創新工業物聯網資安防禦架構在智慧製造產業的運用

A Novel Secure Industrial Internet of Things (IIoT) Framework for Smart Manufacturing

張智為
國立政治大學資訊管理系
107356509@nccu.edu.tw

洪為璽
國立政治大學資訊管理系
fhung@nccu.edu.tw

摘要

工業物聯網(Industrial Internet of Things, IIoT)使得智慧製造(Smart Manufacturing)技術快速發展，這是一個結合資訊技術(Information Technology, IT)與運營技術(Operational Technology, OT)於一體的整合系統，但囿於智慧裝置極其輕巧的特性使得其實體安全防護不足，加上特殊工作場域的條件運作限制，使工業物聯網將面臨比單純 IT 資通訊系統更為嚴竣的資安威脅。

有鑑於過去專注研究工業控制系統中所存在的資安與管理問題之文獻並不多見，本研究彙整物聯網的應用系統架構，並嘗試在製造業系統妥適可用和生產效率優先的前題下，先研究 OT 技術的普渡模型(Purdue Enterprise Reference Architecture, PERA)架構維繫製造業的核心精神，接著汲取現有 IT 資訊安全所累積的豐富防護經驗，從而找出工業物聯網的關鍵資安弱點，在可用性與生產力優先的條件下，本文提出一個新的安全物聯網架構與部署流程，從中建議部署必要的安全防護功能，並建立必要資安管理機制、有效提昇關鍵節點的安全防禦能力，強化工業物聯網系統的資訊安全防護能力，達成高可用性、高效率與高產能且安全的智慧製造目標。

關鍵詞：物聯網、工業物聯網、智慧製造、物聯網安全、資訊安全

Abstract

The Industrial Internet of Things (IIoT) has led the rapid development of Smart Manufacturing technology. It is an integrated system that combines Information Technology (IT) and Operational Technology (OT). However, most of smart devices are light-weighted and lack comprehensive physical security protection. Those are very vulnerable to the cyber-attack. Moreover, in order to meet the availability and productive operational requirements of the industrial control environment, the IIoT system will face a more serious security threat than the conventional IT system.

Industrial Control System (ICS) security with its management issues are seldom discussed issues in information security research. In this paper we analyzed the whole architecture of the Internet of Things, and try to apply Purdue Enterprise Reference Architecture to meet the requirement of the availability, efficiency and productivity characteristic on manufacturing system. Then incorporated our expertise accumulated from existing IT security to the Industrial Internet of Things application. With then we can find out the most critical security threats in the IIoT system. Finally, we propose a novel secure IoT framework and implement flow which included the essential security protection mechanisms and management at industrial control fields. We believe our solutions can strengthen cybersecurity protection capabilities of IIoT systems. In this way, the goal of smart manufacturing with highly availability, efficiency, productivity and safety can be achieved.

Keywords: Internet of things, Industrial Internet of Things, Smart Factory, IoT Security, Cyber security