，可參茲考應用者如下。

Ⅰ. MEC應用架構：

過去典型通訊系統的模式是將資料傳輸至雲端平臺以進行處理。然而，此類方法不僅耗費大量頻寬資源，同時伴隨相對昂貴的營運成本，並導致整體資料處理延遲的增加。此外，這樣的模式存在著資安風險，特別對於國家關鍵基礎設施台電而言，被視為無法接受的安全風險。故傳統的無線通訊技術因此難以滿足電網的複雜需求。

5G加入MEC的網路架構，將移動運算主機轉移至使用端網路邊緣，減少資料處理延遲時間。5G提供高頻寬、低時延的無線通訊技術，並透過MEC整合現有網路、計算、以及儲存等資源，此舉可有效實現資訊的迅速處理及存取，無需

doi:10.6342/NTU202401322

再遠距傳輸資料至中央資料系統，由此將資料處理延遲縮短至毫秒級。這種架構同時降低了骨幹頻寬的資料負載，並從長遠來看，有望顯著降低營運成本。值得注意的是，此一體系確保資料保留在本地，不經由第三方通訊業者流通，進一步確保資訊的安全性。

II. 企業專網&商頻專網：

企業專網係透過政府所頒布之特定頻譜，讓企業得以構建私有之企業專用網路。此種架構與電信業者相異，不須進行與國家通訊委員會（NCC）的頻段競標，但須向相應主管機關提出申請，提交網路建置規劃書等文件，同時負擔每年相關使用費用。企業專網憑藉政府公告之專用頻段，不同於電信業者商用頻段，有效避免用戶間頻寬資源爭奪問題。企業還可進行客製化網路設定，提升對相關網路管理的靈活性，更貼合企業內部需求，同時享有專網的高度安全性。

商頻專網是指企業網路與電信業者相同商用頻段，雖由電信業者提供專用網路服務，但企業需與一般用戶共享相同網路。雖商頻專網成本較低、技術要求較簡單，然而用戶之間可能存在相互干擾的情況，進而影響企業用戶的網路使用。5G企業專網模式有助於保障資料在公司內部網路中的流通，防範資訊洩漏至其他業者。相較於4G，5G提供更多安全措施，對於電力系統整體安全性具有不可忽視的重要性。

儘管5G企業專網模式成本較高，然網路管理方面而言，企業專網更符合電力系統的需求。從下圖10可見，目前5G企業專網主要應用樣態和架構，可分為四種，包括：

- 網路切片：

  這個架構下，服務方面與一般用戶相同，企業用戶與電信業者租用網路服務，但電業者者會透過網路切片功能，將一般用戶與企業網路切隔開來，確保通訊品質，雖然此架構自我網路控制相對較少，但企業用戶花費成本最低。

doi:10.6342/NTU202401322

- 企業專用基地台：

  與第一個架構相比，此架構多了基地台的掌握，基地台變為企業專用，不在需要提供給一般用戶，這樣架構下，企業可以隨意調整基地台位子，使其覆蓋範圍效益提高，空中傳輸介面也不在有其他用戶共用，無線傳輸品質也提高。

- 企業專用基地台及資料面核心網路：

  此架構與前一個相比，多了雲端服務，其網路服務與MEC架構相同，讓資料可以直接落地，降低資安風險，減少資料延遲時間。

- 獨立組網

  此架構下，企業用戶花費最高，但網路控制方面則是最高，從終端連線控制，到基地台TDD傳輸上下行配置，雲端連接數量等，都可以自我控制，因整個網路控制能力高，所以資安風險相對也是最低。雖然此架構成本最高，但對於網路需求要求較高的場域，是較佳的選擇。

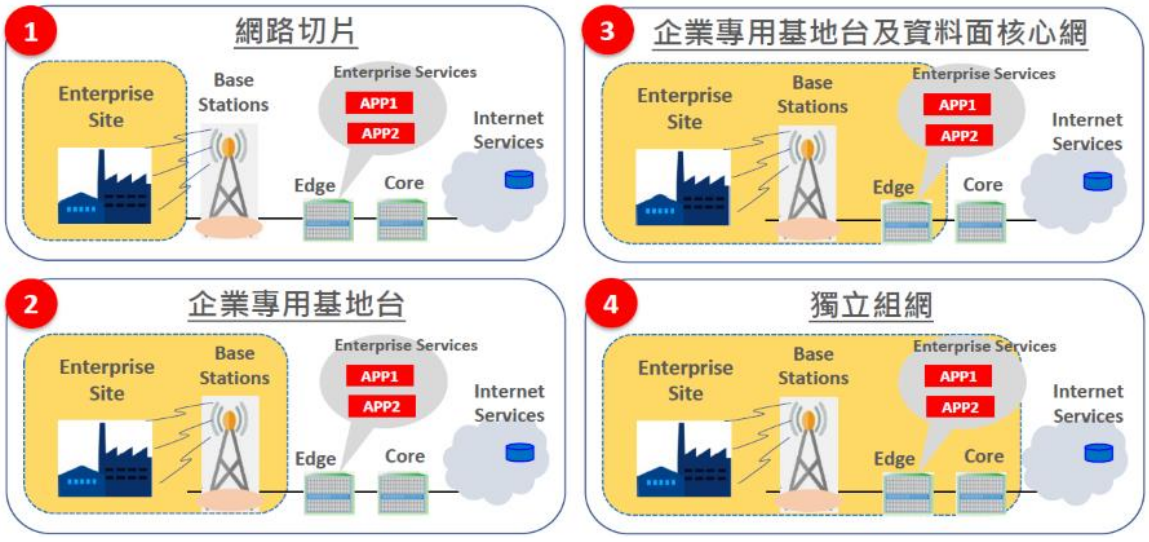

圖 10　企業專網架構[19]

doi:10.6342/NTU202401322

III. 5G結合其他不同通訊技術：

5G與WiFi彼此相輔相成，其通訊特性在不同環境中呈現互補關係。在室外環境下，5G通訊相較於WiFi更穩定且傳輸距離更遠；然而，一旦進入室內，5G信號強度則相對減弱，而WiFi在室內環境下則較為穩定，成本也較低。因此，5G Customer Premises Equipment（CPE）通常會將這兩種技術融和，在CPE端進行5G與WiFi之間的轉換，以實現對外提供5G和WiFi通訊服務。由於5G和WiFi皆建立在相同的無線通訊基礎上，它們彼此可以相互協同支援，滿足不同的使用案例，提供更為優越的無線通訊網路。

智慧電網中，存在許多不同實體通訊協定，在網路通訊技術方面，包含了SDN、多協議標籤交換（Multi Protocol Label Switching, MPLS）、被動光纖網路（Passive Optical Network, PON）和PLC等通訊技術，這些技術需要網路控制技術、網路邏輯控制技術、遠端連線控制技術等等。舉例來說，SDN提供網路切片（Network Slicing）服務，這是一種網路邏輯控制技術，能夠創建多個虛擬邏輯網路，以滿足應用服務的不同傳輸速率、優先度和安全性等需求。加上實體網路對於資料延遲的要求極高，需要精密控制和調整設備。

然而，實體網路存在一些不足，例如當網路結構調整或設備更動時，需要重新拉線和更改網路設定，導致大量資源浪費。導入5G移動通訊技術解決了實體網路所面臨的一些挑戰。5G不僅滿足了技術上的需求，提供了低延遲和邏輯控制等技術通訊，同時無需重新拉線和更改網路設定，解決了設備更動所帶來的資源浪費問題。5G與實體網路技術可以相互結合，提供企業專網多樣化的客制化應用，實現網路的彈性運用，使得不同服務之間相互獨立且不干擾。

IV. 智慧電網通訊應用架構：

經由前述討論可見，5G技術具有提供新型低延遲、穩定、高速的無線網路架構的潛力。此外，其可與各種實體通訊技術和無線通訊技術相容，使其能夠串接多樣的服務，滿足不同通訊需求。因此，預期未來的智慧電網通訊網路架構將以

doi:10.6342/NTU202401322

電力領域實務應用需求為前提，融和前述MEC應用架構，5G企業專網四種架構，以及由5G結合其他不同通訊技術，包括：SDN、MPLS、PON和PLC等通訊技術打造5G確實性網路，以便符合智慧電網對於多元化通訊技術之需求，詳如下圖11所示。

圖 11　5G智慧電網網路架構圖

doi:10.6342/NTU202401322

3.4 未來潛藏的資安風險

在對5G系統有了深入瞭解之後，接者轉向對5G安全機制的研析，資安議題與智慧電網的整合息息相關，尤其是從智慧電網資通安全責任等級來看，係列為國家基礎設施中關鍵資訊基礎設施（Critical Infrastructure Information, CII）極高的場域。因此，本論文另一個研究主題，就是探討5G系統的資訊安全性，並深入瞭解5G SBA中與安全相關的核心功能。

I. 安全錨功能（Security Anchor Function, SEAF）：

在5G網路中，SEAF的角色突顯在UE及AUSF認證伺服器功能間的身分認證過程。AUSF向SEAF提供的密鑰（KSEAF）成為焦點，而SEAF則負責為主要身分驗證生成統一的錨密鑰，以確保對UE未來通信和服務的安全保護。不同於4G的EPS-AKA，5G引入了5G-AKA協議，對認證向量進行單向變換，從而提升了安全性，特別是對漫遊用戶的認證。

II. 訂閱標識符去隱藏功能（Subscription Identifier De-concealing Function, SIDF）：

SIDF的任務是透過對訂閱隱藏標識符（Subscription Concealed Identifier, SUCI）的解密，取得真實的身分識別。在5G網路中，強調用戶身分一直以來都使用加密方式進行無線介面的傳輸。這是保護用戶隱私和確保安全性的重要步驟，與4G中以明碼傳送IMSI的方式形成鮮明對比，有效地降低了被偽造基地台或無線訊號攔截的風險，有效地防範潛在的駭客攻擊。

這些安全功能的實現不僅確保了5G網路對用戶身分和數據的妥善保護，同時也提供了對於智慧電網等安全要求較高應用場景的強大支持。

在 5G 通信中，密鑰管理的演進顯著提高了系統的安全性。與 4G 相比，5G 引入了兩個新的中間密鑰，即 KAUSF 和 KAMF，使得認證過程更為複雜。UE

doi:10.6342/NTU202401322

認證的結果還會被發送到 UDM 進行記錄，這一步驟為系統的安全性提供了額外的保障，而在 4G 的認證流程中，僅生成認證向量而不對結果進行驗證。

在 3GPP 5G 的安全框架（5G Security Architecture）中，對網路接入的安全性進行了重點強調，確保 UE 能夠通過網路安全地進行身份驗證和接入服務。這包括了 3GPP 接入和非 3GPP 接入，特別注重防止對無線接口的攻擊。此外，安全框架還包括了從服務網路到接入網路的安全上下文傳遞，其中涉及到網路節點安全地交換信令數據和用戶平面數據的安全功能。該安全框架還覆蓋了保護用戶接取移動設備（Mobile Equipment, ME）的應用程序域安全，使得用戶和提供者中的應用程序能夠安全地交換信息。在 SBA 架構下，網路功能實現了在網路域內和其他網路域間通信的安全性，包括網路功能註冊、發現和授權的安全性，以及對服務介面的保護。詳如下表 8 所示。

表 8　4G 與 5G 安全架構差異處

	4G	5G
認證	EPS	EAP-AKA'和 5G-AKA
	SAE 架構 使用 MME 及 HSS	SBA 架構 AUSF.UDM.ARPF.SIDF
	NAS	NAS / EAP
	eNB 之間密鑰 隔離	eNB 之間密鑰隔離 AMF 間密鑰隔離
	Diameter	HTTP-based web APIs
	每次切換密鑰 都要更新	PDCP 實體不變下，密 鑰可以不用更新
手機 隱私	IMSI 用明文 發送	IMSI 透過 SUPI 加密發送
網路 安全	NDS/IP	SBA 安全架構 端到端的安全

綜上所述，5G 的安全框架相對於 4G 來說，引入了應用程序域安全和 SBA 安全，這進一步加強了整個系統對各種威脅的防範能力。這一演進為未來智慧電

doi:10.6342/NTU202401322

網等安全要求較高的應用場景提供了堅實的支持。

5G 使用了新的認證架構，對 UE 身分驗證的機制進行了革新，與 4G 相比，安全性顯著提升。這種安全認證機制在 4G 中並不存在，因此 5G 在安全性方面相對更為優越。而 5G 資安議題可大致分成下面五種。

- 無線電接取網路威脅的部分：

  實體層（Physical Layer）攻擊：基地台並未受機房保護，可能遭受實體入侵攻擊。用戶隱私資料竊聽與阻斷服務（Denial of service, DoS）攻擊：可能偽裝成用戶通過中間人攻擊手法，來竊取客戶流量或進行DOS攻擊。
- 惡意基地台：駭客自己架設偽造基地台，來竊取用戶連線資料。而空中介面威脅部分，可能遭受惡意蓋台攻擊，或是資料加密等級強度不足導致遭到竊聽等。
- MEC的部分：

  有關MEC實體層攻擊部分，MEC通常架設在業主附近，缺乏專業管理，容易遭受實體層面攻擊，MEC本身也需要定期維護和更新，故有管理上的資安風險。而在MEC應用部分，MEC大多採用NFV架構，可能會因為設計不良導致駭客入侵。
- 資料傳輸的部分：

  最常見的是DDOS攻擊的問題，5G時代將有大量設備連網，管理難度提升，如管理不佳可能遭到駭客利用，藉此發動DDOS攻擊或是被攻擊。
- 核心網路的部分：

  未經授權接取是其中最大的問題，駭客可透過受感染的UE進行惡意行為，或是用戶身分可能造到竊取。

Ravishankar Borgaonkar在2021年的IEEE期刊上發表文章“Improving smart grid security through 5G enabled IoT and edge computing”一文，此案例探討了IoT裝置在智慧電網中的應用，此一應用有望推動多個領域邁向數位轉型，尤其是電

doi:10.6342/NTU202401322

力系統領域。然而，面臨的一大挑戰是在考慮成本和效能之間的權衡時確保IoT的安全性。在該研究中，著重於配電系統方面的使用案例，深入分析了IoT通訊的需求，同時建立了相應的資安威脅模型[20]。

本文透過深入研究5G規範，討論了其在特定智慧電網應用案例中的安全應用。儘管5G網路無法解決所有IoT安全問題，但其提供了一種具有內建安全優勢的可靠通訊通道，特別適用於智慧電網基礎設施。

在科學上，該研究總結了使用5G進行IoT網路時智慧電網安全的最新技術水準。建立了一個案例，用於評估未來安全機制。同時，指出了需要進一步研究的領域，特別是關於大規模5G IoT網路的實驗室研究。對於配電電力系統運營商（DSO），提出了一個的威脅模型，供其在更新變電站通訊策略時參考。文中還提供了5G在安全性方面為DSO提供哪些功能以及仍需考慮哪些限制的相關資訊。透過現有的資料整理來看，5G與智慧電網都有GPS資安風險。本論文將針對這點進行後續實驗室等級的資安檢測與風險評估。

doi:10.6342/NTU202401322

Chapter 4　5G 資安風險檢測與評估

4.1 智慧電網導入 5G 資安風險

在深入研究5G通訊技術和智慧電網系統後，會發現這兩種系統都相似的特性，訊息傳輸以及時間同步的要求相當高，皆需要使用PTP（Precision Time Protocol, PTP）等級以上的時間同步機制。基於目前所整理的文獻資料審視，本論文提出了一個研究上的推測，亦即對時間同步進行干擾可能導致5G系統與智慧電網同時異常運作。若此一干擾手法成功實施，將可帶來5G系統與智慧電網鉅大之安全性的資安議題，值得進一步深入研究。

