Regular Paper

Communications of the CCISA
Vol. 30 No. 4 Nov. 2024

運用智慧合約提升工業控制設備運作安全

吳穎誠[1]、劉奕賢[2]、李忠憲[3*]
[1 2 3]國立成功大學電腦與通信工程研究所
[1] ycwu@cans.ee.ncku.edu.tw、[2] ihliu@cans.ee.ncku.edu.tw、[3] jsli@cans.ee.ncku.edu.tw

摘要

隨著工業物聯網的快速發展和工業控制協定的標準化，針對工業控制系統的網路攻擊威脅正在逐漸增加。由於工業控制系統被廣泛應用在各式的關鍵基礎設施，因此，針對工業控制系統的網路攻擊可能危害人民的生命安全，進而影響社會的穩定運作。隨著工業控制系統的網路安全受到越來越多的重視，因此需要設計一套安全的機制，儲存工業控制設備的運作資料，提升系統的運作安全。透過將區塊鏈技術應用於工業控制系統資料的儲存，將有助於降低資料遭到篡改成功的機會，並且在儲存資料的同時，利用智慧合約判斷這些資料值是否屬於正常的範圍內，以提升系統的運作安全。

關鍵詞：區塊鏈、智慧合約、工業控制系統

* 通訊作者 (Corresponding author.)

Regular Paper

Communications of the CCISA
Vol. 30 No. 4 Nov. 2024

Improving Industrial Control System Security with Smart Contract Technology

YingCheng Wu [1], I-Hsien Liu [2], Jung-Shian Li [3*]
[1 2 3] Institute of Computer and Communication Engineering, National Cheng Kung University
[1] ycwu@cans.ee.ncku.edu.tw, [2] ihliu@cans.ee.ncku.edu.tw, [3] jsli@cans.ee.ncku.edu.tw

Abstract

With the rapid development of the industrial internet of things and the standardization of industrial control protocols, the threats of cyberattacks targeting industrial control systems are gradually increasing. Given that industrial control systems are widely used in various critical infrastructures, cyberattacks on these systems can endanger public safety and impact the stable operation of society. As the cybersecurity of industrial control systems gaining increasing attention, there is a need to design a more secure mechanism for storing operational data of industrial control devices to improve their safety. By applying blockchain technology to the storage of data within industrial control systems, the chances of data tampering can be reduced. Additionally, while storing data, smart contracts can be employed to determine whether the values of this data fall within a normal range, further improving the operational safety of the system.

Keywords: Blockchain, Smart Contract, Industrial Control Systems

壹、前言

隨著工業控制系統技術發展的逐漸成熟和工業控制協定的標準化，針對工業控制系統的網路攻擊威脅數有著正在成長的趨勢。工業控制系統被廣泛應用在各式的關鍵基礎設施，例如水資源系統、能源系統和電力系統等重要設施 [3]。

參考過去發佈的多則新聞報導與研究調查後，發現近年來曾經發生多起針對工業控制系統的網路攻擊事件。2022 年，位於烏克蘭的一間電力公司遭到駭客惡意攻擊，駭客嘗試在高壓變電站部署惡意軟體，可能造成當地電力系統的中斷 [6]。2023 年，位於美國的一間小型水處理廠遭到駭客入侵，駭客在遭到攻擊的工業控制系統設備螢幕顯示訊息，聲稱這次的攻擊是針對以色列製造的設備為目標 [14]。2024 年，位於美國的一間水處理廠遭到駭客攻擊，導致水箱內的水溢出，水廠人員隨後採取了防範措施，以免系統再次受到攻擊 [5]。

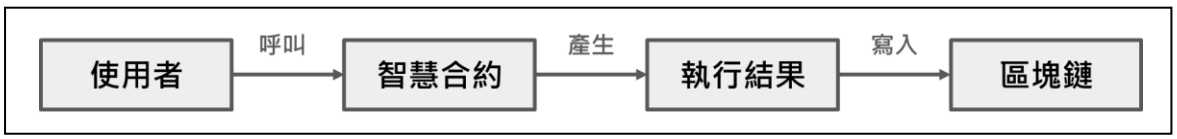
根據過去針對工業控制系統的眾多攻擊案例可以發現，這些網路攻擊可能會造成嚴重的生命威脅和財產損失。因此，本研究提出應用於工業控制系統的智慧合約平台架構，以提升工業控制設備的資料和運作安全。

貳、文獻探討

2.1 區塊鏈

區塊鏈的概念最早是中本聰提出，主要是透過將重要資料以區塊的形式來進行雜湊和封裝，確保區塊內的資料完整與安全 [10]。如果未經授權的人員試圖篡改資料，就會導致整個區塊的雜湊值產生改變。即使是對資料的細微修改，都會因雜湊結果變得明顯，這種特別現象在密碼學稱為雪崩效應 [15]。

