MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

First edition
2020-05-05

Guidelines for Secure Industrial Control System (ICS)

Reference number:
MyVAC-3-GUI-1-ICS-v1

REGISTERED OFFICE:

CyberSecurity Malaysia,
Level 7 Tower 1,
Menara Cyber Axis,
Jalan Impact,
63000 Cyberjaya,
Selangor Darul Ehsan, Malaysia
Email: myvac@cybersecurity.my

COPYRIGHT © 2020 CYBERSECURITY MALAYSIA

The copyright of this document belongs to CyberSecurity Malaysia. No part of this document (whether in hardcopy or electronic form) may be reproduced, stored in a retrieval system of any nature, transmitted in any form or by any means either electronic, mechanical, photocopying, recording, or otherwise without the prior written consent of CyberSecurity Malaysia. The information in this document has been updated as accurately as possible until the date of publication.

NO ENDORSEMENT

Products and manufacturers discussed or referred to in this document, if any, are presented for informational purposes only and do not in any way constitute product approval or endorsement by CyberSecurity Malaysia.

TRADEMARKS

All terms mentioned in this document that are known to be trademarks or service marks have been appropriately capitalised. CyberSecurity Malaysia cannot attest to the accuracy of this information. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

DISCLAIMER

This document is for informational purposes only. It represents the current thinking of CyberSecurity Malaysia on the security aspects of the Industrial Control System environment. It does not establish any rights for any person and is not binding on CyberSecurity Malaysia or the public. The information appearing on this guideline is not intended to provide technical advice to any individual or entity. We urge you to consult with your own Industrial Control System advisor before taking any action based on information appearing on this guideline or any other documents to which it may be linked.

Contents Page

1 Introduction

Industrial Control Systems (ICS) is a combination of hardware, software, and networking devices to perform monitoring, controlling and/or safeguarding the process of the industrial facility. A disruption to ICS can result in people's safety, environmental degradation, asset damage and/or production disruption and/or reputational loss. This guideline is developed to provide a reference for the implementation of security controls to secure ICS, which is mainly used in Critical Infrastructures. This document is divided into three chapters. Chapter 1 provides an overview of ICS for the benefit of those who are new to the ICS environment. Chapter 2 highlights the security issues involving ICS, as well as the security approach used in this document. Chapter 3 provides practical guides to secure the components in ICS.

1.1 Scope

In this guideline, the ICS-specific security controls are mostly based on NIST SP 800-82r2, and the security control families are as defined in NIST SP 800-53r4. The security control families are categorized into people, process, and technology, which is used as the systematic approach in Information Security Management System (ISMS).

The ICS reference architecture used in this guideline is a modified Purdue Enterprise Reference Architecture (PERA) model, which is used in ISA-99[1]. The emphasis of this security guideline is on level 0 until level 3 of the ICS reference architecture.

1.2 Objective

This document aims to be a quick reference to Malaysian organizations or companies that run an ICS facility. It provides a high-level guide on security controls that need to be implemented to secure an ICS facility. However, for a complete guide and detailed implementation of ICS security, this document needs to be read together with other security standard documents such as NIST SP 800-53r4[2], NIST SP 800-82r2[3], ISO/IEC 27001[4], CIS CSC[5], ISO/IEC 62443-2-1[6] and COBIT 5[7].

1.3 Intended audience

This guideline is not intended to provide comprehensive background information on ICS and ICS security in any of its chapters as it focuses on providing a practical security guide. Hence, this document is intended to benefit the audience who are already in the business of ICS and have an idea about the importance of ICS security. The following audience are identified but not limited to:

a) Engineers or individuals, who are authorized to design, implement, administer, patch, assess or secure ICS.
b) Managers who are responsible for ICS.
c) Researchers who want to learn more about the practical implementation of ICS security.
d) Vendors who are involved in the design, development or supply of ICS equipment.

---

[1] Byres, Eric, P. Eng, and I. S. A. Fellow. "Using ANSI/ISA-99 standards to improve control system security." *White paper, Tofino Security* (2012).

[2] Force, J. T., & Initiative, T. (2013). Security and privacy controls for federal information systems and organizations. *NIST Special Publication*, *800*(53), 8-13.

[3] Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to industrial control systems (ICS) security. *NIST special publication*, *800*(82), 16-16.

[4] Disterer, Georg. "ISO/IEC 27000, 27001 and 27002 for information security management." (2013).

[5] Valladares, Cindy. "Critical Security Controls: Control 7—Wireless Device Control"." *Tripwire—The State of Security, tripwire.com* (2013).

[6] ISA-99 Committee, ISA-62443 series of standard: *Security for Industrial Automation and Control Systems, International Electrotechnical Commission (IEC*) (2010).

[7] AC11069413, Anonymus, ed. *COBIT 5: A business framework for the governance and management of enterprise IT*. Isaca, (2012).

It is advisable that the readers who are not familiar with ICS and ICS security to refer to other available sources of information while looking up to this document.

2 Terms, definitions, abbreviated terms and acronyms

2.1 Terms and definitions

For this document, the following terms and definitions apply.

2.1.1
Asset
anything that has value to the organization

[ISO/IEC 13335-1:2004]

2.1.2
Availability
the property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 13335-1:2004]

2.1.3
Confidentiality
the property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-1:2004]

2.1.4
Information security
preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved

[ISO/IEC 17799:2005]

2.1.5
Information Security Management System
ISMS
that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security

Note: The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

2.1.6
Integrity
the property of safeguarding the accuracy and completeness of assets

[ISO/IEC 13335-1:2004]

2.1.7
Risk assessment
the overall process of risk analysis and risk evaluation

[ISO/IEC Guide 73:2002]

2.2 Abreviated terms and acronyms

APT	Advanced Persistent Threats
CI	Critical Infrastructure
DCS	Distributed Control Systems
DH	Data Historian
EWS	Engineering Workstation
HMI	Human-Machine Interface
ICS	Industrial Control System
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IED	Intelligent Electronic Device
ISA-99	International Society of Automation- 99- Industrial Automation and Control Systems Security
IT	Information Technology
LAN	Local Area Network
NIST	National Institute of Standards and Technology
OT	Operational Technology
PCS	Process Control System
PERA	Purdue Enterprise Reference Architecture
PLC	Programmable Logic Controllers
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SIS	Safety Instrumented Systems
TCP/IP	Transmission Control Protocol/ Internet Protocol

3 Overview of Industrial Control System (ICS)

Industrial control system (ICS) is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control systems that act together to achieve an industrial objective. The convergence of Operational Technology (OT) and Information Technology (IT) in ICS has increased the operational and cost efficiency but opens up to more threats that could lead to system unavailability and espionage.

3.1 Types of ICS

ICS are characterized according to their use as well as according to the geographic separation between the controller (i.e., PLC, RTU, IED) and the supervisory components such as the HMI and Data Historian. There are a few types of ICS as listed below:

3.1.1 Process Control System (PCS)

PCS is an automation process in a manufacturing environment. It allows operators to make control decisions, which might then be relayed upstream, downstream, or to parallel processes for execution by the same system.

For example, an ICS might gather information from endpoint devices that allow operators to assess that a leak may have opened in a pipeline. The system aggregates this information at a central site, which (hopefully) contains intelligence and analytics alerting a control station and operators that the leak has occurred. Operators then carry out necessary analysis to determine if and how the leak may impact operations, safety, and regulations (environmental, health, and safety).

3.1.2 Distributed Control Systems (DCS)

DCS distributes its function into smaller sets of semi-autonomous subsystems covering specific process or geographic areas of the plant. Provide the automation functionality of the manufacturing process by integrating regulatory control logic with procedural languages to support obtaining values from field and supply values to the field in term of:

a) Basic control and monitoring
b) Intermediate and advanced regulatory control
c) Provision of information exchange to other systems/subsystems.

3.1.3 Supervisory Control and Data Acquisition (SCADA)

SCADA system links all site nodes to a central station. The system is used to monitor the facilities and control of the critical parameters, e.g., flow. The physical link at each facility uses Remote Terminal Unit (RTU) or PLC to field devices.

3.1.4 Safety Instrumented Systems (SIS)

SIS is designed to avoid dangerous situations in the production system by stopping or shutting down processes if unsafe conditions develop. It used for monitoring the state of the ICS infrastructure. SIS is dedicated to process safety.

SIS has sensors sending input signals to a controller, which is programmed to actuate equipment to prevent an unsafe state or mitigate the impact of hazardous operations.

In general, ICS systems perform the following tasks:

a) Collect data from endpoint devices
b) Send the collected data to an HMI (Human-machine Interface) to be displayed
c) Apply automatic, semi-automatic or operator-controlled changes to endpoint devices

3.2 ICS components

Components in an ICS are commonly referred to as assets. Assets include both field components and control system components. Field components in ICS are sensors, actuators, motor drives, gauges, and indicators. As for the control system components in ICS, there are few of them as listed below:

3.2.1 Programmable Logic Controller (PLC)

PLC- a microprocessor-controlled electronic device that reads input signals from sensors, executes programmed instructions using these inputs as well as orders from supervisory controllers, and creates output signals which may change switch settings or move actuators.