首先，在智慧電網的架構中，時間同步係一項孰不可忽視的關鍵議題，尤其在涉及變電站之間的通訊與變電站內部IED的資料傳輸等關鍵應用情境，確保系統中各節點具備統一且高精準的時戳，時間同步是實現PMU（Phasor Measurement Unit,　PMU）資料收集、系統自動調度、控制以及故障檢測等重要輔助性技術之一。

在討論時間同步之前，得先瞭解GPS（Global Positioning System），GPS提供精確時間和準確定位，利用4顆以上的衛星訊號，降低地形和天氣等因素對同步的影響，並且全球範圍均能接收到GPS信號。最重要的是，GPS是一種國家級戰略資源。

就GPS本身而言，主要提供了兩種重要的定位服務，即標準定位服務（Standard Positioning System, SPS）和精密定位系統（Precision Positioning System, PPS）。SPS具有水平定位精度10公尺、垂直精度20公尺和時間精度40微秒的特性，適用於廣泛的商業應用，如汽車導航系統等。而PPS則使用鎖碼訊號，其水平定位精度達到5公尺，垂直為10公尺，時間精度為40微秒。PPS主要為軍事和政府機構提供，具有更高的安全性和定位精準度。

doi:10.6342/NTU202401322

為了最佳化智慧電網的時間同步機制，降低損害風險，首要一步即在於深入瞭解目前所採用的同步機制，進行詳盡的優缺點分析。目前廣泛應用的同步機制包括：

I. 網路時間協定（Network Time Protocol，NTP）：

- 一種廣泛運用於變電站時間同步的協定。
- 通常可以在一般公共網際網路保持幾十毫秒的誤差，並且在理想的區域網路環境內，可以實現約1毫秒準確度。
- 雖足以支持目前電力系統，未來智慧電網需要更精確的時間同步機制。

II. IRIG（Inter Range Instrumentation Group, IRIG）：

- 分為並行和串行時間碼格式。
- 串行時間碼有六種格式，同步準確度約為10 μs～20 μs。

III. 精確時間協定（Precision Time Protocol, PTP）：

- 區域網路內可以實現亞微秒範圍內的時鐘精度
- 適用於測量和控制系統

這些同步機制各有其優勢和限制，因此在智慧電網的實際應用中，必須依據系統需求與特性，精心挑選最為適切的機制。精確的時間同步不僅關係到系統的正常運作，更直接影響智慧電網的穩定性和可靠性。

在研究台灣電力系統導入IEC 61850並對時間同步提出PTP的要求時，必須深刻理解PTP的重要性。PTP追求奈秒級的同步速度，相較於先前使用毫秒精度的NTP技術，其性能更為卓越。尤其在智慧電網的複雜環境中，這種高精密度的時間同步對於電力系統的穩定運行至關重要，詳如表9所示。

doi:10.6342/NTU202401322

表 9　時間同步分析表[21]

	IRIG-B	NTP	PTP
時間精準度	10μs-20μs	1ms-10ms	100ns-1ms
傳輸介質	同軸電纜	乙太網路	乙太網路
同步協議	Master-slave	Client-server	Master-slave
內建延遲校正	No	Yes	Yes
更新時間	依據種類	數分鐘	10ms-1s

在5G通訊頻段，特別是採用TDD傳輸機制的情境下，時間同步的重要性更加凸顯。若同步機制存在超過150微秒的差異，可能導致基地台無法正確解析封包，進而觸發整體系統的異常情況。如缺乏相應的保護機制可能引發連鎖效應，將對整個通訊網路產生嚴重影響。

而在深入研究台灣電力系統的特點時，瞭解到台灣供電頻率為60Hz的情境下，考慮到每秒需傳輸3600筆資料的資訊同步需求，時間延遲超過20毫秒可能導致裝置異常或停止服務，進而對電力系統的穩定運行帶來嚴峻的挑戰。

在此背景下，可以深刻理解時間同步機制在電力系統和5G通訊中的關鍵性。這個機制不僅關係到系統的正常運行，更關係到資訊的精準傳輸和裝置之間的協同作業。在電力系統中，精確的時間同步是實現PMU資料收集、系統自動調度及控制、故障檢測等重要應用的基礎。而在5G通訊中，高精密的時間同步是確保訊號解析和基地台協同運作的關鍵。因此，時間同步機制在這兩個系統中都扮演了不可或缺的角色，其可靠性直接關係到整個系統的運行和穩定性。

總括文獻的整理，可以得見干擾時間同步機制確實可能產生嚴重的資安問題，尤其是在高度時序敏感的5G通訊和電力系統中，資安防護勢必成為當務之急。以下先針對GPS攻擊進行相關文獻回顧。

根據2021年的研究[22][23]，國際學者進行了對電力系統全球導航衛星系統（Global Navigation Satellite System, GNSS）的攻擊可能性的深入探討。在歐盟的

doi:10.6342/NTU202401322

Strike3 （Standardization of GNSS Threat reporting and Receiver testing through International Knowledge Exchange, Experimentation and Exploitation）項目中，進行了系統性的監測，以評估GNSS中斷對電力系統的頻率和潛在威脅。研究結果顯示，在城市中心區域，每週可能發生多達100次停電，這揭示了GNSS可能受到環境因素影響的脆弱性，而人為引發的攻擊可能導致更嚴重的後果。

根據國際新聞回顧[24][25]，2016北韓曾經針對南韓進行GPS干擾，當時有超過1000架飛機及船，和數千個基地台受到干擾，並根據RTI International的報告，如GPS受干擾一個月美國將損失300億美元。

GPS對於精密的系統來說，是一個不可缺少的系統，愈是精密的通訊系統，對於時間同步的要求就愈高，從前面5G技術以及電力系統時間同步中研究以及國際案例的參考，對兩個系統進行干擾GPS，則會對系統造成極大影響，是未來必須考慮的資安重要防護之所在。

本論文在後續章節中，將聚焦於GPS與時間同步，詳細探討其中可能產生的影響，並藉此進行相關5G資安實驗架構設計和檢測。期望有助於深化對5G系統和智慧電網資安防護的理解，替未來更進一步系統化的研究，奠定基礎。

doi:10.6342/NTU202401322

4.2 實驗室檢測與評估

本次的實驗旨在對5G通訊系統進行GPS干擾，以探討其可能帶來的影響情況。將詳細觀察干擾對系統的影響，包括影響的時間範圍以及產生的系統異常紀錄等相關資訊。這些紀錄將提供寶貴的數據，以進一步瞭解時間同步干擾對5G通訊系統和智慧電網所造成的潛在問題。

在台灣，5G基地台的普及已經相當普遍，基地台通常建置在各種地方，包括公寓和民宅的樓頂，高度約在5到6層樓之間。這種分佈特性能夠觀測不同位置的基地台GPS，並瞭解台灣架設基地台的現況，並作為GPS干擾可行性評估緣由之一。

根據台灣國家通訊傳播委員會（NCC）今年10月公布的統計資料[26]，台灣目前5G純網覆蓋率為87%，已落實的基地台數量達到62849座。5G的信號強度（Reference Signal Received Power, RSRP）是用來反映當前通信路徑中的訊號衰減程度，在區域選擇或重選以及切換等通信過程中扮演重要角色。通常範圍值約-44~140dBm，值越大越好。信號質量（Reference Signal Received Quality, RSRQ）是用來反映和指示當前通道的品質，主要包括SNR和干擾水平。通常範圍值約-3~19dB，值越大越好。訊號品質的訊雜比（Signal-to-noise ratio, SNR）是科學和工程中所用的一種度量，用於比較所需訊號的強度與背景雜訊的強度，越高表示越好。

在理解5G通訊的服務品質指標及基地台建設實況後，可以得知一般環境下5G通訊技術的現況作為實驗基準。以及瞭解到大多數基地台直接暴露於室外環境，本研究假設並驗證對特定場域進行干擾是有可能的。為測試上述假說，本文設計並實施實驗進行完實際監測，實驗架構涵蓋以下主要步驟：

I. 系統確認與初始檢測：

- 在實驗前進行系統初始狀態檢測，以驗證系統運作的正常性。

doi:10.6342/NTU202401322

- 檢視衛星連線數量，確保充足的GPS信號連接。

II. GPS天線干擾實驗：

- 對GPS天線進行干擾與防禦實驗，模擬潛在攻擊情境。
- 觀察GPS干擾對系統的實際影響，包括通訊異常等。

III. 效益評估：

- 評估GPS干擾的效益，深入瞭解其對系統的影響程度。
- 觀測GPS干擾開始到系統通訊異常的時間，進行時間序列分析。

實驗的設計旨在於深入瞭解GPS干擾對5G通訊系統的實際影響，同時提供觀察與評估的數據。在進行實驗的過程，詳盡記錄所有相關數據和觀察結果至為重要，以支持深入的分析和研究。實驗系統架構詳細下圖12所示。

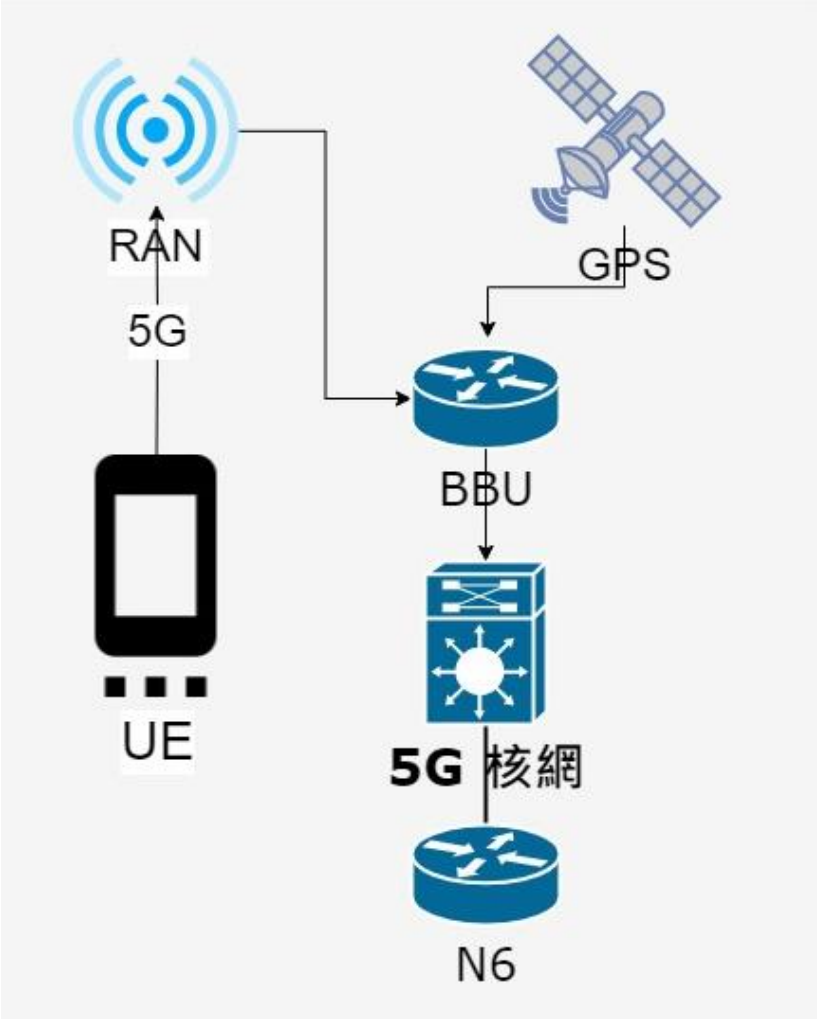

圖 12　本實驗系統架構圖

doi:10.6342/NTU202401322

5G系統的應用中，本實驗使用的是商用5G系統。下圖13是GPS接收天線。根據資料顯示，每個人的頭頂上，通常都可接收到約9至8顆的GPS衛星訊號。故通常狀況下，天空隨時提供了穩定的GPS信號，有助於確保順暢的衛星定位與通訊連接。

圖 13　GPS 天線

而在圖14中，Sync Staatus顯示目前同步狀態，綠燈為正常反之紅燈為異常，Statellite Signal Map X軸顯示目前有看到的衛星編號以及Y軸SNR表示目前訊號強度，每家同BBU要求不太相同，以此圖為例SNR 20以上則視為可以使用（In use），目前系統連線數量有19顆，In use中的有9顆。

圖 14　GPS連線情況

doi:10.6342/NTU202401322

此外，本論文也使用了另一套5G系統進行實驗觀察，如圖15所示。試驗開始前，GPS正常運作，右側圖中顯示目前使用中有3顆（通常為4到5顆）衛星。5G系統的各項服務在試驗開始時維持正常，各項指標皆呈現綠燈狀態。這些觀測數據有助於深入瞭解在GPS干擾情境後，5G系統的行為及其對整體通信環境的影響。