由於區塊鏈強調的是要不同節點之間應對儲存的區塊內容達成共識，因此必須保證各個節點所儲存的資料內容完整和一致。如果一個節點的區塊資料遭到篡改，就會導致區塊資料的雜湊值因為和其他節點不同，無法和其他節點同步，這樣的機制確保了區塊鏈系統整體的資料安全 [12]。



圖一：智慧合約執行流程圖

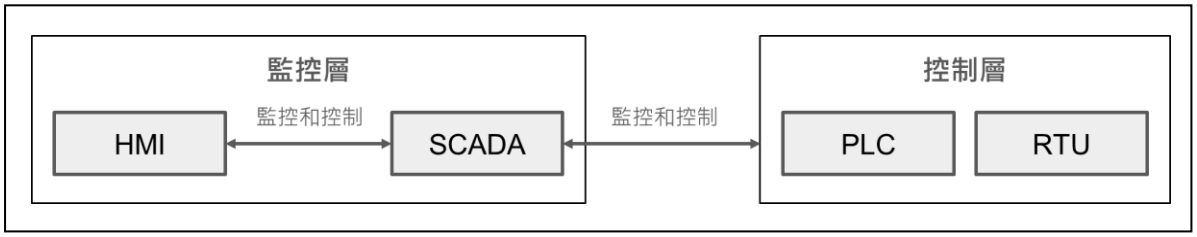
智慧合約的概念最早是尼克提出，主要概念是透過自動執行的方式，達成傳統合約的自動履約功能 [4]，執行過程如圖一。當智慧合約達到原先設定的條件，就會依照預

先設定的條款，自動進行履約，不需要人為的額外介入和操作，即可完成智慧合約自動執行條款內容和履約的功能 [7]。

最早實作智慧合約功能的平台是以太坊，以太坊平台透過虛擬機的技術，將編寫好的智慧合約儲存在區塊鏈後，再交由虛擬機執行 [11]。這種將智慧合約交由平台虛擬機執行的做法，不僅避免了傳統合約情況的中心化問題，更降低了智慧合約內部設定條件的程式碼遭受未授權人員篡改的機會 [9]。

2.2 工業控制系統

工業控制系統主要由人機互動界面 (HMI)、資料採集與監控系統 (SCADA)、可程式化邏輯控制器 (PLC) 和遠端終端單元 (RTU) 所組成，基本架構圖如圖二。



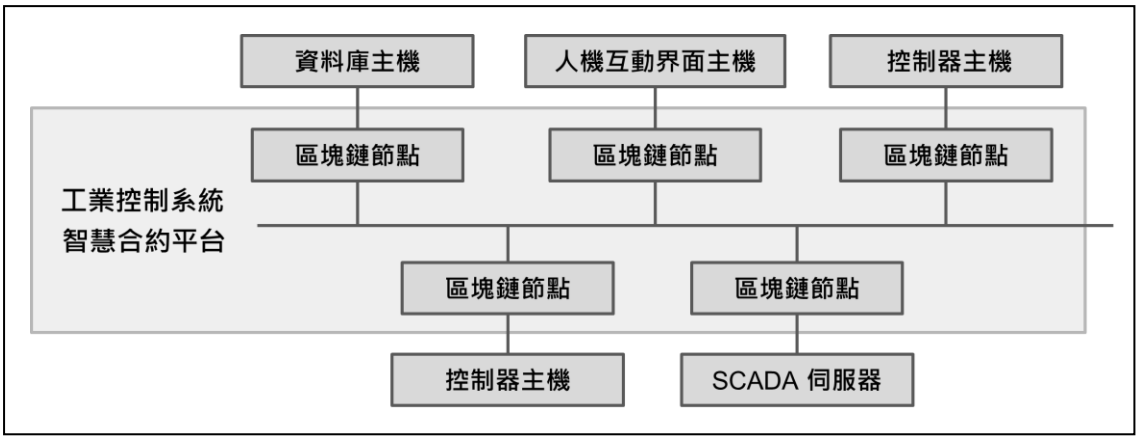
圖二：工業控制系統基本架構圖

資料採集與監控系統負責從控制層接收資料或者是向控制設備發送命令，人機互動界面則負責將資料以圖形化的方式呈現給操作人員 [8]。可程式化邏輯控制器是一種工業控制器，負責向實體控制設備發送命令或接收資料 [1]。遠端終端單元的功能和可程式化邏輯控制器有一些相似，然而和可程式化邏輯控制器相比之下，通常較重視傳輸功能 [2]。