PLC is the first type of ICS controllers and is the boundary between the cyber world and the "real-world". A PLC is often rugged to operate in remote locations under harsh environmental (e.g., temperature, heat, vibration, electromagnetic fields) conditions.

3.2.2 Remote Terminal Unit (RTU)

The RTU collects input signals from machinery or other infrastructure and stores this data until the control center automation polls the RTU. After polling the RTU, either the control center automation or a human operator may direct the RTU in how to control the physical processes. Besides polling, RTU communicates with the control center may deliver on event-based. The RTU also can be programmed to take control actions independently of the control center.

There are two types of RTU, which are Field RTU and Station RTU. Field RTUs receive input signals from field devices and sensors and then execute programmed logic with these inputs. The field RTU gathers data by polling the field devices/sensors at a predefined interval. Field RTUs are interfaces between field devices/sensors and the station RTU. Station RTUs are also found at remote sites and receive data from field RTUs as well as orders from supervisory controllers.

The station RTU then creates output values to control physical devices and through the physical processes. A control center communicates with a station RTU.

3.2.3 Intelligent Electronic Device (IED)

IED is a microprocessor-based controller of power system equipment. It is also known as a digital protective relay. It performs five functions, which are protection, control, monitoring, metering, and communications.

It receives data from sensors and power equipment and able to issue control commands, such as tripping a circuit breaker, should the need arise.

Examples of IEDs are protective relay and voltage regulator, which used for substation automation in the power system. IEDs usually have communication capability. Utility companies are deploying IEDs to their substations to improve automation and information flow to their enterprise networks.

3.2.4 Human-Machine Interface (HMI)

HMI is a software application that provides situational awareness of the automation processes to plant operators such as alarm, data trends, and many more in visualization forms such as diagrams, graphics, charts, etc.

Human operators use this device to view data collected from field devices and also to enable human operators to control specific devices.

3.2.5 Data Historian (DH)

DH is a specialized software system, usually, a desktop workstation or server running under Microsoft Windows or Linux that collects real-time process data from automation processes and aggregates the data in a database for concurrent and later analysis.

DH is not an IT database system. It is designed for a very fast ingest of data without dropping data and does not support referential integrity in tables. It also uses industrial interface protocols.

3.2.6 Business information consoles and dashboards

Extensions of supervisor workstations are designed to deliver business intelligence to upper management.

Data comes from HMI or data historian systems.

3.2.1 Engineering Workstation (EWS)

It is a desktop computer or server running a standard operating system such as Microsoft Windows or Linux. This machine hosts the programming software for controllers such as PLC, RTU, IED, and applications. Changes to controller logic and industrial application are made using this machine.

3.3 ICS protocols

There are various proprietary and nonproprietary protocols used in ICS, for example:

a) Proprietary protocols: Honeywell CDA, General Electric SRTP, Siemens S7.
b) Nonproprietary / licensed protocols: OPC, Modbus, DNP3, ICCP, CIP, PROFIBUS, IEC 60870-5-101, IEC 60870-5-104.

Some of the protocols have been adapted to operate over Ethernet and TCP/IP networks. This enables data from ICS to be transmitted over the public Internet. Examples of protocols that worked over Ethernet and TCP/IP are Modbus over TCP/IP, DNP3 over TCP/IP, IEC 60870-5-104. These protocols are treated as application layer protocols by TCP/IP.

3.4 ICS reference architecture

This guideline uses the modified Purdue Enterprise Reference Architecture (PERA) model, which is used in ISA-99. This model serves as a foundation for ICS network segmentation. Figure 1 depicts the reference architecture, and Figure 2 shows the zone segmentation of business and ICS architecture.

