# CYBER SECURITY GUIDELINE FOR INDUSTRIAL CONTROL SYSTEM

CyberSecurity Malaysia

November, 2019

**REGISTERED OFFICE:**
CyberSecurity Malaysia,
Level 7 Tower 1,
Menara Cyber Axis,
Jalan Impact,
63000 Cyberjaya,
Selangor Darul Ehsan, Malaysia



**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 (ICS). 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 ICS advisor before taking any action based on information appearing on this guideline or any other documents to which it may be linked.

## PUBLIC COMMENT

You may submit electronic comments and suggestions at any time for CyberSecurity Malaysia consideration to ics@cybersecurity.my. Comments may not be acted upon by CyberSecurity Malaysia until the document is next revised or updated.

## ACKNOWLEDGEMENT

CyberSecurity Malaysia wishes to thank the following individuals who have contributed and/ or reviewed this document.

External Contributors/ Reviewers:

Internal Contributors/ Reviewers:

# CONTENTS

# 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 results in people safety, environmental degradation, asset damage and/or production disruption and/or reputational loss. This guideline is developed to provide a reference for holistic 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.

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 more 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 [1], NIST SP 800-82r2 [2], ISO/IEC 27001 [3], CIS CSC [4], ISO/IEC 62443-2-1 [5] and COBIT 5 [5].

## 1. Scope

In this guideline, the ICS-specific security controls are majorly 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 [6]. The emphasis of this security guideline is on level 0 until level 3 of the ICS reference architecture.

## 2. Target Audience

This guideline is not intended to provide a comprehensive background information on ICS and ICS security in any of its chapter 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 has 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 wants to learn more about practical implementation of ICS security.
d) Vendors who are in charge in ICS business.

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.

## 3. Terms and Definition

For the purposes of this document, the following terms and definitions apply.

**3.1**
**asset**
anything that has value to the organization

[ISO/IEC 13335-1:2004]

**3.2**
**availability**
the property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 13335-1:2004]

**3.3**
**confidentiality**
the property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 13335-1:2004]

**3.4**
**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]

**3.5**
**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.

**3.6**

**integrity**

the property of safeguarding the accuracy and completeness of assets

[ISO/IEC 13335-1:2004]

**3.7**

**risk assessment**

overall process of risk analysis and risk evaluation

[ISO/IEC Guide 73:2002]

## 4. Abbreviated terms

| | |
|---|---|
| APT | Advanced Persistent Threats |
| CI | Critical Infrastructure |
| DCS | Distributed Control Systems |
| DH | Data Historian |
| EW | 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 | 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 |

# 5. Chapter 1: Overview of 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 increase the operational and cost efficiency, but opens up to more threats that could lead to system unavailability and espionage.

## 5.1 Types of ICS

ICSs 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 few types of ICS as listed below:

### 5.1.1 Process Control System (PCS)

a) 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.

b) 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).

### 5.1.2 Distributed Control Systems (DCS)

a) DCS controls multiple automation processes of a single site/plant. A DCS may monitor and supervise several PCSs at a plant. DCS also may control all factory automation. Example of DCS include the control processes at oil refineries, drinking water and wastewater treatment

plants, and car assembly lines. A DCS communications can be characterized as process-driven polling between a HMI and PLC within a small geographic area.

### 5.1.3 Supervisory Control and Data Acquisition (SCADA)

a) SCADA collects data and monitors automation across geographic areas which can be thousands of miles apart. SCADA system may supervise on or more DCSs or PCSs, hence they may use different communications methods than a DCS or PCS.

b) SCADA systems support coordination of infrastructure rather than exercising control over the discrete element of these infrastructures.

### 5.1.4 Safety Instrumented Systems (SIS)

a) SIS are 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 are dedicated to process safety.

b) 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 unsafe 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

## 5.2 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 control system components in ICS, there are few of them as listed below.

### 5.2.1 Programmable Logic Controller (PLC)

a) PLC- a microprocessor-controlled electronic device which 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.

b) 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.

### 5.2.2 Remote Terminal Unit (RTU)

a) 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 communicate with the control center may d on event-based. The RTU also can be programmed to take control actions independently of the control center.

b) 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.

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

### 5.2.3 Intelligent electronic device (IED)

a) 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.

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

c) Examples of IEDs are protective relay and voltage regulator, which used for substation automation in 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.