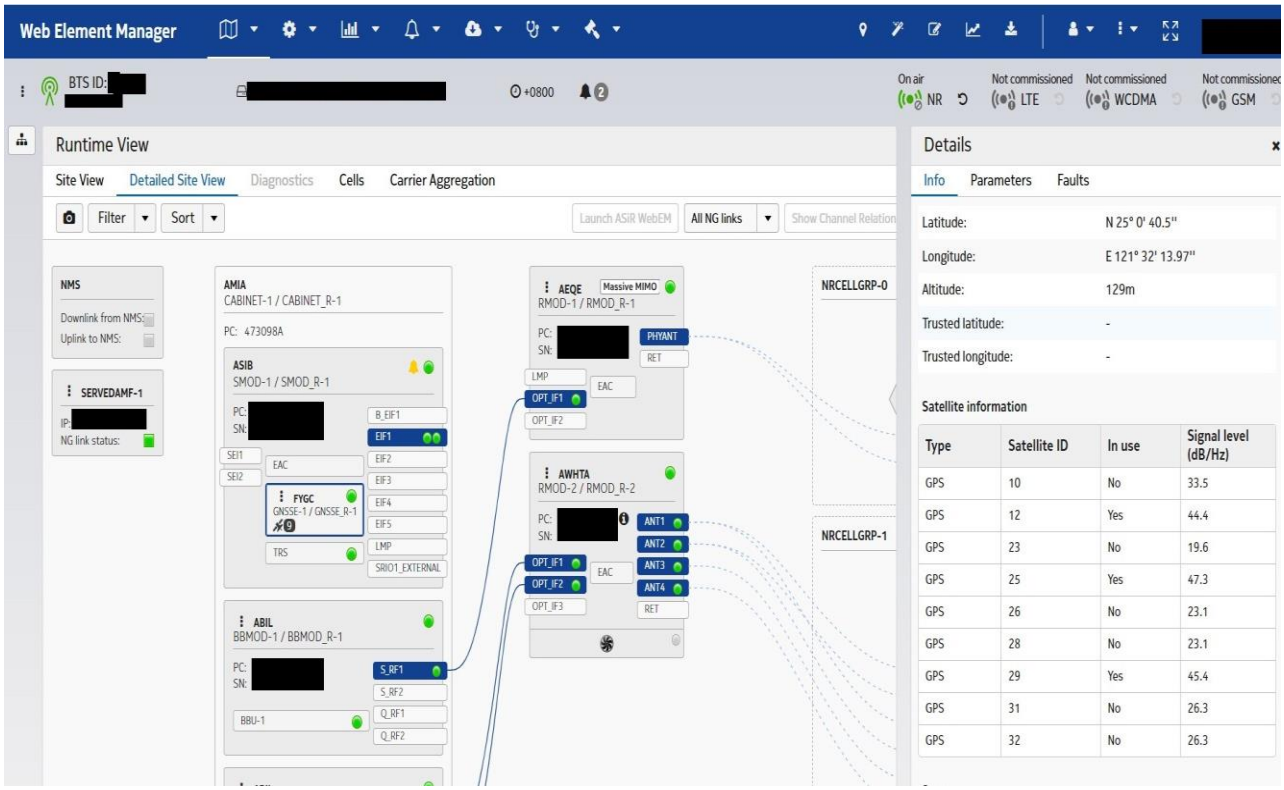

圖 15　5G 系統 GUI 介面 GPS 連線情況確認

doi:10.6342/NTU202401322

從下圖16所示可見，目前使用的頻段為4.8~4.9Ghz，並非使用台灣商用頻段。

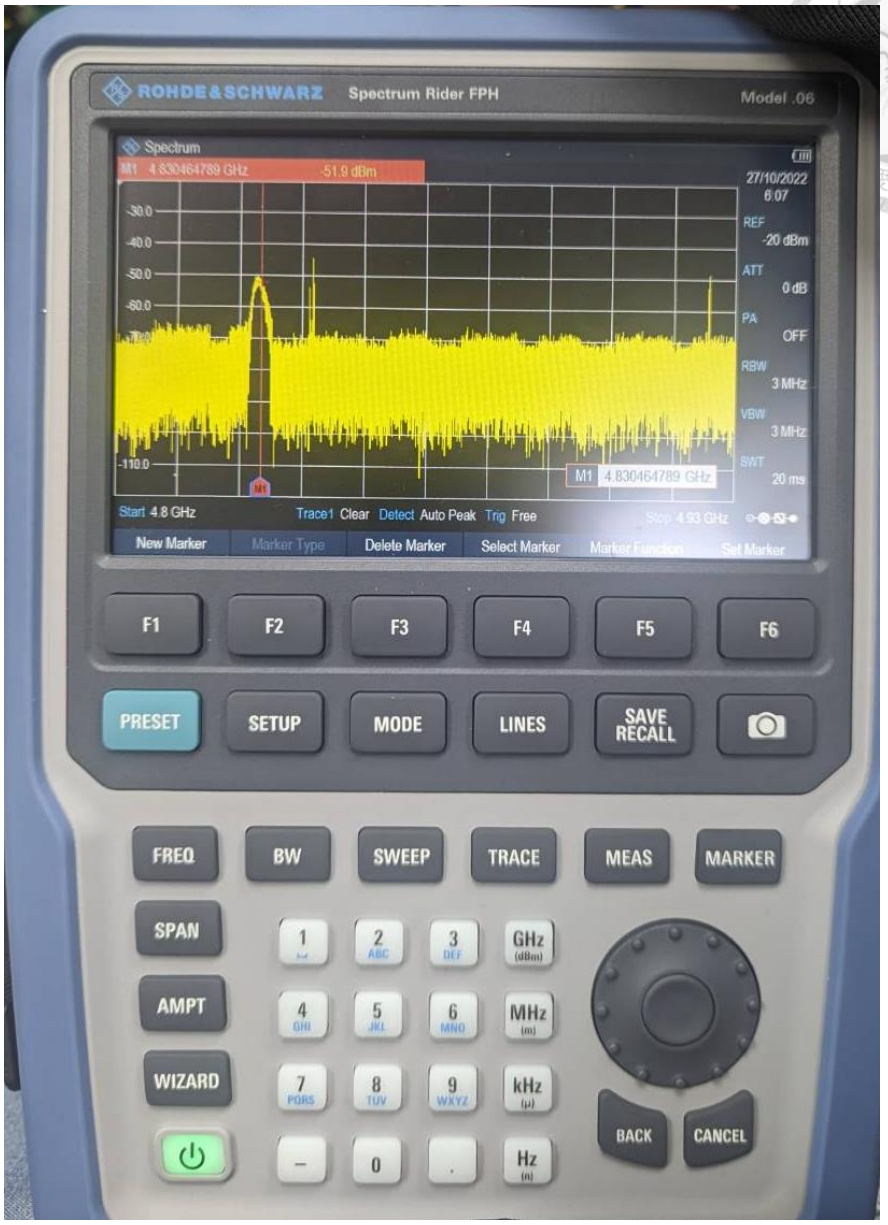

圖 16　使用頻譜儀確認發射訊號

doi:10.6342/NTU202401322

本論文藉由自製的SIM卡成功與5G系統建立連線，進行實驗前仔細檢視手機的連線狀態，手機有成功獲取IP地址，實驗中所選用的是N79頻段（4.8GHz~4.9GHz）。其RSRP達到-58dBm，RSRQ為-11dB，同時訊號品質的SNR達到27dB。

依照台大大門口前測量和實驗室收訊的值來看，大門RSRP約-70 dBm ～-90dBm，RSRQ約-15dB～-25dB，SNR約5dB～-20dB。由此可見實驗使用的通訊品質較佳，這些詳盡的連線參數確保在實驗開始前能夠獲得可靠而準確的數據，有助於進一步的觀察與研究。詳如下圖17所示。

圖 17　手機端確認 5G 系統正常

doi:10.6342/NTU202401322

測試前，使用手機 Ping N6 port 證明目前網路通暢，也可表示目前 5G 系統服務一切正常，手機端正再傳送 ping 封包給位於 N6 位子的筆電，後端的筆電可正常收到 Ping 封包，如圖 18 所示。

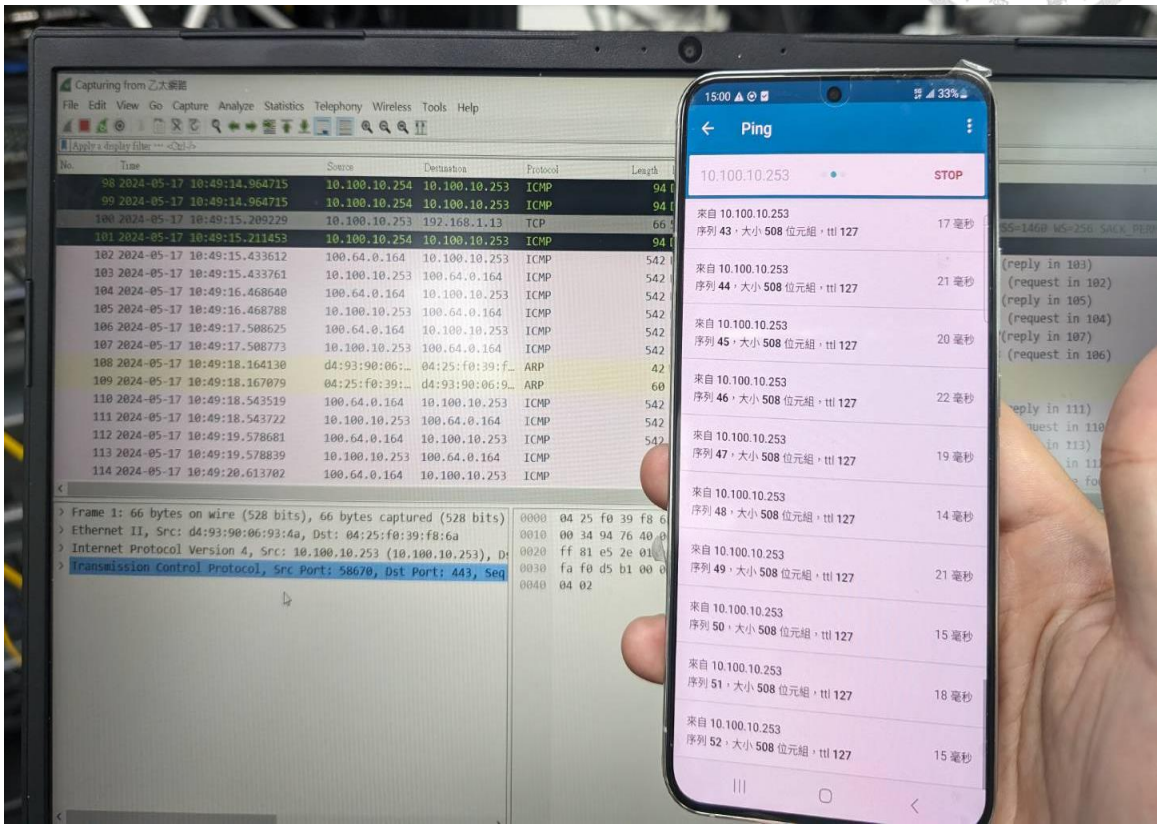

圖 18　測試前，5G 網路傳輸正常

doi:10.6342/NTU202401322

本次實驗於 14:51 分開始干擾 GPS，在 GPS 訊號遭受干擾的情境下，進行了對時間同步機制影響的觀測，以探究整個系統中可能發生的事件和時間變化。從下圖 19 中，觀察到時間同步的訊號狀態轉變為紅燈，同步狀態呈現為 poor，而 GPS 連線表格中也沒有任何 GPS 被標示為「In use」。這樣的狀態顯示了在實驗過程中發生的 GPS 訊號干擾成功。

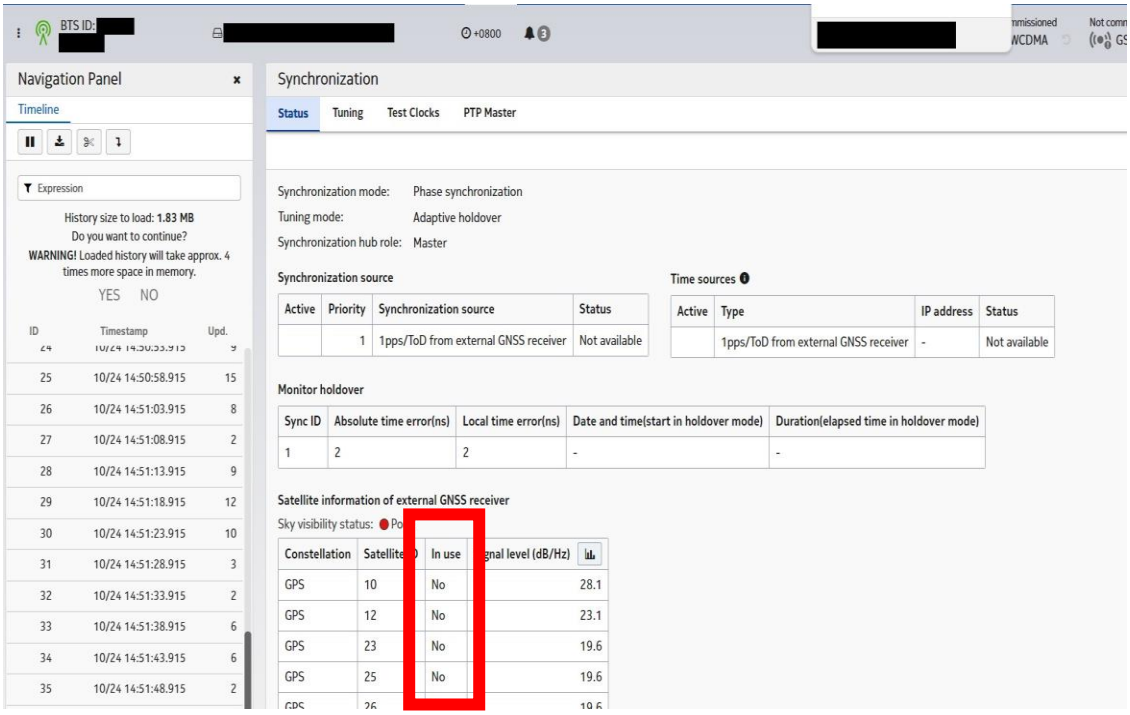

圖 19　GPS 系統干擾開始

doi:10.6342/NTU202401322

在GPS受到干擾的情境下，伴隨著GPS訊號異常的告警，觀察到系統GUI介面也異常顯示。這結果進一步確認了GPS受到干擾的狀況下，會對整個系統運作造成不利影響，詳如下圖20所示。告警顯示「Fault ID：GPS receiver alarm：not tracking satellites」，可從此告警得知，GPS目前已確實遭受到干擾，服務已發生異常。