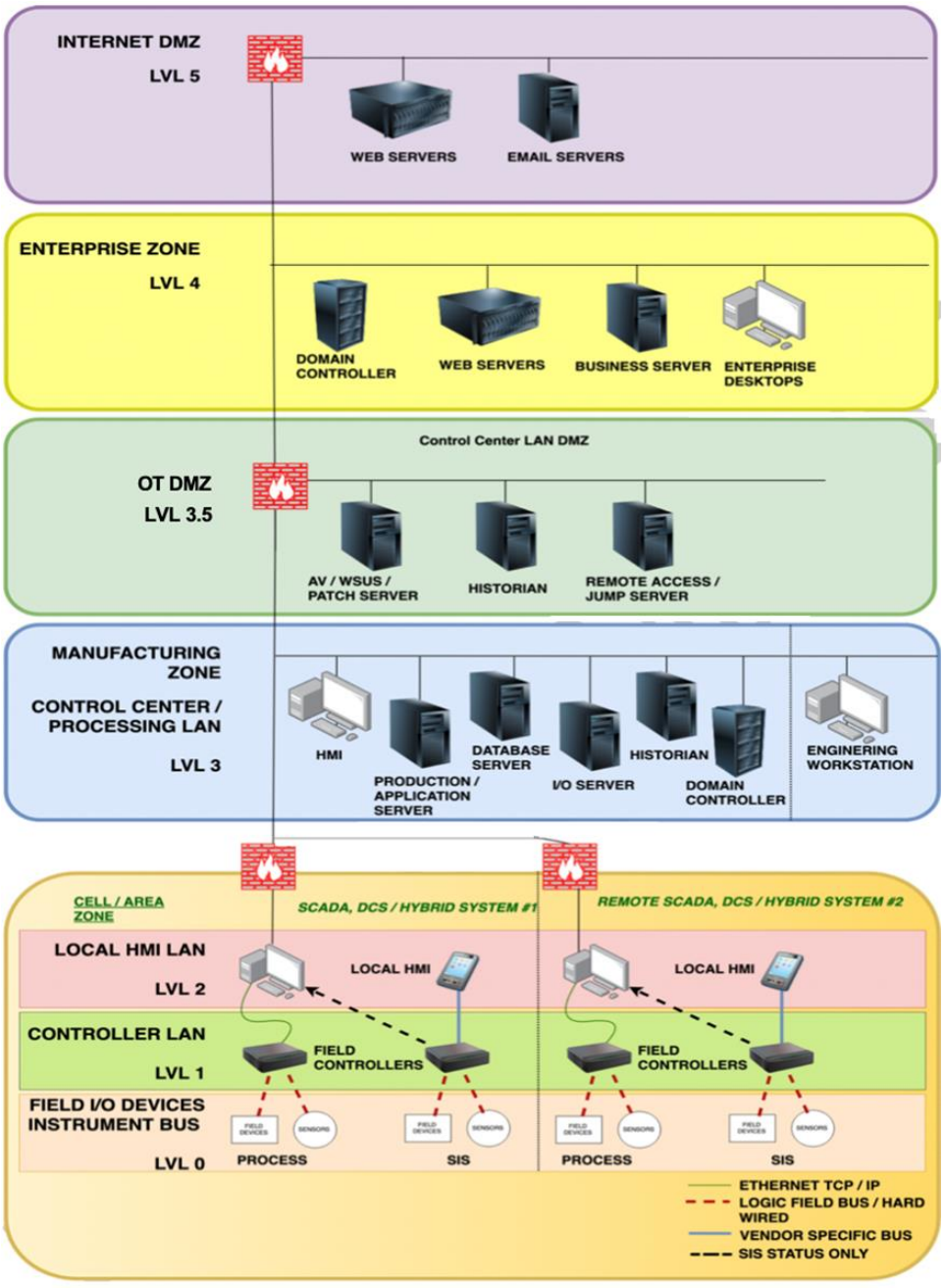


Figure 1: The ICS Architecture

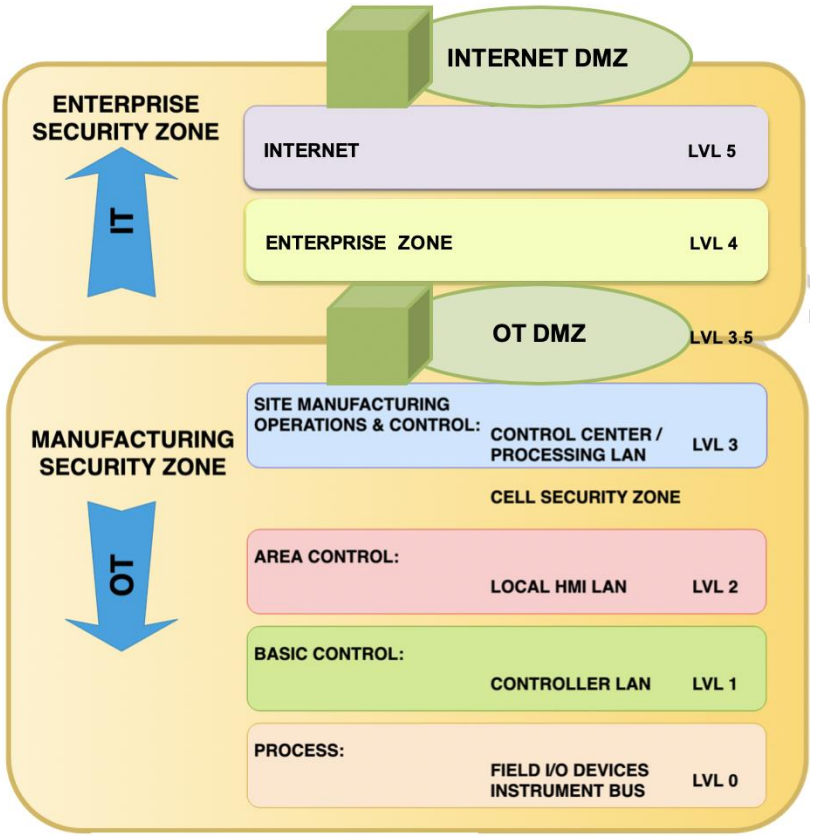


Figure 2: The zone segmentation

Focusing on the ICS environment, the ICS reference architecture is divided into two parts which are Information Technology (IT) and Operational Technology (OT), which is reflected in figure 2. IT is known as Enterprise Security Zone, whereas OT contains Manufacturing Security Zone and Cell Security Zone. The Demilitarized Zone exists between these two parts. IT's top priority is to preserve the data. OT's preference, however, is to protect the availability and integrity of the process with security (confidentiality) coming last.

3.4.1 Enterprise Security Zone

This zone includes connectivity to the Internet, peer locations, and backup or remote offsite facilities (Enterprise network connectivity –Level 5). It also connects the business networks that include corporate communication, email servers, Domain Name System (DNS) servers, and IT business systems (in level 4). Many risks exist in this zone due to numerous connectivity and systems involved; hence this zone is considered as untrusted.

3.4.2 Demilitarized Zones

This zone, which is also known as a perimeter network, is a physical and logical subnetwork that acts as an intermediary for connected security devices so that they evade exposure to a more extensive and untrusted network. Each DMZ holds one or more critical components such as data historian, the wireless access point, or remote and third party access systems. The primary risk with this architecture is when the threat actor compromises a computer in the DMZ and uses that to launch an attack against the control

network. Therefore, an organization should create multiple DMZs for separate functionalities and access privileges such as peer connections, the data historian, ICS communication protocols, and many more[8].

3.4.3 Manufacturing Security Zone

This zone involved monitoring and control (Level 3). It is a critical area for the continuity and management of a control network. This zone is central to the operation of end devices and provides required connectivity to the Enterprise Zone. This zone is a high risk, and the risks are associated with its direct connectivity to any external systems or networks.

3.4.4 Cell Security Zone

This zone is where the level 2, level 1 and level 0 are located and this zone contains system used for Local Area Network (LAN). Level 2 contains the system used for local and remote area control. Level 1 stationed the field located HMIs, RTUs, PLCs, and their controls. Most of the devices in level 1 support the Transmission Control Protocol/ Internet Protocol (TCP/IP) and other common protocols. Whereas level 0 places the basic input/output devices such as actuators and sensors. Since in this area, the control function affects the physical end devices; therefore the priority of this zone is very high.

In the event of the Subscriber require to perform risk assessment, the Subscriber may refer to the template of risk assessment based on the link provide below.

http://download.microsoft.com/documents/australia/enterprise/Risk_Framework_Template_Tool.xlsm

4 ICS security

This chapter discusses Advanced Persistent Threats (APT) to ICS, which may weaken the ICS system. The findings were based on a cybersecurity assessment done by U.S Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). The assessment was conducted over 673 discoveries through 137 architecture design reviews and network traffic analyses[9].

4.1 Top six weaknesses in ICS

Table 1 list the top weaknesses and risks in ICS. The assessment methodology in 2017 ICS-CERT classifies weakness based on the National Institute of Standards and Technology's (NIST) Special Publication 800-53, known as "Security and Privacy Controls for Federal Information Systems and Organizations," control family sub-categories. The report indicates that the six categories represented roughly 33 percent of the total vulnerabilities discovered across assessed Critical Infrastructure (CI) sectors[10].

[8] Homeland Security, Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, https://www.us-cert.gov/sites/ default/files/recommended_practices/NCCIC_ICS CERT_Defense_in_Depth_2016_S508C.pdf (2016)

[9] NCCIC, ICS-CERT Annual Assessment Report Industrial Control Systems Cyber Emergency Response Team FY 2016, https://www.us-cert.gov/sites/default/files/Annual_Reports/ FY2016_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf (2016)

[10] NCCIC, ICS-CERT Monitor November/December 2017, https://www.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Nov-Dec2017_S508C.pdf (2017)

Table 1: Top ICS Weaknesses and Their Security Risks

No.	Area of Weakness	Description	Risk
1.	Boundary Protection	Controls associated with the monitoring and control of communications at the ICS external electronic boundaries and key internal boundaries, the implementation of subnetworks to separate critical systems, and the implementation of managed protective interfaces for external connectivity to critical systems.	1. Undetected unauthorized activity in critical systems 2. Weaker boundaries between ICS and enterprise networks.
2.	Least Functionality	Controls associated with minimizing the computing resources of systems functions, ports, protocols, and services to only those required to support essential system operations.	1. Increased vectors for malicious party access to critical systems Rogue internal access established
3.	Identification and Authentication (Organizational Users)	Controls implemented for the identification and authentication of authorized organizational users (or processes acting on behalf of organizational users)	1. Lack of accountability and traceability for user actions if an account is compromised 2. Increased difficulty in securing accounts as personnel leave the organization, especially sensitive for users with administrator access
4.	Physical Access Control	Management of controlling user's physical access to an organization's assets that include data, hardware, software, and process.	Unauthorized physical access to field equipment and locations provides increased opportunity to: a) Maliciously modify, delete, or copy device programs and firmware b) Access the ICS network c) Steal or vandalize cyber assets d) Add rogue devices to capture and retransmit network traffic
5.	Allocation of Resources	Management of scheduling to support cybersecurity-related activities and events, and resources required by the activities by taking into consideration the resource availability and project time.	1. Lack of accountability and traceability for user actions if an account is compromised. 2. Increased difficulty in securing accounts as personnel leaves the organization, especially sensitive for users with administrator access.
6.	Account Management	Management of access to an organization's particular accounts that maintain a relationship between the organization and its users.	Compromised unsecured password communications a) Password compromise could allow trusted unauthorized access to systems.

Table 1 indicates that the primary weakness was flawed in network architecture boundaries, and followed by the problem in user identification due to the increasing use of shared and group accounts. Accounts that are shared by a group of users typically use a simple password, which can easily be guessed. A shared account also makes it hard to identify the actual user, hence allow the malicious actors to use them with anonymity.

Another concerning issue was the attrition of the skilled staff, which is extremely important in securing the ICS. Having an experienced team contributes to the increment of work output. However, if a business has a poorly trained workforce, then it's missing out on a relatively low-cost way of overall improvement.

Besides that, the ICS components and infrastructure should only be accessible to authorized personnel to ensure their security. Hence, physical access control to the ICS components and infrastructure needs to be monitored closely and rigorously. The information from Table 1 can be used as a reference for organizations to focus their effort on securing their ICS infrastructure. To facilitate this, Chapter 3 in this document provides a guide on securing ICS with a focus on the OT layers.

4.2 Possible ICS security attacks

Due to the security weaknesses as described in Table 1 above, various security attacks can be conducted on ICS. According to the ENISA report, Communication network Dependencies for ICS/SCADA Systems, which was released in December 2016, security attacks may be conducted through ICS system compromise, insiders, or malware. Examples of possible attack scenarios are represented in the tables below. Please refer to appendix A and B for impact level and likelihood level.

Table 2: Example of Attack Scenario 1

Attack scenario 1: Insider threat	
Staff in an ICS field, either in-house staff or external personnel such as contractors, maintenance workers may have knowledge, experience, or access to a variety of internal systems involving smart devices (IIOT), physical and logical ICS network & installation details or anything in the perimeter of ICS. There is always a degree of risk, and making it more challenging is the fact that insider threats coming from these individuals that fit in the role of staff have the advantage of going undetected due to their privileged knowledge of the ICS organizations.	
Impact	**Likelihood**
Critical: It could range from low (information leakage) to very high (actuator or sensor data manipulation).	**Medium**: Depends on the number of users, external staff and contractors but due to the privileges and knowledge this is more common than other attacks.
Ease of detection	**Cascading effect risk**
Due to the internal knowledge these users have, these attacks tend to be hard to detect and identify the source, which allows them to pass undetected for long periods of time and is also complex to investigate and recover from.	Internal staff and contractors have access to internal systems (including critical infrastructures) and have the potential of causing changes that affect the whole system expanding to other environments and/or sectors and directly affecting the population, either by the malfunction of the operations or they cease.

