Chapter 1

Overview

December 2023

This chapter should be cited as

ERIA study team (2023), 'Overview', in Oikawa, K. and Y. Hatakeyama (eds.), *Operational Technology Security in ASEAN.* ERIA Research Project Report FY2023 No. 19, Jakarta: ERIA, pp.1-7.

Chapter 1

Overview

1. Background and Objective

In commemoration of the 50th anniversary of Japan–Association of Southeast Asian Nations (ASEAN) friendship and cooperation, this study provides an overview of the current challenges and proposes collaborative solutions between Japan and ASEAN to address operational technology security, which has become an important issue in the ASEAN region.

The official friendship and cooperation between ASEAN and Japan began with the Japan–ASEAN Synthetic Rubber Forum in 1973. Against the backdrop of significant appreciation of the yen following the Plasa Accord in 1985 and the advancement of information and communication technology (ICT) around 1990, multinational companies in Japan established sophisticated international production networks (IPNs) in the ASEAN and East Asian regions. Direct investments from Japan to the ASEAN region have led to industrial upgrading and economic growth. The IPNs built by ASEAN and Japan demonstrated resilience during the shock of the coronavirus disease (COVID-19) pandemic (Oikawa et al., 2021) and played a crucial role in supporting the regional economy.

While the robust IPNs in the ASEAN and Japan region serve as a source of significant competitiveness, there are numerous challenges that need to be addressed to maintain and enhance it. One such challenge is the advanced digitalisation of supply chains and the corresponding need for heightened security measures. Globally, the digitalisation of critical infrastructure has brought attention to the disparity in operational technology security risks, security regulations across countries, and governance frameworks of various entities.

In ASEAN, awareness of ICT security has been increasing. However, awareness and preparedness levels regarding operational technology security remain insufficient. It is essential to upgrade cyber-resilience across Asia and prioritise the strengthening of operational technology security in critical infrastructure and manufacturing supply chains.

Improving the security levels of ASEAN countries and the related nations is crucial, along with creating an environment where ASEAN enterprises can easily participate in global value chains. Therefore, in the short term, it is necessary to raise the security levels of ASEAN countries and the security levels of countries, industries, and enterprises closely related to these supply chains.

This research clarifies the current state and desired state of operational technology security measures in ASEAN, evaluates the gap between the current situation and the desired state, and subsequently considers policies to enhance operational technology security. The goal is to contribute to the improvement of ASEAN's cybersecurity readiness, as well as the sustainability of IPNs.

2. Importance of Operational Technology Security

According to the International Electrotechnical Commission (IEC) website, operational technology refers to 'the hardware and software systems that are used to control and monitor physical processes in industries such as manufacturing, energy, transport and utilities' (IEC, 2023). Specific examples include supervisory control and data acquisition systems used to monitor and control the flow of electricity in power plants; building automation systems used to control heating, ventilation, and air conditioning systems in commercial buildings; industrial control systems (ICSs) used to control manufacturing processes and assembly lines in factories; and transportation systems such as traffic control systems used to manage the flow of vehicles on highways and in urban areas.

Cybersecurity measures in operational technology systems are called operational technology security. In security, there are three elements: 'Confidentiality,' 'Integrity,' and 'Availability'. Confidentiality is to restrict access to information to a limited number of people; Integrity is to protect information from unauthorised tampering; and Availability is to allow users to access information when they need it. In ICT security, the importance of protecting sensitive information is paramount, so the order of importance is 'Confidentiality,' 'Integrity,' and 'Availability'. Operational technology security, on the other hand, requires 24/7/365 operation, so the importance order is 'Availability', 'Integrity',' Confidentiality'. Therefore, it is difficult to ensure the frequency of security measures such as equipment replacement and software updates. Furthermore, since some machines are used for decades, they tend to become what is known as legacy equipment. Legacy equipment used in operational technology systems tends not to have enough memory for installing security software. As a result, equipment with insufficient security measures can be left behind. As noted above, operational technology security has different characteristics from ICT security, so specific discussion and measures are required.

