ERIA Research Project Report FY2023 No. 19

Operational Technology Security in ASEAN

Edited by

Keita Oikawa

Yoichiro Hatakeyama

ERIA
Economic Research Institute
for ASEAN and East Asia

Operational Technology Security in ASEAN

Economic Research Institute for ASEAN and East Asia (ERIA)
Sentral Senayan II 6th Floor
Jalan Asia Afrika No. 8, Gelora Bung Karno
Senayan, Jakarta Pusat 12710
Indonesia

ERIA Research Project Report FY2023 No. 19
Published in December 2023

The findings, interpretations, conclusions, and views expressed in their respective chapters are entirely those of the author/s and do not reflect the views and policies of the Economic Research Institute for ASEAN and East Asia, its Governing Board, Academic Advisory Council, or the institutions and governments they represent. Any error in content or citation in the respective chapters is the sole responsibility of the author/s.

List of Authors

Keita Oikawa

Economist, Economic Research Institute for ASEAN and East Asia (ERIA), Jakarta, Indonesia.

Yoichiro Hatakeyama

Senior Policy Advisor at the Economic Research Institute for ASEAN and East Asia (ERIA), Jakarta, Indonesia.

Koichi Hasegawa

Managing Director & Partner at Boston Consulting Group, Tokyo, Japan.

Masami Shibatani

Associate Director at Boston Consulting Group, Tokyo, Japan.

Eisuke Tanaka

Project Leader at Boston Consulting Group, Tokyo, Japan.

Junichi Ida

Consultant at Boston Consulting Group, Tokyo, Japan.

Yoko Yarimizu

Senior Associate at Boston Consulting Group, Tokyo, Japan.

Table of Contents

List of Figures

Executive Summary

This study commemorates the 50th anniversary of Association of Southeast Asian Nations (ASEAN)–Japan friendship and cooperation by examining the challenges and proposing collaborative solutions for operational technology security in the ASEAN region. Multinational companies in Japan established international production networks (IPNs) in ASEAN and East Asia, which proved resilient during the coronavirus disease (COVID-19) pandemic and supported the regional economy. However, maintaining competitiveness requires addressing challenges such as advanced supply chain digitalisation and the associated need for increased security measures. Operational technology security risks, regulatory disparities, and governance frameworks are global concerns in the digitalisation of critical infrastructure. To enhance IPN competitiveness, cyber-resilience across Asia must be improved, prioritising operational technology security in critical infrastructure and manufacturing supply chains. This research bridges the gap between current and desired operational technology security states, proposes policies, and contributes to ASEAN cybersecurity readiness and IPN sustainability in collaboration between ASEAN and Japan.

While awareness of information and communication technology security is rising in ASEAN, operational technology security awareness and preparedness remain insufficient. In ASEAN, few countries have launched initiatives on operational technology security as a country. Singapore has developed its own standards based on International Electrotechnical Commission (IEC) 62443 and has also developed product certification for operational technology security in a way that is tied to government procurement requirements. Malaysia has begun to develop its own standards from 2023, by adopting IEC 62443. However, in other ASEAN countries no national initiatives have yet been seen.

As for current operational technology security level in ASEAN companies, while some are highly sensitive to it due to high awareness of enhanced governance and the occurrence of related incidents, others are not taking measures due to delays in digitalisation and lack of understanding of its necessity. Global companies and some local companies (e.g. companies in industries where operational technology-related incidents have occurred in the past, companies related to critical infrastructure, etc.) tend to take voluntary measures by referring to global standards, regardless of the existence of local standards. However, there are many companies that understand the importance of operational technology security but have yet to take systematic measures due to high cost, lack of experts, or lack of clear government guidelines. There are also many local companies that have not taken measures due to low priority caused by lack of understanding of the importance of operational technology security. In addition, there are companies that are not required to take operational technology measures due to the lack of automation in their plants.

In contrast to current status, ideally, coordinated efforts to enhance operational technology security should be promoted throughout the region, and regulations should be introduced by each government based on a regional agreement, and corporate operational technology security measures should mature based on these regulations. In recent trends, due to the expansion of global supply chains, the importance of coordination throughout the region is increasing more and more, and if countries and companies pursue their individual optimal efforts, they may lose global business opportunities. In this context, Japan can contribute to solving issues that are difficult for governments and companies in ASEAN countries to solve. Specifically, it is believed to be beneficial to deepen

support in the following two directions. The first is to foster and horizontally develop operational technology security measures using a third-party perspective, such as hosting meetings where government, industry groups, and major companies gather to share best practices, or conducting cybersecurity exercises for major companies. The second is to support the development of a common ASEAN framework based on global standards, the establishment of a common company and product certification system, and the standardisation of procurement requirements, which is support for the development of common systems.

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.

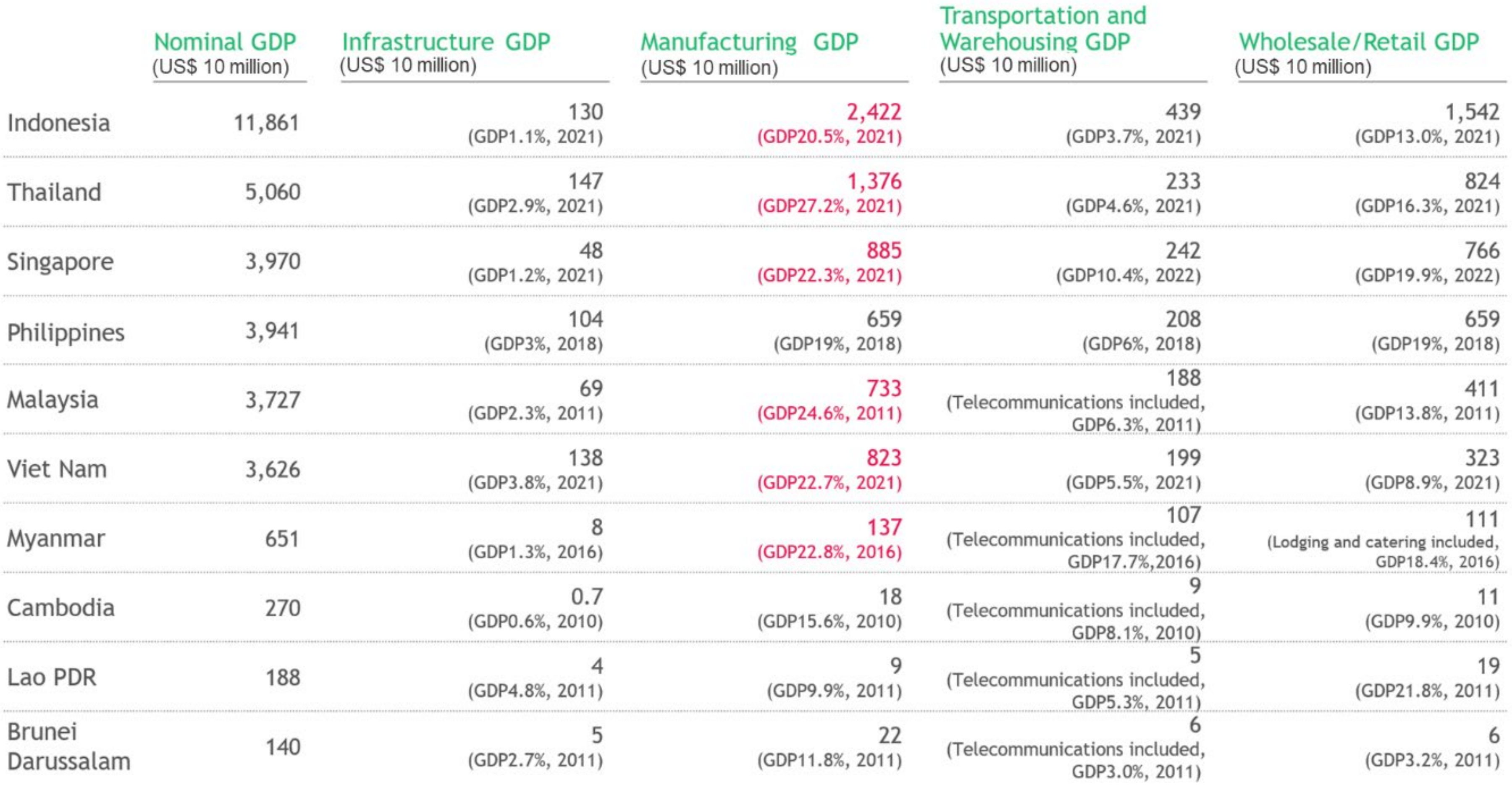
Targeted Countries

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

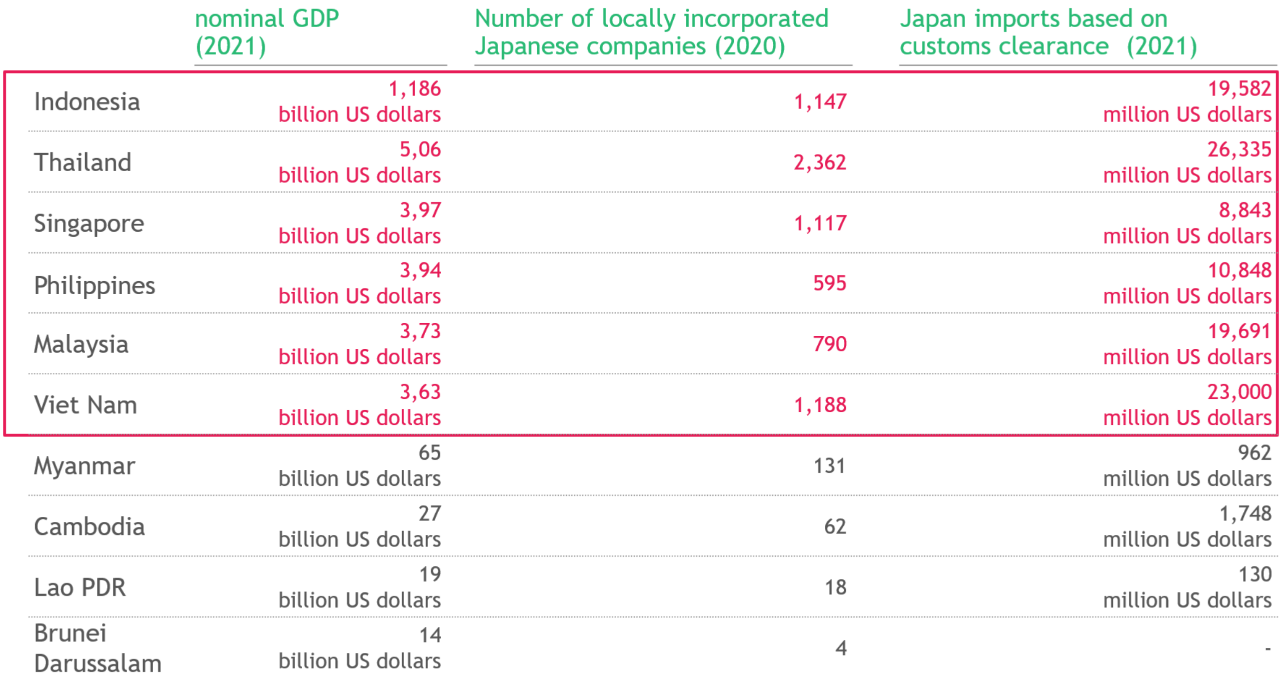


	Nominal GDP (US$ 10 million)	Infrastructure GDP (US$ 10 million)	Manufacturing GDP (US$ 10 million)	Transportation and Warehousing GDP (US$ 10 million)	Wholesale/Retail GDP (US$ 10 million)
Indonesia	11,861	130 (GDP1.1%, 2021)	2,422 (GDP20.5%, 2021)	439 (GDP3.7%, 2021)	1,542 (GDP13.0%, 2021)
Thailand	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).

