Chapter 2

Current Status of Operational Technology Security

December 2023

This chapter should be cited as

ERIA study team (2023), ‘Current Status of Operational Technology Security’, in Oikawa, K. and Y. Hatakeyama (eds.), *Operational Technology Security in ASEAN.* ERIA Research Project Report FY2023 No. 19, Jakarta: ERIA, pp.8-25.

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.

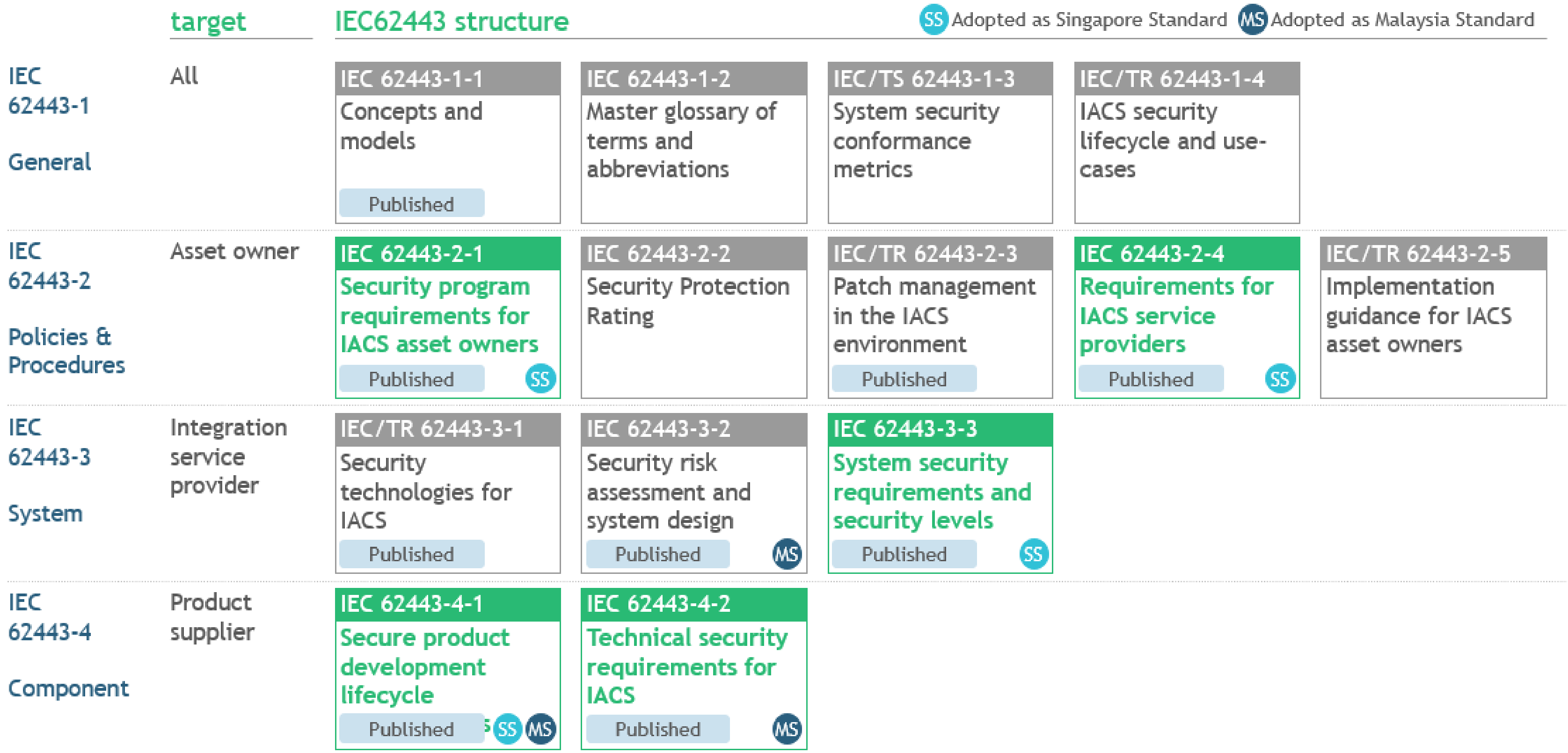
IEC 62443-4 defines requirements for product providers as the security of their products.

‘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.

Standard / Guideline

- 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).