台電工程月刊927期(11月)目錄

智慧電網資安規劃策略與實際應用情形　專輯
Special Issue: Smart Grid Cybersecurity Planning Strategies and Actual Application Scenarios

實踐國際資安標準：ISA/IEC 62443 在智慧電網分散式能源與變電站保護中的應用

Applying International Cybersecurity Standards: The Application of ISA/IEC 62443 in Distributed Energy Resources and Substation Protection in Smart Grids

林上智*
Lin, “SZ” Shang-Jyh

摘 要

隨著智慧電網與再生能源快速發展，電力系統面臨複雜資安威脅，傳統實體隔離防護已難因應。分散式能源(DER)與數位變電站大量部署，使電網攻擊面顯著擴大，對穩定營運與基礎設施安全構成挑戰。

ISA/IEC 62443 為工業控制系統資安國際標準，提供涵蓋政策制定、技術架構與生命週期管理的完整框架，已被美國、歐盟等主要經濟體納入關鍵設施資安規範。本文以智慧電網中的分散式能源與數位變電站為核心，分析導入 ISA/IEC 62443 標準的實務方法，並針對跨部門協作、老舊設備與供應鏈安全等挑戰提出建議。

實施策略採用「三階段導入模式」：(1)現況盤點與風險基線建立、(2)核心安全控制實施、(3)持續監控與改善機制；結合「三構面防護架構」，涵蓋管理面(政策制定與人員治理)、實體面(場域與設備安全)與技術面(通訊防護與存取控管)。透過此策略，電力場域可強化資安治理成熟度，提升韌性防護能力，與國際標準接軌，為未來區域合作與法規遵循奠定基礎。

Abstract

With the rapid development of smart grids and renewable energy, power systems are increasingly exposed to sophisticated cybersecurity threats that can no longer be mitigated by traditional physical isolation. The widespread deployment of Distributed Energy Resources (DER) and digital substations has significantly expanded the attack surface of the grid, creating serious challenges for operational stability and the protection of critical infrastructure.

ISA/IEC 62443, the international standard for industrial control system cybersecurity, provides a comprehensive framework encompassing policy formulation, technical architecture, and lifecycle management. It has been incorporated into critical infrastructure cybersecurity regulations in major economies such as the United States and the European Union. This paper focuses on the role of DER and digital substations in smart grids, examining practical approaches for adopting the ISA/IEC 62443 standard, and offering recommendations to address challenges including cross-departmental collaboration, legacy equipment, and supply chain security.

The proposed implementation strategy follows a three-phase deployment model：(1) current-state assessment and risk baseline establishment, (2) implementation of core security controls, and (3) continuous monitoring and improvement mechanisms. This is integrated with a three-dimensional protection framework that addresses the management dimension (policy development and personnel governance), the physical dimension (facility and equipment security), and the technical dimension (communication protection and access control). By applying this strategy, power facilities can strengthen the maturity of cybersecurity governance, enhance resilience against evolving threats, achieve alignment with international standards, and establish a foundation for future regional cooperation and regulatory compliance.

關鍵詞(Key Words)：工業自動化與控制系統資訊安全標準(ISA/IEC 62443)、智慧電網資安(Smart Grid Cybersecurity)、分散式能源(Distributed Energy Resources, DER)、變電站資安(Substation Cybersecurity)、縱深防禦(Defense-in-Depth)、工業控制系統資安(Industrial Control System Cybersecurity)、關鍵基礎設施防護(Critical Infrastructure Protection, CIP)、營運技術資安(Operational Technology Cybersecurity, OT Cybersecurity)。

*國際自動化協會臺灣分會

台電工控場域入侵偵測系統(IDS)部署經驗分享與未來展望

Deployment Experiences and Future Outlook of Intrusion Detection System (IDS) in Taipower's Industrial Control Environments