Chapter 2

Current Status of Operational Technology Security

This study summarises the status of operational technology security initiatives in six ASEAN countries (Singapore, Malaysia, Thailand, Indonesia, Viet Nam, and the Philippines) based on interviews with people from implementing companies and a survey of public documents. In addition, major initiatives in the US, Europe, and Japan are also summarised.

In this report, information was gathered based on interviews and a survey of publicly available information. For each country, we interviewed people involved in operational technology security operations in the manufacturing and infrastructure industries. Through the interviews, we planned to dig deeper if we found that there were differences in the countermeasure status of each industry. However, we have found out that operational technology security standards and certifications are common regardless of the industry. Therefore, in the following sections, we will explain the general status of operational technology security in each country regardless of the industry.

While there are several sectors within the manufacturing industry, such as heavy industry and light industry, and their priorities for operational technology security measures may vary, the overall measure for operational technology security remains unchanged. Therefore, the investigation was conducted in a manner that does not differentiate between them.

In this study, we investigated the status of ‘standards/guidelines,’ ‘certification,’ and ‘training’ in order to measure the maturity of each country’s government in terms of operational technology security.

As elaborated in the subsequent session, an internationally recognised and firmly established model for operational technology security governance has already formulated. For a government seeking to enhance the operational technology security level within its jurisdiction, the strategy involves adopting this model as a blueprint for national implementation. This approach entails the initial establishment of national standards or guidelines, delineating the requirements to be complied with. Subsequently, the framework involves the development of certification qualifications to externally demonstrate that companies, products, or individuals conform these established standards or guidelines. Finally, a comprehensive training system is established to facilitate the process of obtaining certification.

Based on the above thinking, by investigating the status of ‘standards/guidelines,’ ‘certification,’ and ‘training,’ we confirmed the maturity of each country's government in terms of operational technology security.

1. Global Initiatives

Global standards/guidelines

An official global standard is established through consensus building amongst experts of various countries so it becomes the norm for all companies worldwide. Although global standards themselves are not mandatory, they are used as a reference when national institutions create new standards and certifications for domestic use. For companies, they can be used as a baseline and best-practice material when considering their own policies.

IEC 62443 exists as the only global standard for operational technology security. It is a series of international standards, also known as the ISA/IEC 62443 series, published by the IEC and the International Society of Automation (ISA). IEC is the world's leading organisation for the preparation and publication of international standards for all electrical, electronic, and related technologies. ISA is a non-profit professional association of engineers, technicians, and management engaged in industrial automation. Furthermore, the Component Security Assurance certification, which is an authentication system for industrial internet of things (IoT) devices used in the US and Japan, is based on IEC 62443.

This series focuses specifically on operational technology, not ICT, and covers industrial automation and control systems (IACS) in terms of hardware and software, as well as organisations and processes.

IEC has been releasing the standards sequentially since 2009. Figure 2.1 shows the scope and outline of the four IEC 62443 standards and the publication status and titles of four sections and the 14 parts.

IEC 62443-1 defines the concepts and terminology underlying operational technology, which should be read by all interested parties. In 'Part 1-1: Terminology, concepts, and models', seven foundational requirements are explained:

1) **Access Control**. Reliably identify and authenticate all users (humans, software processes and devices) attempting to access the IACS.

2) **Use Control**. Enforce the assigned privileges of an authenticated user to perform the requested action on the system or assets and monitor the use of these privileges.

3) **System Integrity**. Ensure the integrity of the IACS to prevent unauthorised manipulation.

4) **Data Confidentiality**. Ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorised disclosure.

5) **Restrict Data Flow**. Segment the control system via zones and conduits to limit unnecessary flow data. Zones consist of the grouping of cyber-assets that share the same cybersecurity requirements and conduits are the paths between zones.

6) **Timely Response to Events**. Respond to security violations by notifying the proper authority reporting needed evidence of the violation and taking timely corrective action when incidents occur.

7) **Resource Availability**. Ensure the availability of the control system against the degradation or denial of essential services.

‘Part 1-2: Master glossary of terms and definitions’ is not published yet but it will be a list of terms and abbreviations used throughout the series. ‘Part 1-3: System security conformance metrics’ is not published yet but it gives an overview on methodology to develop quantitative metrics derived from the process and technical requirements in the standards. ‘Part 1-4: IACS security lifecycle and use cases’ is not published yet but it is supposed to provide more detailed description of the underlying lifecycle for IACS security, as well as several use cases that illustrate various applications.

IEC 62443-2 provides asset owners with the information of requirements for cybersecurity management systems as management (administrative and operational) policies and procedures for asset owners. ‘Part 2-1: Establishing an IACS security program’ describes what is required to define and implement an effective IACS cybersecurity management system (CSMS). It is based on information security management system (ISMS), the standard of ICT security, and it defines the requirements of how the organisation should handle the IACS-related risk. The intended audience includes asset owners who have responsibility for the design and implementation of such a program. ‘Part 2-2: IACS security program ratings’, which is not published yet, provides a methodology for evaluating the level of protection provided by an operational IACS against the requirements in the ISA/IEC 62443 Series of standards. ‘Part 2-3: Patch management in the IACS environment’ provides technical guidance on patch management for IACS. The intended audience includes anyone who has responsibility for the design and implementation of a patch management programme. ‘Part 2-4: Security program requirements for IACS service providers’ specifies a comprehensive set of requirements for security capabilities for IACS service providers that they can offer to the asset owner during integration and maintenance activities of an automation solution.

‘Part 2-5: Implementation guidance for IACS asset owners’, which is not published yet, provides guidance on what is required to operate an effective IACS cybersecurity programme. The intended audience includes asset owners who have responsibility for the operation of such a programme.

IEC 62443-3 defines computer system network security issues for system integrators. ‘Part 3-1: Security technologies for IACS’ describes the application of various security technologies, such as authentication, filtering/blocking/access control, cryptography/data protection. The intended audience includes anyone who wishes to learn more about the applicability of specific technologies in a control systems environment. ‘Part 3-2: Security risk assessment for system design’ addresses cybersecurity risk assessment and system design for IACS and defines the details of the Zone and Conduit model. This standard is primarily directed at asset owners and system integrators. ‘Part 3-3: System security requirements and security levels’ describes the requirements for seven foundational requirements. It defines four security levels (SL1, SL2, SL3, SL4) and it defines the set of requirements to meet each SL. SL1 is a protection against casual or coincidental violation. SL2 is a protection against intentional violation using simple means with low resources, generic skills, and low motivation. SL3 is a protection against intentional violation using sophisticated means with moderate resources, IACS-specific skills, and moderate motivation. SL4 is a protection against intentional violation using sophisticated means with extended resources, IACS-specific skills, and high motivation. The principal audience includes suppliers of control systems, system integrators, and asset owners.

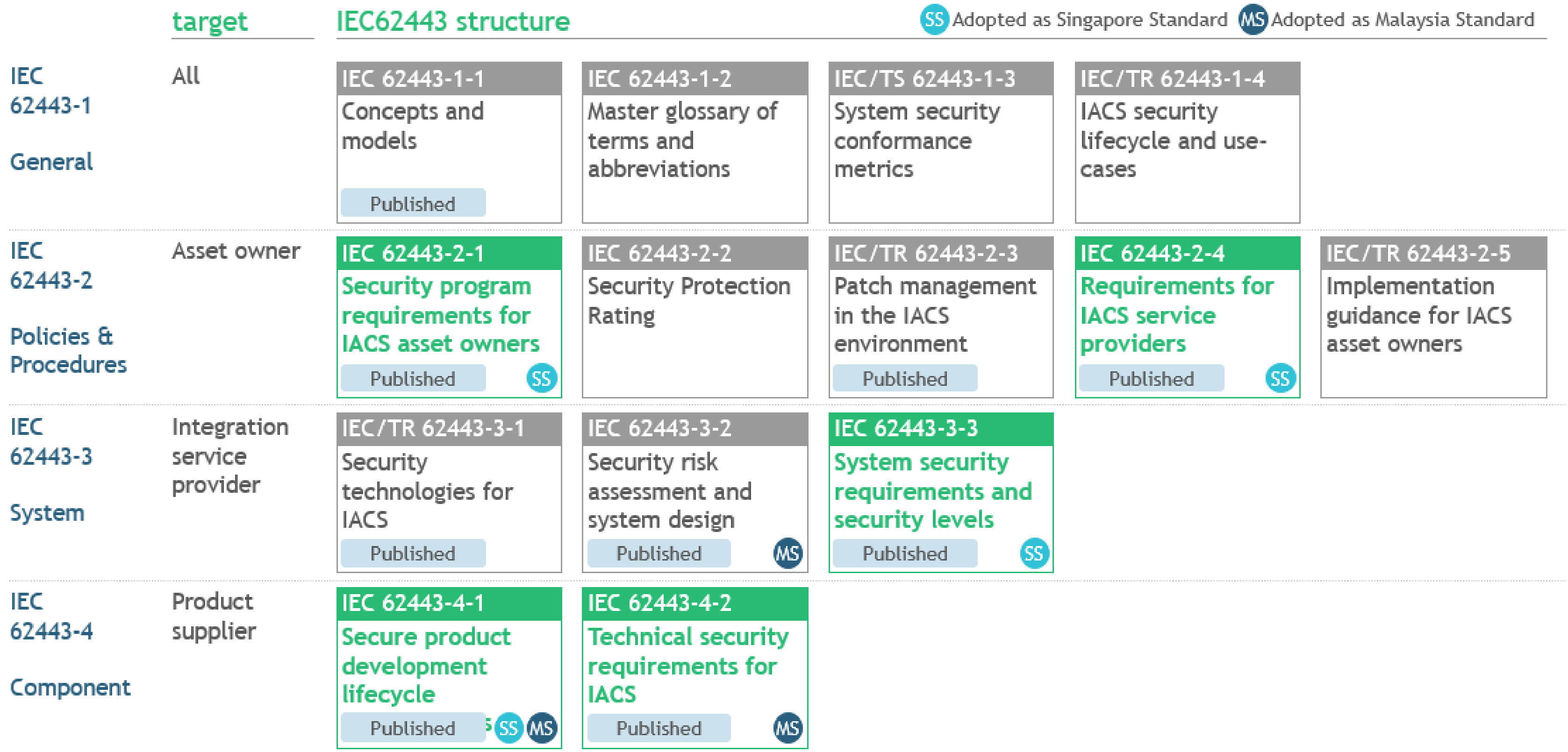
IEC 62443-4 defines requirements for product providers as the security of their products.

