www.otisac.org

WHITEPAPER

BRIDGING THE GAPS IN OT CYBERSECURITY PROGRAMS

CONTRIBUTOR

Deloitte.

Across critical infrastructure sectors like water, energy and rail, Industrial Control System (ICS) environments are foundational to core activities like water treatment, electricity generation or the safe running of trains.

These environments have experienced a significant increase in cyber security incidents over the past few years, and several large malware and ransomware incidents have had massive operational, financial and reputational impact on the affected organisations. Legislation – such as the Cyber Security Agency of Singapore Cybersecurity Act, European Programme for Critical Infrastructure Protection (EPCIP), and the Australian Security of Critical Infrastructure Act (SOCI) as amended 2022 – has been introduced to ensure critical infrastructure is protected and the continuity of critical services is maintained.

As a result of the increased cybersecurity incidents impacting revenue, reputation, and to address requirements of applicable legislation, organisations in critical infrastructure sectors have begun investing in ICS cybersecurity maturity improvement programs.

The aim of many of these programs is to address the potential risks to safety and production from nation-state actors, malicious insiders, and malicious hackers exploiting vulnerabilities in critical infrastructure.

Unfortunately, the reality is that many ICS cybersecurity programs still fail to achieve their objectives.

Drawing from Deloitte's experience supporting different organisations in the ports, mining, transport, utilities and energy sectors across the Asia Pacific region, there are a variety of recurring root causes as to why these programs fail:

1. **Lack of clear ownership and governance.** Many ICS cyber uplift programs are initiated by a cybersecurity function, either independent or under IT. These programs aim to drive significant change and reduce risk within an environment where technology and processes are managed by engineers and technicians under their own C-level function. Without direct involvement of and alignment with ICS leadership from the outset, programs generally fail to gain traction. Similarly, without a clearly defined ownership of cyber risk to ICS and robust governance and operating models for ICS cybersecurity, operational changes driven by cyber uplift programs often fail to be adopted in the field.

2. **Deploying 'OT cyber solutions' without considering the full operational processes and integration**. The cybersecurity industry promotes many solutions in ICS environments, and programs often have a significant focus on deploying tooling to discover assets passively and detect unusual behaviour. However, visibility alone often delivers low reduction in risk until the false positive rate can be reduced, risk weighting applied to the alerts, and actual decisions made on interventions and mitigations.

3. **Human factors.** Cultural differences between the IT security and ICS teams are deeper than before due to an increase in digital transformation initiatives. These differences need to be addressed at the organisational level to ensure the success of ICS cybersecurity programs. Without cross-training IT security and ICS teams and strategically positioning staff in joint initiatives and operations, the gap in culture, knowledge and mutual understanding remains too strong.

4. **Scope of the ICS cybersecurity programs is too narrow.** Many programs do not have sufficient scope around the work needed to make the cybersecurity solutions operational, drive the right decisions or include the right people (especially if the change has risk trade-offs to consider). Deployment of solutions might be in scope but the optimisation of the tools is often ignored.

5. **Imbalance between cybersecurity controls and engineering controls.** Cybersecurity maturity improvement programs have a tendency to be biased towards preventive and detective controls, while the engineering controls in place and those required for response and recovery of operations (i.e., critical spares, ability to mobilise support, process safety design) are not given due consideration.

6. **Inefficient tracking of control effectiveness.** Tracking the effectiveness of implemented controls through periodic testing is not often conducted, leading to a lack of confidence in cybersecurity controls implemented as part of the program. Controls are not often tested for effectiveness after changes to system configuration or as part of planned exercises and periodic audits.