參、方法

3.1 系統平台

圖三為應用於工業控制系統的智慧合約平台示意圖，一般來說，工業控制系統都會設有至少一個的資料採集與監控系統伺服器。然而，隨著不同工業控制系統的複雜度和功能考量，可能會設置更多的主機。

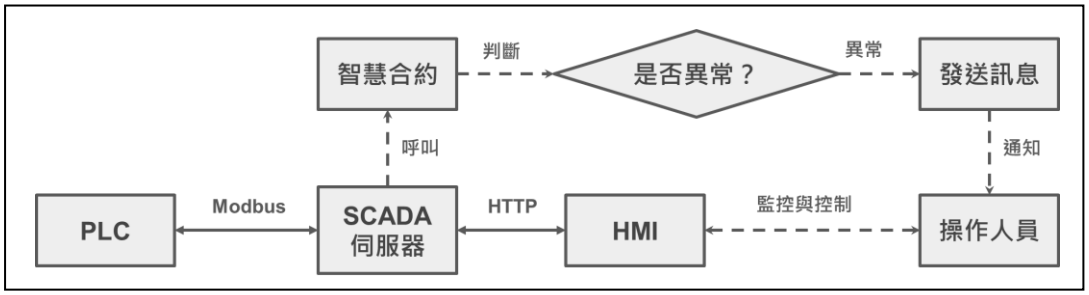


圖三：系統平台示意圖

透過在這些主機上部署區塊鏈節點，將形成一個適用於工業控制系統的智慧合約平台。在這個應用於工業控制系統的智慧合約平台裡，由於工業控制設備資料被分散儲存在區塊鏈的節點，針對單一節點的攻擊將無法對其他節點的資料造成影響，因此確保了系統整體的資料安全。

3.2 程式架構

圖四為應用於工業控制系統的智慧合約程式架構示意圖，可程式化邏輯控制器和資料採集與監控系統伺服器之間以工業控制協定 (Modbus) 進行溝通，主要功能是對可程式化邏輯控制器傳送指令或請求資料。



圖四：程式架構示意圖

當伺服器收到工業控制設備運作資料後，就會將資料上傳到智慧合約，接著智慧合約會主動判斷資料是否正常，當資料正常時，智慧合約就不會採取動作。然而，當智慧合約發現資料有異常時，將會向伺服器發送警告訊息，再交由伺服器向操作人員發送通知，提醒相關操作人員注意，有工業控制設備發生設備資料異常事件。

肆、結果

本實驗所使用的系統平台和執行環境如表一，區塊鏈平台採用以太坊支援的區塊鏈平台，智慧合約程式語言則採用以太坊支援的 Solidity 進行測試。

表一：系統平台執行環境整理表

中央處理器	Intel Core i5-7500 CPU
作業系統	Windows 10 Enterprise 64-bit
記憶體	16GB
區塊鏈平台	Go Ethereum
智慧合約程式語言	Solidity

4.1 交易速度

交易速度是測試區塊鏈交易處理能力的重要指標，智慧合約交易速度的實驗結果如表二。根據表格的實驗結果顯示，智慧合約的平均交易速度大約是每秒 110 筆到 120 筆交易。實驗中的交易速度是以平均新增的確認交易數進行測量，每 5 秒測量一次新增的確認交易數，再將新增的確認交易數除以測量區間的時間後，即可得知智慧合約的平均交易速度。

表二：智慧合約交易速度實驗結果表

經過時間	新增的確認交易數		
	節點數		
	1	2	3
5秒後	570	543	536
10秒後	568	535	494
15秒後	543	560	503
20秒後	551	580	571
25秒後	612	580	530
30秒後	552	589	539
35秒後	623	642	591
40秒後	652	618	570
平均交易數	583.9	580.9	541.8

觀察交易速度實驗結果的表格後，可以發現，隨著節點數的增加，交易速度沒有顯著的上升或下降。因此可以推論，在節點數量不多的情況下，節點數的增加不會對交易速度產生重大影響。雖然智慧合約的交易處理能力存在著極限，然而，由於工業控制設備資料的產生速度並不快，因此這樣的交易速度應該符合大多數的工業控制系統應用場景。

4.2 反應時間

反應時間是指從設備將資料傳給智慧合約，智慧合約判斷是否異常，當發現異常後，將判斷結果傳送給使用者的這段期間所花費的時間，智慧合約反應時間的實驗結果如表三。本實驗針對智慧合約的反應時間進行數次的測試，每次的實驗以編號的形式呈現於表格中。