蔡修竹* Tsay, Shiou-Jwu　李建隆* Li, Chien-Lung　陳治宇* Chen, Chih-Yu　黃于庭* Huang, Yu-Ting

摘　要

隨著數位時代資安威脅日益增加，台電公司分階段於發電、供電及配電等工控場域建置入侵偵測系統(Intrusion Detection System, IDS)。OT IDS 透過流量側錄與單向閘道器達成高安全性的監控與即時警示。本公司入侵偵測系統部署策略採五階段流程，從探索、設計、部署、測試到交付，每階段皆詳實規劃並以場域作業穩定不中斷為原則。實際成果方面，截至 2024 年底已完成 23 個場域部署，全年共偵測 234 筆告警，其中以未授權新資產進入場域比例最高，凸顯維持場域封閉性的重要性。未來台電公司亦將持續進行工控場域資安強化規劃，包含導入 USB 離線掃描、端點防護與建置 OT 入侵偵測與防禦(IDP)，達成網路微分段與異常阻擋，持續強化智慧電網整體資安韌性。

Abstract

As cybersecurity threats continue to escalate in the digital era, Taipower has undertaken a phased deployment of Intrusion Detection System (IDS) across industrial control environments, including power generation, transmission, and distribution systems. The Operational Technology Intrusion Detection System (OT-IDS) ensures secure monitoring and real-time alerting through traffic recording and unidirectional gateways.

The deployment strategy follows a five-phase process, exploration, design, deployment, testing, and delivery, each carefully planned with the guiding principle of maintaining stable and uninterrupted field operations. By the end of 2024, IDS had been deployed at 23 sites, generating a total of 234 alerts throughout the year. The majority of these alerts were related to unauthorized assets entering the environment, underscoring the critical importance of preserving system isolation.

Looking ahead, Taipower will continue strengthening cybersecurity in its industrial control environments. Planned initiatives include the adoption of USB offline scanning, endpoint protection, and the deployment of OT Intrusion Detection and Prevention (IDP) systems. These measures are designed to enable network micro-segmentation and anomaly blocking, thereby enhancing the overall cybersecurity resilience of the smart grid.

關鍵詞(Key Words)：入侵偵測系統(Intrusion Detection System, IDS)、營運科技(Operational Technology, OT)、入侵偵測與防禦(Intrusion Detection and Prevention, IDP)、工業控制系統(Industrial Control System, ICS)、入侵預防系統(Intrusion Prevention System, IPS)、進階持續性威脅(Advanced Persistent Threat, APT)。

*台灣電力公司資訊系統處

IEC 61850 智慧電網通訊與網路安全研究

A Study on IEC 61850 Communication and Cybersecurity in Smart Grids

張哲豪* 許博堯*
Chang, Che-Hao Hsu, Po-Yao

摘 要

IEC 61850 為電力系統設計的國際通訊標準，在智慧電網數位化中扮演關鍵角色，特別於變電所自動化，提升效率與互通性。然而，隨著電力網路高度互聯，資安威脅日益嚴峻，如惡意軟體、阻斷服務、MiTM 攻擊及設備漏洞，對系統穩定與公共安全構成風險。本研究探討多種防護策略，包括 Canvas 指紋等身份驗證技術、低延遲環境下的入侵偵測系統應用，以及依循 IEC 62351 標準並結合硬體加速以強化通訊安全。此外，討論以 ISA99/Purdue 模型為基礎的 OT 導向縱深防禦與高可用性設計，確保電力網路於極端情況下仍能穩定運作，為智慧電網建構兼具效能與資安的實務參考。

Abstract

IEC 61850 is an international communication standard for power systems that plays a vital role in the digitalization of smart grids, especially in substation automation, by improving operational efficiency and interoperability. However, as power grids become increasingly interconnected, cybersecurity threats, including malware, denial-of-service (DoS) attacks, man-in-the-middle (MiTM) attacks, and device vulnerabilities, pose growing risks to system stability and public safety.

This study investigates multiple protective strategies, including authentication techniques such as Canvas fingerprinting, the application of intrusion detection systems (IDS) optimized for low-latency environments, and the adoption of the IEC 62351 standard augmented with hardware acceleration to reinforce communication security. Furthermore, it examines an OT-oriented defense-in-depth approach and high-availability design based on the ISA99/Purdue model to ensure reliable operation under extreme conditions.

