DOI 10.15302/J-SSCAE-2020.04.015

Convergence of OT and IT for Internet Plus

Hong Xuehai [1, 2], Cai Di [1, 3]

1. Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China
2. Computer Network Information Center, Chinese Academy of Sciences, Beijing 100190, China
3. School of Computer Science and Technology, University of Chinese Academy of Sciences, Beijing 100049, China

Abstract: The convergence of operational technology (OT) and information technology (IT) has become the key to industrial digital transformation and high-quality development in the manufacturing industry. This study analyzes the demands for the convergence of OT and IT and summarizes the convergence status of the two technologies from the aspects of the industrial Internet of Things, cross-platform analysis framework, open platforms, and supervisory control and data acquisition system based on cloud deployment. It also proposes technical paths for the convergence of OT and IT, including the establishment of a full set of computing stacks, continuous promotion of the industrial Internet, and strengthening of the security assurance. To promote the China's Internet Plus initiative in industrial manufacturing, the standardization of the convergence of OT and IT should be strengthened and a security system should be established by carrying out a risk assessment of key assets, focusing on underlying data, developing a detection system with antiintrusion functions, detaching the communication function, and promoting the application of artificial intelligence.

Keywords: Internet Plus; operational technology; information technology; technology convergence

1 Introduction

The combination of Internet and consumption, service, and other fields has produced numerous consumer Internet Plus applications and promoted the development of China's consumer Internet industry. The Internet, Internet of Things (IoT), big data, artificial intelligence (AI), edge computing, high-performance computing, and information technology (IT) increasingly penetrate the industrial field and integrate with the industrial technology. The industrial Internet Plus integrated application represented by the industrial Internet has been produced. These issues are of significance in promoting the development of the digital transformation of China's industry and China's transformation from a large country to a powerful country in the manufacturing industry.

The essence of Operational Technology (OT) is the comprehensive application of electronic, information, software, and control technologies. OT can be defined as software and hardware technologies that monitor or control all types of terminals, processes, and events in an enterprise, including data acquisition and automatic control technologies. Therefore, OT includes not only hardware facilities (such as robots, motors, valves, and computer numerical control machine tools), but also various software technologies that control these facilities.

The convergence of OT and IT, particularly the computing technology, has become an important direction for industrial digital transformation and upgrading. IT, OT, and communication technology (CT) are deeply integrated, which enables the industrial Internet to preliminarily realize the comprehensive connection between data and entities, promote service and data innovation, promote the realization of data value, and enable real-time decision-making [1–5]. In this study, the convergence and development of IT and OT are discussed, the requirements, current status, and progress of the convergence of OT and IT are studied, an approach to the convergence of OT and IT in the future is demonstrated, and the security issues of the convergence of OT and IT are presented. Countermeasures and

Received date: June 01, 2020; **revised date:** June 29, 2020

Corresponding author: Hong Xuehai, Professor from the Institute of Computing Technology, Chinese Academy of Sciences. Major research fields include high performance computing, cloud computing and big data, information technology and informatization development strategy. E-mail: hxh@ict.ac.cn

Funding program: CAE Advisory Project "Strategic Studies on the Internet Plus Action Plan (2035)" (2018-ZD-02)

Chinese version: Strategic Study of CAE 2020, 22 (4): 018–023

Cited item: Hong Xuehai et al. Convergence of OT and IT for Internet Plus. *Strategic Study of CAE*, https://doi.org/10.15302/J-SSCAE-2020.04.015

suggestions are proposed to provide a theoretical reference for the development of the Internet Plus action in the field of industrial manufacturing in China.

2 Demand analysis of the convergence of OT and IT

Digital transformation is the major development direction of the world's industrial powers. The release of numerous industrial digital transformation strategies, represented by Industry 4.0 (Germany), marks the arrival of the industrial digital era. To realize the industrial digital transformation, it is crucial to solve the problem of the convergence of IT and industrial technology; the OT becomes an application bottleneck.