3. Approach

The primary objective of this study is to understand the present conditions, also referred to as the 'As-Is' state, of various ASEAN countries. Given the need for targeted focus, we select specific industries and countries within the ASEAN region for examination. This selection is based on several factors including the market size of the industries involved in operational technology, their relative importance, and the overall market size of the countries themselves.

Next, we initiate a survey aimed at understanding the global initiatives that can potentially impact each ASEAN country, as well as those initiatives shared across all ASEAN nations. We scrutinise each country's progress from both a governmental and corporate perspective, focusing on the existence of standards, certifications, and training related to operational technology security, as well as the state of corporate security measures.

In order to gain insight into the desired future state, also referred to as the 'To-Be' state, we also study the practices of countries known for their advanced operational technology security initiatives, such as the United States (US), European Union (EU), and Japan. This offers a glimpse into potential paths that these ASEAN countries could follow.

The research is primarily conducted through desk-based research and through interviews with international experts and business representatives. This combination allows for a comprehensive understanding of both the current and potential future states of operational technology security in the ASEAN region.

4. Deep Investigation Targets

In this study, we have chosen the **infrastructure industry** and the **manufacturing industry** for deep investigation targets, based on the high necessity of operational technology security and the size of the market. The reason for using the necessity of operational technology security as a criterion is because it was determined that industries with a large ripple effect to other sectors when an incident occurs should be the top priority for investigation and policy consideration. For this reason, the infrastructure industry was selected as the first main subject for detailed investigation. The reason for using the size of the market is, similarly, from the viewpoint of reducing operational technology security risks in the ASEAN region: it was determined that industries that would incur a large amount of damage when an incident occurs should be the top priority for investigation and policy consideration. For this reason, the manufacturing industry was chosen as the second main subject for detailed investigation.

As for countries, we have chosen the following countries for deep investigation targets: **Indonesia, Thailand, Singapore, the Philippines, Malaysia,** and **Viet Nam**, based on the size of nominal gross domestic product (GDP) and the depth of relations with Japan. The reason for using the size of the nominal GDP is the same as the reason for narrowing down the industries: it was decided that industries that would suffer a large amount of damage when an incident occurs should be the highest priority for investigation and policy consideration. The reason for using the depth of relations with Japan as a criterion is because it was decided that countries where the effectiveness of measures can be expected should be given priority. For these reasons, Indonesia, Thailand, Singapore, the Philippines, Malaysia, and Viet Nam, all with a nominal GDP of over $300 billion in 2021, were selected.

Targeted Industries

Among the industries classified by the Statistics Bureau of Japan, the industries that require operational technology security are mainly the manufacturing industry, where industrial control systems are increasingly used in factories, and the infrastructure industry, where monitoring and control systems are increasingly used in power plants. Other industries include the transportation and warehousing industry and the wholesale and retail industry, where operational technology security needs exist due to the increasing automation of asset management, means of transportation, and warehouses (TENABLE, 2023a). Needs also exist in the building maintenance industry within the real estate sector because the potential for attacks on building management systems also exists. In fact, the Ministry of Economy, Trade and Industry (METI) of Japan has prepared and published ‘Guidelines for Cyber Physical Security Measures in Building Systems’ (METI, 2023). In addition, operational technology security needs exist for select medical fields and for companies that manufacture medical devices, similar to those of manufacturing plants (TENABLE, 2023b).

In particular, the infrastructure industry has a high priority for countermeasures because of the social impact of a cyberattack. In September 2010, it was announced that a cyberattack had targeted uranium enrichment centrifuges at a nuclear fuel facility located in Natanz, Iran, and was said to be the world's first cyber-weapon targeting a control system (IPA, 2020). In the energy sector, cyberattacks targeting power systems in Ukraine caused large power outages in 2015 and 2016 (Noguchi and Ueda, 2017). In 2021, Colonial Pipeline, an oil pipeline system that primarily transports gasoline and jet fuel to the southeastern US, suffered a cyberattack that forced it to shut down all pipeline operations (The White House, 2021).