Through this framework, the research provides practical references for building smart grid infrastructures that balance performance and cybersecurity, thereby strengthening resilience and ensuring both operational continuity and public safety.

關鍵詞(Key Words)：智慧電網(Smart Grid)、網路安全(Cybersecurity)、製造訊息規範(MMS)、通用物件導向變電所事件(GOOSE)、阻斷服務攻擊(Denial-of-Service Attack)、中間人攻擊(Man-in-the-Middle Attack)、資料機密性(Data Confidentiality)、縱深防禦(Defense-in-Depth)。

*財團法人電信技術中心

智慧電網之 AI 資安治理技術發展趨勢

Emerging Trends in AI Cybersecurity Governance for Smart Grids

卓傳育* 呂姵萱* 林育生* 羅翊萍*
Cho, Chuan-Yu Lu, Pei-Hsuan Lin, Yu-Sheng Luo, Yi-Ping

摘 要

本報告針對智慧電網面臨的資安需求與挑戰進行分析，強調由於多元參與者的導入、OT 與 IT 技術的整合，以及裝置與通訊協定的多樣性，導致資安攻擊面顯著擴大。為因應此一挑戰，國際技術報告 IEC TR 62351-12 提出針對分散式能源資源(DERs)的五層資安架構，協助電網系統強化保護機制。此外，本報告探討智慧電網所面對的 AI 相關資安威脅、潛在攻擊動機與對關鍵基礎設施的影響，並以智慧電網為例，說明 AI 導入可能帶來的新型資安風險。為提升防護能力，本報告提出以自動化、易用、易管理為目標的微網段實踐方案，展望自動化風險隔離如何提升智慧電網可靠性，成為未來資安治理的重要趨勢。最後，介紹 AI 治理與評測技術如何應用於智慧電網場域，以達到風險可控與可信任 AI 的目標。

Abstract

This report analyzes the cybersecurity requirements and challenges faced by smart grids, highlighting how the participation of diverse stakeholders, the integration of OT and IT technologies, and the heterogeneity of devices and communication protocols have substantially expanded the attack surface. To address these challenges, the international technical report IEC TR 62351-12 introduces a five-layer security architecture for Distributed Energy Resources (DERs), designed to strengthen protection mechanisms in power grid systems.

In addition, this report examines AI-related cybersecurity threats to smart grids, potential attack motivations, and their implications for critical infrastructure. Using smart grids as a case study, it illustrates the novel security risks that may arise from the integration of AI technologies. To enhance defense capabilities, this report proposes a micro-segmentation approach that emphasizes automation, usability, and manageability, envisioning how automated risk isolation can improve the reliability of smart grids and emerge as a key trend in future cybersecurity governance. Finally, it discusses how AI governance and evaluation technologies can be applied in the smart grid domain to achieve risk-controllable and trustworthy AI deployment.

關鍵詞(Key Words)：智慧電網(Smart Grid)、人工智慧(Artificial Intelligence, AI)、資安威脅(Cybersecurity Threats)、微網段隔離(Micro-Segmentation)、AI 評測(AI Evaluation)。

*財團法人工業技術研究院

採用對稱防禦生成對抗網路偵測對抗性 DDoS 攻擊

Detection of Adversarial DDoS Attacks Using Symmetric Defense Generative Adversarial Networks

謝欽旭* Shieh, Chin-Shiuh
阮青俊** Nguyen, Thanh-Tuan
洪盟峰* Horng, Mong-Fong

摘 要

分散式阻斷服務(DDoS)攻擊是一種由大量受駭電腦系統，同時對特定目標發動的網路攻擊，對網路安全構成嚴重威脅，及早偵測 DDoS 攻擊至關重要。近年來，諸多研究將機器學習和深度學習應用於 DDoS 偵測，並取得不錯的成效。然而，本研究探討一種名為「對抗式 DDoS 攻擊」的新型攻擊，這類攻擊能輕易規避現有偵測系統。我們使用 CycleGAN 這個對稱生成對抗網路架構來生成這類攻擊流量，並用來驗證對抗式 DDoS 攻擊的嚴重影響。實驗結果顯示，這種合成的攻擊能輕易滲透多種基於機器學習的偵測系統，包括隨機森林、K-最近鄰、支持向量機和樸素貝葉斯。於此，我們提出了一個創新的 DDoS 偵測框架：對稱防禦生成對抗網路(SDGAN)。這個框架利用兩個對稱的辨識器，能夠同時識別對抗式 DDoS 流量。比較研究顯示，SDGAN 的表現更為優異，其真陽性率達到 87.2%，展現了強大的防禦能力。