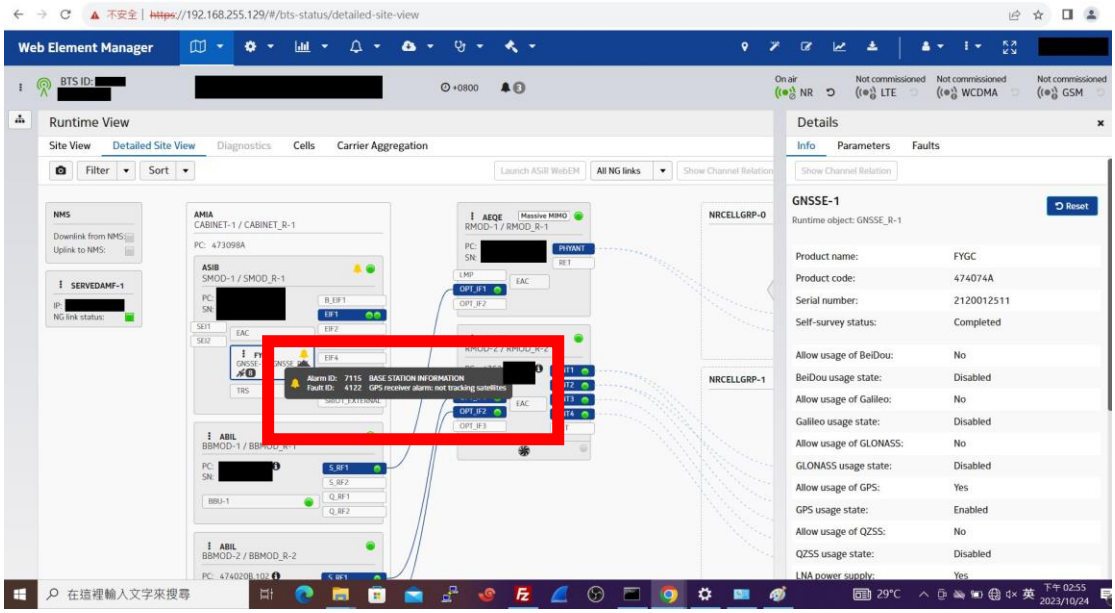

圖 20　GUI 介面上確認干擾

doi:10.6342/NTU202401322

更進一步，可以從系統告警系統中，確認出現「PPS reference missing」告警相關訊息。如下圖21所示。

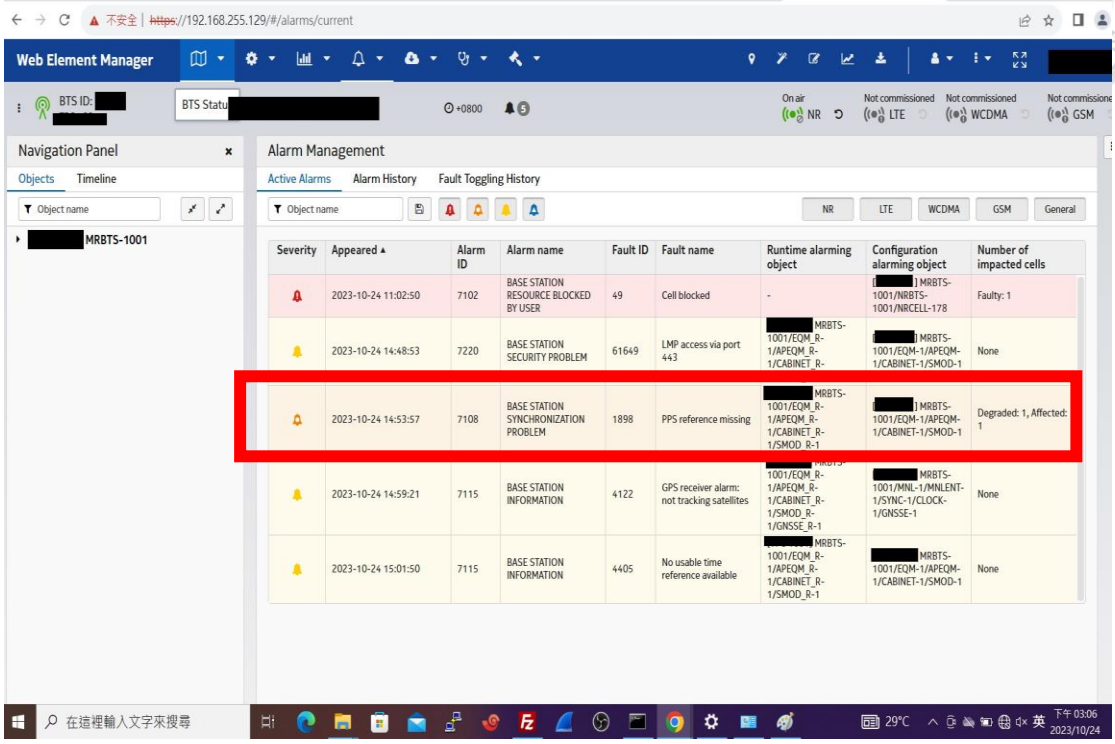

圖 21　系統告警確認 GPS 系統干擾開始

而透過資料及日誌檔案分析，確認在GPS干擾實驗初期，即時觸發系統發出告警訊息，這證實了攻擊獲得實質效果。接下來，將透過手機對N6 port進行持續的ping操作，有助於更深入地觀察5G系統的通訊狀況，並關注是否會出現異常情況。這樣的分析進一步揭示了攻擊對5G通訊系統的實際影響，有助於更全面地瞭解整個實驗的進展。本次實驗於14:18左右連線出現異常如下。可看到ping到中途，出現連線逾時的狀況，由此可證明5G通訊系統已無法提供正常服務，判定本次實驗GPS干擾攻擊成功，詳如圖22、圖23所示。

doi:10.6342/NTU202401322

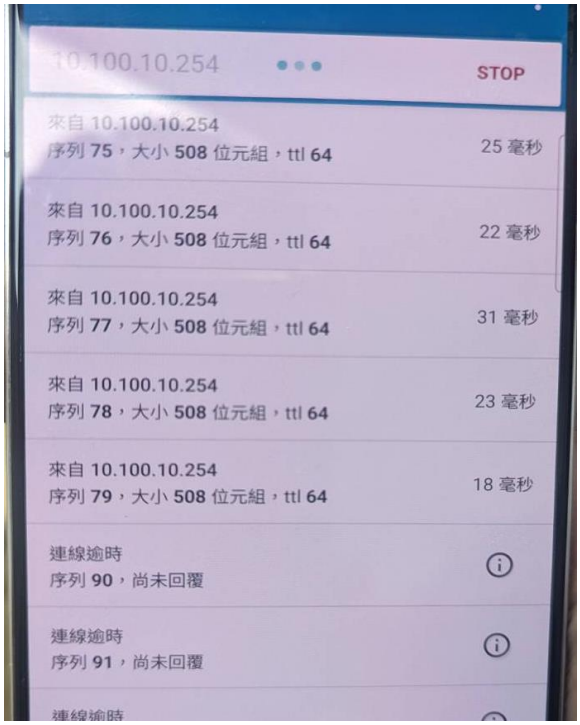

圖 22　5G 通訊異常確認

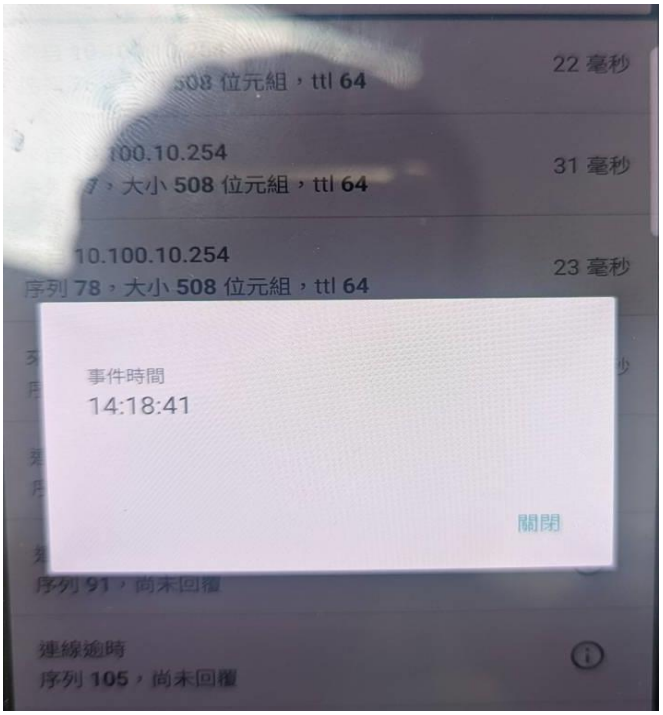

圖 23　5G 通訊異常時間確認

doi:10.6342/NTU202401322

本次實驗也針對IED設備進行GPS干擾測試，觀測電力系統如遇到GPS受干擾時，電力系統的反應為何，以及其事件資料的細節紀錄。本實驗所使用IED設備如圖24所示，該設備可以發送Goose封包。

圖 24　本次實驗所使用的 IED 設備

doi:10.6342/NTU202401322

本次實驗傳送的Goose封包內容如圖25所示，GOOSE 訊息在需要快速事件傳播和近乎即時決策發揮作用。這包括差動保護等保護方案，其中對故障情況的快速響應對於防止設備損壞和維持電網穩定至關重要。

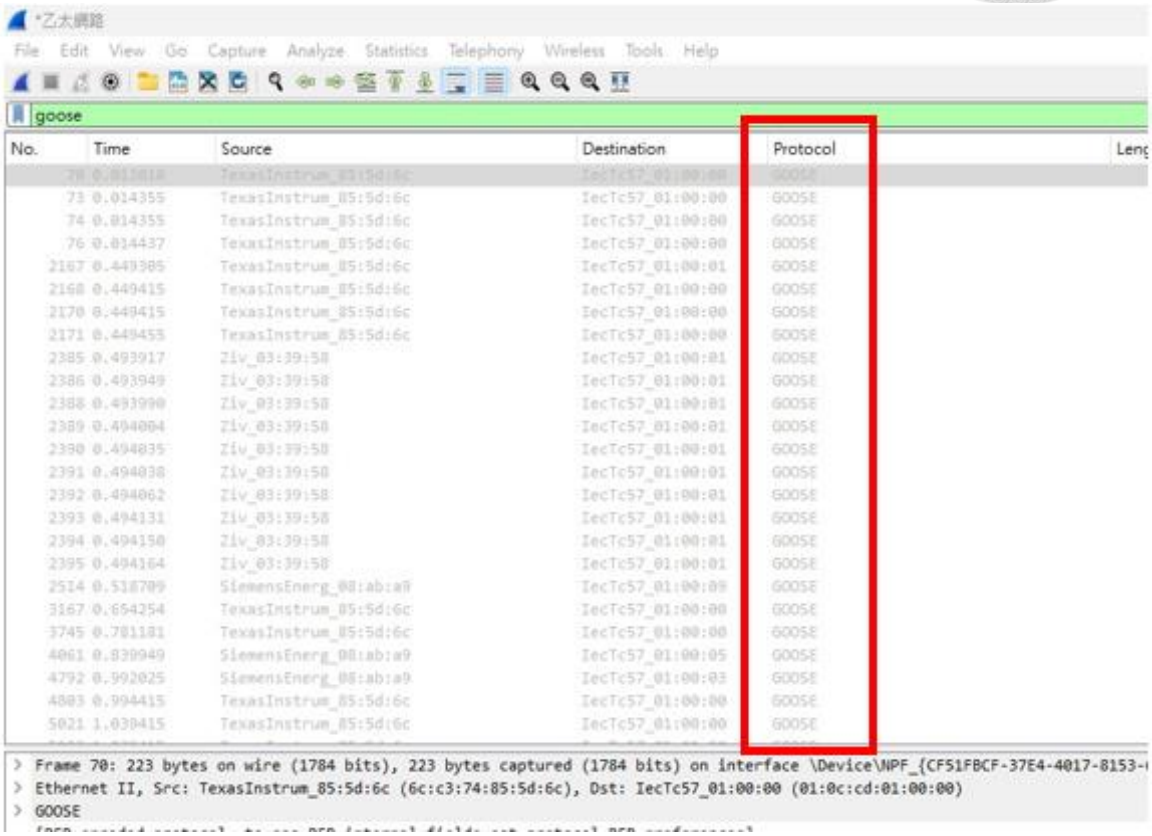

圖 25　本實驗用的 Goose 封包

doi:10.6342/NTU202401322

圖26中，Goose第一個封包編號NO.436中，展開封包內容後可以與圖紅框處看到關於時間的資料，其中Time delta form previous captured frame為0. 00000000 seconds ，以及Time delta form previous displayed frame為0.00000000 seconds。可以證明是本次實驗的第一個Goose封包。而Time since reference or first frame為0.090486000 seconds。

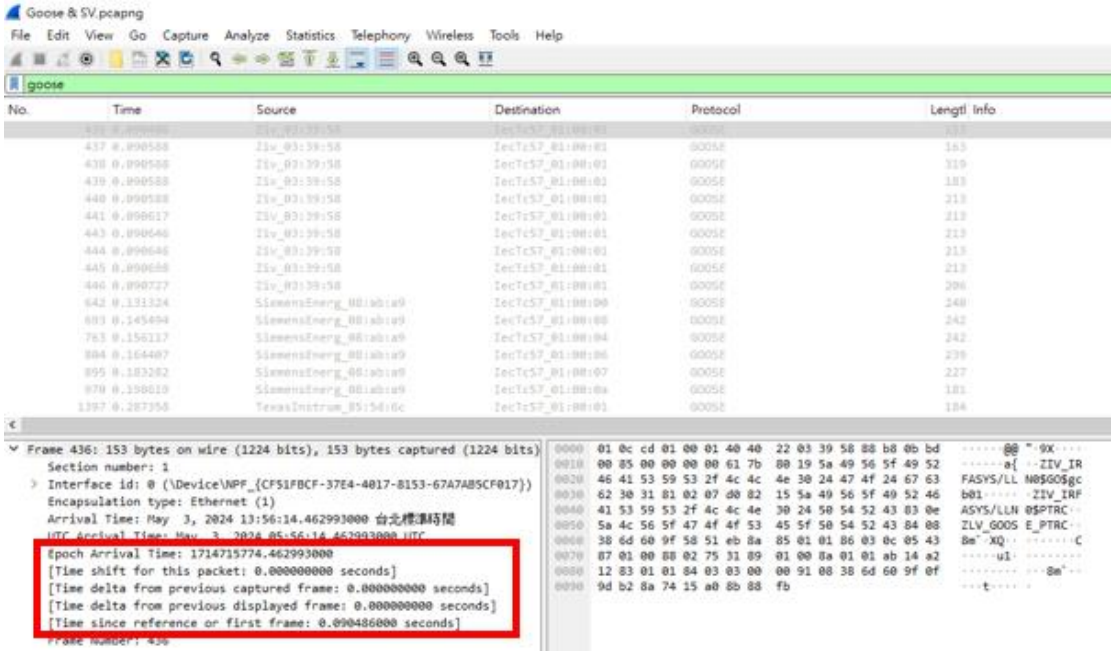

圖 26　本實驗第一個 Goose 封包的時間資料

doi:10.6342/NTU202401322

圖27中，Goose第二個封包編號NO.437，展開封包內容後可以與圖紅框處看到關於時間的資料，其中Time delta form previous captured frame為0. 000102000 seconds ，以及Time delta form previous displayed frame為 0. 00010200 seconds。而Time since reference or first frame 剛好等於第一個封包的0.090486000+0. 00010200 = 0.09058800 seconds，則表示參考或第一幀以來的時間。可以證明時間同步確實與Goose封包息息相關。

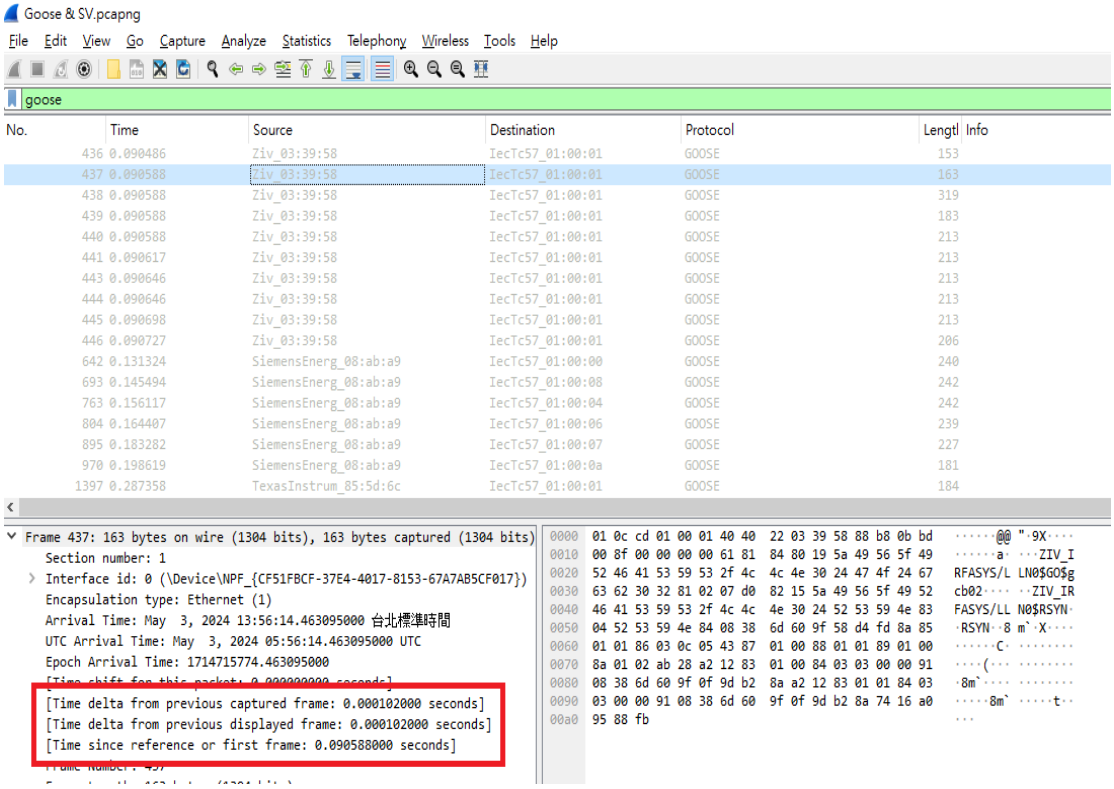

圖 27　第二個 Goose 封包的時間資料

doi:10.6342/NTU202401322

本次實驗傳送的SV（Sampled Values）封包如下圖28所示，SV是類比測量值電壓和電流作為數位資料流傳輸。這些數據對於相量測量單元 (PMU) 等應用至關重要，這些應用需要精確的同步和精度來進行電網監控、廣域保護和動態狀態估計。