The convergence of OT and IT aims to reduce industrial costs, optimize industrial business processes, reduce industrial process risks, implement the development and integration faster, and promote the standardization of communication and control industrial process equipment. After the convergence of the two technologies, the existing IT hardware and software and their environmental devices can easily access OT devices and their operational process data, which can then be transmitted through the IT infrastructure to share these devices and process data throughout the enterprise (or on a larger scale). In the process of operation, new IT technologies (such as AI, edge computing, and block chain) can be used to quickly and accurately analyze industrial equipment and industrial process data to realize the global optimization of enterprise information-sharing methods and provide comprehensive decision support for industrial manufacturing and process management.

The convergence of OT and IT can connect OT equipment and data of environmental facilities as well as IT infrastructure to realize two-way interoperability. The OT system uses IT infrastructure to obtain data on industrial equipment and processes and uses various algorithm models of the IT field to carry out state monitoring and risk boundary estimation of OT industrial equipment and processes, which effectively reduces potential risks of industrial organizations. New technologies such as cloud and virtualization in IT can improve the accessibility, stability, and mobility of OT industrial equipment and process data. By deploying general IT infrastructure, considering the storage and flow of OT data, the OT side can access the massive data of the IT side. With cloud and virtualization technologies, servers in an enterprise plant or production floor can be migrated to the cloud without affecting the work of the supervisory control and data acquisition (SCADA) system of the OT side, helping reduce the number of devices and facilitate the updates.

3 Current status of the convergence development of OT and IT

In the industry 3.0 era, OT and IT have independent interfaces without tendency for their convergence. In the era of Internet Plus and Industry 4.0, the convergence trends of OT and IT have emerged, but the interface between them determines the degree and direction of integration. The relational interface is mainly manifested in 10 aspects, including the function, domain, access, assets and personnel, frequency of change, environment, interface and network, lifecycle, target, and operating system. The convergence of OT and IT is also mainly carried out in terms of these 10 aspects. The industrial Internet of things (IIoT), industrial Internet, cloud-based deployment, and other aspects are the focus of the convergence of OT and IT research.

3.1 IIoT

The establishment of IIoT is the key measure to realize the convergence of OT and IT. With the rapid development of the IIoT technology, industrial manufacturing enterprises use the IoT technology for reference to deploy the IIoT business, and thus the traditional industrial equipment and process management transform toward the direction of IoT. An optimized job shop scheduler monitoring system based on IIoT is proposed to track the tasks being performed by the machine and provide a closed-loop feedback path, to realize automatic detection of job completion time and dynamic rescheduling [6]. The dual microcontroller unit architecture was developed to ensure the flexible control of IIoT equipment such as the programmable logic controller (PLC) [7]. A data center network based on a single virtualization platform with highly integrated technologies has been established, which is capable of supporting the infrastructure of the IoT [8]. An advanced analysis framework has been proposed, which can be used as the standardization application of IIoT for industrial and mining enterprises [9].

3.2 Cross-platform analysis framework

According to the IIoT application requirements of traditional industrial manufacturing enterprises, the market provides candidate solutions based on various technologies and platforms. However, considering their compatibility,

DOI 10.15302/J-SSCAE-2020.04.015

the process of choosing solutions by enterprises is usually time-consuming and tedious. Therefore, the compatibility advantages of the cross-platform analysis framework can meet the practical needs of traditional manufacturing enterprises for IIoT. Based on the application of mining enterprises, a cross-platform analysis framework [10] was developed, which integrates IIoT and multiple types of advanced analysis technologies and has the function of using IIoT as the data source of the analysis framework. The performance of the system is evaluated through a layer-by-layer analysis, which enables to easily evaluate the services and technologies under different architectures to realize the optimization of the enterprise deployment scheme [9].