表三：智慧合約反應時間實驗結果表

編號	反應時間（秒）		
	節點數		
	1	2	3
1	5.061	5.073	5.083
2	5.071	5.083	5.070
3	5.064	5.047	5.069
4	5.070	5.049	5.039
5	5.075	5.115	5.061
6	5.069	5.083	5.077
7	5.074	5.066	5.079
8	5.048	5.084	5.078
平均反應時間	5.067	5.075	5.070

根據表格的實驗結果顯示，智慧合約的反應時間平均大約在 5 秒左右。隨著節點數的增加，智慧合約的反應時間沒有明顯的變化。因此從表格的結果可以得知，在節點數量不多的情況下，區塊鏈的節點數量的增加或減少，通常不會對智慧合約的反應時間產生重大影響。

伍、結論

隨著工業控制系統攻擊事件數量的增加，針對工業控制系統的網路安全問題因此逐漸獲得重視 [13]。本研究提出了一個應用於工業控制系統的智慧合約平台系統架構，透過在智慧合約記錄工業控制設備資料的方式，提升了資料的完整於安全。除此之外，智慧合約還會對資料進行判斷，當智慧合約發現資料異常時，主動向操作人員發送通知，進而提升了工業控制設備的運作安全。最後，本研究設計了用來評估系統效能的實驗，結果顯示，應用於工業控制系統的智慧合約平台效能良好，交易速度通常可以符合一般工業控制系統場景。在反應時間方面，數秒的反應時間對於一般運作速度較慢的工業控制系統來說，應該相對足夠。

[誌謝] Acknowledgment

感謝國科會計畫 NSTC 112-2634-F-006-001-MBK 提供經費支持本研究。

參考文獻

[1] E. R. Alphonsus and M. O. Abdullah, "A review on the applications of programmable logic controllers (PLCs)," *Renewable and Sustainable Energy Reviews,* vol. 60, pp. 1185 - 1205, 2016.

[2] S. A. Boyer, *SCADA: Supervisory Control and Data Acquisition*, International Society of Automation, 2010.

[3] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk assessment methods for SCADA systems," *Computers & Security*, vol. 56, pp. 1-27, 2016.

[4] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of things," *IEEE Access,* vol. 4, pp. 2292 - 2303, 2016.

[5] CNN, "Russia-linked hacking group suspected of carrying out cyberattack on Texas water facility, cybersecurity firm says," 2024. [Online]. Available: https://edition.cnn.com/2024/04/17/politics/russia-hacking-group-suspected-texas-water-cyberattack/index.html. [Accessed 20 Oct 2024].

[6] CNN, "Russian military-linked hackers target Ukrainian power company, investigators say," 2022. [Online]. Available: https://edition.cnn.com/2022/04/12/politics/gru-russia-hackers-ukraine-power-grid/index.html. [Accessed 11 Oct 2024].

[7] P. Fraga-Lamas and T. M. Fernández-Caramés, "A review on blockchain technologies for an advanced and cyber-resilient automotive industry," *IEEE Access,* vol. 7, pp. 17578 - 17598, 2019.

[8] B. Galloway and G. P. Hancke, "Introduction to industrial control networks," *IEEE Communications Surveys & Tutorials,* vol. 15, no. 2, pp. 860 - 880, 2012.

[9] H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain: Research and Applications,* vol. 3, no. 2, 2022.

[10] S. He, W. Ren, T. Zhu, and K.-K. R. Choo, "BoSMoS: A blockchain-based status monitoring system for defending against unauthorized software updating in industrial internet of things," *IEEE Internet of Things Journal,* vol. 7, no. 2, pp. 948-959, 2020.

[11] S.-Y. Lin, L. Zhang, J. Li, L.-L. Ji, and Y. Sun, "A survey of application research based on blockchain smart contract," *Wireless Networks,* vol. 28, pp. 635-690, 2022.

[12] S. Luo, T. Hu, N. Han and Y. Qian, "A smart-contract-based policy-domain access control framework for distributed industrial IoT," *IEEE Internet of Things Journal,* vol. 11, no. 7, pp. 11427 - 11443, 2023.

[13] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, "SCADA security in the light of Cyber-Warfare," A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke*,* vol. 31, no. 4, pp. 418-436, 2012.

[14] The Associated Press, "Breaches by Iran-affiliated hackers spanned multiple U.S. states, federal agencies say," 2023. [Online]. Available: https://apnews.com/article/hackers-iran-israel-water-utilities-critical-infrastructure-cisa-554b2aa969c8220016ab2ef94bd7635b. [Accessed 12 Oct 2024].

[15] D. Upadhyay, N. Gaikwad, M. Zaman, and S. Sampalli, "Investigating the avalanche effect of various cryptographically secure hash functions and hash-based applications," *IEEE Access,* vol. 10, pp. 112472-112486, 2022.