‘Part 4-1: Product security development life cycle requirements’ describes the requirements for a product developer’s security development lifecycle. The principal audience includes suppliers of control system and component products. ‘Part 4-2: Technical security requirement for IACS components' describes the requirements for IACS components based on security level. The principal audience includes suppliers of component products that are used in control systems.

Of the 14 parts, five (IEC 62443-1-2, IEC 62443-1-3, IEC 62443-1-4, IEC 62443-2-2, IEC 62443-2-5) are still in the planning stage and are not yet published; as noted in Section 2.2, Singapore and Malaysia have adopted parts of IEC 62443 as their national standards.

There are still some parts that have not been released to the public, especially those items with requirements (IEC 62443-2-1, IEC 62443-2-4, IEC 62443-3-3, IEC 62443-4-1, IEC 62443-4-2) that have already been released. As a result, it is considered to have all the necessary content for companies to take countermeasures. In addition, since there is no single answer, it would be desirable for each company to secure security personnel who can interpret and understand the requirements appropriately and enhance their operational technology security in line with them. New parts that will be released in the future are likely to play the role of a guide by narrowing the range of interpretation and making it easier to understand the image of concrete measures, as can be inferred from their names. It is important to note, however, that this assertion remains speculative.

Figure 2.1. IEC 62443



SS Adopted as Singapore Standard MS Adopted as Malaysia Standard

	target	IEC62443 structure				
IEC 62443-1 General	All	IEC 62443-1-1 Concepts and models Published	IEC 62443-1-2 Master glossary of terms and abbreviations	IEC/TS 62443-1-3 System security conformance metrics	IEC/TR 62443-1-4 IACS security lifecycle and use-cases	
IEC 62443-2 Policies & Procedures	Asset owner	IEC 62443-2-1 Security program requirements for IACS asset owners Published SS	IEC 62443-2-2 Security Protection Rating	IEC/TR 62443-2-3 Patch management in the IACS environment Published	IEC 62443-2-4 Requirements for IACS service providers Published SS	IEC/TR 62443-2-5 Implementation guidance for IACS asset owners
IEC 62443-3 System	Integration service provider	IEC/TR 62443-3-1 Security technologies for IACS Published	IEC 62443-3-2 Security risk assessment and system design Published MS	IEC 62443-3-3 System security requirements and security levels Published SS		
IEC 62443-4 Component	Product supplier	IEC 62443-4-1 Secure product development lifecycle Published SS MS	IEC 62443-4-2 Technical security requirements for IACS Published MS			

IACS = industrial automation and supply system, IEC = International Electrotechnical Commission.
Source: Authors.

Global certification

As mentioned at the beginning of the chapter, the development of certification qualifications is a meaningful viewpoint to capture status of operational technology security. Certifications usually consist of corporate certification, product certification and individual certification; we have looked at global certification for each of the above.

Corporate certification is important because it can be an indicator for companies to aim for. As for corporate certification, third-party organisations provide certification based on IEC 62443. For example, system security assurance (SSA) certification is based on IEC 62443-3-3 issued by ISA (ISASecure, 2023). In addition, although not a certification, there are companies and organisations that provide assessment services based on IEC 62443, which are used by companies that are responding to it.

Product certification pertains to products such as software/hardware/service. As a product certification, there is the Component Security Assurance certification offered by ISA (ISASecure, 2019), which is in line with ISA 62443-4-1 and IEC 62443-4-2.

Certification for individuals is useful as an indicator of an individual’s knowledge of security. For companies, it can also be used as a criterion for hiring experts or as a milestone in internal training. As for individual certification, there are institutions that provide certification based on IEC 62443. There are four certifications, which are Cybersecurity Fundamentals Specialist, Cybersecurity Risk Assessment Specialist, Cybersecurity Design Specialist, and Cybersecurity Maintenance Specialist, according to content and level. Each certificate requires people to successfully complete a course and pass the exam. Successful completion of Certificate 1: ISA/IEC 62443 Cybersecurity Fundamentals Specialist is required before taking exams for certificates 2, 3, and 4. The ISA/IEC 62443 Cybersecurity Expert certificate is awarded automatically upon successful completion of all four certificates (ISA, 2023).

Other individual certifications such as the Global Industrial Cyber Security Professional Certification by Global Information Assurance Certification (GIAC, 2023a) and the GIAC Response and Industrial Defense (GIAC, 2023b) exist.

Training

Country-led training will be discussed in the following country-specific sections. However, training that is made available in multiple countries by global companies is described in this section as a global initiative.

Globally, training by private companies exists. As from the interview (Appendix 1.4, 1.8), companies are utilising those non-government global training for their employee training. For example, SANS offers multi-month training and certificate issuance on operational technology (SANS, 2023). Also, security tool vendors provide training (TREND MICRO, 2023).

2. ASEAN Initiatives

As mentioned, for each of six targeted ASEAN countries, we investigated the status of ‘standards/guidelines,’ ‘certification,’ and ‘training’ in order to measure the maturity of each country’s government in terms of operational technology security.

2.1. ASEAN

ASEAN has not yet undertaken any initiatives specific to operational technology security, with the only document it has released that mentions cybersecurity being the Cybersecurity Cooperation Strategy. The strategy has a 2017–20 version and a 2021–25 version (ASEAN, 2023).

The 2017–20 version aimed to create a roadmap for regional cooperation, and the strategy included the establishment, strengthening, and coordination of a computer emergency response team, clarification of the organisation responsible for coordinating the above activities, and capacity building implementation. Based on this strategy, the ASEAN Summit Statement on Cybersecurity Cooperation was released in 2018, the ASEAN Cybersecurity Coordination Committee (ASEAN Cyber-CC) was established in 2020, the ASEAN Ministerial Conference on Cybersecurity was implemented, and the ASEAN Digital Master Plan 2025 was formulated in 2021.

In the 2021–25 version, the strategy was updated to consider the accelerating digitalisation of ASEAN, including the increase in the number of internet users, and the growing sophistication of cyber-attacks. Specifically, the five strategies are: promoting cyber-readiness cooperation, strengthening regional cyber policy coordination, enhancing trust in cyberspace, building regional capacity, and international cooperation.

Although the content of the Cybersecurity Cooperation Strategy is focused on ICT security, not operational technology security, the strategies described are common and necessary for both.

2.2. Singapore

Singapore’s Cyber Security Agency (CSA) oversees domestic cybersecurity and leads the development of policies and guidelines for ICT and operational technology. The CSA is overseeing domestic cybersecurity and leading the development of policies and guidelines for ICT and operational technology security. However, discussions for operational technology security measures are still ongoing, and the country is still in the phase of continuing efforts to raise the level of corporate measures. While working to strengthen its own countermeasures, Singapore will also work to strengthen cooperation with the EU, the US, and other countries, and to provide information to other Asian countries.

Singapore adopted some items of the IEC 62443 series as Singapore Standard in 2018 (Singapore Standard, 2023). Of the published items of IEC 62443, not all have been adopted, but those related to specific requirements (SS IEC 62443-2-1:2018; SS IEC 62443-2-4: 2018; SS IEC 62443-3-3: 2018; SS IEC 62443-4-1: 2018) have been adopted. There is no difference in content between the home standard and the IEC standard.

CSA has also developed the Operational Technology Cybersecurity Competency Framework as a framework that maps the cybersecurity skill sets that operational technology experts should have (CSA, 2021a).

For critical infrastructure, the Cybersecurity Code of Practice for Critical Information Infrastructure (CSA, 2023a) defines what operators must comply with. However, the description is focused on ICT more than operational technology, and there is a possibility that the Code will be updated in the future in order to specify operational technology measures for critical infrastructure providers.

The National ICT Evaluation Scheme (NITES) and the Cybersecurity Labelling Scheme (CLS) exist as product certifications, but since they are for ICT and IoT, the Operational Technology Cybersecurity Expert Panel (OTCEP) is currently discussing how to update the content and develop new certifications. OTCEP, established in May 2021, is an organisation of internationally renowned experts and others from the government, critical information infrastructure (CII) sector, academia, and other operational technology industry cybersecurity practitioners, operators, researchers, and policy makers in Singapore (CSA, 2021b).

NITES is a certification scheme for ICT products launched in November 2009 by CSA. Certified products will be added to the Government Evaluated Security Product List; products that handle government data are not added, so obtaining this certification is practically mandatory (ENTRUST, 2023). CLS is also a certification launched by CSA. It is a certification for IoT devices, and certification marks are assigned according to ranks based on the evaluation of the security level of IoT devices. CLS is compatible with Finnish and German product certifications.

The Data Protection Trustmark (DPTM) is an enterprise certification provided by Infocomm Media Development Authority, a public organisation of Singapore. It is a voluntary enterprise-wide certification to demonstrate accountable personal data protection practices. Companies can get the certification by asking for an independent assessment. DPTM-certified organisations that apply for cyber insurance can enjoy faster application processing and competitive offers.

In addition to the global individual certification, CSA also offers the operational technology Train-The-Trainer (TTT) programme, which launched in November 2021 to address the shortage of operational technology trainers (CSA, 2021c). This programme aims to build up a pool of local trainers; in order to provide realistic hands-on exercises, operational technology TTT was conducted at Singapore University of Technology and Design's renowned iTrust research centre water security test bed. It includes 4-day, hands-on sessions and provides trainees with a deeper understanding of the various tools, while acquiring control system cybersecurity skills. CSA also offers long-term training courses in general security, such as the Cybersecurity Development Programme and the Cyber Security Associates and Technologists Programme (CSA, 2023b). The 15-month Cybersecurity Development Programme equips recent graduates and mid-career professionals with cybersecurity skills and knowledge. The programme's aim is to effectively build the cybersecurity capabilities in the public sector and keep Singapore's cyberspace safe and secure. Trainees will have opportunities to undergo on-the-job training programmes and participate in local and overseas attachments identified by the CSA training partners.

[Column: Singapore's Cooperation with Other Countries]

Singapore is beginning to become a hub for providing information to other countries for the benefit of the Association of Southeast Asian Nations. In particular, Malaysia, Thailand, and Indonesia are benchmarking Singapore's standards and certifications in order to develop their own standards, and the Cybersecurity Agency (CSA) is providing support for this. The development of standards and certifications with a certain degree of compatibility amongst multiple countries is beneficial to Singapore because it leads to lower costs for domestic and foreign companies and expands the possibility of developing new markets. This is why Singapore is considered proactive in such efforts.

Singapore has also established cooperative relationships with non-Asian countries (United States, United Kingdom (UK), Australia, and Israel) for each element of cybersecurity. Rather than building relationships only with specific countries, Singapore is aiming to exchange knowledge with countries that are open to advanced initiatives and discussions on each theme. For example, Singapore has been interested in supply chains in recent years, and shares common interests with the UK, so they are communicating on supply chains vis-à-vis cybersecurity.