3.3 Open platform

The rapidly advancing cloud computing drives the shift of enterprise applications and data from private to open platforms. The development of an open platform is a practical choice to cope with this trend. The Predix Basic System platform launched by General Electric (GE; United States), as an open platform, can be applied to industrial manufacturing, energy, medical, and other industrial fields. It provides a complete application scenario for various industrial equipment, including equipment health and fault prediction, production efficiency optimization, energy consumption management, scheduling optimization, and other complete applications. By combining the data drive and mechanism, the problems faced by traditional industrial enterprises in balancing quality, efficiency, energy consumption, and other aspects are solved, which promotes the rapid transformation of industrial enterprises to digital. The MindSphere platform, launched by SIEMENS, which employs the open IoT architecture based on cloud, transmits the industrial field equipment data collected by sensors, controllers, and various information systems to the cloud in real time through secure channels and, in the cloud, provides enterprises with big data analysis and mining, industrial application development, and intelligent application value-added services. The creation of a technology-integrated data center network on a virtualization platform to support the operation of the infrastructure of the IoT, providing flexibility, scalability, and functional expansion capabilities for the application of the IoT in the data center has been studied in [8].

3.4 SCADA system based on cloud deployment

Referring to the International Standard for Enterprise Systems and Control System Integration (ISA-95) developed by the US Instrument, Systems, and Automation Association, the industrial automation model is divided into five levels: business and planning, production operation management, supervisory control, plant control, and physical processes. The first two levels belong to the IT level, while the last three belong to the OT level. The supervisory control layer (i.e., the layer where the SCADA system is located) can be regarded as the interface between IT and OT and key point of the connection between IT and OT. If cloud-based deployment is implemented at this level, industrial systems with user (or operator) remote monitoring (using sensors) and control (using actuators) capabilities can be built, largely improving the efficiency and flexibility of the OT and IT connectivity. Extensive studies have been carried out to analyze the deployment scenarios involved in cloud deployment of SCADA systems [11], design a benchmark system for virtualization and additional network connection with cloud data center and increased computing load due to security measures, and obtain the performances of a cloud deployment SCADA system under different configurations. The model standard framework is established for the cloud-linked SCADA system. The behavior of the SCADA system has been formally defined [12]. The cloud-based SCADA system developed based on a microservice architecture significantly improves the performance of the SCADA system [13].

4 Technology path prediction for the convergence of OT and IT

The integration of OT and IT can not only promote the networked, cloud-based, and intelligent role of IT on the OT side, but also ensure that the OT side better uses the enabling technology of the IT side. The fusion mode is mainly divided into two types: to connect the information on the OT side with the IT side, i.e., to establish the connection between the IT side and OT side; and to output the information on the OT side to the IT side, so that the information on the OT side is shared in a wider scope, i.e., the information on the OT side is clouded.

The ideal convergence of OT and IT lies in the pursuit of a unified fusion technology framework (such as power industry application demonstration [14]). To realize the two-way fusion between OT and IT, the fusion is mainly promoted by the establishment of a full set of computing stack systems and development of industrial Internet, while strengthening the system security measures of the convergence of OT and IT.

4.1 Full set of computing stacks for the convergence of IT and OT

The manufacturing industry is characterized by a large quantity and wide range of products. The equipment of manufacturing production lines is the main battlefield for the convergence of IT and OT, crucial for the high-quality development of the industrial manufacturing industry. The applications of PLC and computer numerical control are considered as the breakthrough points to strengthen the research and development of a complete set of autonomously controllable computing stacks (Fig. 1). Based on the realization of the real convergence of the OT and IT sides and promotion of the wider sharing and application of OT-side information, the upgrade (transformation) of low-grade production line equipment to middle and high grades is levered by a full set of autonomously controllable computing stacks. While striving to narrow the gap with the international advanced level, we should improve the profit margin and international competitiveness of China's manufacturing industry and build an intelligent equipment ecosystem suitable for China's national conditions.