This paper provides more insight into the current state we observe in organisations that use ICS, constructive recommendations, and common pitfalls to avoid. There are several standards and guidelines available for use by organisations to improve ICS maturity, namely ISA 62443 series of standards; the National Institute of Standards and Technology (NIST) 800-82 Revision 2 – Guide to Industrial Control Systems (ICS) Security; European Programme for Critical Infrastructure Protection (EPCIP); and NIST Cyber Security Framework (CSF) that provides controls for ICS environments through informative reference mapping with ISO 27001- Information Security Management. Out of these standards and guidelines, ISA 62443 series of standards are internationally accepted and provide a holistic coverage of policies and procedures, ICS asset level controls and ICS component level of controls. Additionally, the ISA 62443 series of standards provide a framework to manage the entire lifecycle of ICS assets from design, commissioning through to maintenance, which are not matched by other standards and guidelines. This paper covers ISA 62443-2-1 (99.02.01)-2009 - Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program (ISA 62443-2-1),which defines the elements required to establish an ICS Cyber Security Management System (CSMS) along with detailed steps and considerations to ensure successful ICS cybersecurity maturity programs. Our paper’s analysis is based on the elements defined in ISA 62443’s CSMS Lifecycle:

·Section 1 – Introduction (this section).
·Section 2 – Risk analysis.
·Section 3 – Addressing risk with a CSMS.
·Section 4 – Monitoring and improving the CSMS.
·Section 5 – Conclusion.

Risk Analysis

This section focuses on the business rationale and the risk analysis element groups as defined in the ISA62443-2-1 CSMS. The risk analysis process in the ISA62443-2-1 lifecycle is a critical element of the ICS cybersecurity program that defines how the rest of the elements of ISA62443-2-1 are implemented and monitored.

The risk analysis should include consideration of threat actors initiating threat events to exploit vulnerabilities in systems and components that can result in impact to the ICS asset. It is very important for the organisation to understand the needs of their ICS cybersecurity program as well as the current risk exposure of the organisation. ISA 62443-2-1's risk analysis is based on two element groups:

- Business rationale – which focuses on the need for the organisation to address its ICS cybersecurity risk
- Risk identification, classification and assessment – which focuses on the ICS cybersecurity risks, the likelihood, and their impact.

We often come across environments where the business rationale and risk identification, classification, and assessment do not align with the business objectives. Further analysis on the recommendations to address the current state and the pitfalls to avoid is provided below.

COMMON CURRENT STATE	HOW TO IMPLMENT A CSMS?	COMMON PITFALLS TO AVOID
Business rationale · Management has only a basic understanding of the business impact of a cybersecurity incident affecting operations. · Organisations lack visibility of their ICS assets and the inter-dependencies between them, and are unaware of the ICS cybersecurity vulnerabilities and risks to each site. · Organisations have a distributed operating model for managing cybersecurity programs and projects. While this may be set by the organisational structure and geography of the assets, it creates challenges with visibility of site-specific risks, reporting and standardised maturity.	**CSMC program initiation:** · Conduct an assessment of current maturity, the cyber threat landscape, and the impact of a potential cyber security attack. · Establish a dedicated Project Management Office (PMO) for ICS cyber security. · Implement an ICS cybersecurity operating model with clearly defined roles and responsibilities. · Implement an ICS asset management system as a single source of truth for all assets managed by the organisation. · Review the existing Business Continuity Plan (BCP) to ensure it supports business objectives.	**CSMC program initiation:** · Senior management is unaware of ICS security risks and their impact on the business resulting in a bottom-up approach where the operational team is carrying out tasks without knowing the problems they are meant to resolve in the face of business objectives. · Lack of clearly defined ownership of ICS security risk resulting in isolated initiatives not fully aligned to organisational risks. · The organisation's risk profile and tolerance are not relevant to the organisation's business.