In addition, to share knowledge on cybersecurity, CSA hosts the annual Singapore Cyber Week event to create a forum for policy discussions. Policymakers, industry leaders, and top academics from around the world come together to discuss emerging digital opportunities and cyber-threats, cyberspace and cybersecurity policy evolution, cyber-norm enforcement, Internet of Things, and operational technology security. It is an open forum for sharing and discussion to exchange best practices and strengthen international cooperation, making Singapore a cybersecurity hub.

Source: Authors.

2.3. Malaysia

Malaysia has adopted the international standard IEC 62443 as its standard for management methods related to operational technology security. Malaysia has been developing its own standards with the aim of providing guidelines on operational technology security to its own companies. Not all the published items in IEC 62443 were adopted, and only three items (ISA/IEC 62443-3-2, ISA/IEC 62443-4-1, and ISA/IEC 62443-4-2) were adopted in January 2023. Other items may be added in the future. In the national standardisation, the Department of Standards Malaysia organised a review committee to identify changes to customise the standard to Malaysia's needs; as a result of discussions, the standard was finally adopted without major changes. The changes are only trivial such as replacing commas with points or periods, 'this International Standard' to 'this Malaysian Standard' (ISA, 2022).

Malaysia is still at the stage where its own standardisation has been developed in 2023, and there are no Malaysian operational technology-related certifications or training programmes provided by the government. In addition, many Malaysian companies do not have a high level of operational technology measures, and efforts are expected to be made to raise the level in the future.

[Column: Strengthening Cooperation with Firms in Other Countries]

A partnership between the United Kingdom (UK) and Malaysian firms has been formed. Velum Labs Sdn Bhd (VLSB), a cyber-intelligence company in Sia, developed a partnership with TriCIS Ltd, a UK company in the same industry in March 2023. VLSB is a leading cyber-intelligence and cybersecurity company in Malaysia. TriCIS is a UK-based company specialising in the design and engineering of highly secure integrated solutions that meet the highest government and military security standards, with over 40 years of experience and a trusted supplier to the UK Ministry of Defence and the North Atlantic Treaty Organization.

VLSB's objective in this partnership is to acquire more advanced solutions. On the other hand, TriCIS's objective is to partner with an Asian company to access the rapidly growing Asian cybersecurity market.

Source: Authors; https://www.mida.gov.my/mida-news/malaysia-uk-firms-to-collaborate-to-create-cyber-security-regional-hub/.

2.4. Thailand

There are no unique laws, standards, certifications, or government-provided training specific to operational technology in Thailand. However, it is said that Thailand is beginning to consider its own standards specific to operational technology together with companies. Currently, Thai companies are left to develop their own standards and certifications.

Large global companies also need to monitor and analyse data for key performance indicator management, and operational technology is becoming increasingly digitalised. For example, in companies with multiple locations, although control is closed to each location, integrated monitoring systems have been realised, and data collected by operational technology systems are being used for business purposes. Many large companies that need such operational technology measures are studying their own standards and measures based on IEC 62443. Some companies can continuously improve the level of operational technology measures by having their efforts assessed by external auditors. On the other hand, many local small and medium-sized enterprises have not progressed with digitalisation, or have not been able to afford taking measures even if they do need operational technology security.

2.5. Indonesia

Indonesia does not have its own operational technology-specific laws, standards, certifications, or training, and it is necessary to develop them in order to raise the level of measures taken by Indonesian companies in the future.

Many local companies neglect investment in operational technology security due to the lack of sufficient regulations in Indonesia. However, in the animal feed manufacturing industry, where there are memories of cyberattacks in the past, the importance of operational technology measures is well understood, and both global and local companies seem to be relatively advanced in taking measures.

Indonesia has its own regulation, ITE11/2008, which is not related to operational technology. This regulation covers all electronic device transactions, but its definitions and contents were found to be insufficient as a security measure in 2010 (Lubis and Maulana, 2010). In addition, although initially intended to address the rapid development of information technology and to fill legal gaps on issues such as electronic transactions and the position of digital information and signatures in Indonesian law when it was first published in 2008, Articles 27, 28, and 29 of the law include provisions on ‘immorality,’ ‘defamation,’ and problems that have been used to control speech since the insertion of a problematic article criminalising ‘hate speech’ (University of Melbourne, 2021).

2.6. Viet Nam

Viet Nam does not have its own operational technology-specific laws, standards, certifications, or training provided by the government. Therefore, companies are left to implement measures on their own initiative. In order to raise the level of measures taken by Vietnamese companies in the future, it is necessary for Viet Nam to develop its own standards and certifications.

Viet Nam has many global companies that can implement voluntary measures by utilizing global standards. On the other hand, there are many local companies whose operations have not been digitalised to begin with and do not require operational technology measures. Among local enterprises, some of those with advanced digitalisation still lack sufficient ICT security measures, and many of them do not have systematic operational technology countermeasures in place.

2.7. Philippines

The Philippines does not have its own operational technology-specific laws, standards, certifications, or training provided by the government. Therefore, the Philippines is in a state where companies are left to take their own initiatives, and it is necessary to develop their own standards and certifications.

As confirmed from the interview (Appendix 1.4), a global enterprise with high security awareness is developing its own measures referring the global standard. However, many local companies are considered to have inadequate countermeasures.

3. Initiatives Outside of ASEAN

To gain insight into the desired future state, we also looked at the practices of countries known for their advanced operational technology security initiatives, such as the US, EU, and Japan. The US and the EU are leading the world in the development of governance not only for operational technology security, but also for overall security and personal data protection, amongst other things. In addition to that, the EU is ahead of ASEAN in terms of regional cooperative initiatives. Therefore, we believe that there is significant value in reviewing the efforts of both the US and the EU in operational technology security.

3.1. US

The US is ahead of ASEAN in terms of developing its own standards/guidelines with reference to global norms.

In the US, the National Institute of Standards and Technology (NIST) is taking the lead in creating security standards. NIST was founded in 1901 and is now part of the US Department of Commerce. The mission of NIST is to promote innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

NIST SP800-82 is a standard for operational technology security similar to IEC 62443. NIST SP800-82 is a guide for ensuring operational technology security (NIST, 2022a). In this document, operational technology is used to include building automation, transportation systems, physical access control systems, etc., in addition to ICSs. In addition, as a guide to ensuring operational technology security, the document explains the characteristics of operational technology compared to ICT systems and provides specific instructions on how to evaluate operational technology security, build a security architecture, ensure network security, and manage risks. In addition, it also describes network architecture patterns using systems such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers, which are well-known methods of operational technology digitalisation.

This document indicates that the following four points should be implemented as efforts to strengthen operational technology security.

Development of a cybersecurity programme for operational technology

Develop and document a comprehensive programme to implement operational technology security and establish a cross-functional team to cover the entire operational technology region, and a guiding charter to persuade management of the benefits of enhanced security and the potential damage that could result if it is not implemented.

Risk management in operational technology systems

Risk is managed on an ongoing basis through a risk management process consisting of four elements: conception, evaluation, response, and monitoring. In operational technology, safety and availability (ensuring business continuity) are particularly important matters. In addition, risks related to the supply chain are also important to maintain the availability of critical operational technology systems and components.

Building an operational technology cybersecurity architecture

It is vital to build an architecture that takes into account key points such as the separation of ICT and operational technology networks. Many organisations are embracing a multi-layered architecture, such as physical/network/hardware/software. It also allows secure coding when developing components in-house.

Application of security measures

In accordance with the NIST Cybersecurity Framework, the project will implement measures to strengthen identification, protection, detection, response, and recovery. Operational technology-specific recommendations are also identified, such as operations for physical security and lack of password recovery for operational technology systems.

NIST has also issued standards for supply chain management, SP 800-161 (NIST, 2022b) and SP 800-171 (NIST, 2020). SP 800-171 defines the security standards that must be met by private companies in the federal supply chain and provides a guide to meeting those standards. SP 800-171 is also a procurement standard for the US Department of Defense.

Another useful guideline is the ICS Matrix by MITRE ATT&CK, which was released in 2020 (MITRE, 2023). This reference document, which is issued by MITRE, a non-profit organisation funded by the US federal government, organises what specific measures exist for each operational technology risk.

The Cybersecurity & Infrastructure Security Agency offers a variety of ICS training (CISA, 2023). It offers content that can be viewed anytime on the web, and offers courses such as ‘Cybersecurity for Industrial Control Systems’ and ‘ICS Evaluation’ with credentials for completion. The US Department of Energy’s Office of Cybersecurity, Energy Security, and Emergency Response (CESER) hosted the 11th annual GridSecCon 2022. CESER offered a 4-hour practitioner training course for energy system owners and operators, Cybersecurity for the Operational Technology Environment (CyOTE™), at the 11th GridSecCon 2022 Conference (CESER, 2022). It also supports energy providers by making related materials available on its website (CESER, 2023).

3.2. EU

The EU is ahead of ASEAN in terms of developing regional operational technology security law and initiatives.

In the EU, the European Cybersecurity Act was enacted in June 2019 to strengthen the authority of the European Network Information Security Agency (ENISA) and develop a new cybersecurity certification system (ENISA, 2019). Subsequently, in December 2020, the NIS2 Directive was developed with the aim of resolving differences in cybersecurity requirements and implementation of measures in the member states to further improve resilience and incident response capabilities in both the public and private sectors and the EU (European Council, 2022).

In addition, the Cybersecurity Resilience Act is currently under consideration (Cyber Risk GmbH, 2022). Its development was announced in the General State of the Union Address in September 2021, and the European Cyber Resilience Bill was announced in September 2022. By establishing requirements in procurement, development, and manufacturing, the Act aims to strengthen cybersecurity for a variety of products with digital elements, both hardware and software, sold in Europe.

Efforts also exist in individual European countries. For example, Germany has established KRITIS, the new version of which became operational in 2021, as a regulation for critical infrastructure (Federal Office for Information Security, 2023; TUV Austria, 2022). The government obligates critical infrastructure operators to conduct an annual review of whether their facilities are KRITIS-relevant. In addition, VDI/VDE 2182, published in 2020, exists as a national standard for recommendations in line with IEC 62443 (VDI, 2023).

3.3. Japan

Japan is ahead of ASEAN in terms of certification and training.

In Japan, the local adoption of global standards has not yet progressed. Japan’s own standards do not exist either. For companies, there are ‘Guidelines for Cyber Physical Security Measures in Factory Systems’ and ‘Guidelines for Cyber Physical Security Measures in Building Systems’. ‘Guidelines for Cyber Physical Security Measures in Factory Systems’ was published in 2022 by Japan's Ministry of Economy, Trade and Industry for operational technology security measures in the manufacturing industry. The first edition of the ‘Guidelines for Cyber Physical Security Measures in Building Systems’ was published in 2019 also by Japan's Ministry of Economy, Trade and Industry. The second edition was published in 2023 against a backdrop of more sophisticated building systems.

The Defense Industry Cyber Security Standard was developed by the Defense Acquisition Agency, which is responsible for the management and procurement of defence equipment, as a procurement standard for the interrelated supply chain; the content of this standard is based on NIST-800-171 (防衛装備庁, 2022). This will be effective from April 2023.