Assets affected	
Human Machine Interfaces, PLCs and sensors, Data Historian	
Possible attack steps by attackers	
1. A disgruntled employee gained physical/remote access (due to IIOT) to control center and installations. 2. The employee with malicious intent to compromise an organization's operational facilities used either own or forged credentials. 3. Equipped with privileged knowledge on an organization's network and systems, the employee bypassed the defense and performed data theft stealing sensitive information. 4. The organization's operations are disrupted with the access gained to several ICS systems, where employees disabled the recovery systems and alert mechanism. 5. The security of the ICS organization is further threatened when data theft with sensitive details may be sold to the black market or competitor.	
Recovery time	**Recommendations**
The main issue is the time taken to detect the data or system that has been manipulated, which can be **several days/weeks** or even months in extreme cases. Also, as the potential access that these employees can have, both logical and physical, the damage may be greater and difficult to recover from, potentially requiring system reboots, resets **several days** or replacements. This could take, on average, to return to standard operations.	Need to harden applications, systems and equipment; restrict access to only what is needed, implement access and activity logging controls.

The illustration of this attack is depicted in Figure 3.

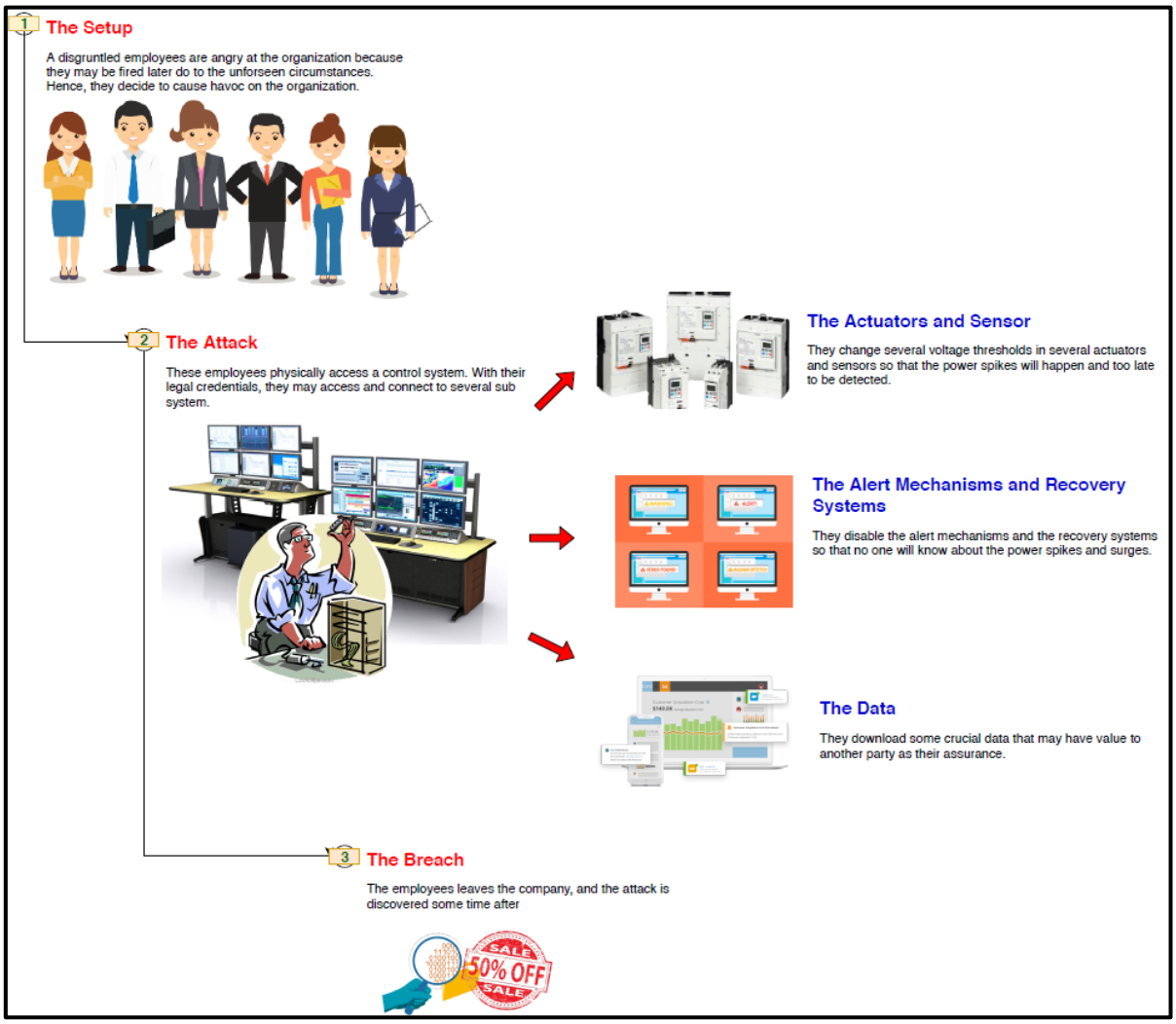


Figure 3: Attack Scenario 1

Table 3: Sample of Attack Scenario 2

Attack scenario: Vulnerability exploit	
This attack covers an infection designed to take control of one or multiple ICS assets within a network. It is crafted to manipulate or crash the network where causes undesired effects on assets such as malfunction, corruption, or physical damage. This attack also will affect the overall infrastructure and system.	
Impact	**Likelihood**
Critical: The compromise of ICS systems can cause them to a malfunction or cease operating, directly affecting the related production processes and potentially causing physical or infrastructure damage.	**Medium**: ICS systems and assets are becoming more interconnected and exposed to the Internet and other networks. This adds a new attack layer that did not apply in the past to these devices, increasing the number of potential attacks against them.

Ease of detection	Cascading effect risk
The changes made on ICS systems can be detected by security control systems and sensors, as long as those are not compromised as well. Having redundant or secondary control systems would allow better detection.	The compromise of these systems can result in their manipulation, compromise or interruption, which can directly affect other interconnected systems (other companies, sectors, etc.), and even translate to direct effects on the population (e.g. blackouts, floods, etc.).
Assets affected	
ICS systems, HMI (Human-Machine Interfaces), Centralised Control System	
Possible attack steps by attackers	
1. The attacker gathers information on the target organization and the relevant, targeted control center. 2. Information regarding the operators and staff of the control center is gathered, and the attacker will launch a social engineering campaign to gain an entry point into the corporate network. 3. An internal users' credentials are stolen and used to gain access to the computer inside the network, and further information gathering is done to identify the vulnerable systems. 4. Once a vulnerable computer is discovered, an attack is launched against to gain access, and a backdoor is installed to maintain access to that system. 5. In a case where the system does not have access to the ICS network, either remotely or directly, more systems will be kept on compromise. 6. The moment the system with access to the ICS network is discovered, the attacks phase stops and the attacker uses the compromised system to attack the ICS systems. 7. Once been compromised, the ICS systems are "updated" with modified firmware that permits exclusive access to the attacker and confines other remote accesses. 8. This makes the ICS assets to be reconfigured, which make the whole system collapse. 9. The corporate local power supply and backup supply systems are compromised too; hence, the operators of the ICS system will not getting any information about this. 10. Lastly, when the ICS collapse, the operations stop, and the control center is unable to act since their corporate systems are deactivated and removed.	
Recovery time	**Recommendations**
It depends on the area where the assets are compromised and the number of assets that are infected. It can range from a few hours and **up to several days** if critical systems are compromised (e.g. nuclear sectors).	Need for restricting physical access to ICS network components in order to reduce the risk of unauthorized access to them. The use of anomalous behavior detection systems and active system monitoring and logging is good protection measures for this attack.

The illustration of this attack is depicted in Figure 4.

