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.

Measures required by the government from a corporate perspective

- 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

Laws and Standards

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

Certification

Viet Nam's own certification does not exist.

Status of operational technology security at Viet Nam companies

- 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.

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

- 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.