As for enterprise certification, the Cyber Security Management System (CSMS) certification has existed since 2014 (ISMS Accreditation Center, 2023). Japan Information Processing Development Corporation has established the CSMS Certification Standard based on IEC 62443-2-1 in 2014; certification can be obtained by undergoing evaluation based on this standard.

In terms of training, Industrial Cyber Security Center of Excellence (ICSCoE) has conducted the 'Indo-Pacific Exercise on Cyber Security of Industrial Control Systems' in October 2022 (IPA, 2022), which is a training for foreign companies. For Japanese companies, ICSCoE provides the 'Core Human Resource Development Program', 'Cyber Resilience Enhancement eXercise by Industry (CyberREX)', 'Cyber Crisis RESponse Tabletop Exercise (CyberCREST)', and 'Cybersecurity Exercise for Control Systems (CyberSTIX)' for practitioners (IPA, 2023). The Core Human Resource Development Programme is a 1-year comprehensive training (from July to June of the following year) themed on strengthening cybersecurity measures for social and industrial infrastructures, through which trainees will learn operational technology and ICT, management skills, and business fields. CyberREX is for managers, and it aims to enhance readiness and resilience on cybersecurity within divisions and departments and to strengthen the entire business organisation with an awareness of industry characteristics. CyberCREST is for those responsible for overseeing cybersecurity measures, e.g. a Chief Information Security Officer, and the participants will learn the skills and methods necessary to protect their organisation. CyberSTIX is for practitioners and participants who will utilise our simulated process control networks and experience the cyberattacks used to unlawfully control devices to learn the security of industrial control systems.

4. Conclusion

Among the ASEAN countries that have their own national standards of operational technology security, Singapore has the most mature operational technology security measures, with the development of its own national standard based on IEC 62443, along with product certification and its use in procurement conditions.

Malaysia, on the other hand, has already developed its own standards based on IEC 62443, but has yet to make full use of them, relying instead on voluntary efforts by companies. Indonesia has standards for cyberspace, but none that are specific to operational technology.

On the other hand, outside of the ASEAN countries, the US is ahead of ASEAN in terms of developing its own standards/guidelines with reference to global versions. In addition, the EU is ahead of ASEAN in terms of developing regional operational technology security law and bottoming up operational technology security initiatives within the region. Also, Japan is ahead of ASEAN in terms of certification and training; this information will provide useful input for the Japanese government to consider what kind of operational technology security measures to implement for ASEAN countries in the future.

<u>Standard / Guideline</u>

- Global
  - ➢ IEC 62443
- Singapore

    - Adoption of IEC 62443 to Singapore Standard
    - Cybersecurity Code of Practice for Critical Information Infrastructure
- Malaysia
    - Adoption of IEC 62443 to Malaysia Standard
- US
    - NIST SP800-82
    - NIST SP800-161
    - NIST SP800-171
- EU
    - the European Cybersecurity Act
    - the NIS2 Directive
    - the Cybersecurity Resilience Act
- Germany
    - BSI-KritisV
    - VDI/VDE 2182
- Japan
    - Guidelines for Cyber Physical Security Measures in Factory Systems
    - Guidelines for Cyber Physical Security Measures in Building Systems
    - The Defense Industry Cyber Security Standard

Certification

- Singapore
    - The National ICT Evaluation Scheme
    - The Data Protection Trustmark
- Japan
    - CSMS Certification

Training

- Global
    - Training by private companies
- Singapore
    - operational technology Train-The-Trainer (TTT) programme
    - the Cybersecurity Development Programme (CSDP)
    - the Cyber Security Associates and Technologists (CSAT) Programme
- US
    - ICS Training by CISA
    - Cybersecurity for the Operational Technology Environment (CyOTE™) by CESER
- Japan
    - Indo-Pacific Exercise on Cyber Security of Industrial Control Systems
    - Core Human Resource Development Programme
    - Cyber Resilience Enhancement eXercise by Industry (CyberREX)
    - Cyber Crisis RESponse Tabletop Exercise (CyberCREST)
    - Cybersecurity Exercise for Control Systems for practitioners (CyberSTIX)

References

ASEAN (2023), ‘Key Documents’, https://asean.org/key-documents/ (accessed 15 November 2023).

ATC (2023), ‘Singapore International Cyber Week (SICW) 2022’, https://dig.watch/event/singapore-international-cyber-week-2022 (accessed 15 November 2023).

Acquisition, Technology & Logistics Agency (ATLA) 防衛装備庁(2022), ‘防衛産業サイバーセキュリティ基準の整備について’ [Establishment of Defence Industry Cybersecurity Standards], https://www.mod.go.jp/atla/cybersecurity.html (accessed 15 November 2023).

CESER (2022),‘CESER Debuts Operational Technology (OT) Cyber Training at GridSecCon 2022’ https://www.energy.gov/ceser/articles/ceser-debuts-operational-technology-ot-cyber-training-gridseccon-2022 (accessed 15 November 2023).

CESER (2023), ‘CyOTE’, https://cyote.inl.gov/ (accessed 15 November 2023).

CISA (2023), ‘ICS Training Available Through CISA’, https://www.cisa.gov/ics-training-available-through-cisa (accessed 15 November 2023).

CSA (2021a), ‘Operational Technology Cybersecurity Competency Framework (OTCCF)’, https://www.csa.gov.sg/Tips-Resource/publications/2021/operational-technology-cybersecurity-competency-framework-(otccf) (accessed 15 November 2023).

CSA (2021b), ‘Operational Technology Cybersecurity Expert Panel’, https://www.csa.gov.sg/Explore/who-we-are/committees-and-panels/operational-technology-cybersecurity-expert-panel (accessed 15 November 2023).

CSA (2021c), ‘Singapore Launches Operational Technology Train-The-Trainer Programme’, https://www.cisa.gov/sites/default/files/ICSJWG-Archive/QNL_JUN_2022/Singapore%20Launches%20OT%20Train-The-Trainer%20Programme_s508c.pdf

CSA (2023a),‘Codes of Practice / Standards of Performance’, https://www.csa.gov.sg/legislation/Codes-of-Practice (accessed 15 November 2023).

CSA (2023b), ‘Training & Education Programs’, https://www.csagroup.org/standards/services/training-education-programs/ (accessed 15 November 2023).

Cyber Risk GmbH (2022), ‘The European Cyber Resilience Act (CRA)’, https://www.european-cyber-resilience-act.com/(accessed 15 November 2023).

ENISA (2019), ‘The EU Cybersecurity Act: a new Era dawns on ENISA’ https://www.enisa.europa.eu/news/enisa-news/the-eu-cybersecurity-act-a-new-era-dawns-on-enisa (accessed 15 November 2023).

ENTRUST (2023),’ National ICT Evaluation Scheme (NITES) Certification’, https://www.entrust.com/digital-security/hsm/solutions/compliance/certifications/nites (accessed 15 November 2023).

European Council (2022), ‘Strengthening EU-wide Cybersecurity and Resilience – Provisional Agreement by the Council and the European Parliament’, https://www.consilium.europa.eu/en/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen/(accessed 15 November 2023).

Federal Office for Information Security (2023), ‘What Are Critical Infrastructures?’, https://www.bsi.bund.de/EN/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html (accessed 15 November 2023).

GIAC (2023a), 'Global Industrial Cyber Security Professional Certification (GICSP)', https://www.giac.org/certifications/global-industrial-cyber-security-professional-gicsp/(accessed 15 November 2023).

GIAC (2023b), 'GIAC Response and Industrial Defense (GRID)', https://www.giac.org/certifications/response-industrial-defense-grid/(accessed 15 November 2023).

IPA (2022), '2022 年度「インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィーク」を実施' [US-EU Industrial Control Systems Cybersecurity Week for the Info-Pacific Region 2022] https://www.ipa.go.jp/jinzai/ics/global/ics20221031.html (accessed 15 November 2023).

IPA (2023), 'Nurturing Talents and Professionals for the Digital Age', https://www.ipa.go.jp/en/it-talents/ics/humandev.html (accessed 15 November 2023).

ISA (2023), 'ISA/IEC 62443 Cybersecurity Certificate Program', https://www.isa.org/certification/certificate-programs/isa-iec-62443-cybersecurity-certificate-program (accessed 15 November 2023).

ISA (2022),' The Adoption of ISA/IEC 62443 as a Malaysian Standard', https://gca.isa.org/blog/the-adoption-of-isa/iec-62443-as-a-malaysian-standard (accessed 15 November 2023).

ISASecure (2019), 'Component Security Assurance Certification', https://isasecure.org/certification/iec-62443-csa-certification (accessed 15 November 2023).

ISA Secure (2023), 'System Security Assurance (SSA) Certification', https://isasecure.org/certification/iec-62443-ssa-certification (accessed 15 November 2023).

ISMS Accreditation Center (2023), 'CSMS 適合性評価制度の概要' [CSMS (Control System Security Management System) Overview of the Conformity Assessment System], https://isms.jp/csms/about.html (accessed 15 November 2023).

Lubis, M. and F.A. Maulana (2010) 'Information and Electronic Transaction Law Effectiveness (UU-ITE) in Indonesia,' Proceeding of the 3rd International Conference on Information and Communication Technology for the Moslem World (ICT4M) 2010, Jakarta, Indonesia, 2010, pp.C-13–C-19.

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).

MIDA (2023),' Malaysia, UK Firms to Collaborate to Create Cyber-Security Regional Hub' , https://www.mida.gov.my/mida-news/malaysia-uk-firms-to-collaborate-to-create-cyber-security-regional-hub/(accessed 15 November 2023).

MITRE (2023), 'ICS Matrix', https://attack.mitre.org/matrices/ics/ (accessed 15 November 2023).

NIST (2020), 'SP 800-171 Rev. 2', https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final(accessed 15 November 2023).

NIST (2022a), 'SP 800-82 Rev. 3', https://csrc.nist.gov/publications/detail/sp/800-82/rev-3/draft(accessed 15 November 2023).

NIST (2022b), 'SP 800-161 Rev. 1', https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final(accessed 15 November 2023).

SANS (2023), 'Cybersecurity Courses & Certifications', https://www.sans.org/cyber-security-courses/ (accessed 15 November 2023)

Singapore Standard (2023), ‘Singapore Standards’, https://www.singaporestandardseshop.sg/ (accessed 15 November 2023).

TÜV AUSTRIA GROUP (2022), ‘ICT-SiG 2.0 and new BSI-KritisV – 2022 is all about Critical Infrastructure Security’, https://it-tuv.com/en/it-sig-2-0-and-new-bsi-kritisv-2022-is-all-about-critical-infrastructure-security/ (accessed 15 November 2023).

TREND MICRO (2023), ‘セキュリティトレーニング’, [Security Training: Provision of Technology and Knowledge by Experts] https://www.trendmicro.com/ja_jp/business/products/support-services/education.html (accessed 15 November 2023).

University of Melbourne (2021), ‘Attempts to Revise Draconian ITE Law Stumble’, https://indonesiaatmelbourne.unimelb.edu.au/attempts-to-revise-draconian-ite-law-stumble/ (accessed 15 November 2023).