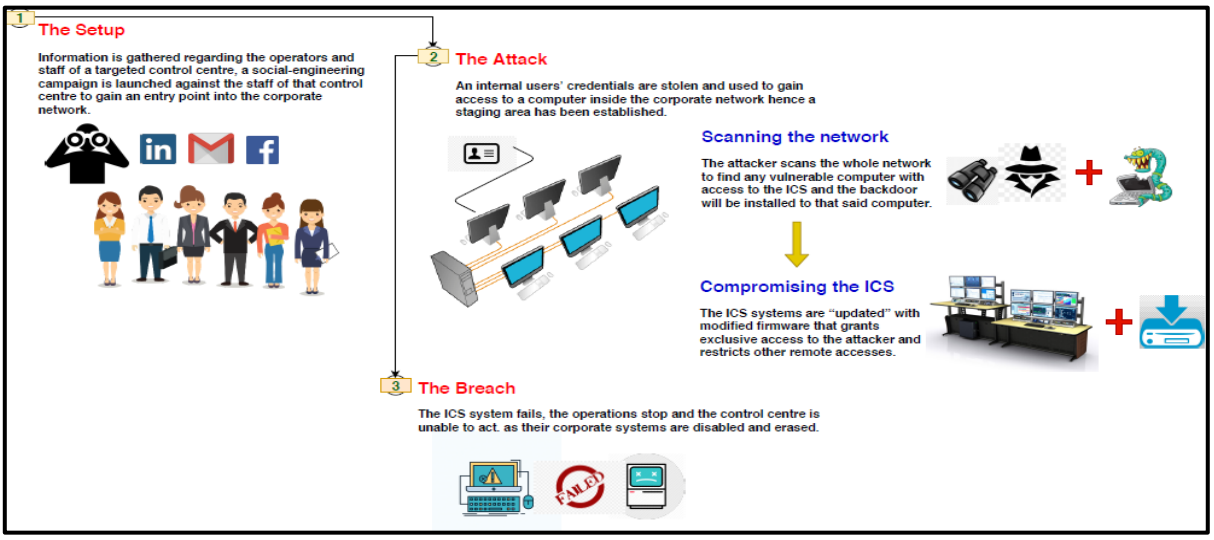


Figure 4: Attack Scenario 2

Table 4: Example of Attack Scenario 3

Attack scenario 3: Malware infection	
Similar to other IT-based systems, ICS systems and devices also require periodic maintenance and upgrades (through patches, feature updates and security fixes) to ensure that they are up to date and able to operate efficiently and securely. During this maintenance or upgrade operation, the risk of the devices being infected by malware or being installed with infected firmware is largely increased due to the need to connect a laptop to the ICS devices directly. The risk is further increased because most technicians would use standard corporate laptops to carry out the maintenance or upgrade tasks, where the laptop is also used by the technicians to perform other office-related tasks such as working with documents, reading emails and browsing the Internet. Another aspect that we also need to pay attention to is the source of the updates and patches. If the server hosting the update/patch files is not properly secured, or if the technicians' laptop has been compromised in a certain way, they could end up downloading an infected file, which, in turn, would infect the ICS devices when the upgrade operation is performed.	
Impact	**Likelihood**
Critical: Due to the maintenance, connections usually are directly done with the ICS systems and devices (either locally or through a VPN); therefore the malware or infection can be carried out easily.	**High:** Maintenance is done regularly to ensure the proper operation of the systems; therefore, each time an external system is connected, the network and systems are at risk.
Ease of detection	**Cascading effect risk**
The detection will greatly depend on the security measures in place, as this will determine the chance of detection. Perimeter and network security measures (such as antivirus or IDS) may be able to detect these threats.	Maintenance operations are usually done internally, connecting directly to the systems and bypassing intranet a locally implemented security measures. This leads to the risk of infecting the internal systems and aiding on their expansion, potentially extending to other environments and sectors.

Assets affected	
ICS assets, HMI, data historian, PLCs, Common systems	
Possible attack steps by attackers	
1. The technician decides to use a corporate laptop to update ICS devices, where this laptop is also used to perform office-related tasks such as reading emails and browsing the Internet. 2. An attacker has compromised the server hosting the firmware update file and infect the file with a Remote Access Trojan Horse (RAT) malware. Other patch files hosted by the server may also be infected. 3. The technician, unaware that the firmware file has been infected, download the file and the other patch files and use them to update the ICS devices. This would cause ICS devices to be infected with malware. 4. The malware infection may cause ICS devices to malfunction, create backdoors, or carry out other malicious activities. 5. The infected ICS devices may also spread the infection to other devices, which may result in the modification and corruption of their systems, leading to a crash in the whole system and a full operation halt. 6. At the same time, the infected files downloaded by the technician may also infect the laptop used to download them. That malware running on the laptop may perform the following malicious activities: a) Connects to a C&C server to enable remote access to the attackers. b) Search for information on the infected laptop to find other potential victims and steal business information. c) Use the laptop as a staging point for further infection of other systems. d) Intercept data packets traveling to and from the infected laptop to steal private and sensitive information.	
Recovery time	**Recommendations**
For advanced malware versions, it can take weeks before it is discovered. Furthermore, the recovery of the devices can be complex if the maintenance systems have also been compromised, and a complete clean-up may take **several days**.	It is recommended for the whole chain (from manufacturers and up to the final operators) to understand the security threats they are exposed to, and how they can become an unwilling means of distribution if they do not control their systems and secure their maintenance and operation procedures.

The illustration of this attack is depicted in Figure 5.

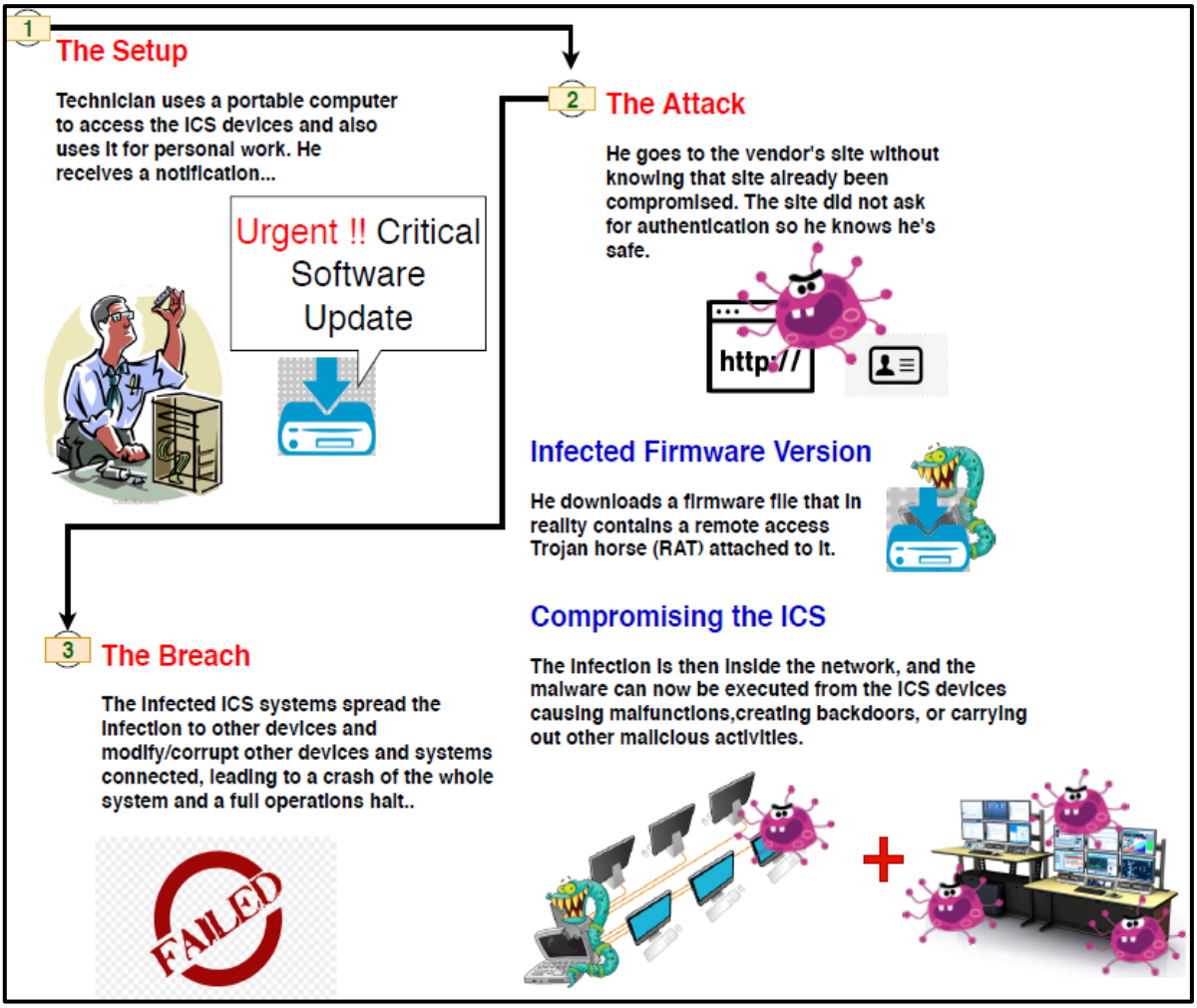


Figure 5: Attack Scenario 3

4.3 A holistic approach to ICS security - People, Process and Technology

For cybersecurity to be effective, organizations should take a holistic approach to manage cybersecurity. A systematic approach used in ISMS is to consider these three aspects: people, process and technology. People refer to individuals who directly or indirectly interact with any of the ICS components, regardless of whether they are employees or vendors. In an organization, people can be assets of greater risks to security, and most of the time, people are the weakest link in the organization concerning security. Ensuring that people can behave securely would increase the security of the whole system.