Abstract

Distributed Denial of Service (DDoS) attacks, which exploit large numbers of compromised computer systems to overwhelm a specific target, pose a serious threat to network security. Timely detection of DDoS attacks is therefore of critical importance. In recent years, machine learning and deep learning techniques have been widely applied to DDoS detection, yielding encouraging results. However, this study focuses on a novel variant known as adversarial DDoS attacks, which are capable of easily evading existing detection systems. To simulate such attacks, we employed CycleGAN, a symmetric generative adversarial network architecture, to generate adversarial traffic and evaluate its impact. Experimental results demonstrate that these synthetic attacks can readily bypass various machine learning-based detection systems, including Random Forest, K-Nearest Neighbors, Support Vector Machine, and Naïve Bayes. To counter this threat, we propose a novel detection framework termed Symmetric Defense Generative Adversarial Network (SDGAN). This framework leverages two symmetric discriminators to simultaneously detect adversarial DDoS traffic. Comparative experiments show that SDGAN achieves superior performance, with a true positive rate of 87.2%, thereby exhibiting strong defensive capability against adversarial DDoS attacks.

關鍵詞(Key Words)：分散式阻斷服務(Distributed Denial of Service, DDoS)、機器學習(Machine Learning)、生成對抗網路(Generative Adversarial Network)。

---

*國立高雄科技大學
**越南芽莊大學

IEC 61850 二次變電所資安風險識別與防禦機制研究

Cybersecurity Risk Identification and Defense Mechanisms for IEC 61850-Based Secondary Substations

林呈鴻* Lin, Cheng-Hung　黃暐珩* Huang, Wei-Heng　許博堯** Hsu, Po-Yao

摘　要

本研究聚焦於 IEC 61850 標準下的二次變電所資安風險識別與防禦機制佈署。隨著智慧電網的發展，變電所自動化系統日益複雜，同時也面臨著更多的網路安全威脅。本文透過系統化的 ICS 資安風險評估方法，探討 IEC 61850 環境下的風險評估流程與實施，開發了專門的資產設備漏洞探勘和分析平台，為電力系統的網路安全管理，提供了實用的方法和工具支持，並針對網路分區、安全配置基線、持續監控等面向提出防護對策。研究成果可為變電所營運、設備製造商提供重要參考，有助於提高智慧電網的整體安全性和可靠性。

Abstract

This study investigates cybersecurity risk identification and defense mechanism deployment for secondary substations under the IEC 61850 standard. With the growing complexity of smart grids, substation automation systems are becoming increasingly sophisticated while simultaneously exposed to heightened cybersecurity threats.

Using a systematic Industrial Control System (ICS) risk assessment methodology, this research examines the risk assessment process and its implementation in IEC 61850 environments. A dedicated vulnerability discovery and analysis platform was developed to support asset-level risk identification, providing practical tools for enhancing cybersecurity management in power systems.

Furthermore, the study proposes defense strategies in key areas such as network segmentation, security configuration baselines, and continuous monitoring. The results offer valuable references for substation operators and equipment manufacturers, thereby contributing to the overall security and reliability of smart grids.