VDI (2023), ‘VDI/VDE 2182 Blatt 4’, https://www.vdi.de/en/home/vdi-standards/details/vdivde-2182-blatt-4-it-security-for-industrial-automation-recommendations-for-the-implementation-of-security-properties-for-components-systems-and-equipment (accessed 15 November 2023).

Chapter 3

Policy Recommendations for ASEAN–Japan Cooperation on Operational Technology Security

Finally, with an understanding of the current initiatives by governments and companies in ASEAN, and the OT security initiatives in the US and EU where OT security measures are relatively advanced, we discussed the necessary efforts for ASEAN–Japan cooperation to enhance OT security in ASEAN. Please note that we have prioritised infrastructure industry and manufacturing industry as the highest focus for enhancing OT security, as explained in 1.4. The following recommendations are mainly formulated with these industries in mind. While there are several sectors within the manufacturing industry, such as heavy industry and light industry, and their priorities for OT security measures may vary, the overall approach to OT security remains unchanged, as explained in chapter 2. Therefore, we believe that these efforts can be applied to any manufacturing industry.

1. Summary

In making policy recommendations, we considered measures in the following steps, with implications drawn from Chapter 2.

Step 1: Current overview of operational technology security in ASEAN enterprises

Step 2: Issues in ASEAN enterprises and what they expect from ASEAN governments

Step 3: Current overview of operational technology security in ASEAN governments

Step 4: Issues in ASEAN governments and what they need for the region

As explained in Chapter 2, the current status of operational technology security measures in ASEAN is such that there are hardly any initiatives taken across the entire region, and only some countries and companies are independently promoting initiatives. On the other hand, ideally, coordinated efforts should be promoted throughout the region, and regulations should be introduced by each government based on a regional agreement, and corporate operational technology security measures should mature based on these regulations. In fact, in regions where operational technology security measures are being promoted, such a picture is being realised. The EU is developing common legal and certification systems throughout the region, and each government is introducing regulations based on a common mechanism. The US government is adopting compliance with its own standards, which have expanded international standards, as procurement requirements, and is raising the operational technology security measures of domestic companies.

Due to the expansion of global supply chains, the importance of coordination throughout the region has been increasing, and if countries and companies pursue their individual optimal efforts, they may lose global business opportunities. It is beneficial to deepen support in the following two directions. The first is to foster and horizontally develop operational technology security measures using a third-party perspective, such as hosting meetings where government, industry groups, and major companies gather to share best practices, or conducting cybersecurity exercises for major companies.

The second is to support the development of a common ASEAN framework based on global standards, the establishment of a common ASEAN company and product certification system, and the standardisation of procurement requirements, which is support for the development of common ASEAN systems.

In the following sections, we will explain in detail about the challenges and policy proposals.

2. Current Overview of Operational Technology Security in ASEAN Enterprises

Currently, there are four types of maturity levels for operational technology security in ASEAN companies.

(i) Companies less involved in global supply chains (GSCs) that have no operational technology security measures at all (mainly local small and medium-sized enterprises)

(ii) Companies involved in GSCs that have no operational technology security measures at all (mainly local small and medium-sized enterprises)

(iii) Companies involved in GSCs that have only ad hoc and passive operational technology security measures (mainly local large enterprises)

(iv) Companies involved in GSCs that have organized and integrated measures (mainly global companies and some local large enterprises)

The group of companies in (i) has not progressed in automation, is not aware of the need for operational technology security in the first place, and has no capability for strengthening operational technology security.

The group of companies in (ii) has not progressed in automation but recognises the need for operational technology security due to their relationship with companies in the supply chain. However, they have no capability for strengthening operational technology security, and have not taken any measures.

The group of companies in (iii) has advanced in automation across networks in one or multiple locations and recognises the need for operational technology security. However, the capability for strengthening operational technology security is insufficient, and measures remain ad hoc.

The group of companies in (iv) has advanced in automation across networks in one or multiple locations and recognises the need for operational technology security. On top of that, they have high capability for strengthening operational technology security and are currently able to take high-level operational technology security measures on their own.

3. Issues in ASEAN Enterprises and What They Expect from ASEAN Governments

The challenges faced and the required measures for governments vary according to the current maturity levels outlined in 3.2.

The problem faced by the group of companies in (i) is their failure to recognise the need for advancing operational technology security measures amidst a lack of digitalisation. Ideally, they should strive for a state of preparedness by proactively increasing the security level, rather than waiting until digitalisation progresses and security risks become apparent. Therefore, ASEAN governments are required to carry out educational activities to emphasise the necessity of operational technology security measures. Specifically, it is necessary to raise awareness about industry trends such as operational technology-related incidents, rising geopolitical risks, and the benefits of strengthening operational technology security.

The problem faced by the groups of companies in (ii) and (iii) is insufficient knowledge and resources to tackle operational technology security measures. Ideally, they should aim for a state where their own operational technology security measures have sufficiently advanced without compromising their own interests. Therefore, ASEAN governments are required to provide specific knowledge and resources to advance operational technology security measures. This includes establishing national standards/guidelines for reference when formulating security policies and roadmaps, and defining skills and developing training for operational technology security personnel to enhance their capabilities.

The problem faced by the group of companies in (iv) is a lack of motivation to continuously update their operational technology security measures and a limited ability to disseminate these measures to suppliers. Ideally, they should aim for a state where their own operational technology security measures are constantly updated, and they are able to promote security measures amongst their suppliers. Therefore, ASEAN governments are required to provide incentives for updating operational technology security and to develop policy tools to involve suppliers. Specifically, for motivation, it is necessary to establish a corporate/product certification system for operational technology security that can be used to build external trust. Additionally, policy tools such as procurement requirements (including government subsidies) should be implemented to ensure compulsory assurances.

4. Current Overview of Operational Technology Security in ASEAN Governments

As detailed in section 3.3, each government is expected to provide enlightenment activities that explain the necessity of operational technology security measures, provide specific knowledge and resources, and provide update incentives and policy tools to involve suppliers. However, the current situation of the ASEAN governments is that while the Singapore government is responding to a certain extent, other countries are not catching up; in Singapore, CSA is disseminating the government's approach to security both domestically and internationally through an event called Singapore International Cyber Week, but in other countries, there is no national initiative.

As for providing specific knowledge and resources, Singapore is implementing part of global standards as national standards and providing training for the development of related personnel. Malaysia has just standardised part of the global standards in 2023, but in other countries, no national initiatives are seen.

In terms of providing incentives to update operational technology security and policy tools to involve suppliers, in Singapore, there are the ICT/IoT product certification systems such as CLS and NITES, and considerations are underway for updating and new certification with operational technology measures in mind. Also, Singapore mandates NITES evaluations for products handling data from government agencies. On the other hand, in other countries, initiatives such as certification and procurement requirements are not seen.

5. Issues in ASEAN Governments and What They Need

As outlined in Section 3.4, the ASEAN governments are currently not fully addressing the requirements expected of them, and there is a need to support regional efforts.

Regarding enlightenment activities, there is a lack of a unified approach amongst ASEAN countries, and while Singapore wishes to lead these activities, it cannot do so justifiably as it is only one member country. However, each government should aim to promote enlightenment activities quickly and broadly to their domestic enterprises.

In terms of providing specific knowledge and resources, there is a risk that disparate systems that deviate from global standards due to each government's limitations might proliferate in each country. However, each government should aim to provide knowledge and resources to their domestic enterprises involved in the global supply chain to ensure their continued participation in it.

Regarding providing incentives, the hurdle for regional collaboration is high. However, each government should aim to implement wide-ranging security regulations based on regional agreements, and to mature and scale them.

To bridge the gap between these challenges and the intended objectives, support is sought in two directions. The first is support for momentum building and lateral development of operational technology security measures, leveraging a third-party position. Specifically, translation and dissemination of global standards into the languages of each ASEAN country, hosting events for governments, industry associations, and major corporations to share best practices, and implementation of cybersecurity exercises for major corporations are all required on a regional basis. The second is support for the establishment of common systems amongst ASEAN countries. Specifically, support is sought for establishing a common framework for ASEAN countries based on global standards, such as the standard based on IEC 62443 and the development of skill definitions and training for operational technology security personnel. In addition, support for inter-country collaboration for further strengthening is also sought. Specifically, the establishment of a common company/product certification system within ASEAN and the adoption of procurement requirements compliant with operational technology security are required.

6. Recommended Policies for ASEAN–Japan Cooperation on Operational Technology Security

As explained in section 3.5, ASEAN governments face challenges and, as such, are seeking support from Japan for the promotion and widespread adoption of operational technology security measures from a neutral third-party perspective and assistance in the establishment of common regulations amongst ASEAN countries. The following provides detailed policy proposals. Going forward, it is expected that Japan will cooperate with ASEAN governments to contribute to the overall strengthening of operational technology security across ASEAN countries.

__Translation and dissemination of global standards in each ASEAN language__

Dissemination of global standards in a form that is easy for each country's government, industry groups, and major companies to refer to.

- Translation of IEC 62443 into each country's language

- Dissemination of information through websites, text messages, and various events, etc.

Organising events where all the governments, industry groups, and major companies from each country meet and share best practices

Aiming to build momentum, share knowledge, and strengthen relationships by sharing knowledge at events where each organisation comes together.

- Host annual events where governments, industry groups, and major companies from each country gather to share best practices in digitalisation through operational technology and efforts to strengthen operational technology security in ASEAN countries from Japan's perspective.
- Hosting sessions where each government, industry group, and major company shares their initiatives on operational technology security as a main theme for 30 minutes each.

Implementing cybersecurity drills for major companies

Conduct exercises for major companies aimed at acquiring correct knowledge for security enhancement, building momentum, and spreading knowledge.

- To acquire correct knowledge, provide information on global standards (conduct lectures to learn about governance establishment methods defined in IEC 62443 and key points for strengthening security during integrated management as explained in SP 800-82).
- To build momentum, share enlightenment activities and the status of initiatives in ASEAN countries (explain industry trends such as increasing incident/geopolitical risks and benefits from strengthening operational technology security. Also, share the status of initiatives such as domestic standards, certified qualifications, training, etc. in ASEAN countries).
- Conduct case studies and hands-on exercises utilising the advantages of drills, as well as exchanging opinions between companies.

Establishment of standards based on IEC 62443

Establish and expand standards compliant with IEC 62443, starting with the bare minimum requirements.

- Start by showing the steps of countermeasures for companies based on the defined requirements.
- It is assumed that effective enlightenment and guideline creation, conscious of gradually raising the Security Level (technical level) and Maturity Level (company maturity level) defined in IEC 62443, will be effective.
- For example, regarding system security requirements, start with achieving SL1 as the minimum line, and then gradually advance to achieve the necessary security level for each company.
- In addition, Singapore and Malaysia have experience in using IEC 62443 as their national standard, so it may be possible to proceed smoothly if implemented in cooperation with these countries.

Skill definition and training for operational technology security personnel

Develop training in line with the phased establishment and expansion of standards to help resolve the shortage of personnel in companies.

- Define the skills of operational technology security personnel in conjunction with the common standard development and expansion in ASEAN countries to clarify the personnel required by companies to strengthen operational technology security.
- Referring to the initiatives of ICSCoE, create training menus that match the digital progress of companies and organise nurturing training to secure the necessary security personnel at each stage to assist in resolving the personnel shortage.