The process addresses the gap between people and technology. The process ensures the security team has strategies in place to proactively prevent and respond quickly and effectively towards the security events. This aspect is including Risk Assessment. Risk assessment is a term used to describe the overall process or method where you identify hazards and risk factors that have the potential to cause harm (hazard identification), analyze and evaluate the risk associated with that hazard (risk analysis, and risk evaluation) and determine appropriate ways to eliminate the hazard, or control the risk when the hazard

cannot be eliminated (risk control)[11]. Risk assessment needs to be conducted at least annually or as and when required or whichever is earlier due to critical changes in the ICS environment. Security controls derived from the risk assessment exercise should be planned and implemented accordingly. Security controls are not limited to policies, procedures, technologies, and processes. To be effective, security processes also need to be yearly reviewed to address current security threats.

The technology or technical solution facilitates rapid detection and mitigation threats. It can be used as countermeasures to address the security risks in ICS whether it is intentional or due to human errors. In short, technology is facilitated by people and is supporting the processes to run smoothly.

5 Practical guides for securing ICS

This chapter provides guidelines to specifically secure OT, while ISO/IEC 27001 is recommended to be used as a guideline to secure IT systems. NIST specifies 18 Security Control Families, where each family contains security and privacy controls related to the general security topics of the family. These Security Control Families are specified in the document NIST SP 800-53r4. The guidance on how to apply these control families to ICS can be found in the document NIST SP 800-82r2. In this guideline, the Security Control Families are categorized into People, Process and Technology, as a systematic approach adopted by ISMS for holistic security. The categorization is depicted in Table 5.

Table 5: Categorization of NIST Security Control Families into People, Process and Technology

People	Process	Technology
AT – Awareness and Training PS – Personnel Security	CM – Configuration Management CP – Contingency Planning IR – Incident Response MA – Maintenance MP – Media Protection PE – Physical and Environment Protection CA – Security Assessment and Authorization SI – System and Information Integrity PL – Planning SA – System and Services Acquisition PM – Program Management	AC – Access Control AU – Audit and Accountability IA – Identification and Authentication SC – System and Communication Protection

The People category contains Security Control Families that are directly applied to people working in the organization. The Process category contains Security Control Families that specify processes that are going to be continuously practiced and implemented by the organization in its operation to ensure the security of the ICS. Technology contains Security Control Families that describe technical security controls to be implemented on the ICS.

[11] Risk Assessment, https://www.ccohs.ca/oshanswers/hsprograms/risk_assessment.html

The Security Control Families under the People and Process categories are compulsory to be implemented by all organizations that run an ICS. The Security Control Families under the Technology category are selectively applied based on the devices, their functions, and the environment in which they operate. For the purpose of ICS, the application of the Technology Security Control Families can be specified based on the ICS levels and their corresponding Risk Assessment results.

5.1 People, Process and Technology security controls for People and Process

This chapter discusses the recommended security controls and guidance for Security Control Families that are categorized under People and Process. All the security controls highlighted in Table 6 are ICS-specific and they are simplified from the security controls guidance explained in NIST SP 800-82r2. Other security controls specified in NIST SP 800-53r4 may still apply.

Table 6: ICS-specific People and Process Security Controls

No.	Security Control Family	Recommended Security Controls and Guidance
1.	Awareness and Training	1. Identify, document and train all personnel having significant ICS roles and responsibilities. 2. Need to include awareness on control system-specific information and training for ICS applications. 3. Awareness and training should cover the physical process being controlled as well as the ICS
2.	Personnel Security	1. Categorize positions with a risk designation and screening criteria. 2. Ensure that each employee has received training relevant and necessary to his job functions. 3. Ensure that the employees have demonstrated their competence in their job functions.
3.	Configuration Management	1. Document the current ICS network and device configuration. 2. Establish a formal change management program to ensure that all modifications to an ICS network meet the same security requirements as the original components identified in the asset evaluation and the associated risk assessment and mitigation plans. 3. Perform a risk assessment on all changes to the ICS network that could affect security, including configuration changes, the addition of network components and installation of new software.
4.	Contingency Planning	1. Establish contingency plans that include business continuity plans and disaster recovery plans that cover the full range of failures or problems that could be caused by cyber incidents. 2. Periodically review contingency plans with employees responsible for the restoration of the ICS, and test the plans to ensure that they continue to meet their objectives.
5.	Incident Response	Establish an incident response plan that includes the following items: a) Classification of incidents b) Response actions c) Recovery actions
6.	Maintenance	There is no ICS-specific security control and guidance for Maintenance family on top of what is specified in NIST SP 800-53 that provides policy and procedure related to maintenance. NIST SP

		800-82r2 recommends the following documents as supplemental guidance for Maintenance family: a) NIST SP 800-63[12] b) NIST SP 800-100[13]
7.	Media Protection	1. Establish physical security controls to address specific requirements (e.g. loss, fire, theft, unintentional distribution or environmental damage) for the safe and secure maintenance of media assets and provide specific guidance for transporting, handling and erasing or destroying the assets. 2. Prevent the use of any unauthorized removable media such as USB memory sticks on any node that is part of or connected to the ICS.
8.	Physical and Environment Protection	1. Protect physical locations in which the ICS is located using fences, guard, gates and locked doors. 2. Implement access control systems to ensure only authorized people have access to controlled spaces. 3. Implement access monitoring systems which include still and video cameras, sensors, and various types of identification systems. 4. Use asset location technologies to track the movement of people and vehicles within the plant. 5. Prevent ICS devices (e.g. computers, laptops, PLCs, etc) from leaving the ICS area, and prevent them from being used outside the ICS network. 6. Ensure ICS devices to have current antivirus and security patches. 7. Place servers, workstations, switches, routers, network jacks and controllers in locked areas protected with proper authentication mechanisms. Even cable runs should be installed in such a way that access is minimized. 8. Remove or lock removable media drives and disable the USB ports. 9. Disable or physically protect the power buttons to prevent unauthorized use.
9.	System and Information Integrity	1. Use antivirus tools on ICS devices, if feasible. However, its use is subjected to compatibility checks, change management issues and performance impact metrics. 2. Deploy network-based IDS (or IPS) between the control network and the corporate network in conjunction with a firewall. 3. Deploy host-based IDS on computers that use general-purpose operating systems. 4. Test patches adequately on offline comparable ICS before applying them to the online ICS to ensure that they do not have an adverse effect on the ICS system or introduce a new security risk. 5. Separate the automated process for ICS patch management from

[12] Grassi, P., M. Garcia, and J. Fenton. "DRAFT NIST Special Publication 800-63-3 Digital Identity Guidelines." *National Institute of Standards and Technology, Los Altos, CA* (2017).

[13] NIST SP 800-100, Information Security Handbook: A Guide for Managers, http://csrc.nist.gov/publications/PubsSPs.html (2006).

		that of the non-ICS. Patching should only be scheduled during planned ICS outages.
10.	Security Assessment and Authorization	There is no ICS-specific security control and guidance for the Security Assessment and Authorization family on top of what is specified in NIST SP 800-53 that provides the basis for performing periodic assessments and providing certification related to security assessment and authorization in ICS. NIST SP 800-82r2 recommends the following documents as supplemental guidance for Security Assessment and Authorization family: a) NIST SP 800-53A[14] b) NIST SP 800-37[15] c) NIST SP 800-100
11.	Planning	Establish a security plan to address the security of an ICS system throughout its lifecycle, from architecture to procurement to installation to maintenance to decommissioning.
12.	System and Services Acquisition	Apply the organization's security policies and procedures to external suppliers (including second and third-tier suppliers) to maintain the overall level of ICS security.
13.	Program Management	There is no ICS-specific security control and guidance for the Program Management family on top of what is specified in NIST SP 800-53 that focuses on independent information security requirements to manage information security programs that are applicable to all systems including ICS.

5.2 Security controls for Technology

The security controls for technology are different in every layer of ICS. Hence, security controls for ICS Level 0 until Level 3 are given in 5.2.1 until 5.2.4, respectively. The security controls guidance given in these sub-chapters are explained in NIST SP 800-82r2 but have been simplified and managed to suit the ICS levels. On the other hand, other security controls specified in NIST SP 800-53r4 may still apply.

5.2.1 Security controls for ICS Level 0

Conventionally, Level 0 consists of a purely analog communication interface referred to as input/output (I/O), supported by a short-run cable from the actual physical process area. The process can include any type of industrial facility in all industrial sectors. Level 0 also includes the sensors and actuators that are directly connected to the process and process equipment.

Nowadays, Level 0 can also be Fieldbus (digital) and wireless. However, the processes remain almost the same with possibly efficiency and other diagnostic capabilities/features are further improved with the advancement of technology.

Table 7 highlights the recommended ICS-specific security controls and guidance that are relevant for Level 0.

[14] NIST SP 800-53A, Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans, http://csrc.nist.gov/publications/PubsSPs.html (2010)

[15] Barker, Elaine, et al. "Nist special publication 800-57." *NIST Special publication* 800.57 (2007): 1-142.

