Bulletin of Networking, Computing, Systems, and Software – www.bncss.org, ISSN 2186-5140
Volume 12, Number 1, pages 18–21, January 2023

A Preliminary Risk Assessment for Operational Technology Systems

Tenzin Tsungmay
Faculty of Social System Science
Chiba Institute of Technology, Chiba, Japan
s2291008cr@s.chibakoudai.jp

Shigeaki Tanimoto
Faculty of Social System Science
Chiba Institute of Technology, Chiba, Japan
shigeaki.tanimoto@it-chiba.ac.jp

***Abstract*---In 2015, the German government launched Industry 4.0, which aims to increase the productivity, cost efficiency, and other aspects of the manufacturing process. Prior to this, the manufacturing process was limited to the factory floor, making it difficult to operate a supply chain from the manufacturing site to the sales department. The advent of Industry 4.0 has enabled an integrated supply chain between the two by linking information technology (IT) and operations technology (OT). However, as OT systems are connected to the Internet, they face increased risks such as cyber security. Additional non-cyber risks stemming from operational aspects in the supply chain due to the linkage of IT and OT are also expected. In this study, we conducted a risk assessment of OT systems connected to the Internet after Industry 4.0 from both cyber and non-cyber perspectives. Specifically, as an initial study, the risks of OT systems were comprehensively extracted using the Risk Breakdown Structure method and a total of 16 risk factors were identified, including the isolation of failures in OT systems and the lack of security functions in existing facilities (cyber side) and the safety management of the combined IT-OT systems (non-cyber side).**

Keywords---Operation technology, Risk Breakdown Structure, IT/OT convergence, Cyber and non-cyber risk

I. INTRODUCTION

Hardware and software that directly monitor and/or control industrial equipment, assets, processes, and events to detect or implement change in the real world are referred to as operation technology (OT). OT systems mostly engage with the physical world. Typical examples include automation and control systems such as Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS). OT has been utilized extensively for industrial control systems, particularly in the fields of manufacturing, transportation, power, pipelines, production, and utilities. Unlike IT, these systems do not require network technology to monitor and coordinate operations because of their limited network environment.

With the recent development and acceptance of digitalized, wireless, and networked architectures, there is a growing tendency in major sectors towards IT/OT convergence, where the open and linked architecture is embraced. Better monitoring and remote control of physical devices has been made possible by the introduction of wireless communication and the like in OT. Furthermore, the ability to collect real-time data from physical devices is now possible thanks to advances in machine learning and machine-to-machine communication technologies.

In the current OT systems, Internet-capable technology has been extended to industrial control systems and supervisory control and data acquisition networks. However, the malware, identity management, and access control issues that IT systems face also plague OT systems. Thus, vulnerabilities in an OT system can expose critical infrastructure to sabotage that can result in life-or-death situations.

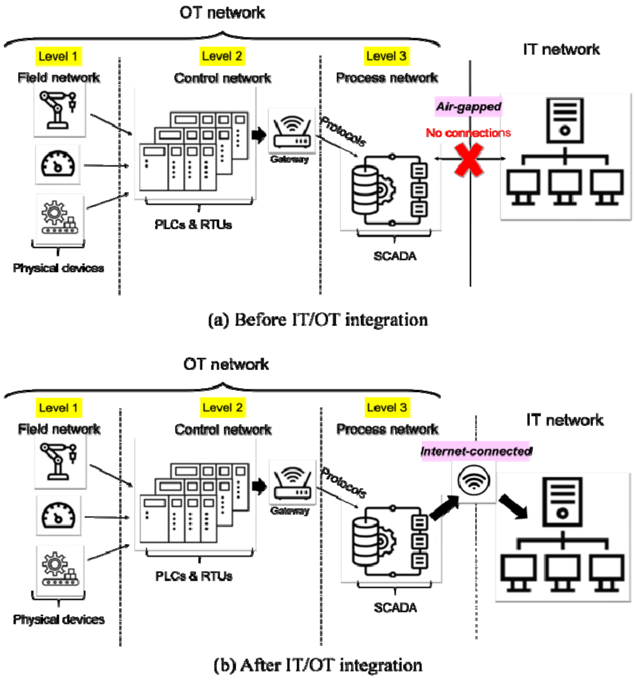
In light of this background, we conducted a risk assessment of OT systems from both the cyber and non-cyber perspectives. Specifically, as an initial study, the risks of OT systems were comprehensively extracted using the Risk Breakdown Structure (RBS) method, and we were able to identify and clarify 16 risk factors including fault isolation and insufficient security functions of existing facilities in OT systems on the cyber side and the safety management of IT-OT linked systems on the non-cyber side.