Establishment of a common company/product certification system in ASEAN

Establish a system to certify efforts toward the established standards, taking into account each initiative.

- Refer to the operational system and certification framework established in Japan's CSMS certification to establish a system to certify efforts towards the established standards compliant with IEC 62443.
- One idea is to establish a certification system for product groups related to operational technology, referring to the efforts of Singapore's CLS.

Adoption of operational technology security compliance as procurement requirements

Adopt standards as common procurement requirements in ASEAN to strengthen supply chain security and facilitate collaboration.

- The US has strengthened supply chain security by adopting NISTSP800-171, and the Japan Defense Equipment Agency has adopted the Defense Industry Cybersecurity Standard as procurement standards.
- Strengthen supply chain security and facilitate collaboration between countries by adopting ASEAN common standards as operational technology security procurement requirements in each government.

Appendix

1. Interview Results

1.1. Interview with Malaysian oil and gas company

Date: 2023/4/26

Expert position: Controls & Instrumentation Specialist

Laws and Standards

- Malaysia has adopted IEC 62443, an international standard, as Malaysian standard.
- A company called PETRONAS has been lobbying for the adoption of IEC 62443 as the Malaysian standard.
- By adopting a standard that is compliant with international standards with some customisation, it sends the message that Malaysian companies should follow this standard.
  - ➢ Since there are global companies in Malaysia, it is important to be in line with international standards and aligning with IEC is optimal.

Certification

- Company Certification: No company certification but can evaluate their own company according to ISA/IEC 62443.
- Individual Certification: Four individual certifications for ISA/IEC 62443 exist (issued by ISA), and individual certification for ICT security is also utilised.

Status of operational technology security at Malaysia companies

- Compared to other ASEAN countries, Malaysia has made progress in implementing measures such as domestic standardisation of ISE 62443, but it is not sufficient.
- Most companies are still in the process of implementing security measures, and the operational technology security maturity level is low.
  - ➢ Even companies that seem to be relatively mature in terms of ICT security have yet to address operational technology security.
  - ➢ Many companies do not focus on risk.
  - ➢ Smaller, growing companies cannot afford to address cyber-risk and it is considered a low priority.
- One Malaysian oil and gas company is using IEC 62443 to address this issue:
  - ➢ Operational technology experts are trained by having them obtain individual certification in IEC 62443. Also, utilise ICT certifications to train ICT experts.
  - ➢ Since operational technology security and ICT security are inseparable, a security response team with experts in both has been established.
  - ➢ The security measures team is improving the security level by creating guidelines in a form that is tailored to each business.

Measures required by the government from a corporate perspective

- Promoting effective training
  - Would like to know how to make training in companies more effective.
  - Would be helpful if the country offers some training for companies and individuals.
- Building an ecosystem of security measures
  - Would like to see an optimal operational technology security ecosystem built using ISMS certification (ICT security certification) / Cyber Security Maturity Model Certification / IEC 62443 standards, and a clear roadmap for corporate initiatives.

1.2. Interview with an expert providing operational technology security support to infrastructure providers in Singapore and Indonesia

Date: 2023/4/28

Expert position: Cyber Security Engineer (ICT/operational technology cybersecurity)

Status of operational technology security at Singapore companies

- CSA oversees cybersecurity in the country and leads the development of policies and guidelines on ICT and operational technology.
  - Operational Technology Cybersecurity Competency Framework
  - Singapore’s Operational Technology Cybersecurity Masterplan
  - Cybersecurity Code of Practice For Critical Information Infrastructure - Guidelines for Critical Infrastructure
  - The National ICT Evaluation Scheme - provides a scheme to evaluate and certify ICT products and add them to the Government Evaluated Security Products List
  - CLS – certification for IoT devices
- CSA as well as Malaysia follows IEC 62443.
  - Singapore is following IEC and NIST trends and has adopted IEC 62443 as Singapore Standard.
- Training is also led by CSA, with the CSA Academy offering courses to train operational technology security specialists and promote their employment in companies.
  - Operational technology cybersecurity workforce development is one of the key thrusts in Singapore's operational technology Cybersecurity Master Plan announced for 2019.
  - Since 2017, CSA Academy offers customised training courses in cybersecurity, including operational technology, that are not readily available in the market.

Status of operational technology security at Indonesian companies

- ICT security is currently underdeveloped, and operational technology security measures have not yet been initiated.
  - operational technology security standards are not yet developed. Many companies have neither the time nor the budget to spend on security measures, and everything is being put on the back burner.
  - When this expert surveyed the situation of infrastructure providers in Indonesia a few years ago, he found that ‘machines using Windows 7 are the mainstream’, ‘old machines are being used deceptively’, ‘there is no understanding of the concept of security

measures, so USB sticks can be inserted into computers and important information can be copied' and 'attackers could pretend to be a related vendor and attack at any time'.

Measures required by the government from a corporate perspective

- Promote awareness of the standard /Raise the level of countermeasures.
  - ➢ Provide information to companies that are unaware of IEC 62443 and NIST is important.
  - ➢ Some large companies are taking measures with consultants, etc., but there are still many companies that do not even recognise IEC and NIST standards, so it is necessary to educate them to raise the level of their measures.
  - ➢ In Indonesia in particular, there are cases where ICT is somewhat well understood, but operational technology measures have not yet been taken, and there is a high possibility that the Indonesian infrastructure is weak.
- Enhance training programs to develop operational technology security specialists
  - ➢ Training course offerings in operational technology security like Singapore should be promoted in other ASEAN member countries.

1.3. Interview with Global Animal Feed Manufacturing Company in Indonesia

Date: 2023/5/9

Expert position: Senior Plant Manager

Laws and Standards

- Global companies also voluntarily refer to international standards.
- However, the main reference is ITE 11/2008, which is a standard within Indonesia.
  - ➢ It is for all electronic device transactions and is a law for both ICT and operational technology.
  - ➢ Although the content is insufficient compared to the global regulations, it is emphasised as it is the only standard for Indonesia.

Certification

- There are no such certifications for companies or products.
- For individuals, there are some training programs offered by vendors that are not official, but there are certifications for completion of training programs offered by the vendor.

Status of measures taken by global animal feed manufacturing companies

- There are about ~10 people in Indonesia as a security team, including a team from the Jakarta office + 1 person from each factory.
  - ➢ HQ is in the Netherlands. Asia Regional Office is in Viet Nam. Indonesia has a head office in Jakarta with four factories.
  - ➢ Daily operations are handled by the Jakarta office and below. When an issue arises, it is reported to the Asia Regional Office. For large issues, the rule is to report to the Netherlands.
- Rules exist based on the guidelines of the HQ in the Netherlands, localised for Indonesia.

    - Data transaction methods, access rights, control room entry management, listing and management of all assets, etc. are performed by cybersecurity staff belonging to the factory based on a routine book.

- Vendor-provided training programs are used for human resource development.

Status of operational technology security at Indonesian companies

- Many local companies are currently neglecting to invest in security because there are not enough regulations as Indonesia
- However, at least in the animal feed industry, the importance of operational technology measures is well understood and relatively well implemented, as CP was attacked in 2006 and had to suspend operations for 3 days, causing a huge loss.

Measures required by the government from a corporate perspective

- Would like the country to clarify the Indonesian standard. As there is no national standard, I am not sure if we are doing the right thing or if it is sufficient ITE11/2008 is not sufficient.
- Would like to see certification for companies realised. If it is possible to establish certification with multiple levels, such as Level 1 for small companies and Level 3 for large companies, it could serve as an indicator for companies. It would also be a good way to disclose the status of compliance to other companies.
- Certification for companies should be achieved. If a multi-level certification can be established, such as Level 1 for small companies and Level 3 for large companies, it could serve as an indicator for companies. It would also be a good way to disclose the status of compliance to other companies.
- Awareness should be raised not only amongst companies, but also amongst the police. Currently, even if a cyber-related incident occurs, the police do not understand the details, so their response is not very thorough.
- Knowledge sharing groups/opportunities should allow for best practices to be captured.

1.4. Interview with Japanese Automaker Subsidiary in the Philippines

Date: 2023/5/11

Expert Position: ICT Operations Manager

Laws and Standards

- There is no law/standard on operational technology security in the Philippines.
- Reference can be made to IEC 62443, etc., but the country needs to develop its own standard.

Certification

- There is no certification unique to the Philippines. There is an ISO standard for factories, but it does not cover plant security.
- As for training for individuals, training from tool providers can be used for tools
    - Examples: endpoint protection and detection courses offered by Trend Micro

Status of operational technology security at the Philippines companies

- The semiconductor industry appears to have a fairly high level of security

- In the automotive industry, Japanese companies and their suppliers are making progress, but other companies are not at a high level.
- Most of the other manufacturing companies are not well prepared for security issues.

Status of Measures Taken by Japanese Automakers' Subsidiaries in the Philippines

Organisation

- Has one assembly plant in the Philippines. Around 40 supplier factories in the Philippines.
- Members in charge of security consist of a global team + regional security teams + factory operators.
    - ➢ A global security team exists in the North American branch of the parent company to consolidate information on incidents, etc.
    - ➢ A security team of about 5 people also exists at the company. The team is responsible for applying common global standards to the company's own standards (proposing measures, collaborating with global teams, etc.).
    - ➢ The factory has about 10 ICT staff in charge of practical operations under the direction of the Philippine security team.

Policies

- Created a global common in-house standard based on IEC 62443 + list of security products and tools to be used.
- This car manufacturer is also focusing on the risk of production stoppages at suppliers and is trying to raise the level of plant security at suppliers and is using the standard.

How operational technology security measures started and developed

- Recognised the importance of plant security after an incident about two years ago in which a cyber-attack shut down production lines at several plants.
- Created a centralised security team + chain of command / Created own standards (rules) based on IEC 62443.
- Rolled out the standards to each region to strengthen ICT and operational technology security.
- In addition, provide suppliers with a simplified version of your standards to encourage compliance.
    - ➢ Although not mandatory, suppliers have raised the priority of operational technology compliance by adding a local agreement on procurement to consider not only the amount but also the compliance with the standard.
- Currently, compliance is at about 80% progress, and having difficulty updating equipment that has already been in use for a long time.

Measures required by the government from a corporate perspective

- Creating a standard + regulations for plants
    - ➢ The content can be as simple as showing what is in the elements of plant security, preferably in the form of localising IEC 62443.
    - ➢ It should also have some degree of enforceability as a set of regulations.

- Should teach the concept of plant security from the basics as a bottom-up exercise
  - ➢ Hands-on exercises are difficult because products differ from company to company. Classes to promote understanding of basic frameworks would be the first step.
- For high-level companies, new threat information provision and exercises are needed to update the rules

1.5. Interview with Malaysian Electricity Company

Date: 2023/5/12

Expert Position: Senior Maintenance Manager

Laws and Standards

- It is significant to make it a Malaysian standard because critical infrastructure must follow Malaysian standards. The content is almost identical to IEC 62443.