COMMON CURRENT STATE	HOW TO IMPLMENT A CSMS?	COMMON PITFALLS TO AVOID
ICS cybersecurity risk management context: · An inventory of assets does not exist across the ICS environment. Partial inventories exist but lack the critical information needed to track vulnerabilities, criticality and ownership. · Key deficiencies exist within ICS cybersecurity governance, including a lack of an ICS security operating model with established roles, responsibilities and processes. · ICS security frameworks are not robust and different ICS security architecture practices and baseline configurations are used across the regions. · Low maturity in the ICS vulnerability management process. This includes a lack of processes to identify vulnerabilities, perform risk assessments, and an inconsistent approach towards patch management. · The level of knowledge or the expertise to develop risk scenarios affecting ICS assets, considering the threats and vulnerabilities and cybersecurity tactics, techniques and procedures (TTPs), does not exist. · Incident response plans do not often consider cybersecurity as a contributor to incidents. Existing processes and procedures are not adequate to cover cybersecurity incidents.	**ICS cybersecurity risk assessment:** · Define a framework for cyber security risk management that can be leveraged to support the ongoing management of risks to the ICS environment. · Layers of Protection Analysis (LOPA) should be used to evaluate high-consequence scenarios to determine if the combination of probability of occurrence and severity of consequences meets an organisation's risk tolerance. · Process hazards (potential hazards associated with an industrial process such as transmission of electricity, cooling Natural Gas to -162 degrees Celsius to make it Liquified Natural Gas (LNG), or signalling systems in trains) should be used as inputs to the risk assessment. · Process safety design should consider the complete design of an industrial process and associated risk management by considering the process hazards to ensure an inherently safer design. · Review ICS architecture to ensure there is appropriate segregation of systems that support various layers of protection in process safety design. · Conduct high-level risk assessments with business stakeholders to identify potential security threats to the ICS environment. · Document risks utilising a mix of scenario-based and asset-based methods. · Conduct detailed-level risk assessments at the site level to make them more relevant and specific to the critical assets at those sites.	**ICS cybersecurity risk assessment:** · Lack of ownership of ICS security risk resulting in risks being assessed in isolation (or at the system level) without considering enterprise risk. · Cybersecurity risk assessments are not aligned to process hazards. · ICS cybersecurity risks do not consider the impacts of Health, Safety and Environmental (HSE). · Detailed risk assessments are conducted at an organisational level as opposed to the site level. · Defining too broad or, conversely, too limited a set of scenario-based risks affecting critical assets. · Risk assessments fail to consider all vulnerabilities due to the lack of an up-to-date asset register and the number of entry and exit points to the ICS environment. · LOPA is not considered when rating the identified risks leading to an unrealistic representation of the residual risk. Component vulnerabilities are often added to the risk registers and classified based on the Common Vulnerability Scoring System (CVSS) score without considering LOPA and existing controls in place.

COMMON CURRENT STATE	HOW TO IMPLMENT A CSMS?	COMMON PITFALLS TO AVOID
	ICS cybersecurity risk assessment: · Employ a Cyber Process Hazard Analysis (CyberPHA) based risk methodology that integrates process safety, industrial automation and cyber security disciplines. Articulate the impact of vulnerabilities as risk statements by considering existing controls and a thorough attack surface analysis.	

Addressing risk with the CSMS

This section builds on the Addressing risk with the CSMS element of the ISA 62443-2-1 standard. We discuss the elements of the ISA 62443-2-1 CSMS that focus on how policies, selection of countermeasures and their implementation where the ICS Cybersecurity Programs often go wrong.

The CSMS as defined by ISA 62443-2-1 outlines a systematic risk-based approach defining organisational procedures, responsibilities and governance to manage cybersecurity risks. This section focuses on the supporting activities required for the selection and implementation of controls, starting with defining the scope of the assets to which the controls should be applied. This category forms the majority of the requirements and implementation guidance of the CSMS.

COMMON CURRENT STATE	HOW TO ADDRESS RISK WITH THE CSMS?	COMMON PITFALLS TO AVOID
Security policy, organisation and awareness · Management is not actively tracking ICS cybersecurity metrics. Key Risk Indicators (KRI) are not defined or tracked. · The systems, processes and ICS assets under the scope of the CSMS are not clearly identified.	**Security policy, organisation and awareness** · Develop, publish and enforce an ICS cyber security policy that clearly defines the purpose and objectives. · Train the cybersecurity and ICS teams in areas of identified gaps and formalise a target operating model.	· Lack of management support of ICS cybersecurity policies. · ICS cybersecurity policies do not account for the functions of specific systems (Control Room Operator Consoles with Emergency Shut Down functions are required to have lock screens when the compensating physical security controls to the facilities may suffice etc.).