II. CURRENT STATUS AND ISSUES OF OT SYSTEMS

A. Current status of OT systems

OT is critical for both industry and society at large. It is usually integrated into core business processes at the organizational level. The architecture of an OT system generally consists of basic segments such as Supervisory Control and Data Acquisition (SCADA), a Human-Machine Interface (HMI), and Programmable Logics Controller (PLC) / Remote Terminal Units (RTU).

Figure 1 depicts a basic industrial network architecture, where level 1 is known as a “field network” because it operates out in the real world/field. This includes physical machinery such as valves, pumps, sensors, etc. This physical machinery is controlled by level 2, known as the “control network”, which includes PLCs/RTUs that are physically connected to the machines. Level 2 is connected to level 3, known as the “process network”, which is basically an HMI. This HMI is the component in charge of displaying process data to a human operator, who monitors and controls the processes through the HMI. The HMI is typically linked with SCADA or DCS. SCADA is a system that collects data from various sensors at a factory, plant, or in other remote areas and then sends it to a central computer (IT network), which then manages and controls the data.



(a) Before IT/OT integration

(b) After IT/OT integration

Figure 1 Transition of industrial network architecture [2].

Figure 1 shows the industrial network architecture (a) before integration and (b) after integration of the IT and OT systems. The basic operations of factories are often carried out using an OT system, and hospitals utilize OT devices to diagnose various illnesses in their patients. Maintaining a vital infrastructure for businesses and other organizations thus often depends on OT services. An outage would severely impair or even halt these activities. For example, a ransomware attack caused the Colonial Pipeline to shut down in May 2021 [1]. This pipeline, which is itself considered an OT system, transports 2.5 million barrels of fuel each day, and its shutdown resulted in a major fuel shortage on the East Coast. This example highlights the importance of operational technologies.

B. *Security in OT systems*

It is crucial for organizations to be aware of the challenges involved in establishing an OT system featuring an open and connected architecture. OT systems present several difficulties due to their very nature. In an industrial setting, it is common to find OT equipment that is several decades old, even though other OT systems in the same setting may be modern and complex. It is extremely difficult and costly to connect modern IT systems to older devices due to their age and proprietary design. Converging IT and OT systems also has the drawback of potentially increasing cybersecurity threats. This is especially true for old OT systems, as it is not likely that these technologies were originally intended to be linked to an IT infrastructure. It was presumably anticipated that such gadgets would work well in a solitary environment and thus wouldn't need to be protected from cybersecurity risks. Security must come first for any organization attempting to consolidate its IT/OT infrastructure.

Application development for the industrial sector, which is currently moving toward IT/OT convergence and technological improvements, must take security and robustness into account. Security vulnerabilities are becoming more prevalent along with the growth of sophisticated electronic gadgets. When security vulnerability awareness first emerged in 1997, there were just two examples. After a quick leap into 2010, this index expanded to 19 widely known security vulnerabilities, and the number increased to 189 over the following five years [3]. Among these, 91% were rated as medium to high risk according to the Common Vulnerability Scoring System (CVSS) v2 and v3 scoring methods (refer to Fig. 2).

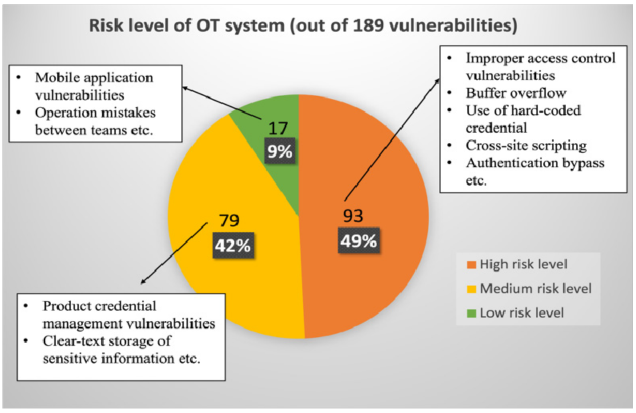


Figure 2 Security associated risk levels [4].