Status of Measures Taken by an Electricity company in Malaysia

Company Profile

- Owns several power plants. Products from multiple vendors are used in the power plant systems, including boilers from MHI.
- The digitalisation progress of the operational technology system configuration can be classified into three levels, and the company has achieved level 2.
  - ➢ Level 0 is a state where the situation can be quantified by sensors.
  - ➢ Level 1 is connected to a distributed control system, and the equipment can be controlled using a human interface. A distributed control system is built to enable real-time management of the power plant's operational technology system. Required software licenses were purchased and configuration was done by the ICT team.
  - ➢ Level 2 is a situation where the entire situation at multiple power plants can be monitored in real time; there is a monitoring room at the HQ to constantly monitor for any problems. However, the DCS is a local network and can only be monitored and not operated from HQ.

Organisation

- There is an operational technology system monitoring team at HQ. However, operational technology security is a part of the business since the entire ICT is their scope.
- A dedicated task force has been formed for assessment in the actual power plant and is in charge of operational technology security improvement. Assessments based on topology were conducted with the help of consultants.

Policy

- A task force under the CIO developed a policy called ISMS, which covers both ICT and operational technology and references IEC 62443 and ISO 27000.

Certification

- ISO 27001 certification was obtained depending on the content of the ISMS. ISMS is continuously updated for continued certification (currently v10).

- ICT and Physical are at a much higher level, but operational technology is struggling to raise the level of measures.
    - ➢ operational technology is proceeding with a budget, and awareness is not low, but it is difficult to deal with because equipment from multiple companies, including Toshiba and MHI, is used.
    - ➢ There is also the issue of not being able to install countermeasure software due to the memory size of the devices.

<u>Measures required by the government from a corporate perspective</u>

- Since CII is a common asset of the country, it may be necessary to support operational technology measures by subsidising their costs.
- In addition, public facilities such as power plants are selected by bidding, and operational technology measures should be included in the bidding requirements.
    - ➢ If operational technology measures are not included, the direction will be to build cheaply anyway, and operational technology measures will be neglected.
    - ➢ By including operational technology measures in the requirements, it is possible to receive orders at a reasonable price with operational technology measures in mind.

1.6. Interview with Experienced Refinery Operator in Viet Nam on operational technology Measures

Date: 2023/5/15

Expert Position: Head of ICT Department

<u>Laws and Standards</u>

- No Viet Nam-specific laws/standards exist.
- IEC 62443 and NIST 800 are available for reference. NIST is more recognised in Viet Nam.

<u>Certification</u>

Viet Nam’s own certification does not exist.

<u>Status of operational technology security at Viet Nam companies</u>

- Viet Nam has many global companies, and global companies are using global standards to implement voluntary measures, even if Viet Nam does not have its own standards.
    - ➢ Samsung is the largest global company for Viet Nam, but we have heard that they are taking operational technology measures based on their own standards.
- As for local companies, digitisation of operations has not progressed, and there are many companies that do not need to take operational technology measures.
- However, there are also local companies that need operational technology measures, but their ICT security measures are still middle of the road, and operational technology measures are insufficient.
    - ➢ There are no clear guidelines from the government and not enough experts, so it is difficult to know where to start.

Status of measures taken by a refinery company in Viet Nam

- The company operates a single refinery in Viet Nam, and most of the operations are completely machine-controlled, except for maintenance and other tasks.
  - ➢ Approximately 3,000 people work in the refinery, Since many processes cannot be automated, such as maintenance.
- There is no in-house security standard, but NIST 800 is used as a reference for assessment and implementation of measures.
  - ➢ There are no in house rules, which can be described as haphazard, but the perception is that minimum measures are in place.
  - ➢ Have heard of IEC62443, but since they refer to NIST standards for ICT measures, we also refer to NIST for operational technology.
- Dozens of in-house ICT teams, but only one person in charge of operational technology security, working with vendor providing DCS.
  - ➢ Manage assets, monitor traffic, update software, etc.
- No reporting line, but may get advice from sponsors Idemitsu and Mitsubishi Chemical.
- Challenges for operational technology include legacy and lack of human resources.
  - ➢ Only few, but legacy software remains and is vulnerable.
  - ➢ ICT, but especially operational technology, has a problem of lack of human resources and must rely on vendors a lot.

Measures required by the government from a corporate perspective

- Development of standards and guidelines to raise the level of operational technology measures in local Vietnamese companies.
  - ➢ No national standards exist, so companies do not know where to start.
- Increase the number of experts in the operational technology security field by providing training.

1.7. Interview with an expert in Thailand who has experience supporting operational technology security measures for multiple companies

Date: 2023/5/16

Expert Position: Senior Control System Engineer (operational technology / Network Security)

Laws and Standards

- Nothing unique to Thailand exists.
- Many companies refer to global standard IEC 62443.

Certification

- Thailand does not have its own certification.
- TUV and DNV issue corporate certification as a global common private certification.

Status of operational technology security at Thailand companies

- Large companies are digitising the operation and utilise data for business, so operational technology security is necessary.
    - ➢ Companies with multiple locations will realise an integrated monitoring system, although control is closed to each location.
    - ➢ In manufacturing, key performance indicator management is important, so data monitoring is quite important.
    - ➢ Also, the data collected by the operational technology system are used by the analysis team on the ICT side for business purposes.
    - ➢ However, we do not hear much about data integration with other companies.
- Many large companies are discussing and achieving their own standards and measures based on IEC 62443.
    - ➢ Many companies choose IEC but NIST is also helpful.
    - ➢ Large companies are at least aware of IEC 62443 and understand it as a best practice.
    - ➢ Internal or external auditors can scrutinise the status of efforts and continue to improve the level of operational technology measures.
- Many local companies have not made progress in digitalisation, or even if they have, they are not able to afford the cost of the measures.

Measures required by the government from a corporate perspective

- Raise awareness of the importance of operational technology security.
- Raise the level of countermeasures by creating a minimum national standard and guidelines.
    - ➢ IEC 62443 is a hurdle for small local companies.
    - ➢ The government side should start by providing a guideline for risk mitigation, which should be done at least from now on. The content should be at a level that is feasible in terms of budget.
- Domestic standard based on IEC 62443
    - ➢ Large companies have already taken measures, so there is not much benefit from domestic standardisation.
    - ➢ However, there is a certain significance in aligning with it.
- Industry standards are not necessary with respect to operational technology security.
    - ➢ The basic level of operational technology security measures is well defined and updated in IEC 62443.

1.8. Interview with an expert in US who has experience in managing operational technology security team in global beverage company

Date: 2023/5/18

Expert Position: operational technology Cyber Security Lead

Laws and Standards

- NIST 800-82 exists. IEC 62443, a global standard, can also be referenced.

- IEC 62443 and NIST 800 are not very different in content, but NIST is rather more risk management-oriented.

Certification

- ISO certification exists for ICT, but there is no company certification for operational technology, so only self-assessment is possible.
  - ➢ Companies use audits by third-party organisations (KPMG, PWC, Deloitte, etc.).
  - ➢ The results of audits and the company's countermeasure status are not made public externally (public disclosure is synonymous with disclosure of vulnerabilities).
- Individual certification and training are not country-driven, but private certifications and training are used.
  - ➢ Example: SANS, a trusted for-profit organisation, provides training on operational technology + issues certificates. In US, there are many options.
  - ➢ There may be state-sponsored exercises, but consumer goods companies are not very aware of them.

Status of operational technology security at US companies

- Critical facilities such as government agencies and power plants are required to comply with NIST 800.
  - ➢ No company certification exists to indicate whether they are complying with NIST
- Many other companies also use NIST 800 as a reference for their own operational technology security measures, even if it is not mandatory.
  - ➢ Even if not mandated by the government, there is a certain awareness of the importance of operational technology measures, so they are taking action.
- There is basically no data linkage between companies. Even if there is, it is outside the scope of discussion of operational technology measures because it is an area of data utilisation in ICT that is separated from the operational technology control area.
  - ➢ Data utilisation within companies is progressing in many companies.
- From a data protection perspective, it is important to clearly distinguish the operational technology control area from the ICT database with firewalls.
  - ➢ Data can be monitored and collected in real time; however, the control functions should be independent as operational technology systems.

Status of Measures Taken by a global beverage company in US

Organisation & Systems

- Created process procedures based on ICT when ICT risk was the only consideration (e.g. incident review, incident triage, etc.).
  - ➢ Chief Information Security Officer is responsible for security.
  - ➢ Security response teams exist in 3 locations worldwide (US, Australia, Poland).
- With the advent of operational technology risk, additional mechanisms are in place while leveraging the organisation and systems in place for ICT risk.
  - ➢ Operational technology’s own process procedures.
  - ➢ New staffing for operational technology (new acquisitions + training for ICT teams).

    - Regional operational technology Director position established as regional level.
    - Regionals will proceed based on blueprints given by Global.
- The biggest challenge for both Global and Regionals is to secure human resources.
    - Operational technology measures are a new area and require in-house training.
    - Training provided by the private sector will be utilised for training.
    - In fact, much of the cost of operational technology measures is spent on training to secure human resources.

Internal policies and their governance

- The top policy was originally created with ICT risk in mind.
- The above is not directly applicable to operational technology systems, so additional policies were created for operational technology.
    - Based on the ICT policy, the security governance team and risk management team, together with operational technology experts, created a policy.
    - Created five policies as not too specific at an achievable level.
- Distribute the above operational technology policies from Global to the business segment sectors in each region, along with an approximate achievement flow (blueprint).
    - Distribute some budget once initially, without providing ongoing costs.
    - The method of achievement after that can be left to the regions.
    - Shows the goal and how to climb the mountain to some extent, but not the detailed status of each region, so regions should be given the initiative.
- ~5 years to encourage achievement and continuous monitoring until it is achieved.
    - Unlike ICT, operational technology takes time to respond, so it is important to create a journey that spans several years to 10 years.
    - As a global team, create a risk control framework for achievement and conduct quarterly status checks based on the framework.
- Challenges in bringing ownership to regions
    - If not enforced top down, regions will not move because there is no operational technology measure benefit (in the short term).
    - Also need to educate people to understand the importance of operational technology measures.

Measures required by the government from a corporate perspective

- Cost is an issue for companies, although there are costs associated with NIST 800 and requests to outside organisations, etc.
- Measures can be taken without government support.

1.9. Interview with German Automaker Subsidiary in Thailand

Date: 2023/5/22

Expert Position: Cyber Security Analyst

Laws and Standards

- Currently does not exist, but discussions are underway between the government and private companies to develop their own standards.
  - ➢ Discussions are also involving global companies with subsidiaries in Thailand.

Status of operational technology security at German Automaker Subsidiaries in Thailand

- Global cybersecurity team exists in Germany to develop corporate policy and common rules within the company
  - ➢ The company refers to both IEC62443 and NIST Standard.
- ICT teams exist in each country to review specific measures and create a checklist of sorts.
- A German team visits Thailand twice a year to audit the status of countermeasures in Thailand.
- The company also review contracts with suppliers on a quarterly basis, and the rules for information management related to operational technology measures are also reviewed in the contracts.
  - ➢ This contractual arrangement is important because we sometimes procure parts with software from suppliers.