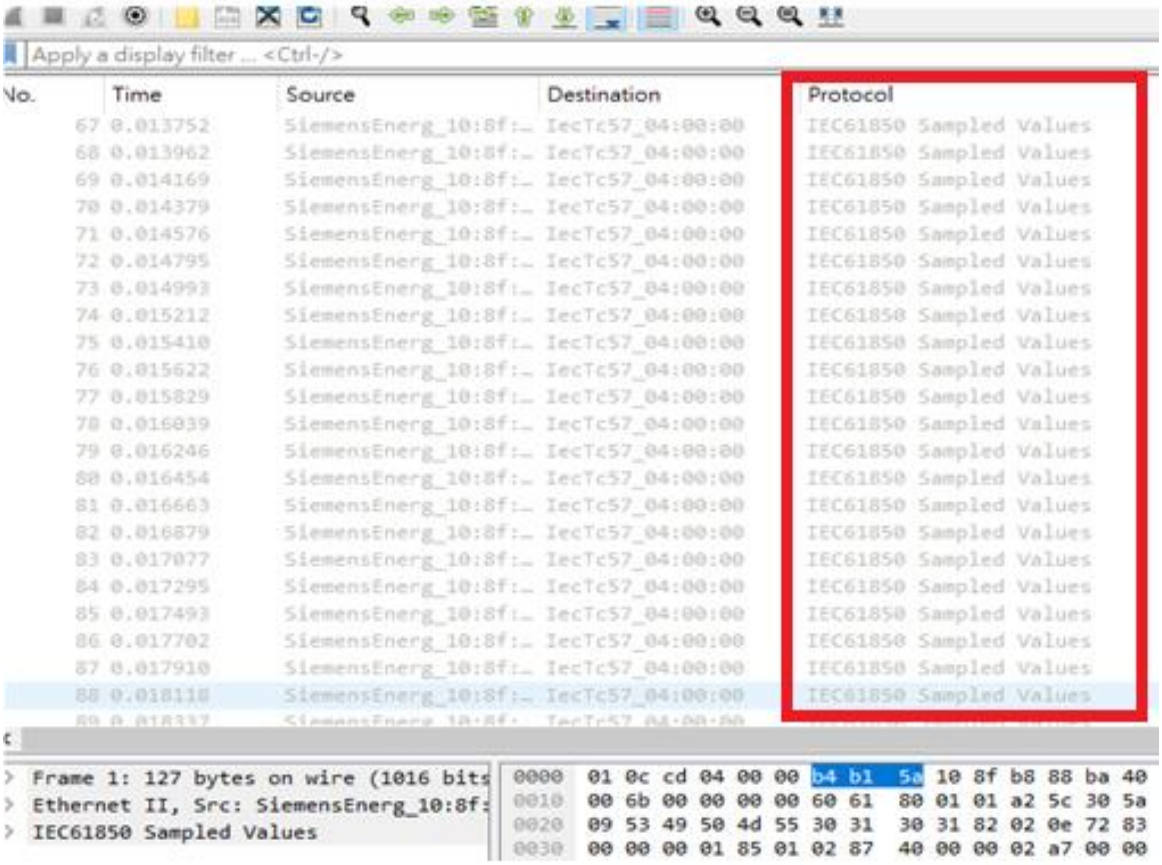

圖 28　本實驗用的 Sampled Values 封包

doi:10.6342/NTU202401322

與 Goose 相同，Sampled Values 也有相關時間資料，如圖 29 紅框處。

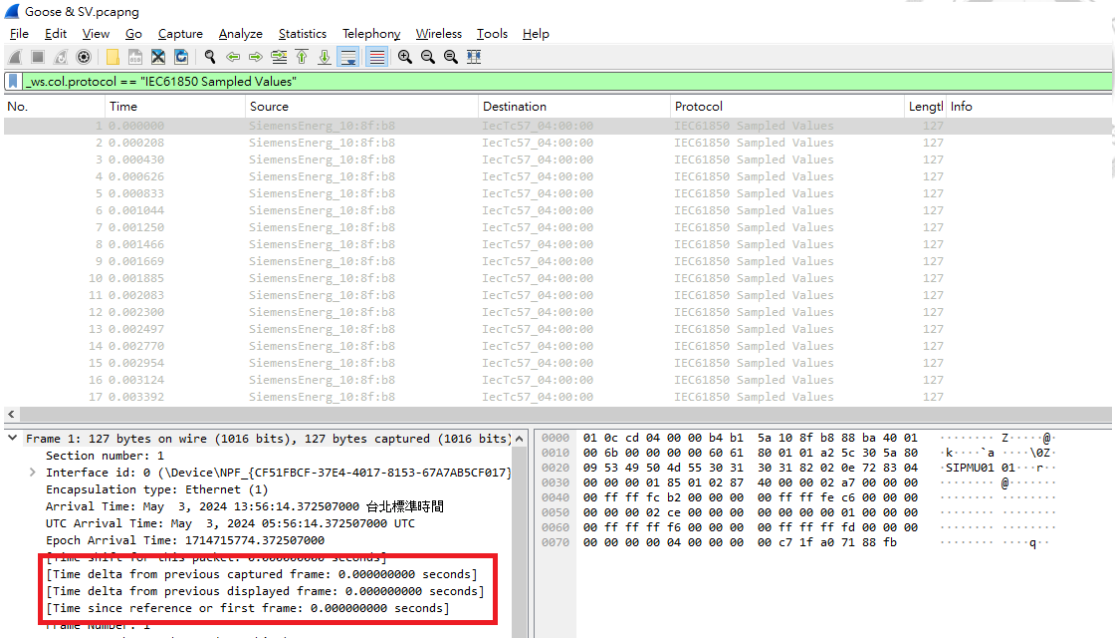

圖 29　Sampled Values 封包中的時間資料

本次實驗傳送的PTP封包如圖30所示，PTP是用來同步IED封包，本次實驗中是時間的量測基準來源。

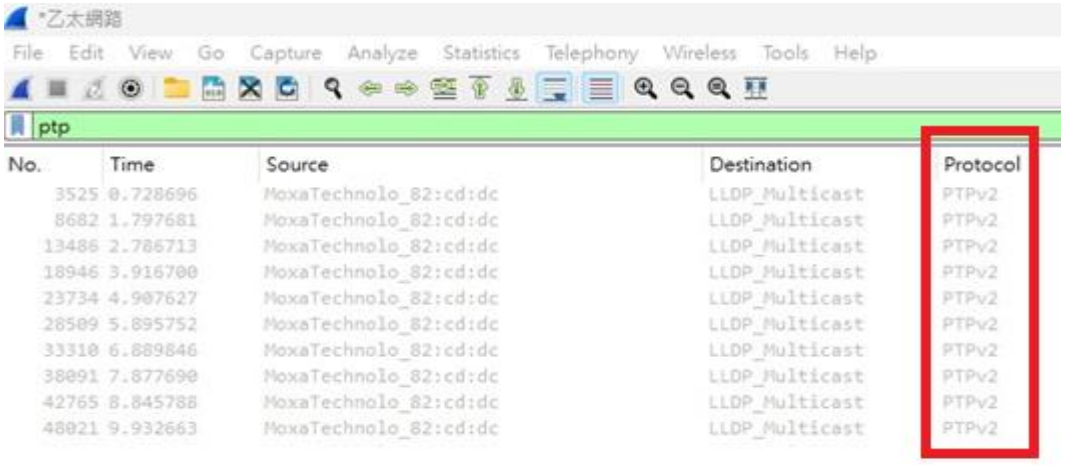

圖 30　本實驗用的 PTP 封包

GPS干擾實驗開始前，已開始傳送PTP封包，校準Switch設備的時間，Switch會再將時間同步封包傳給IED進行時間同步，圖31中，黃色是GPS時間，藍色是Switch上的時間。黃色GPS 1PPS的線有將藍色Switch 1PPS包住。並且在紅框處可

doi:10.6342/NTU202401322

以看到Switch與GPS時間誤差值顯示為40.0ns，符合PTP高精度時間和頻率同步標準，在這個狀態下Goose和SV封包有其精確性和可靠性。

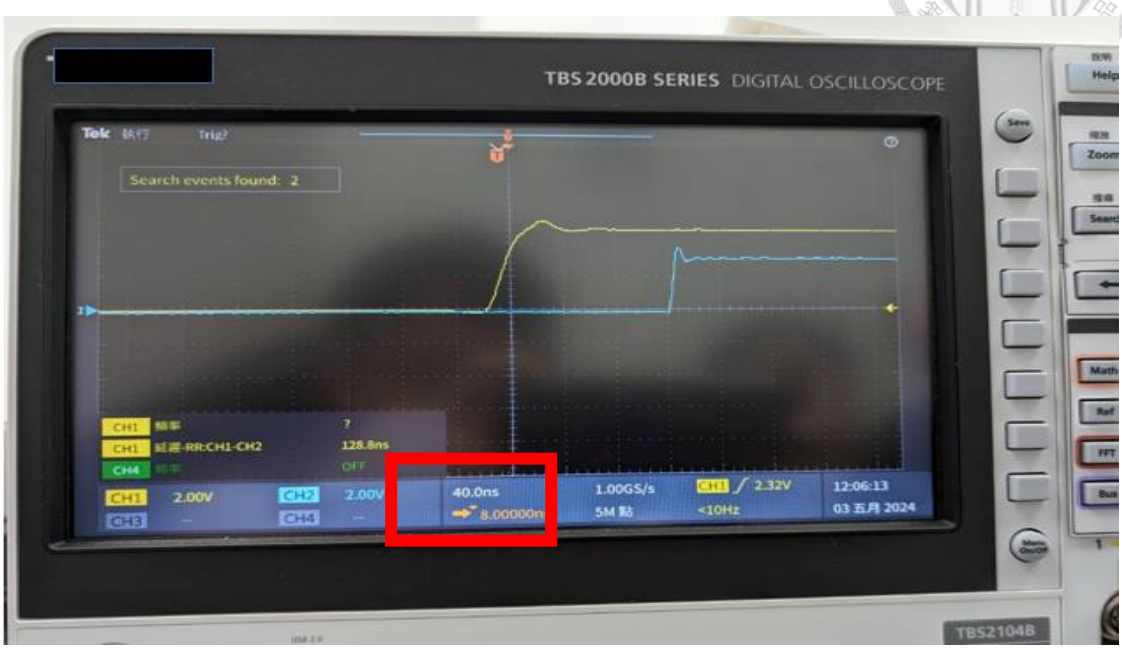

圖 31　IED 時間同步精準度量測

IED首先連到Switch進行互相溝通，如圖29所示，左上角可以看到GPS燈號為綠燈，表示Switch上GPS同步訊號一切正常。

圖 32　本次實驗用 Switch 設備

doi:10.6342/NTU202401322

Switch GUI介面顯示時間同步機制正常，如圖30所示，PTP Slave Port為1-4，PTP Sync Status為Locked。

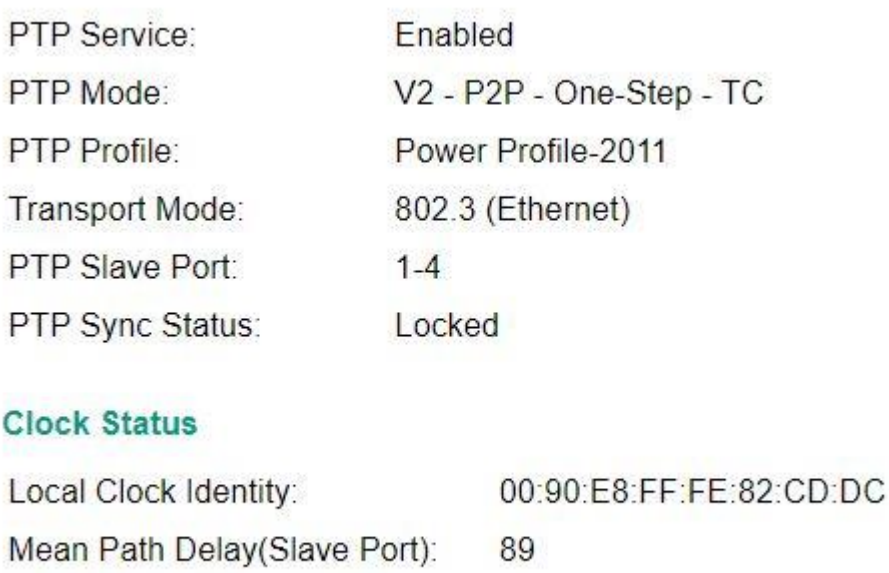

圖 33　實驗開始前的時間同步狀態

doi:10.6342/NTU202401322

在確認各項設備為正常後，GPS干擾實驗開始，左上角燈號變成橘燈，顯示GPS同步訊號異常，如圖34所示。可證明目前系統中GPS已經失去連線，時間同步源已開始受到影響及干擾。

圖 34　Switch 上確認 GPS 系統干擾開始

doi:10.6342/NTU202401322

Switch GUI介面顯示時間同步源尋找中，PTP Slave Port變為None，PTP Sync Status變為Freerun。確認GPS同步源已受干擾消失，如圖35所示。在此狀態下，系統會啟動備援機制，尋找其他IED作為主時鐘，與其他IED設備進行同步。

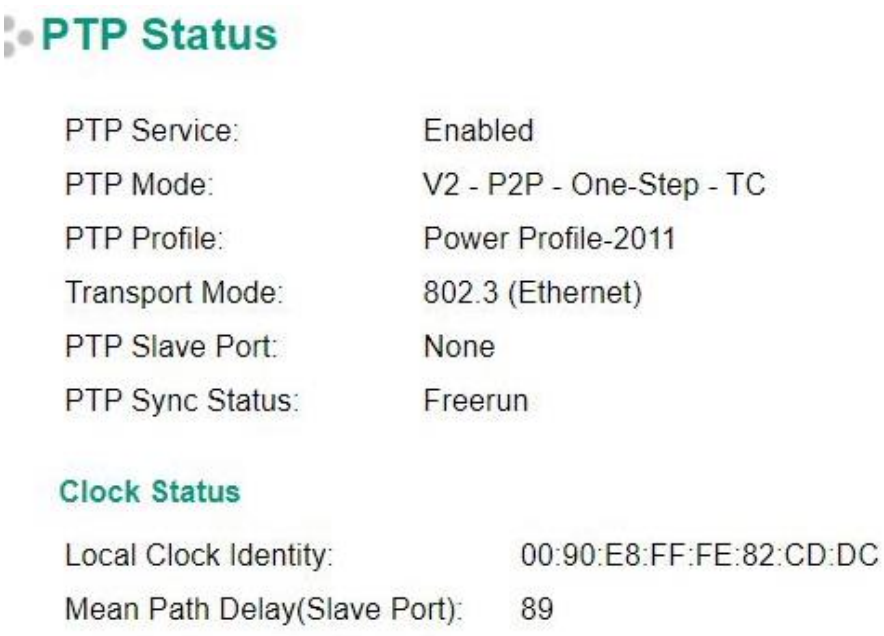

圖 35　GUI 上確認 GPS 系統干擾開始

doi:10.6342/NTU202401322

GPS干擾開始同時觀測到，IED與GPS之間時間誤差增加到4.0μs（約為4,000 ns），誤差是開始前的100倍。可以觀測到代表Switch的1PPS藍色時間線，明顯與GPS黃色時間線不合，雙方時間和頻率已開始不相同，可證明時間已開始有誤差，如圖36所示。兩個不同顏色的方框距離越遠，則代表兩個設備彼此之間的時間誤差越來越大。