III. RISK ASSESSMENT OF OT SYSTEMS

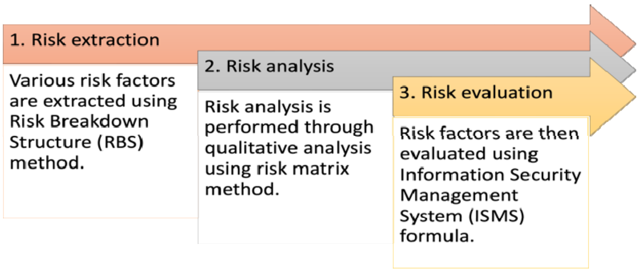
In general, a risk assessment is conducted in three consecutive steps: 1) risk extraction, 2) risk analysis, and 3) risk evaluation [5], as shown in Fig. 3. In this paper, we conduct a risk assessment of OT systems based on the first procedure.

A. Risk extraction of OT systems

We systematically extracted the risk factors of OT systems through a multi-viewpoint literature survey using the RBS method [6]**.** In general, OT systems deal with the physical environment and the recently developed interconnected IT architecture. Thus, risk factors are simply divided into two categories, cyber risk and non-cyber risk, as the first hierarchy of RBS. Cyber risk is further classified into hardware, software, and IT/OT convergence. Non-cyber risk is further classified into education and training, psychological, and safety environment. We then extracted 16 risk factors related to these viewpoints along with brief explanations, as shown in Table 1.

B. Main risk factors of OT systems

As shown in Table 1, the main risk factors are 1) failure isolation in OT systems and insufficient security functions of existing equipment on the cyber side and 2) safety management of IT-OT collaborative systems on the non-cyber side.



Various risk factors are extracted using Risk Breakdown Structure (RBS) method.

Risk analysis is performed through qualitative analysis using risk matrix method.

Risk factors are then evaluated using Information Security Management System (ISMS) formula.

Figure 3. Risk assessment steps [5].

Table 1. Risk extraction results for OT systems.

No.	1st Level	2nd Level	3rd Level / Risk Factors	Contents
1	**1. Cyber**	**1.1. Hardware**	1.1.1. Lack of processing capacity of edge devices	Many edge devices have limited computing power and insufficient storage.
2			1.1.2. Connection of legacy OT devices	Extremely difficult and costly to connect legacy devices with the modern IT system.
3			1.1.3. Isolation of failure issue	Isolation issues when network equipment (firewalls, switches, routers, etc.) and OT devices fail.
4		**1.2. Software**	1.2.1. Scalability issues	Impact on IT systems due to increase in number of devices in OT systems.
5			1.2.2. Lack of system patching policy	Inconsistent patch policies between IT and OT systems.
6			1.2.3. Lack of edge device security features	Insufficient implementation of security features due to lack of resources in edge devices.
7			1.2.4. Lack of IP whitelists in OT systems	Even in OT systems, without IP whitelists, the likelihood of encountering viruses, malware, and other cyber-attacks increases.
8		**1.3. IT/OT Convergence**	1.3.1. Insufficient security policy for combining IT and OT systems	Implementing strict security policies in the OT field is required for IT/OT convergence.
9			1.3.2. Lack of standard operation practices in IT system and OT system	Insufficient operational practices for combining IT and OT systems.
10	**2. Non-cyber**	**2.1. Education and Training**	2.1.1. Lack of education/training of IT/OT convergence systems	Lack of education/training of IT/OT convergence systems may lead to human errors.
11			2.1.2. Lack of guidelines/manuals for IT/OT convergence system	Lack of guidelines and manuals for IT/OT convergence systems may pose a rudimentary threat.
12		**2.2. Psychological**	2.2.1. Social engineering	Social engineering attacks are assumed to exploit gaps in the newly opened OT system.
13			2.2.2. Operational mistakes due to differences in perspectives of IT/OT teams	Operational mistakes due to differences in perspectives, roles, and other areas of expertise between the IT and OT teams are assumed.
14			2.2.3. Security fatigue	Operational mistakes etc. are assumed due to security fatigue resulting from the increased number of security procedures related to the linkage of IT and OT systems.
15		**2.3. Safety Environment**	2.3.1. Employee safety when a changing network environment	With the newly open network environment, there is a need to ensure employee safety in the factory.
16			2.3.2. Lack of specialists in IT/OT convergence systems	Lack of IT/OT convergence system specialists will make it difficult to operate efficiently.