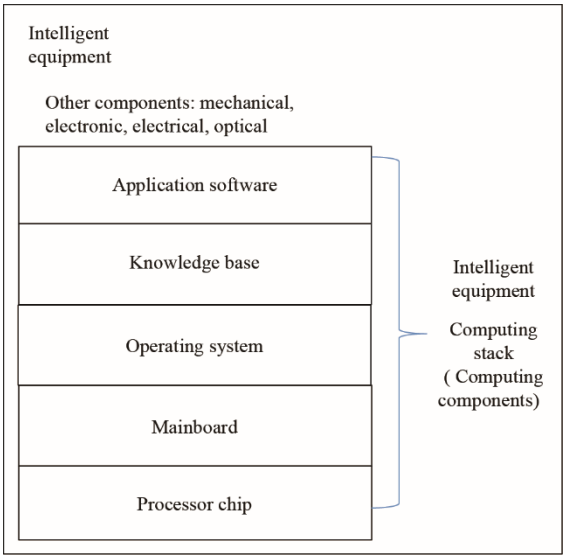

Fig. 1. Full set of computing stacks for the convergence of OT and IT.

Foreign enterprises and products still dominate the knowledge base, design tool software, operating system, and numerous other aspects; however, domestic products or open-source communities have an alternative basis. Foreign products dominate the processor chip market; however, domestic products have the foundation of alternative technology. Domestic products dominate other computer hardware and application software. As a computing component of industrial equipment, an intelligent equipment computing stack is crucial to realize the convergence of OT and IT. Its relationship with industrial equipment is similar to that between the Android technology stack and smart phones.

4.2 Continuous promotion of the industrial Internet

The industrial Internet is an important carrier and key platform to realize the integration of OT and IT. It is of significance to continuously promote the related technology research and development and deepen the application of the industry. The development history of the industrial Internet is interwoven with the three main lines of IT, OT, and CT [15]. The platform functional architecture (Fig. 2) is very similar to the cloud computing architecture, but with additional edge layers. The key elements, including infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS), are also similar to cloud computing. The edge layer is essentially the production site, which belongs to the OT part. OT is located at the bottom to implement data acquisition and action execution, CT connects all nodes and is responsible for data transmission, and IT is on top and responsible for data computing and analysis.

4.3 Strengthening of the security guarantee for the convergence of OT and IT

As the industrial system develops from the early isolated state to today's open environment and from the initial use of serial communication to the current widely used communication based on transmission control protocol/internet protocol, information security-related problems inevitably arise. The security challenges faced by

DOI 10.15302/J-SSCAE-2020.04.015

OT and IT in the process of convergence development mainly include two aspects. One of them is the defects of the OT system. In retrospect, OT and critical infrastructure are designed to be isolated from the network and thus not subject to external cyber security threats. However, after the digital transformation, these once-isolated systems have become connected devices, which makes them high-value targets for attackers. In addition, safety risks faced by SCADA, PLC, and other systems tend to emerge. The second aspect are the security risks of the convergence of OT and IT. Owing to the extensive application of IT, traditional OT devices do not run independently on isolated networks and proprietary platforms, but need to interoperate with other systems. Their convergence fundamentally solves the problem of inter-system connectivity, but leads to potential security risks such as external attacks, internal malicious vulnerability attacks, and wrong operations, which are embodied in the following aspects.

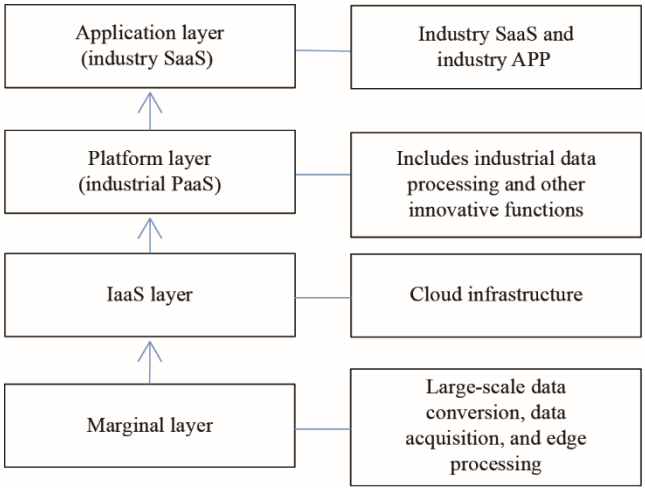

Fig. 2. Functional architecture of the industrial Internet platform.