圖 36　時間同步量測儀器上確認 GPS 系統干擾開始

doi:10.6342/NTU202401322

如圖37所示，從GUI介面可以看到，Switch已開始備援機制，將時間同步源鎖定到其他台IED設備作為時間主鐘。PTP Slave Port為2-4，PTP Sync Status為Syncing。

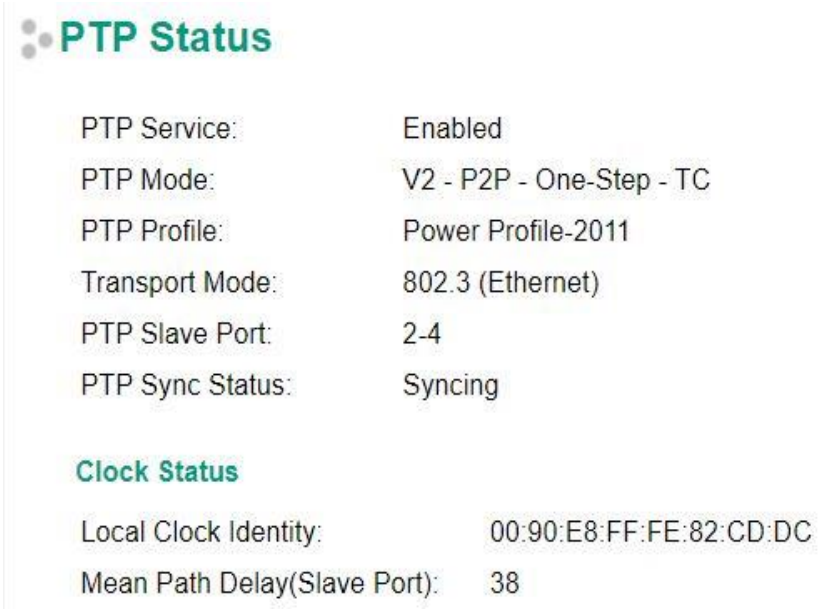

圖 37　與其他 IED 進行時間同步中

doi:10.6342/NTU202401322

如圖38所示，GPS干擾開始約5秒鐘後，時間誤差增加到10.0ms（約10,000,000ns），其時間誤差是開始前的250,000倍，如圖31所示。在這個狀態下，已經無法符合PTP毫秒等級的時間同步機制，同時Goose與SV封包的準確性和可靠性已消失。

圖 38　IED 與 GPS 時間不同步

doi:10.6342/NTU202401322

如圖39所示，GUI顯示PTP Sync Status從Syncing變成Locked，可證明切換成其他IED當主鐘步驟已完成。

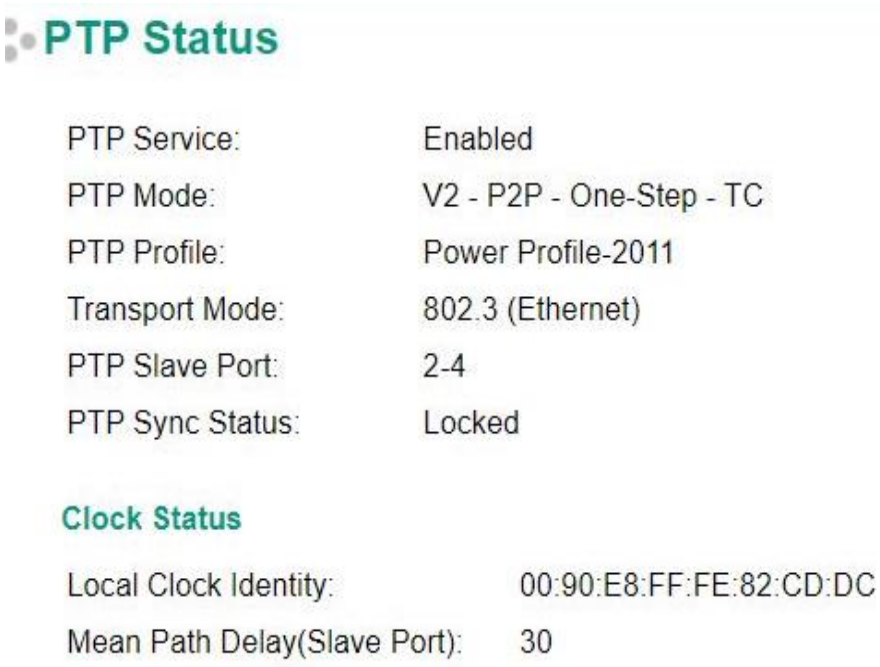

圖 39　時間同步源切完成其他 IED

doi:10.6342/NTU202401322

從電腦紀錄進行時間同步干擾觀測，如表10。

表 10　本次實驗時間表

本機時間（S）	時間差（ns）	頻率誤差（ns）	線路延遲時間（ns）
7204.880	669	136	355
7205.877	355	23	335
7206.914	230	5	255
7208.121	45	-111	223
7209.121	-48	-191	208
7210.024	-51	-208	208
7211.021	-25	-198	208
7212.018	-26	-206	208
7213.185	GPS 時間同步訊號中斷		
7215.843	切換成其他 IED 當主鐘		
7217.781	54420	3626731	215
7218.852	-3811052	-222415	215
7219.777	-3567832	-1122511	215
7220.762	-2410522	-1035550	215
7221.894	-1184047	-532232	312
7222.887	-606851	-310250	696
7223.872	-252809	-138263	1139
7224.865	-66948	-28245	2663
7225.850	10673	29292	2635
7226.889	32770	54590	2635
7227.788	29146	60797	2635
7228779	18988	59383	2635
7229.812	9862	55954	2635
7230.772	6273	55323	1055
7231.805	1991	52923	423
7232.796	49	51578	28
7233.882	-1049	50495	28

從表10的數據中可以得知，從GPS干擾開始，到切換成其他IED當主鐘完成為止（誤差回到49ns），需要約15秒左右，時間源切換成其他IED設備當主鐘後，雖然時間誤差率有明顯下降，但根據圖31可知，Switch時間與GPS時間相比，仍

doi:10.6342/NTU202401322

有一段差距。且時間誤差已超過毫秒，此狀態下的Sampled Values 及Goose封包因時間誤差的關係，皆不符合IEC 61850通訊的標準，而這樣的狀態下，變電所內短期會有系統日誌及中央SCADA系統紀錄發生偏差的情況，會導致這段期間內發生的故障或是系統事件難以分析原委，如該電廠有保護電驛，則會直接失去作用，輕則造成區域型停電，重責影響該變電站，與電網連結切斷造成供電異常。

本文驗證GPS攻擊對於5G系統以及電力系統的影響之後，接下來將會驗證時間同步的防禦機制：異地備援機制。此機制構架下，系統本身除了本地時間同步機制外，還會另接一條來自不同地區的時間同步封包，確保系統時間同步機制可以保持穩定。故為了觀察此機制切換的情況，使用了兩台時間同步設備提供同步的封包，如圖40。

圖 40　兩台時間同步源設備

doi:10.6342/NTU202401322

兩台設備都接到同一台switch中，如圖41紅框處。兩台時間同部主機分別插在port 3及port 4。

圖 41　模擬時間同步備援機制

實驗開始前，使用時間同步量測儀器確認設備目前時間同步的狀況，如圖。紅色是圖40最上面那一台，黃色線是中間那一台，藍色線是外接樹梅派，圖42中是以藍色樹梅派為基礎，兩台時間同步設備誤差在-123.1ns ~-12.46ns之間。在可接受範圍。

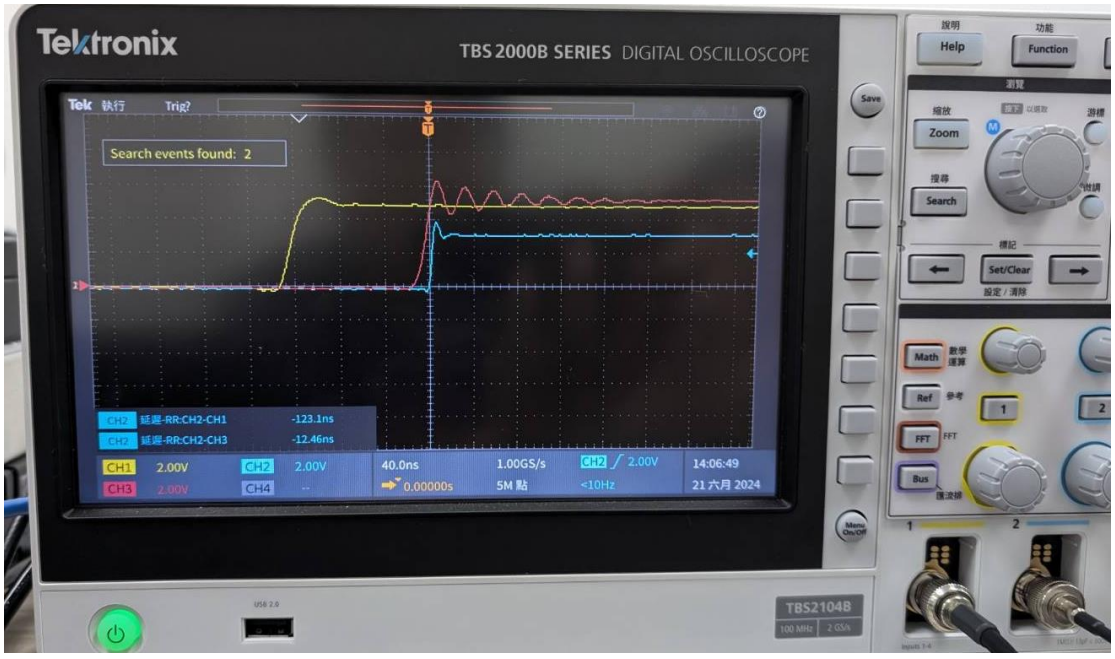

圖 42　備援機制時間同步精準度

doi:10.6342/NTU202401322

測試開始前進入設備查看，IED與port 3的時間同步機器進行同步，故使port 3連線失效進行觀察。觀測情形圖表11。

表 11　本次實驗時間表

本機時間（S）	時間差（ns）	頻率誤差（ns）	線路延遲時間（ns）
5362.694	-3	-403	145
5363.694	2	-399	145
5364.826	-7	-407	145
5365.806	-6	-408	145
5366.837	-21	-425	146
5367.815	4	-406	145
5368.846	16	-393	145
5369.807	13	-391	145
5373.377	Port3 時間同步訊號中斷		
5376.793	切換成 Port 4 當主鐘		
5377.823	-3282	-3682	145
5378.789	695	-690	145
5379.717	3525	2349	145
5380.694	897	778	146
5381.81	-240	-90	145
5382.829	-773	-695	145
5383.828	-578	-732	145
5384.709	-199	-526	145
5385.729	-71	-458	145
5386.754	-17	-425	145
5387.769	14	-399	146
5388.792	2	-407	145
5389.811	31	-377	145
5390.803	5	-394	145
5391.835	4	-394	146

從表11可知，從Port 3切換到Port 4，並且時間要恢復到穩定（時間差恢復到中段前），約從5373.823開始到5386.754，其中間間格約13秒。可以得知，時間源切換並非立刻切換，切換過程仍需要一段時間進行同步調整，此切換時間在未

doi:10.6342/NTU202401322

來資安分析時需要注意。

並且本文嘗試是偽造PTP封包，並將錯誤時間同封包傳入系統中。從圖43中可以看到各設備的時間，藍色為本次偽造時間來源，明顯與受測試黃色線和紅色線有間距。其時間誤差約在13.48μs ~ 13.57μs。與本實驗正常狀態的時間同步40.0ns相比，藍色相差了約13476ns，可見誤差非常明顯。

圖 43　偽造時間同步主機精準度間距

doi:10.6342/NTU202401322

在藍色線主機中嘗試調整PTP封包中的Priority等級為1（預設通常為128）。如圖44，此設定是為了搶奪其他設備的時間同步優先權，Priority等級越小，優先度越高。