IV. RELATED WORKS

In the current literature, numerous papers have focused on the cyber risk aspect of operational technology and the challenges involved in converging OT and IT systems.

Filkins et al. presented a study of the Top 2019 initiatives taken by various corporations for increasing OT/control system and network security. [7]. Khunrak et al. discussed the challenges and risks of Industry 4.0 from various perspectives including human, goods, money, and information in the global supply chain model [8]. Murray et al. highlighted some of the possible results of cyber-attacks in industrial applications in the OT field [9]. Paes et al. extracted some of the measures that can be taken to ensure system reliability and security when integrating OT and IT [10]. Conklin et al. presented a new method for measuring the security in OT systems by adding resilience as a driving factor [11].

Each of the above examples highlights the value of security in the context of operational technology and the need for improved risk assessment that considers the dynamism and resource-constrained nature of OT systems.

In contrast, the current paper systematically investigated the risk factors for OT systems on the basis of cyber and non-cyber risk perspectives and extracted 16 of them. In future work, we will analyze these risk factors in detail and develop effective countermeasures that encompass both cyber and non-cyber risks.

V. CONCLUSION AND FUTURE WORK

In this paper, we conducted a risk analysis for an open OT architecture integrated with IT networks while considering the non-cyber aspects of risk as a new perspective. Specifically, as an initial study, the risk factors for OT systems were comprehensively extracted and a total of 16 were identified. The main risk factors include fault isolation in OT systems and inadequate security functions of existing equipment on the cyber side and the safety management of IT-OT linked systems on the non-cyber side.

In future work, we will perform the remaining two procedures of risk assessment: risk analysis and risk evaluation. We will also develop new countermeasures to increase the risk reduction in IT/OT integrated systems.

ACKNOWLEDGEMENT

This work was supported by JSPS KAKENHI Grant Number JP 19H04098.

REFERENCE

[1] B. Posey et al., Operational Technology (OT), https://www.techtarget.com/whatis/definition/operational-technology

[2] M. Waters, et al., “Open Source IIoT Solution for Gas Waste Monitoring in Smart Factory, Mitsubishi Electric Air-Conditioning Systems Europe Ltd., 2022. https://www.mdpi.com/1424-8220/22/8/2972

[3] Cyberthreats to ICS systems, Kaspersky Lab, Moscow, 2014.

[4] O. Andreeva, et al., Industrial control systems vulnerabilities statistics, Kaspersky Lab, Moscow, 2016. https://media.kasperskycontenthub.com/wpcontent/uploads/sites/43/2016/07/07190426/KL_REPORT_ICS_Statistic_vulnerabilities.pdf

[5] Project Management Institute, “A guide to the project management body of knowledge PMBOK Guide”, Sixth Edition, PMI, 2017.

[6] S. Wangyal, et al., A Study of Multi-viewpoint Risk Assessment of Internet of Things (IoT), 9th International Congress on Advanced Applied Informatics (AAI2020), pp.643-648, 2020.

[7] B. Filkins, et al., SANS 2019 State of OT/ICS Cybersecurity Survey, June 2019.

[8] W. Khunrak, et al., A study on Business resources for Risk Management in Global Supply Chain Model, 12th International Conference on Project Management, 2018.

[9] G. Murray, et al., The Convergence of IT and OT in critical infrastructure, 2017.

[10] R. Paes, et al., A Guide to Securing Industrial Control Network, 20, Dec 2019.

[11] W. A. Conklin, et al., IT vs OT Security: A Time to Consider a Change in CIA to Include Resilience, 2016.