COMMON CURRENT STATE	HOW TO ADDRESS RISK WITH THE CSMS?	COMMON PITFALLS TO AVOID
· There is no dedicated ICS cybersecurity risk owner in the organisation. · The roles and responsibilities for ICS cybersecurity are not well documented or understood. · IT cybersecurity teams lack ICS skills, and ICS engineers lack cybersecurity skills. · Change management procedures are not defined for the ICS environment, and changes to hardware, software or networks are not authorised. · Cybersecurity policies and procedures are not consistently implemented across all sites and, in several cases, are not based on the organisation's risk tolerance. **Selected security requirements** ·**Personnel security:** Background checks are conducted for permanent employees, but contractors and casual staff are managed differently in different sites. ·**Physical and environmental security:** Physical access and entry to high-risk ICS zones are not managed and monitored. ·**Network segmentation:** Several sites have flat networks across ICS on different layers of protection (or multiple fully connected networks). ICS at a site do not all have the same risk and require the same level of protection from cyber-attacks. Having a flat network means an attacker can compromise a low value target and then move laterally within the network and compromise critical systems or even safety systems which are supposed to be segregated from even the ICS managing the normal industrial process.	· Develop, publish and enforce an ICS cyber security policy that clearly defines the purpose and objectives. · Train the cybersecurity and ICS teams in areas of identified gaps and formalise a target operating model. · Develop Key Risk Indicators (KRI) and Key Performance Indicators (KPI) so that they are used to inform leadership outside of the cyber security risk functions about the control effectiveness of ICS security controls implemented to improve maturity. · Establish a baseline of security controls required to be implemented across the sites. · Implement change management, Permit to Work (PtW) or Management of Change (MoC) processes that consider the business impact of changes to ICS prior to approval. **Selected security requirements** Develop a roadmap of security countermeasures for the domains below. These should be planned for implementation in the order of priority determined by the risk assessments (Do now, Do next, Do later or similar). ·**Personnel security:** o Establish a standardised process for background checks for onboarding employees, contractors and vendors. ·**Physical and environmental security:** o Define high-risk zones with critical systems in a site and monitor physical access including alarms and system alerts where required.	· The scope of the ICS assets and systems in scope for the CSMS is defined very broadly or too restrictively. · Roles and responsibilities for ICS cyber security are not formalised and communicated with all the stakeholders. · Key personnel and stakeholders are not involved, especially if there is insufficient documentation to provide a detailed overview of the current network. · ICS asset owners and users are unwilling to sacrifice the ease of use and access provided by a flat network. · ICS vendors are not included in the security countermeasure selection and implementation. ICS vendors need to be aware and approve any changes as they need to support the ICS. · The organisation is unwilling to tolerate the down time required to implement and test segmentation controls. · Only wired networks are considered for implementing security countermeasures and wireless communication mechanisms (Wi-Fi, 3G/4G and radio networks are often ignored). · Segmentation of the ICS infrastructure is performed based on the vendor for the ICS as opposed to the ICS function. For example, all ICS from a vendor (Feeder Automation, Variable Frequency Drive (VFD) systems, HMIs, telemetry and SCADA systems and Safety Instrumented Systems (SIS)) are placed in one network segment as opposed to segmenting the network by functions and security level targets (SL-T) determined during the risk assessments.