關鍵詞(Key Words)：IEC 61850、二次變電所(Secondary Substation)、工業控制系統安全(Industrial Control System Security)、資安風險評估(Cybersecurity Risk Assessment)、漏洞分析(Vulnerability Analysis)。

*台灣電力公司綜合研究所
**財團法人電信技術中心

電力系統滲透測試案例及防禦應用研究

Case Studies of Penetration Testing and Defense Applications in Power Systems

黃暐珩* 林呈鴻*
Huang, Wei-Heng Lin, Cheng-Hung

摘 要

本研究案基於 IEC 62351 電力系統強健性及符合性檢測平台建置之研究，進一步進行漏洞掃描與滲透測試，並將測試對象從原檢測平台擴展至儲能資通訊模控系統及太陽光電發電系統。

本測試計畫涵蓋三個場域：IEC 62351 電力系統強健性及符合性檢測平台、IEC 61850 儲能資通訊模控系統、以及太陽光電發電系統暨智慧監控平台。IEC 62351 電力系統強健性及符合性檢測平台是一個專門設置的資訊安全測試環境，主要用於資安工具的功能驗證與安全訓練，與真實環境隔離最遠。IEC 61850 儲能資通訊模控系統位於實驗室，包含部分模擬設置與部分實體設備，提供介於真實場域與純實驗環境之間的測試場景。太陽光電發電系統暨智慧監控平台在本案中最接近真實場域。測試項目包括漏洞檢測與漏洞驗證兩大部分。

Abstract

Building on the development of an IEC 62351-based robustness and compliance testing platform, this study advances into vulnerability scanning and penetration testing, extending the scope of evaluation from the original testing platform to include an IEC 61850-based energy storage information and communication monitoring and control system, as well as a photovoltaic (PV) power generation and smart monitoring platform.

The testing plan encompasses three domains：(1) the IEC 62351 Power System Robustness and Compliance Testing Platform, a dedicated cybersecurity testing environment primarily used for validating security tools and conducting training, and the most isolated from real-world systems；(2) the IEC 61850 Energy Storage Information and Communication Monitoring and Control System, located in a laboratory setting with both simulated configurations and physical equipment, offering a semi-realistic testing environment；and (3) the PV Power Generation and Smart Monitoring Platform, which most closely resembles real-world operational conditions.

The penetration tests comprise two main components：vulnerability detection and vulnerability verification. The outcomes provide practical insights into the identification of cybersecurity risks and the formulation of defense strategies, offering valuable references for enhancing the security and resilience of power systems.

關鍵詞(Key Words)：漏洞利用(Vulnerability Exploitation)、滲透測試(Penetration Testing)、連網產品安全弱點檢測工具(SecDevice)、開源安全工具(Metasploit)。

---

*台灣電力公司綜合研究所

XMPP 資安強化與應用研析

Security Enhancement and Application Analysis of XMPP in Smart Grids

卓啟翔*
Cho, Chi-Shiang

張廖俊魁*
Chang Liao, Chun-Kuei

許乃倫*
Hsu, Nai-Lun

蘇亮宇*
Su, Liang-Yu

劉懷然**
Liu, Huai-Jan

吳緯峻***
Wu, Wei-Jun

摘　要

配合國家智慧電網總體規劃，台電公司任務為智慧電網之建置與執行，其中資通安全與分散式能源應用為公司推動智慧電網之重要執行項目。

由於分散式再生能源大量佈建且分散於各處，企業通訊網路不易涵蓋，致資訊蒐集整合不易，且通訊具有跨網域、跨 Internet 特性，因此資安議題格外重要。

本文進行智慧電網核心標準介紹，研析 XMPP 通訊協定與資安強化，並研析分散式能源資安法規與檢測應用。

Abstract

In line with the national smart grid development plan, Taipower is tasked with the construction and implementation of the smart grid. Among its key initiatives, information and communication security, as well as the application of distributed energy resources, are critical components in advancing smart grid deployment.

The large-scale and geographically dispersed deployment of distributed renewable energy resources poses challenges for enterprise communication networks, which often cannot provide full coverage. This makes data collection and integration difficult. Moreover, communication across domains and over the Internet further amplifies cybersecurity concerns.

This paper introduces core smart grid standards, analyzes the XMPP communication protocol and its security enhancement mechanisms, and further examines cybersecurity regulations and testing applications for distributed energy resources.

關鍵詞(Key Words)：分散式能源(Distributed Energy Resources)、智慧電網核心標準(Smart Grid Core Standards)、XMPP 通訊協定(XMPP Protocol)、資通安全(Cyber Security)。

*台灣電力公司綜合研究所
**國立台灣科技大學
***台灣電力公司配售電事業部配電處