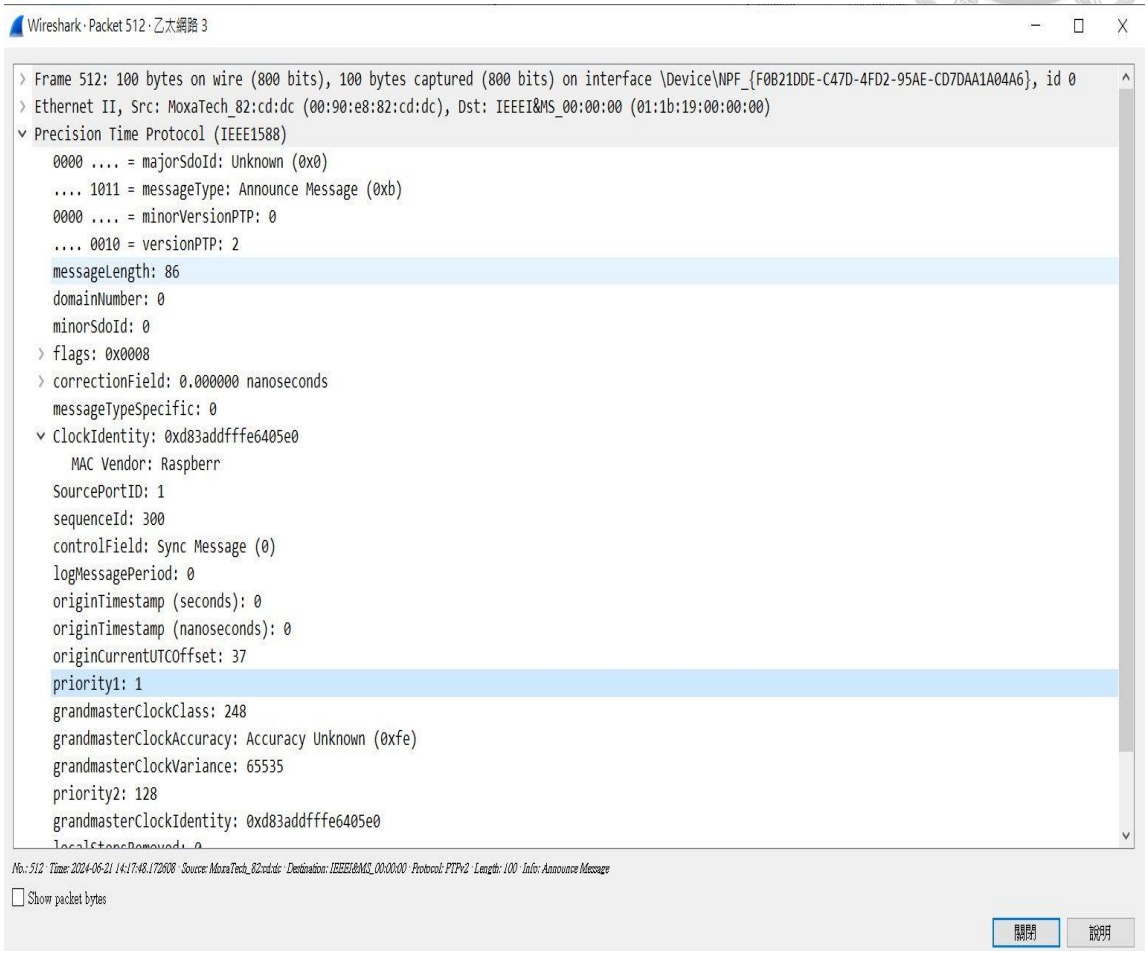

圖 44　偽造的時間同步封包

doi:10.6342/NTU202401322

實驗結果如圖45，圖中可以看到兩台IED時間同步來源不相同，IED編號AA1J1Q01A1的同步源是來自偽造的封包。

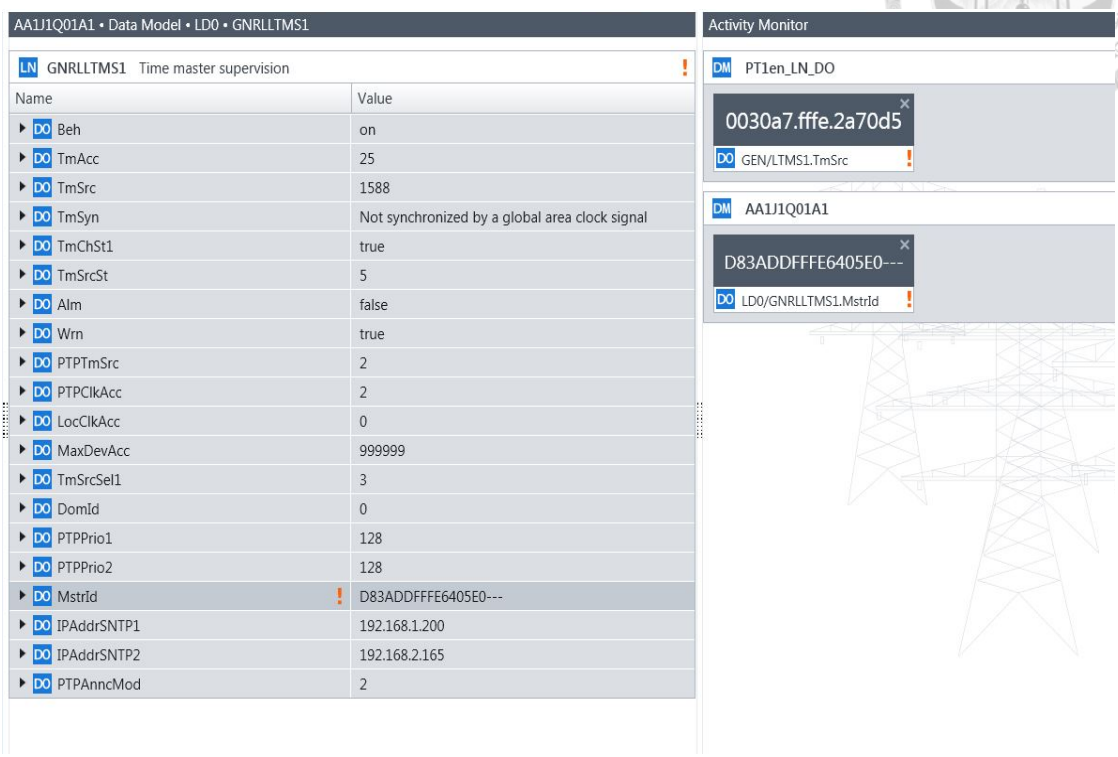

圖 45　偽造PTP封包攻擊成功

也可以透過偽造時間精準度進行系統干擾，如圖46，圖中時間精準度為100ns。

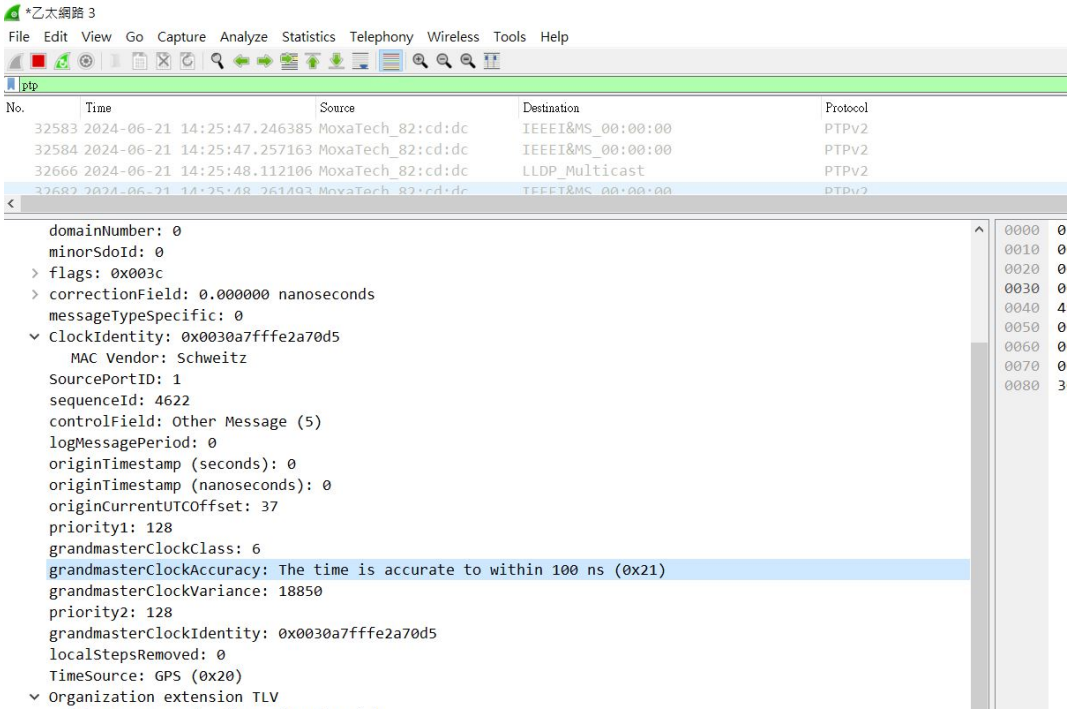

圖 46　模擬時間同步備援機制

doi:10.6342/NTU202401322

經由本次實驗可知， GPS干擾對於5G系統和電力系統來說，會影響整個系統服務。並且可以透過RSRP、Cell ID等資訊，透過資料收集進而反推可能提供服務的基地台地址，進而提高實際GPS干擾的成功率，可能會造成更嚴重的資安危害。如圖47所示，透過筆電收集到的資料，反推基地台地址（紅框處）。

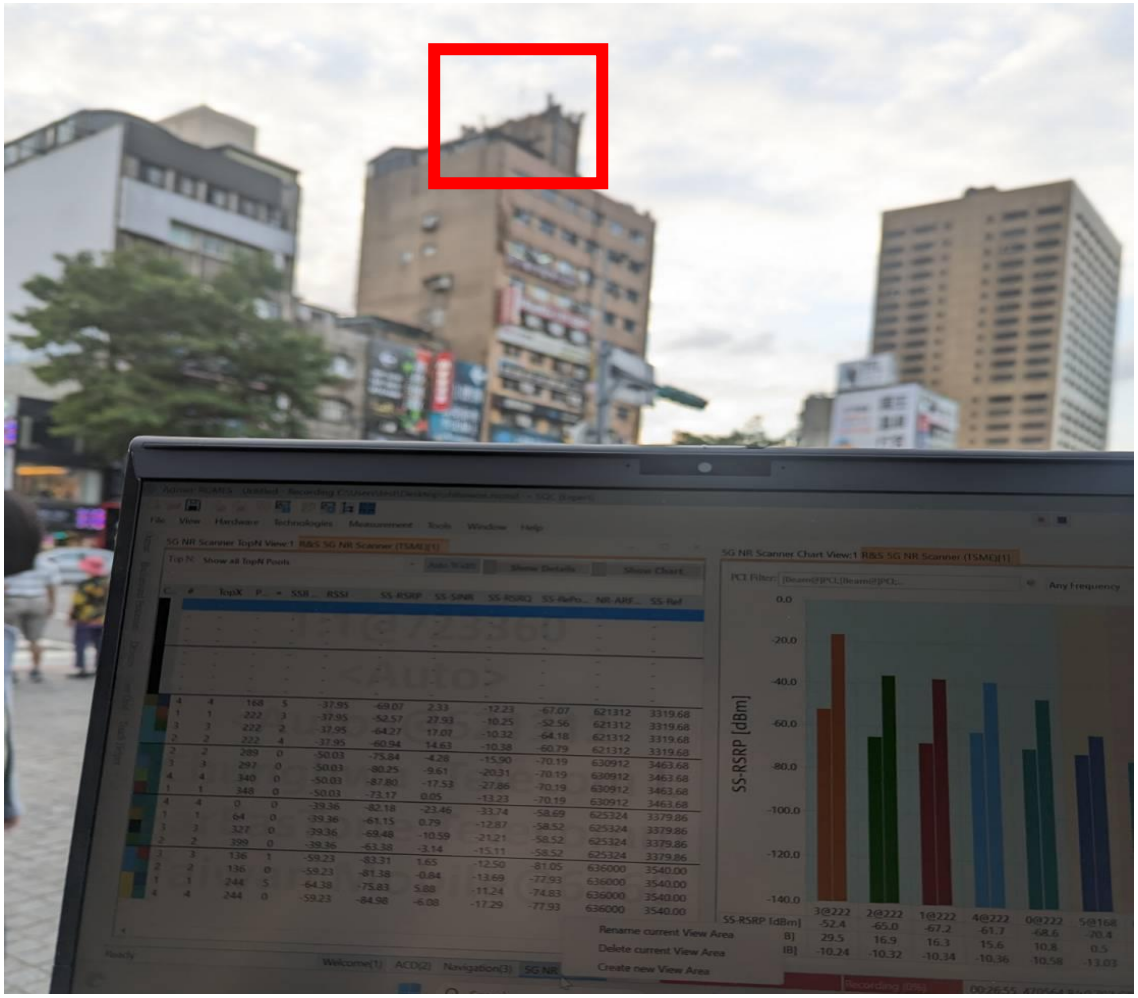

圖 47　透過 5G 量測訊號反推基地台地址，台大正門

透過本次實驗，觀察到GPS干擾會造成的5G系統通訊異常狀態，其整個過程大約為27分鐘，電力系統則是有立即性的影響。其中斷發生的時間長短與使用的GPS和設備等級及品質有相關性。更低等級的設備可能導致較短的服務中斷時間，而較高等級的設備可能需要更長的時間才會中止服務。

doi:10.6342/NTU202401322

在台灣，5G基地台的普及已經相當普遍，它們通常建置在各種地方，包括公寓和民宅的樓頂，其高度約在5到6層樓之間。這種分佈特性能夠觀測不同位置的基地台受到GPS干擾時可能產生的差異。這次實驗的結果將有助於未來制定有效的防禦手段，以減少時間同步對5G通訊系統和智慧電網的潛在影響。如圖48所示（圖源來自Google）。

圖 48　桃園大潭電廠內疑似 GPS 接受器

doi:10.6342/NTU202401322

加上GPS天線通常設置在室外，缺乏機房的保護，且暴露於室外環境，5G基地台通常架設在地面高度不超過500~600公尺的公寓頂樓。這使得有心人士可以利用無人機或其他方式進入頂樓，實施對GPS的干擾。如5G服務中斷，電廠內的智慧巡檢、智慧工安等服務都會中斷，將會造成變電所內人員受傷或是供電異常的事件發生。如圖49所示。

圖 49　台灣隨處可見的 5G 基地台

doi:10.6342/NTU202401322

特別是在5G專網推廣的情境下，基地台將會推出企業專用的服務狀態，以本文為例，如針對提供電力系統特殊專用服務的基地台進行干擾，可能提高攻擊的精確性，進而導致更嚴重的損害，如圖50所示（圖源來自Google）。

圖 50　台中火力發電廠內基地台

並且根據台電公告，雖然每次停電連續未滿十分鐘時，不予計算，但造成的社會形象損失，難以估計。可如造成大規模停電，根據台電815停電事件的資料，2017年8月15日16時51分開始停電，最終於同日23時始恢復正常供電，歷時7小時，台電當時賠償總額約3.6億元，此金額不包含電廠後續修復、社會責任、人員損害等金額賠償。總和上述可知，對電力系統進行駭客攻擊，將會造成巨大危害。

doi:10.6342/NTU202401322

4.3 5G 資安解決方案

前述章節，透過實驗發現針對5G網路GPS進行攻擊，極容易干擾5G通訊系統上的時間同步之運作，進而更可能癱瘓整體智會電網上時間同步之運行。有具於時間同步係維繫智慧電網之命脈，因此，透過本論文簡易的實驗觀察，未來電力系統導入數位化，智慧化的同時，亦須一併將5G內建的資安防護規劃進來，並視為是首要任務。有關5G內建資安防護措施，茲羅列分述如下：

- 時間同步的部分：

  5G通訊系統因GPS攻擊導致系統無法運作，故須針對GPS通訊的部分進行相關防護，需要構建對應的冗餘增強機制。基於冗餘理論，本論文提出兩種系統建議方案：一是採購加裝同步主時鐘（GrandMaster clock，GM），將所需干擾時間延長，實現長期穩定性優化；二是構建區域性多點GPS信源輸入，實踐GPS冗餘機制。上述冗餘機制不僅可有效對應GPS干擾，也為系統構建了應急備份和故障切換機制。在此架構下，預估可有效增強5G基站的抗干擾能力與可靠性，並防止惡意人士的蓄意攻擊。

- 無線電接取網路防禦的部分：

  因基地台並未受機房保護，可能遭受實體入侵攻擊。故須加裝門禁等，控管通網基地台出入口，減少駭客入侵的風險。為防禦駭客自行架設偽造基地台，進行惡意蓋台攻擊等行為，定期檢測空中頻段，查詢是否有偽造或是干擾的訊號，也須確認5G加密機制是否有正常運作，藉此防止基地台偽造攻擊行為。

- MEC的部分：

  因MEC主機已脫離電信機房，搬移到企業用戶端，故MEC需自行維運及維護，需要定期維護和更新，並加裝防火牆進行資安防禦，藉此降低

doi:10.6342/NTU202401322

資安風險。

- 資料傳輸的部分：

  為了防止DDOS攻擊，5G網路相關裝置，須盡量避免IP曝光，故在建置的時候，就須考量整體網路架構，減少內部對外部的直連需求，並在相關閘道架設防火牆進行防禦。

- 核心網路的部分：

  企業需在各節點加裝IDS（Intrusion-detection system, IDS）或IPS（Intrusion Prevention Systems, IPS）設備即時監測各用戶網路使用行為，如發現有異常，可從核心網路端進行管理控制，並且為了保持整體網路的穩定性，需定期進行教育訓練及檢查，確保系統符合企業用戶各種資安規範。

doi:10.6342/NTU202401322

4.4 智慧電網導入 5G 資安防護架構

前有述及，智慧電網係一大型IoT系統，在導入茲安防護規劃上，首要遵循的是工控資安標準（IEC 62443），其次是專網針對規範智慧電網的資安標準（IEC 62351）；另外，參考國外電力公司的作法，IoT的資安標準亦須納入一併規範。基此，未來智慧電網在導入5G通訊系統時，除須納入前節所述5G內建資安防護要求外，一須納入此地所列IEC 62443、IEC 62351，以及IoT資安之要求等。