Table 7: ICS-specific Technology Security Controls for Level 0

No.	Security Control Family	Recommended Security Controls and Guidance
1.	Access Control	Implement physical security control to the environment that contains Level 0 devices to ensure that only authorized personnel is allowed to enter the area.
2.	System and Communication Protection	Most of Level 0 devices only communicate with Level 1 devices. In the case of the Industrial Internet of Things (IIoT) environment, even Level 0 devices may have their IP addresses and, therefore, can be accessed remotely. It is NOT RECOMMENDED to allow direct remote access to IIoT devices. However, if direct remote access is required due to specific requirements, remote access from external users should only be allowed through a VPN in the enterprise zone. From the enterprise zone, access to these Level 0 devices should be done through a remote access server located in the DMZ.

5.2.2 Security Controls for ICS Level 1

Level 1 contains the functions involved in sensing and manipulating the physical process. Process monitoring equipment reads data from sensors, executes algorithms if necessary, and maintains process history. Examples of process monitoring systems include tank gauging systems, continuous emission monitors, rotating equipment monitoring systems, and temperature indicating systems.

Process control equipment reads data from sensors, executes a control algorithm, and sends an output to a final control element (e.g., control valves or motor controls). Level 1 controllers are directly connected to the sensors and actuators of the process. This level includes continuous closed-loop control, sequence control, batch control, and discrete control. Many modern controllers include all types of control in a single device.

Level 1 also includes Safety Instrumented Systems (SIS) and protection systems that monitor the process and automatically return the process to a safe state if it exceeds safe limits. This level also includes systems that monitor the process and alert an operator of impending unsafe conditions. Examples of level 1 equipment are DCS controllers, SIS controllers, PLCs and RTUs. Table 8 below highlights the recommended ICS-specific security controls and guidance that are relevant for Level 1.

Table 8: ICS-specific Technology Security Controls for Level 1

No.	Security Control Family	Recommended Security Controls and Guidance
1.	Access Control	1. Implement physical security control to the environment that contains Level 1 devices to ensure that only authorized personnel is allowed to enter the area. 2. Identify the users who have access to the data, as well as make changes to the configuration of Level 1 devices. 3. Implement Role-based Access Control (RBAC). 4. If the device has an embedded version of Web, FTP or email servers that are used for remote configuration, if

		feasible, use the secure version of the protocol (i.e. HTTPS instead of HTTP). 5. If VLAN is used, assign each automation cell to a single VLAN. 6. If wireless LAN is used, access to the wireless network should be properly secured.
2.	Identification and Authentication	1. For Level 1 devices that support authentication, enable the authentication mechanism. 2. If a password is used, make sure the factory set password is changed. 3. Use a secure password that follows the best-practice of password usage. 4. Multi-factor authentication, if supported, can optionally be implemented for improved security. 5. The use of authentication should not delay the operator from responding to an emergency event.
3.	System and Communication Protection	1. Even if Level 1 devices have their own IP address and can be accessed remotely, it is NOT RECOMMENDED to allow direct remote access to Level 1 devices. However, if direct remote access is required due to specific requirements, remote access from external users should only be allowed through VPN in the enterprise zone. From the enterprise zone, access to these Level 1 devices should be done through a remote access server located in the DMZ. 2. Encryption feature, if supported, should only be implemented if it is required, and if the latency induced from the use of encryption does not affect the performance or availability of the device or system. Typically devices in Level 1 are communicating over serial communication with specific communication protocols. If system and communication protection is required for serial communication, a temper resistant and security-approved device or security solution that produces negligible latency to the communication should be considered.

5.2.3 Security controls for ICS Level 2 and Level 3

Level 2 includes the functions involved in monitoring and supervisory control of the physical process. This includes the functions to manage specific devices and discrete elements of the workflow. Level 2 functions and equipment include operator human-machine interface (HMI), operator alarms and alerts, supervisory control functions, process history collection, and open-loop control with human intervention.

Level 3 includes the functions involved in managing the workflows to produce the desired end products. Examples include production management, energy management, system performance monitoring, detailed production scheduling, reliability assurance, on-line process simulation, and site-wide control optimization. Both levels 2 and 3 contain general purpose computers, which mostly Windows machines

which need to continually patched and updated with antivirus, failing which will be vulnerable to the cyber attack. The only difference is the scope of work done by computers on these two levels.

Table 9 highlights the recommended ICS-specific security controls and guidance that are relevant for Level 2 and 3.

Table 9: ICS-specific Technology Security Controls for Level 2 and 3

No.	Security Control Family	Recommended Security Controls and Guidance
1.	Access Control	1. Implement physical security control to the environment that contains Level 2/3 devices to ensure that only authorized personnel is allowed to enter the area. 2. Identify users who have access to Layer 2/3 devices and data. 3. Implement Role-based Access Control (RBAC). 4. If the device comes with Web, FTP or email servers that are used for remote configuration, if feasible, use the secure version of the protocol (i.e. HTTPS instead of HTTP). 5. If VLAN is used, assign each automation cell to a single VLAN. If wireless LAN is used, access to the wireless network should be properly secured.
2.	Identification and Authentication	1. An authentication mechanism needs to be enabled in all Layer 2/3 devices. 2. If the device comes with a factory-set password, the password needs to be changed. 3. Use a secure password that follows the best-practice of password usage. 4. Multi-factor authentication, if supported, can optionally be implemented for improved security. 5. The use of authentication should not delay the operator from responding to an emergency event.
3.	Audit and Accountability	1. Enable logging in all devices and applications that support logging: application event logging, server event logging, IDS event logging, firewall event logging. 2. Monitor sensors, logs, IDS, antivirus, patch management, policy management software and other security mechanisms on a real-time basis where feasible. 3. Incorporate system auditing utilities. 4. Perform periodic audits to validate: 5. The security controls present during system validation testing (e.g., factory acceptance testing and site acceptance testing) are still installed and operating correctly in the production system. 6. The production system is free from security compromises and provides information on the nature and extent of compromises as feasible, should they occur.
4.	System and Communication Protection	1. Remote access from external users should only be allowed through a VPN in the enterprise zone. From the

		enterprise zone, access to Level 2/3 devices should be done through a remote access server located in the DMZ. *2.* Install Antivirus and patch management Server for Windows machines in case of *island mode operation/ no DMZ.* 3. the Install *Active Directory/ Domain Controller* to manage identity and access control for OT domain 4. Cryptographic protection should be selected based on a risk assessment and the identified value of the information being protected and ICS operating constraints. 5. Install *Back-up Management Server*. 6. Use remote key management. 7. Use separate plaintext and ciphertext ports.

5.2.4 Security controls for ICS DMZ

A DMZ refers to a perimeter network segment that typically interfaces between the control network and the enterprise network. For ICS, the DMZ locates servers that contain data from the ICS in which the data can be accessed from the corporate network. However, the ICS information or data exchange from the external domain is restricted and can only be through a firewall to protect the ICS domain from outside threats. Table 10 shows the recommended ICS-specific security controls and guidance that are relevant for ICS DMZ.