COMMON CURRENT STATE	HOW TO ADDRESS RISK WITH THE CSMS?	COMMON PITFALLS TO AVOID
o Multiple interconnections exist between IT and ICS networks in the same site. o Firewall rules between IT and ICS interface are not reviewed, or their effectiveness not assessed. Insecure protocols are used across IT and ICS. o Several sites have an aged network infrastructure with multi-mode fibre and not enough cores available to increase bandwidth, etc. o There is an element of scepticism about any down time to production affecting revenue to improve ICS security and reconfiguring flat networks affecting ease of access to systems. **·Access control:** o There is no documented process or policy in place to govern account management or role-based access control. o Authentication: The list of users with access to the various ICS at the sites is not known. **Implementation:** · **Risk management and implementation.** o Lack of ownership, responsibility and accountability for the identified ICS risks. o Control selection and decision making are not aligned with the risk to the business. · **Incident planning and response.** o Incident response plans are not well known and published for employees to understand their roles and responsibilities. o Employees are unsure of the process for reporting cybersecurity incidents. The processes for identifying and assessing cybersecurity incidents affecting ICS are not optimised.	·**Network segmentation:** o Develop zone and conduit diagrams for ICS assets at each site. o Ensure adequate network security controls exist between ICS environments with different security trust levels. o Where down time is not acceptable to the organisation, consider reviewing the network access controls in place along with the layers of protection analysis (LOPA) to determine if segmentation is the best control in this case. o Ensure risk of failure of security controls for a zone will not impact the safety of the operation of the system within the zone. o Develop a detailed understanding of the ICS assets and traffic flows associated with the safe operation of ICS at a site. **·Access control:** o Establish an identity and access management strategy including on-premises access to ICS environments and remote access for third parties to the ICS environment. o Consider using solutions which limit users moving laterally within ICS environments. **Implementation:** **· Risk management and implementation.** o Define a governance model for the management of ICS cybersecurity. o Lack of ownership, responsibility and accountability for the identified ICS risks. o Control selection and decision making are not aligned with the risk to the business. · Incident planning and response. o Develop incident response plans for critical systems and update them as required to keep up with changes in the emerging threat landscape. Establish a schedule of incident response simulations based on identified TTPs.	· There is too much focus on data security and network security with little to no attention on the security configuration of control systems (Open Process Control (OPC), Distributed Network Protocol 3 (DNP3), Open PLC coding practices etc.). · Organisations focus heavily on protective controls and less on response and recovery controls. · Detective controls through vendor products are implemented but are not supported by the system context and the events of interest to be able to provide the relevant information to the security monitoring teams. · Organisations with a Security Operations Centre (SOC) do not have a team with the ICS knowledge needed to configure events of interest or review alerts themselves, relying instead on external IT security professionals. · Vendor selection for security services is conducted without a defined set of requirements. · Security controls are selected without consideration of the LOPA. Too much trust is placed in airgaps without consideration of physical threat vectors.

COMMON CURRENT STATE	HOW TO ADDRESS RISK WITH THE CSMS?	COMMON PITFALLS TO AVOID
	· **Incident planning and response.** o Develop incident response plans for critical systems and update them as required to keep up with changes in the emerging threat landscape. Establish a schedule of incident response simulations based on identified TTPs.	

Monitoring and improving the CSMS

This section builds on the monitoring and improving the CSMS element of the ISA 62443-2-1 standard. This section also discusses the elements of a CSMS program relating to monitoring and continuous improvement and where they often go wrong. Continuous improvement of the CSMS is critical to the ongoing success of the ICS cybersecurity program as cyber threats evolve and controls need to adapt to evolving threats to ensure effectiveness. Feedback from exercises and incidents should be used to evaluate the effectiveness of the assumptions and planned controls.

Monitoring and improving the CSMS involves:

- **Conformance** - ensuring that the CSMS developed for the organisation is being used.
- **Reviewing, improving, and maintaining the CSMS** - reviewing the CSMS for effectiveness with the objective of continuous improvement.

COMMON CURRENT STATE	HOW TO MONITOR AND IMPROVE THE CSMS?	COMMON PITFALLS TO AVOID
Conformance: ▪ ICS assets are not audited against the cybersecurity compliance requirements outlined in the policy. · Control effectiveness testing is not conducted. · Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) for ICS security are not established in the organisation.	**Conformance:** ▪ Develop an annual ICS cybersecurity audit plan and include it in the organisation's Internal Audit (IA) forward plan. · Define KPIs that provide meaningful insights, which assist the ability of the organisation's management to make decisions.	**Conformance:** · Auditing the same ICS assets and sites every year. · Monitoring of ICS configuration against a defined baseline only occurs at defined intervals and does not take place after maintenance or retooling which may change the components (software and equipment) in an ICS. · KPIs for management are not meaningful or inconsistent with the CSMS.