具體而言，在本文3.3章節中，5G技術導入智慧電網的架構時，須從變電所開始，進行資安邊界的規劃。將各個區域明確劃分開來，引入防火牆作為區域之間的隔離措施。每個區域需進行設備、應用、人員等層面的盤點，並針對盤點統計出來的資料進行評估，其目的為了提高整體安全性，並需要引入不同的資安設備和標準作業程序進行防護和監控，其具體的防護手段包括DDoS（分散式阻斷服務）防禦設備、IPS、DMZ（Demilitarized Zone, DMZ）隔離區、身分認證機制等。

並根據本文測試，時間同步機制即使有異地備援機制，實際切換仍須依一點時間，切換的過程中是否會對設備造成影響，須謹慎評估。並且時間同步封包容易偽造及干擾，IPS進行封包過濾時，須了解各現場單位最佳主時鐘演算法（Best Master Clock Algorithm, BMCA）防止誤擋正確的時間同步封包。

doi:10.6342/NTU202401322

其餘智慧電網涵蓋區域，亦須以變電所資安防護架構為例，導入所需規劃和建置，特別是最近數位部所倡導的「零信任機制」（Zero Trust），也是運營科技（Operational Technology, OT）段資安很重要的參考，亦須一併納入考量，詳如下圖51所示。

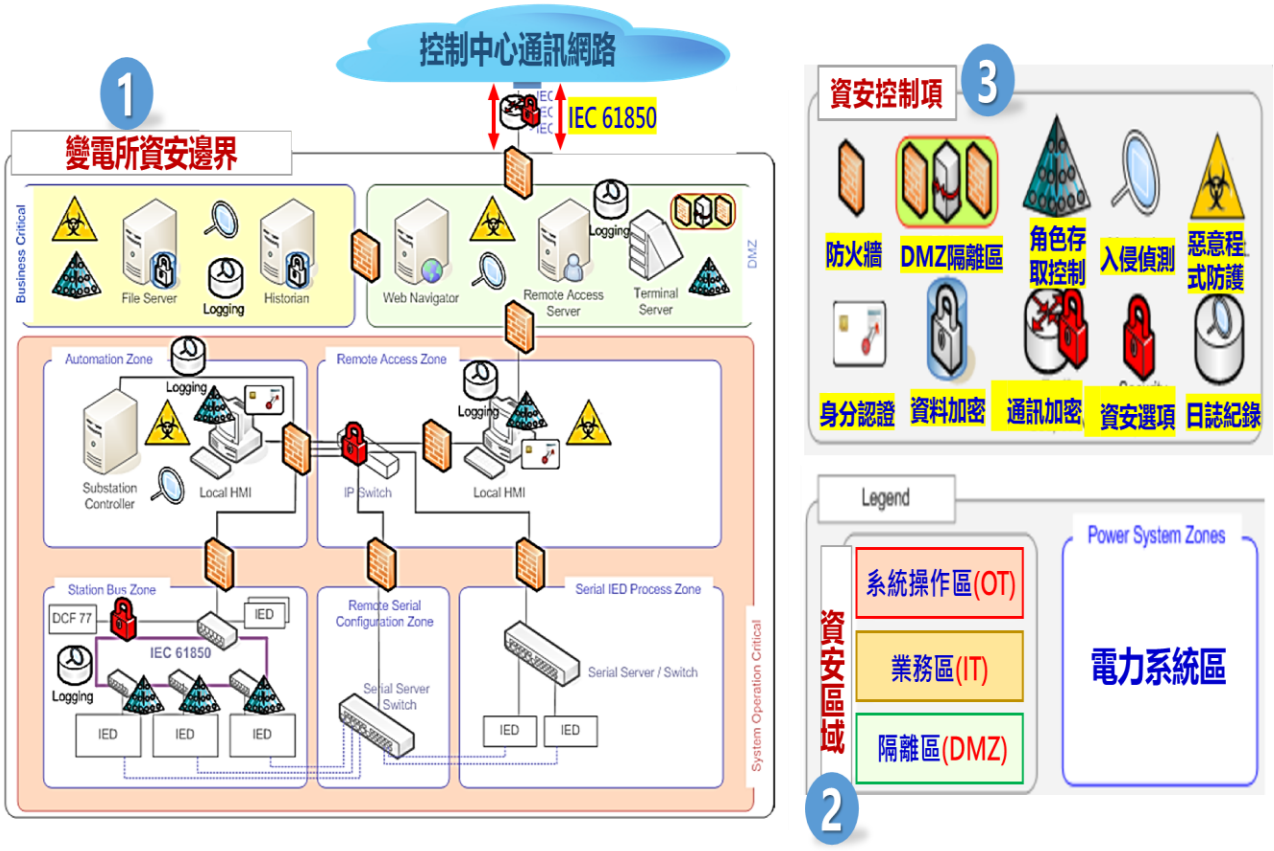

圖 51　變電所資安防護架構[27]

doi:10.6342/NTU202401322

Chapter 5 結論與建議

5.1 結論

本論文旨在於蒐集並整理與5G相關技術以及將其導入智慧電網所需之相關文獻，進而提出一個未來5G導入智慧電網的網路架構。同時，為確保此架構的安全性，論文進行了對5G潛藏的資安風險的評估，針對潛在的資安疑慮進行測試，並提出相應的解決辦法，其目的是為了提供一個更完整且更安全的5G智慧電網網路架構。

本論文研究的主要內容，包括：

- 透過3GPP技術文件，瞭解5G技術，和5G導入智慧電網的可行性，並確認智慧電網之通訊需求。
- 透過收集文獻，和國外電力公司應用案例，研析和規劃合適導入智慧電網之5G通訊網路架構，並明確闡述5G在智慧電網中所能發揮的效用。
- 透過簡易實驗室資安檢測，發現資安之易危害性和可能導致的高風險。
- 提出未來合適導入智慧電網之資安防護架構和多元導入解決方案之建議。

經由本研究結果亦發現，未來的智慧電網通訊網路架構應以電力領域實務應用需求為前提，而任何網路攻擊皆可對智慧電網造成影響。基此，本論文提出5G導入智慧電網架構及其資安風險之防護架構，可強化未來智慧電網網路通訊系統架構，並降低資安風險，同時這也是跨領域專業整合應用，包括：電力專業、通訊技術以及資安解決方案等，希冀經由本研究跨出第一步，提供未來所需之技術和決策支援。

doi:10.6342/NTU202401322

為符合IEC62443以及台電現有規範[28]，智慧電網可能遭到威脅的情況下為系統或設備無法使用的情況，可能會有蠕蟲，以及DDOS阻斷攻擊；或是遭受未經授權取得機敏資料或是未經授權修改資料，如：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。MEC與電力系統網路應要架設防火牆進行隔離，其MEC Sever也需要定期進行弱點掃描。透過通訊日誌紀錄和入侵偵測等機制，防止非系統人員的入侵，並檢測是否有異常的連線終端。最後，須制定相關操作SOP，確保發生異常時，系統人員可以在網路端將異常使用者中斷連線的同時，並確保整個無線通訊網路可正常運作。

智慧電網未來將會加入大量智慧裝置，提高通訊資料量，並要求低延遲高穩定的傳輸，不同於其它無線通訊系統，上述這些特性5G皆符合。並且透過國際案例整理，可以得知各國陸續將5G通訊導入智慧電網中，並加入許多新的應用，如智慧公安、無人機巡檢等無線應用服務，藉此補足電力系統中無線通訊端的不足，

doi:10.6342/NTU202401322

5.2 建議

經由本論文主要研究內容和研究結果，得知5G技術具有在無線網路領域提供新型低延遲、穩定、高速架構的潛力，未來透過結合5G MEC技術、SDN、MPLS、PON和PLC等通訊技術可以打造出肆應於智慧電網所需的5G確定性網路，以便符合智慧電網對於多元化通訊技術之需求。是故，5G企業專頻專網是電力系統建立通訊自主網的一個重要的契機和關鍵，電力公司在導向未來數位化和智慧化的方向時，可以把握此機會，超前部署5G企業專頻專網。

此外，資安的導入，本論文建議亦應搭配智慧電網多元應用的需求，以及電力系統邊界含蓋廣大、異質之特性，也需要有諸多解決方案熔治一爐，朝向多元化方向部署，俾能提供實際應用之需。

透過本文的實驗可知，時間同步異常將會對5G造成應用服務中斷的危害，在未來5G將會用於智慧公安、智慧巡檢等應用服務，在5G通訊中斷或是GPS遭受攻擊的狀況下，小則造成人員危害，或是通訊異常造成的區域性停電，重則人員死亡的公安危險，或是造成電廠之間電力傳輸異常，進而導致發電系統受損等情況。

時間同步對台灣電力系統是非常重要的機制，為了防止受到外部的干擾或是駭客攻擊，從文獻整理及進行相關實驗後，本研究建議台灣電力系統需要打造一個自己的時間同步網路。

最後，本論文建議前述打造5G確定性網路，以及整合資安多元解決方案，均需在智慧電網規劃階段，一併導入融和規劃，讓5G確定性網路和多元資安解決方案，對於智慧電網來說，係猶如原生的DNA般嵌入其中，以便發揮內生最大的效用。

doi:10.6342/NTU202401322

5.3 未來研究展望

承繼前述，5G網路導入智慧電網，除了5G網路相關技術之外，亦需要搭配其他通訊技術，諸如：MEC技術、SDN、MPLS、PON和PLC等通訊技術共同融和打造5G確定性網路。另，整體性資安防護架構在智慧電網上，更需要尋求多元解決方案的協助。此種跨專業、跨技術的應用型研究，需要打造的是一個生態系級別的研究生態來長期支應。有鑑於此，未來研究展望應朝上述相關方向盡早部署和規劃，俾利國家電網盡早登上數位化和智慧化之列，而本文只是一個拋磚引玉的開始。

此外，未來的智慧電網也應考慮導入數位孿生（Digital Twin）技術，透過資料建立虛擬環境的技術，可用於設備的測試、監控、模擬、分析、預測和控制。屆時可將5G確定性網路架構和多元資安解決方案，在智慧電網規劃的階段，均可導入，一併考量，那智慧電網導入數位孿生技術，亦是未來研究展望中重要的研究議題之一。

doi:10.6342/NTU202401322

參考文獻

[1]Securityaffairs, "*SODINOKIBI RANSOMWARE OPERATORS HIT ELECTRICAL ENERGY COMPANY LIGHT S.A*," July. 2020.[Online]. Available: https://securityaffairs.com/105477/cyber-crime/sodinokibi-ransomware-light-s-a.html

[2]ITHOME, "印度核電廠證實遭北韓惡意程式入侵網路" Nov.2019.[Online]. Available:https://www.ithome.com.tw/news/133961

[3]ITHOME, "阻斷服務攻擊（DoS）對於全球設備製造商帶來的挑戰與因應之道" Oct.2020 [Online]. Available:https://www.ithome.com.tw/pr/140574

[4]3GPP, "5G System Overview,"Aug. 2022 [Online]. Available:https://www.3gpp.org/technologies/5g-system-overview

[5]NCC, "5G 行動通訊網路安全：認證安全機制淺談" Oct.2020 [Online]. Available:https://nccnews.com.tw/202010/ch4.html

[6]Ericsson, "*5G synchronization requirements and solutions,*"Jan. 2021.[Online]. Available:https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/5g-synchronization-requirements-and-solutions

[7]3GPP,"TR 22.867" Dec. 2021. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/22_series/22.867/

[8]搜狐, "南方电网 5G 智能电网项目入选 2022 年世界 5G 大会十大应用案例 "Aug. 2022. [Online]. Available: https://www.sohu.com/a/577874677_321349

[9]The Norwegian Smartgrid Centre, "*5G communication for smart grid application*," Apr. 2021 [Online]. Available: https://www.youtube.com/watch?v=NNpDNwrwLRo

[10]Slicenet, "*5G Smart Grid Self-Healing Use Case,*"[Online]. Available: https://slicenet.eu/5g-smart-grid-self-healing-use-case/

[11]Thehansindia, "*How 5G can supercharge India's power sector,*"June. 2022. [Online]. Available: https://www.thehansindia.com/business/how-5g-can-supercharge-indias-power-sector-748877

[12]IEC,"*Power systems management and associated information exchange,*"June. 2017. [Online]. Available: https://www.iec.ch/dyn/www/f?p=103:7:0::::FSP_ORG_ID,FSP_LANG_ID:1273,25

[13]標檢局 "智慧電網標準 112 年第 2 次工作組會議"

[14]IEEE, "*QoS Proposal for IEC 61850 Traffic Under an SDN Environment*,"Jan. 2019. [Online]. Available:https://ieeexplore.ieee.org/document/8613240

[15]台灣電力股份有限公司, "智慧電網規劃" [Online]. Available: https://service.taipower.com.tw/csr/esg/leader/smart-grid

[16]Ericsson, "*A Solar Solution,*" Dec. 2021. [Online]. Available: https://www.ericsson.com/.

[17]Ericsson, "*Building a Greener Network,*" Dec. 2021. [Online]. Available: https://www.ericsson.com/.

doi:10.6342/NTU202401322

[18]Nokia, "*Nokia confirms 5G as 90 percent more energy efficient,*"[Online]. Available: https://www.nokia.com/about-us/news/releases/2020/12/02/nokia-confirms-5g-as-90-percent-more-energy-efficient/
[19]遠傳電信"《5G 頻率政策與產業發展白皮書》" Sep. 2022
[20]IEEE, "*The research of time unified system in smart grid*," Aug. 2012. [Online]. Available:https://ieeexplore.ieee.org/document/6417453
[21]Wiley, "*Improving smart grid security through 5G enabled IoT and edge computing*,"July. 2021 [Online]. Available: https://onlinelibrary.wiley.com/doi/full/10.1002/cpe.6466
[22] 金瀚信安"盘点：全球电力行业十大网络安全攻击事件" [Online]. Available:http://www.jinhansafe.com/2071.html
[23]IEEE, "*GNSS Time Signal Spoofing Detector for Electrical Substations,*"Oct. 2021 [Online]. Available:https://ieeexplore.ieee.org/document/9583423
[24]ITHOME,"GPS 失靈一個月？美國研究：將造成 300 億美元的損失"June. 2019. [Online] Available:https://www.ithome.com.tw/news/131316
[25]ITHOME,"另類網路攻擊！北韓發動 GPS 蓋臺，韓國境內導航系統失效，恐導致所有武器無法定位" Apr. 2016. [Online] Available: https://www.ithome.com.tw/news/105156
[26]NCC,"NCC 與電信業者公私協力 普建 5G 網路建設"Dec. 2021. [Online]. Available:https://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=8&sn_f=46962
[27]IEC, "*IEC 62351 – Cyber Security Series for the Smart Grid,*"Oct. 2021 [Online]. Available:https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/iec-62351/
[28] 台灣電力公司,"台灣電力公司配電級再生能源監控設備 雲端資料系統試驗及管理規範" Dec. 2021. [Online]. Available: https://www.taipower.com.tw/upload/123/2021011514315169391.pdf

doi:10.6342/NTU202401322