4.3.1 PLC security

PLC is mainly faced with the problems of independent guarantee and information security and its design has defects. The PLC employs a scanning working mode (period: 1–100 ms). The data cannot be updated before the end of the scanning period (if the time of the input signal of the PLC is smaller than the response time, misreading is possible). The output and input states are updated once after each execution of the program and before the next execution ("program end regeneration"), leaving a sufficient time for the attacker to execute a malicious attack. In addition, operating systems with a small memory capacity and large security risks as well as the lack of security mechanism of the used communication protocol are also defect factors leading to security risks [16].

4.3.2 Remote terminal unit (RTU) security

RTU is the basic unit of the SCADA system. Its security risks mainly originate from (1) the RTU software platform, which usually employs an embedded real-time operating system, has security vulnerability, and even fails to provide security monitoring and protection mechanisms. (2) After the SCADA system is started, it will run for a long time. It is challenging to repair the security vulnerability in time. Virus infection of the computer will become a security threat source for the RTU equipment. (3) The communication protocol employed by the RTU lacks a security mechanism and transmits information in plaintext, so that the corresponding communication process is simple to monitor and attack. Network intelligent and intelligent security RTUs should be developed. The former can improve the utilization rate of the network and transmit data in real time, while the latter requires encrypting data before data transmission (ciphertext is used for transmission).

4.3.3 Human–machine interface (HMI) safety

With the expansion of factory scale and increase in organizational complexity, the control precision and accuracy of field equipment have become the main factors to ensure production, which has a significant impact on the HMI of industrial control. The traditional HMI has experienced a transformation from text to graphical interface, which basically realizes the diversified expression of multimedia information and ensures users' information perception and processing capability requirements for industrial control field equipment [17]. However, HMI and control PLC are usually equipped with password settings. Therefore, it is a key issue for the HMI design to prevent passwords from being broken, prevent programs from being stolen, and ensuring system security. To solve the above problems,

we should not only prevent the vulnerability of the product's encryption method, but also integrate the central processor and program memory chip into one structure for hardware encryption and cancel the external interface of the communication line.

4.3.4 HMI safety

The security risks of SCADA systems originate mainly from unauthorized illegal access, openness of industrial control standard protocols and general technologies, defects of industrial control hardware and software products, and practitioners [13]. In addition, owing to the deployment of cloud-based SCADA systems, enterprises are associated with system risks that extend from cloud security.

5 Strategies and suggestions

5.1 Strengthening of the standardized application of the convergence of OT and IT

Various types of industrial equipment exist. In addition, the interface standard and communication protocol standard are not sufficiently unified, which makes the data acquisition for industrial equipment and process a relatively complex link. It is also challenging to develop a unified convergence framework to meet the needs of various industrial scenarios. The standardization construction of the convergence of OT and IT needs to be strengthened.

The emerging Open Platform Communications - Unified Architecture over Time Sensitive Networking (OPC UA over TSN) standards based on time-sensitive networks have attracted considerable attention owing to its rich functions. By solving the problem that OT and IT do not agree on network communication standards and data formats, almost any data access capability can be realized. Therefore, it is particularly important for the converged development of OT and IT to focus on the promotion and use of OPC UA over TSN standards based on the actual business needs of domestic industrial enterprises.

5.2 Establishment of a safety guarantee system for the convergence of OT and IT

The first step is to implement the risk assessment of key assets to provide a key reference for system development. The protection of important assets should be reasonably strengthened. The defense measures of conventional assets should be considered to some extent. Through rational division and key safeguards, the defense force is concentrated to implement the system protection more accurately and efficiently.

The second step is to focus on the underlying data. It is suggested to change the current phenomenon of focusing on metadata related to source address, source port, destination address, and destination port [18], to focusing on data related to the bottom layer of the OT system and data transmission. The possible loopholes in the communication security mechanism of the OT system could be avoided and the system security could be accurately guaranteed through an in-depth understanding of the underlying data.

The third step is to develop a detection system that can prevent intrusion. It is necessary to strengthen the research and development of an intrusion-detection system as the first threshold of system protection. It is required to detect network packets, establish a network intrusion behavior database, and keep the database updated in time to shut out a large proportion of network attacks.