COMMON CURRENT STATE	HOW TO MONITOR AND IMPROVE THE CSMS?	COMMON PITFALLS TO AVOID
Continuous improvement: · The existing policies and procedures have not been reviewed periodically. · Where polices and controls are reviewed, the review occurs at the same pre-defined intervals irrespective of the ICS criticality. Risk tolerance is not periodically evaluated by considering changes in operating environments and emerging threats.	**· Continuous improvement** · Establish criteria for the review of policies and procedures affecting the ICS in scope for the CSMS based on the assigned criticality. · Re-evaluate risk tolerance due to changes in external factors and internal factors (such as maintenance, retooling and introduction of new products and functionality). · Monitor and adjust KPIs and KRIs when required, in response to key changes in the threat landscape. · Communicate the performance of controls implemented as part of the maturity improvement program. This will assist leadership with decision making to make any changes to controls required to keep risk at an acceptable level. KPIs should enable management to make decisions that address risks affecting the organisation's ICS.	**· Continuous improvement** · Events of interest from the ICS are not defined for each ICS asset in the site based on criticality, which can lead to a lot of noise in alerts wasting valuable analysis cycles. Changes to the CSMS are not communicated to the relevant stakeholders. This is critical as stakeholders need to be aware of any changes to their responsibilities.

Conclusion

ISA 62443-2-1 provides excellent guidance for an organisation to build and execute a CSMS to improve ICS security maturity. Establishing an ICS cybersecurity CSMS requires a top-down approach and commitment from management. Very often, the ICS cybersecurity programs fail to achieve objectives due to some of the above pitfalls. A successful ICS cybersecurity program execution requires a lot of time and effort with the support of knowledgeable personnel from the control systems and instrumentation teams and those responsible for ICS security. The organisation's management should have a realistic expectation of improvement in ICS cybersecurity posture in an environment where risk culture management practices have historically been sub-optimal. Avoiding the common pitfalls combined with well-defined and managed ICS cybersecurity program can assist organisations in improving their ICS cybersecurity posture.

Deloitte Contributors

Abraham Cherian Specialist Director abcherian@deloitte.com.au	Harish Sashyanth Senior Consultant hsashyanth@deloitte.com.au

OT-ISAC Contacts

John Lee Managing Director +65 6670 6796 jlee@grf.org	AJ Eserjose Regional Director +65 6670 6796 aeserjose@grf.org

Deloitte Contacts

Australia Luke Forsyth Partner +61 8 9365 8010 lforsyth@deloitte.com.au	**Chinese Mainland/Hong Kong** Boris Zhang Partner +86 21 61411505 zhzhang@deloitte.com.cn	**India** Gaurav Shukla Partner +91 80 6188 6164 shuklagaurav@deloitte.com	**Japan** Haruhito Kitano Partner +81 80 3591 6426 haruhito.kitano@tohmatsu.co.jp
Korea Young Soo Seo Partner +82 2 6676 1929 youngseo@deloitte.com	**New Zealand** Anu Nayar Partner +64 4 470 3785 anayar@deloitte.co.nz	**Southeast Asia** Gerry Chng Partner +65 6800 3875 gchng@deloitte.com	**Taiwan** Max Lin Partner +886 2 2725 9988 (ext. 7779) maxylin@deloitte.com.tw

About OT-ISAC

Operational Technology Cybersecurity Information Sharing and Analysis Center (OT-ISAC) is a secure threat information sharing community for Operational Technology-using companies headquartered in Asia Pacific. A member company can securely and anonymously share threat information with OT-ISAC analysts who further enrich and disseminate actionable alerts, intelligence and best practices for all community members to defend themselves and take mitigating action against malicious actors, their tools, and system exploits. OT-ISAC also partners with government, private vendors and other information sharing organisations to acquire and disseminate timely and relevant information for the resilience of member companies.

About Deloitte’s Asia Pacific OT security practice

With the largest cybersecurity services team globally and more than 80 professionals focused on OT security in Asia Pacific, Deloitte brings a wealth of experience including engineers from industry, cyber specialists and experts in governance and change management. We work with all manufacturing and critical infrastructure sectors to help organisations understand their cyber exposure across IT and OT, launch and run cyber transformation programs, build security controls, comply with regulatory and supply chain requirements, and detect and respond to cyber threats. We offer the full range of advisory, implementation and managed services, including cyber process hazard analysis, IT/OT threat monitoring, detection, response and proactive hunting.