An analysis of the GDP contribution by each industry in the ASEAN member countries shows that the manufacturing industry accounts for more than 20% of GDP (see Figure 1.1). Therefore, we conclude that the operational technology security risk in the manufacturing industry is high.

Targeted Countries

We selected countries for in-depth analysis based on the GDP of each country and the level of its relationship with Japan. For the latter, we refer to the number of local legal entities of Japanese firms and the size of exports to Japan (see Figure 1.2).

The GDP of Indonesia is over $1 trillion, and that of Thailand, Singapore, the Philippines, Malaysia, and Viet Nam is over $300 billion, while the GDP of the remaining four countries, Myanmar, Cambodia, Lao People's Democratic Republic (Lao PDR), and Brunei Darussalam, is less than $100 billion. The number of local subsidiaries of Japanese firms in Thailand is also very high. The number of local subsidiaries of Japanese companies is more than 1,000 in Thailand, Indonesia, Viet Nam, and Singapore, and more than 500 in Malaysia and the Philippines, but less than 131 in the remaining four countries. The value of Japan's imports from Thailand, Viet Nam, Malaysia, Indonesia, the Philippines, and Singapore, in that order, is more than $10 billion, while the value is less than $2 trillion in the remaining four countries.

Based on the above, Indonesia, Thailand, Singapore, the Philippines, Malaysia, and Viet Nam are selected for in-depth analysis because their GDP and relationship with Japan are higher than those of the other four countries.

Figure 1.1. GDP by Industry in ASEAN Member Countries

	Nominal GDP (US$ 10 million)	Infrastructure GDP (US$ 10 million)	Manufacturing GDP (US$ 10 million)	Transportation and Warehousing GDP (US$ 10 million)	Wholesale/Retail GDP (US$ 10 million)
Indonesia	11,861	130 (GDP1.1%, 2021)	2,422 (GDP20.5%, 2021)	439 (GDP3.7%, 2021)	1,542 (GDP13.0%, 2021)
Thailand	5,060	147 (GDP2.9%, 2021)	1,376 (GDP27.2%, 2021)	233 (GDP4.6%, 2021)	824 (GDP16.3%, 2021)
Singapore	3,970	48 (GDP1.2%, 2021)	885 (GDP22.3%, 2021)	242 (GDP10.4%, 2022)	766 (GDP19.9%, 2022)
Philippines	3,941	104 (GDP3%, 2018)	659 (GDP19%, 2018)	208 (GDP6%, 2018)	659 (GDP19%, 2018)
Malaysia	3,727	69 (GDP2.3%, 2011)	733 (GDP24.6%, 2011)	188 (Telecommunications included, GDP6.3%, 2011)	411 (GDP13.8%, 2011)
Viet Nam	3,626	138 (GDP3.8%, 2021)	823 (GDP22.7%, 2021)	199 (GDP5.5%, 2021)	323 (GDP8.9%, 2021)
Myanmar	651	8 (GDP1.3%, 2016)	137 (GDP22.8%, 2016)	107 (Telecommunications included, GDP17.7%,2016)	111 (Lodging and catering included, GDP18.4%, 2016)
Cambodia	270	0.7 (GDP0.6%, 2010)	18 (GDP15.6%, 2010)	9 (Telecommunications included, GDP8.1%, 2010)	11 (GDP9.9%, 2010)
Lao PDR	188	4 (GDP4.8%, 2011)	9 (GDP9.9%, 2011)	5 (Telecommunications included, GDP5.3%, 2011)	19 (GDP21.8%, 2011)
Brunei Darussalam	140	5 (GDP2.7%, 2011)	22 (GDP11.8%, 2011)	6 (Telecommunications included, GDP3.0%, 2011)	6 (GDP3.2%, 2011)

ASEAN = Association of Southeast Asian Nations, GDP = gross domestic product, Lao PDR = Lao People's Democratic Republic.