The fourth step is the separation communication function. Most attacks occur when the convergence of OT and IT systems conduct network communication. The functional part responsible for network communication should be separated from the convergence system. It is required to design the independent system for network communication and emphasize the security of information interaction with the main system. In this manner, the risk of attack on the OT–IT convergence system can be largely reduced.

The fifth step is to strengthen the use of AI technology. The AI technology is in a new stage of vigorous development. The related technologies can have a larger role in security convergence between OT and IT. AI endows computers with the ability to learn, recognize, and deal with network attack behaviors, with a huge development space and high potential.

References

[1] Electronic Technology Information Research Institute, MIIT. Industrial Internet of things and Industrial 4.0 core architecture [J]. The Journal of New Industrialization, 2017, 7(5): 68–69. Chinese.

[2] Wang Z M. Design and development of SCADA software system[M]. Beijing: China Machine Press, 2009. Chinese.

DOI 10.15302/J-SSCAE-2020.04.015

[3] Tan W. Design and implementation of industrial control system based on PLC [D]. Wuhan: Huazhong University of Science and Technology (Master's thesis), 2007. Chinese.
[4] General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China, Standardization Administration. Remote terminal unit (RTU) technical specification GB/T 34039—2017 [S]. Beijing: China Quality and Standards Publishing & Media Co., Ltd., 2018. Chinese.
[5] Zhang C G. Research of the interaction term on human-computer interface [D]. Chengdu: Southwest Jiaotong University (Master's thesis), 2015. Chinese.
[6] Malik K, Khan S A. IIoT based job shop scheduler monitoring system [C]. Atlanta: The 12th IEEE International Conference on Internet of Things, 2019.
[7] Niedermaier M, Merli D, Sigl G. A secure dual-MCU architecture for robust communication of IIoT devices [C]. Montenegro: 20198th Mediterranean Conference on Embedded Computing, 2019.
[8] Petrenko A S, Petrenko S A, Makoveichuk K A, et al. The IIoT/IoT device control model based on narrow-band IoT (NB-IoT) [C]. Moscow and St. Petersburg: 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, 2018.
[9] De Moura R L, Ceotto L, Gonzalez A. Industrial IoT and advanced analytics framework: An approach for the mining industry [C]. Las Vegas: The 2017 International Conference on Computational Science and Computational Intelligence, 2017.
[10] Yi M, Mueller H, Yu L, et al. Benchmarking cloud-based SCADA system [C]. Hong Kong: 2017 IEEE 9th International Conference on Cloud Computing Technology and Science, 2017.
[11] Kulik T, Tran-Jorgensen P, Boudjadar J. Compliance verification of a cyber security standard for cloud-connected SCADA [C]. Aarhus: 2019 Global IoT Summit, 2019.
[12] Porrmann T, Essmann R, Colombo A W. Development of anevent-oriented, cloud-based SCADA system using a micro service architecture under the RAMI4.0 specification: Lessons learned[C]. Beijing: IECON 2017- 43rd Annual Conference of the IEEE Industrial Electronics Society, 2017.
[13] Huang H P. Research on some key technologies of information security of industrial SCADA system [D]. Chengdu: Southwest Jiaotong University(Doctoral dissertation), 2016. Chinese.
[14] Garimella P K. IT-OT integration challenges in utilities [C]. Grugaon: The 2nd International Conference on Communication and Computing Systems, 2018.
[15] Alliance of Industrial Internet. Industrial Internet architecture [R]. Beijing: Alliance of Industrial Internet, 2016. Chinese.
[16] Xu Z, Zhou X J, Wang L M, et al. Recent advances in PLC attack and protection technology [J]. Journal of Cyber Security, 2019,4(3): 48–69. Chinese.
[17] Wang Y Y. Research on dynamic components and storage standards of embedded human-computer interface [D]. Hangzhou: Hangzhou Dianzi University (Master's thesis), 2018. Chinese.
[18] Andreu A. Operational technology security—A data perspective[J]. Network Security, 2020 (1): 8–13.