Table 10: ICS-specific Technology Security Controls for ICS DMZ

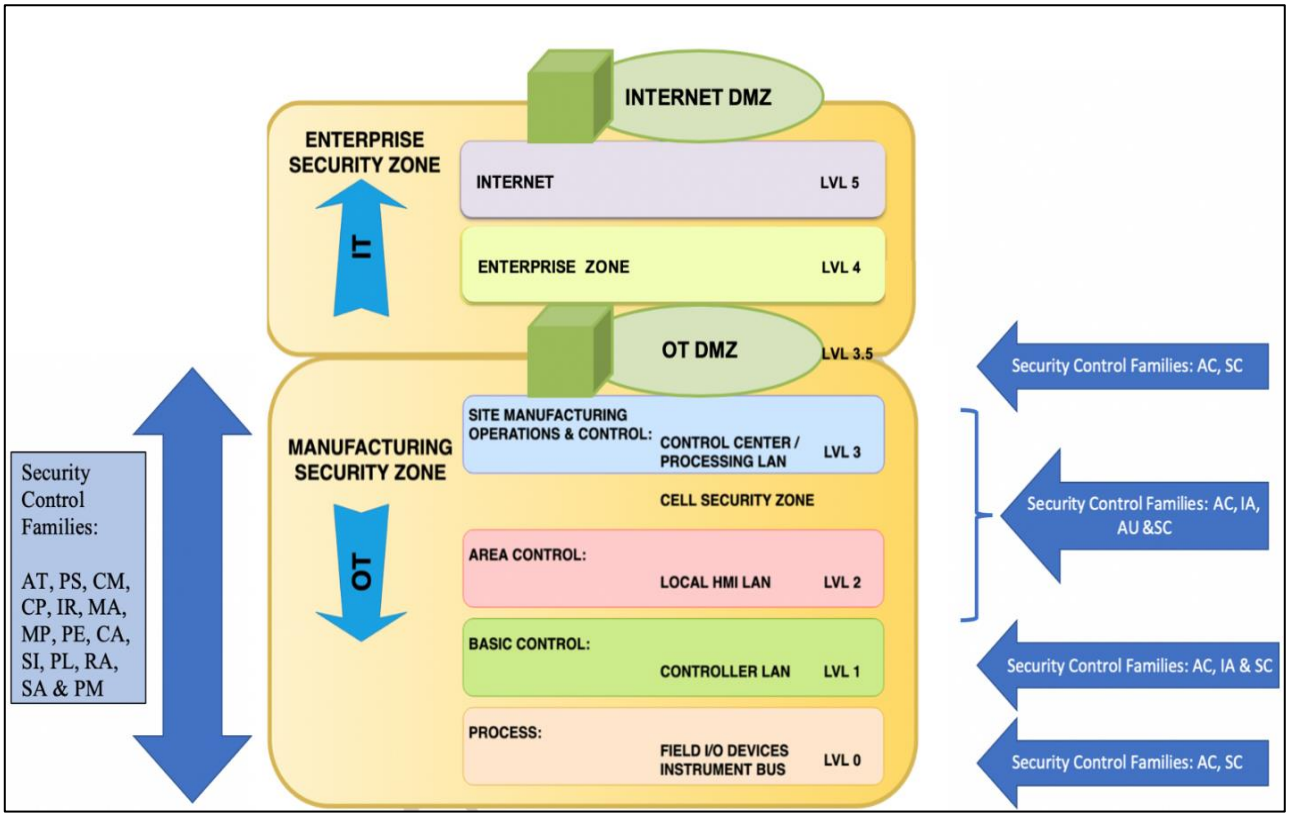
No.	Security Control Family	Recommended Security Controls and Guidance
1.	Access Control	1. Implement boundary protection devices and policies that control the information exchange or access to ICS data from interconnected domains. Only devices that store data that needs to be shared between non-connected networks is allowed. 2. The DMZ connects to the firewall that restricts communication between corporate network and DMZ, and ICS network and DMZ. The most important that the corporate network and ICS network do not communicate directly with each other. No transit traffic is allowed across servers in DMZ. 3. Implement continuous ingress and egress traffic monitoring on the DMZ is recommended. 4. Choice of technology to restrict data flow between Corporate Network and Control Network: a) Dual-homed Computer/Dual Network Interface Cards (NIC) b) A simple two-port firewall c) Use of a router/firewall combination d) Use of firewalls with the ability to establish a DMZ

		e) A variation on the firewall with a DMZ solution using a pair of firewalls f) Data diode
2.	System and Communication Protection	1. Patch management server, an antivirus server and/or other security servers for control network can reside on a single server to allow for controlled and secure updates that are tailored to the specific needs of the ICS environment. a) Domain controller, b) Log controller, c) Remote Access Jumper, d) Secure File Transfer (SFTP) 2. It is recommended that the system such as an antivirus product is not the same as that used for the corporate network to avoid any unforeseen risk. 3. Harden and actively patch all the servers in DMZ.

5.2.5 Summary of security controls for ICS Architecture

Figure 6 shows the summary of the proposed security control families to be applied to ICS with respect to the ICS reference architecture

Figure 6: Security Controls Families for ICS Architecture



Annex A

Impact Level on the security of personal data processing

Level of Impact	Descriptions
Low	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, loss of resources, etc.).
Very High	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

As indicated from the descriptions above, the level of impact is always co-related to the consequences that a personal data security breach might have to the individuals (whose data have been breached)[16].

[16] Guidelines for SMEs on the security of personal data processing, https://www. enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

Annex B

Likelihood Level on the security of personal data processing

Likelihood	Frequency	Ease of misuse and motivation
Very High	Very often, occurs more often than every 10th connection, i.e. more frequently than 10% of the time/cases.	Can be done without any knowledge about the system; or without any additional equipment being used; or it can be performed by wrong or careless usage.
High	Quite often. Occurs between 1 % and 10 % of the time/cases.	Can be done with minor knowledge about the system; or without any additional equipment being used; or it can be performed by wrong or careless usage.
Moderate	May happen. Occurs between 0.1 % and 1 % of the time/cases.	Normal knowledge about the system is sufficient; or normally available equipment can be used; or it can be performed deliberately.
Low	Rare. Occurs less than 0.1 % of the time/cases.	Detailed knowledge about the system is needed; or special equipment is needed; or it can only be performed deliberately and by help of internal personnel.

The likelihood levels can be described as frequency values or concerning how easy it is for a person to exploit a threat. For some threats, it is easier to think of the likelihood in the form of frequency or probability value. This may often be the case for threats related to availability, e.g. caused by problems in software or hardware. For other threats, it is easier to think of likelihood when related to ease of misuse or mistake, or to motivation for performing a malicious action. For each threat or unwanted incident, we choose the most appropriate column or the column that is easiest to use in order to estimate the likelihood of the threat[17].

[17] Definition of likelihood, consequence and risk levels https://ehealthresearch.no /files/documents/Appendix-Definitions.pdf

Bibliography

[1] Force, J. T., & Initiative, T. (2013). Security and privacy controls for federal information systems and organizations. *NIST Special Publication*, *800*(53), 8-13.

[2] Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to industrial control systems (ICS) security. *NIST special publication*, *800*(82), 16-16.

[3] Disterer, Georg. "ISO/IEC 27000, 27001 and 27002 for information security management." (2013).

[4] Valladares, Cindy. "Critical Security Controls: Control 7—Wireless Device Control"." *Tripwire—The State of Security, tripwire.com* (2013).

[5] ISA-99 Committee, ISA-62443 series of standard: *Security for Industrial Automation and Control Systems, International* Electrotechnical Commission (IEC) (2010).

[6] AC11069413, Anonymus, ed. *COBIT 5: A business framework for the governance and management of enterprise IT*. Isaca, (2012).

[7] Byres, Eric, P. Eng, and I. S. A. Fellow. "Using ANSI/ISA-99 standards to improve control system security." *White paper, Tofino Security* (2012).

[8] Homeland Security, Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf (2016)

[9] NCCIC, ICS-CERT Annual Assessment Report Industrial Control Systems Cyber Emergency Response Team FY 2016, https://www.us-cert.gov/sites/default/files/Annual_Reports/FY2016_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf (2016)

[10] NCCIC, ICS-CERT Monitor November/December 2017, https://www.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Nov-Dec2017_S508C.pdf (2017)

[11] Risk Assessment, https://www.ccohs.ca/oshanswers/hsprograms/risk_assessment.html

[12] Grassi, P., M. Garcia, and J. Fenton. "DRAFT NIST Special Publication 800-63-3 Digital Identity Guidelines." *National Institute of Standards and Technology, Los Altos, CA* (2017).

[13] NIST SP 800-100, Information Security Handbook: A Guide for Managers, http://csrc.nist.gov/publications/PubsSPs.html (2006).

[14] NIST SP 800-53A, Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans, http://csrc.nist.gov/publications/PubsSPs.html (2010)

[15] Barker, Elaine, et al. "Nist special publication 800-57." *NIST Special publication* 800.57 (2007): 1-142.

[16] Guidelines for SMEs on the security of personal data processing, https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

[17] Definition of likelihood, consequence and risk levels https://ehealthresearch.no/files/documents/Appendix-Definitions.pdf

Acknowledgments

CyberSecurity Malaysia would like to express our appreciation and gratitude to all members who have participated tirelessly in the development of this guideline. Members of Technical Committee on Guidelines for Secure Industrial Control System (ICS) are as follows:

Ts. Dr. Zahri Yunos/	Cybersecurity Malaysia
Ts. Dr. Solahuddin Shamsuddin/	
Ts. Dr. Maslina Daud/	
Mr. Abdul Fuad Abdul Rahman/	
Mr. Ahmad Hazazi Zakaria/	
Mr. Mohd Faizal Sulong/	
Mr. Muhammad Syahmi Azri Zulkefle/	
Ms. Norahana Salimin/	
Mr. Norhamadi Ja'affar/	
Ms. Nurul A'qilah Hasmizi/	
Mr. Suhairi Mohd Jawi/	
Ms. Ummu Khosyatillah Muzakir	
Ts. Dr. Muhammad Farid Daud/	German- Malaysia Institute
Ts. Ahmad Hafiz Mohd Hashim	
Ir. Michael Ng Chien Han/	PETRONAS
Mr. Azmi Hashim/	
Mr. Shahrul A Rashid/	
Mr. Raihan Ahmad	
Mr. Abdul Halim Johar @ Mazahar/	PRASARANA
Mr. Nik Quosthoni Kamalul Baharin	
Ms. Raja Noraila binti Raja Abdul Rahim	Suruhanjaya Tenaga
Mr. Lukman Hakim Omar/	Universiti Kuala Lumpur
Mr. Yusof Mohd Ekhsan	
Prof. Dr. Izham Datuk Zainal Abidin/	Universiti Tenaga Nasional
Assoc. Prof Dr. Asmidar Abu Bakar/	
Assoc. Prof Dr. Salman Yussof/	
Dr. Ziana Jamil	