Source: Author. Data refer to Japan Bank for International Cooperation Report, National Statistics Bureau data (2011~22). For the infrastructure industry, refer to Public Utilities.

Figure 1.2. GDP in ASEAN Member Countries and its Relationship with Japan

	nominal GDP (2021)	Number of locally incorporated Japanese companies (2020)	Japan imports based on customs clearance (2021)
Indonesia	1,186 billion US dollars	1,147	19,582 million US dollars
Thailand	5,06 billion US dollars	2,362	26,335 million US dollars
Singapore	3,97 billion US dollars	1,117	8,843 million US dollars
Philippines	3,94 billion US dollars	595	10,848 million US dollars
Malaysia	3,73 billion US dollars	790	19,691 million US dollars
Viet Nam	3,63 billion US dollars	1,188	23,000 million US dollars
Myanmar	65 billion US dollars	131	962 million US dollars
Cambodia	27 billion US dollars	62	1,748 million US dollars
Lao PDR	19 billion US dollars	18	130 million US dollars
Brunei Darussalam	14 billion US dollars	4	-

ASEAN = Association of Southeast Asian Nations, GDP = gross domestic product, Lao PDR = Lao People's Democratic Republic.

Source: Author. Data from: Japan Bank for International Cooperation reports, National Bureau of Statistics data, Statistics Japan, 'Basic Survey on Overseas Business Activities / Survey Results: 51st Survey Results (FY2020 Results)'.

References

IEC (2023), 'Cyber Security for Operational Technology', https://iec.ch/blog/cyber-security-operational-technology (accessed 15 November 2023).

IPA (2020), '制御システムのセキュリティリスク分析ガイド補足資料 制御システム関連の サイバーインシデント事例４', [Control System Security Risk Analysis Guide Supplemental Material Control system-related Cyber Incident Case Study 4] https://www.ipa.go.jp/security/controlsystem/ug65p900000197wa-att/000080701.pdf (accessed 15 November 2023).

METI (2023), 'ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第 2 版 ',[Guidelines for Cyber-Physical Security Measures in Building Systems', https://www.meti.go.jp/policy/netsecurity/wg1/building_guideline.html (accessed 15 November 2023).

NISC (2017), '重要インフラの情報セキュリティ対策に係る第 4 次行動計画', [Information Security Measures for Critical Infrastructure Fourth Action Plan], https://www.nisc.go.jp/active/infra/pdf/infra_rt4_r2.pdf (accessed 15 November 2023).

Noguchi, M. and h. Ueda (2017), '重要インフラに対するサイバー攻撃の実態と分析', [Actual Facts and Analysis of Cyber Attacks on Critical Infrastructure]. Tokyo: NEC https://jpn.nec.com/techrep/journal/g17/n02/pdf/170204.pdf (accessed 15 November 2023).

Oikawa, K., Y. Todo, M. Ambashi, F. Kimura, and S. Urata (2021), 'The Impact of COVID-19 on Business Activities and Supply Chains in the ASEAN Member States and India', *ERIA Discussion Paper Series*, No. 384, ERIA-DP-2021-17. Jakarta: Economic Research Institute for ASEAN and East Asia (ERIA).

TENABLE (2023a),'安全で確かなサービスを提供できる、人と物の輸送のための産業用サイバーセキュリティ', [Solutions for Transportation Industrial cybersecurity for the transport of people and goods that can provide safe and reliable services], https://jp.tenable.com/solutions/transportation (accessed 15 November 2023).

TENABLE (2023b) , '医薬および医療機器製造業のための産業用サイバーセキュリティ' [Industrial Cybersecurity for the Pharmaceutical and Medical Device Manufacturing Industry', https://jp.tenable.com/solutions/medical-manufacturing (accessed 15 November 2023).

White House (2021), 'FACT SHEET: The Biden-Harris Administration Has Launched an All-of-Government Effort to Address Colonial Pipeline Incident', https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/11/fact-sheet-the-biden-harris-administration-has-launched-an-all-of-government-effort-to-address-colonial-pipeline-incident/ (accessed 15 November 2023).