### 5.2.4 Human-machine interface (HMI)

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

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

### 5.2.5 Data Historian (DH)

a) 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.

b) 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.

### 5.2.6 Business information consoles and dashboards

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

b) Data comes from HMI or data historian systems.

### 5.2.7 Engineering Workstation (EW)

a) 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.

## 5.3 ICS Protocols

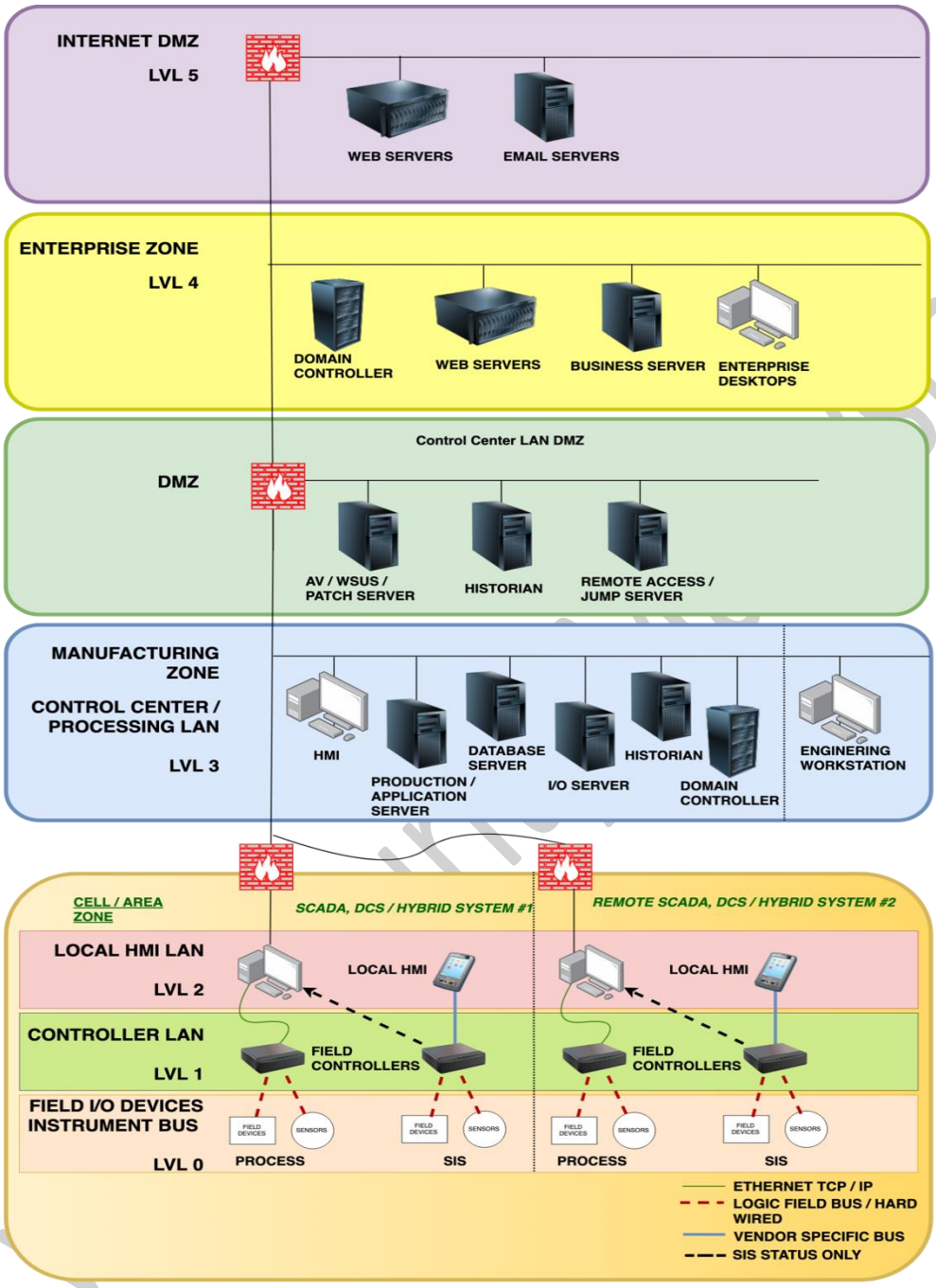
There are various proprietary and nonproprietary protocols used in ICS, for example:

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.

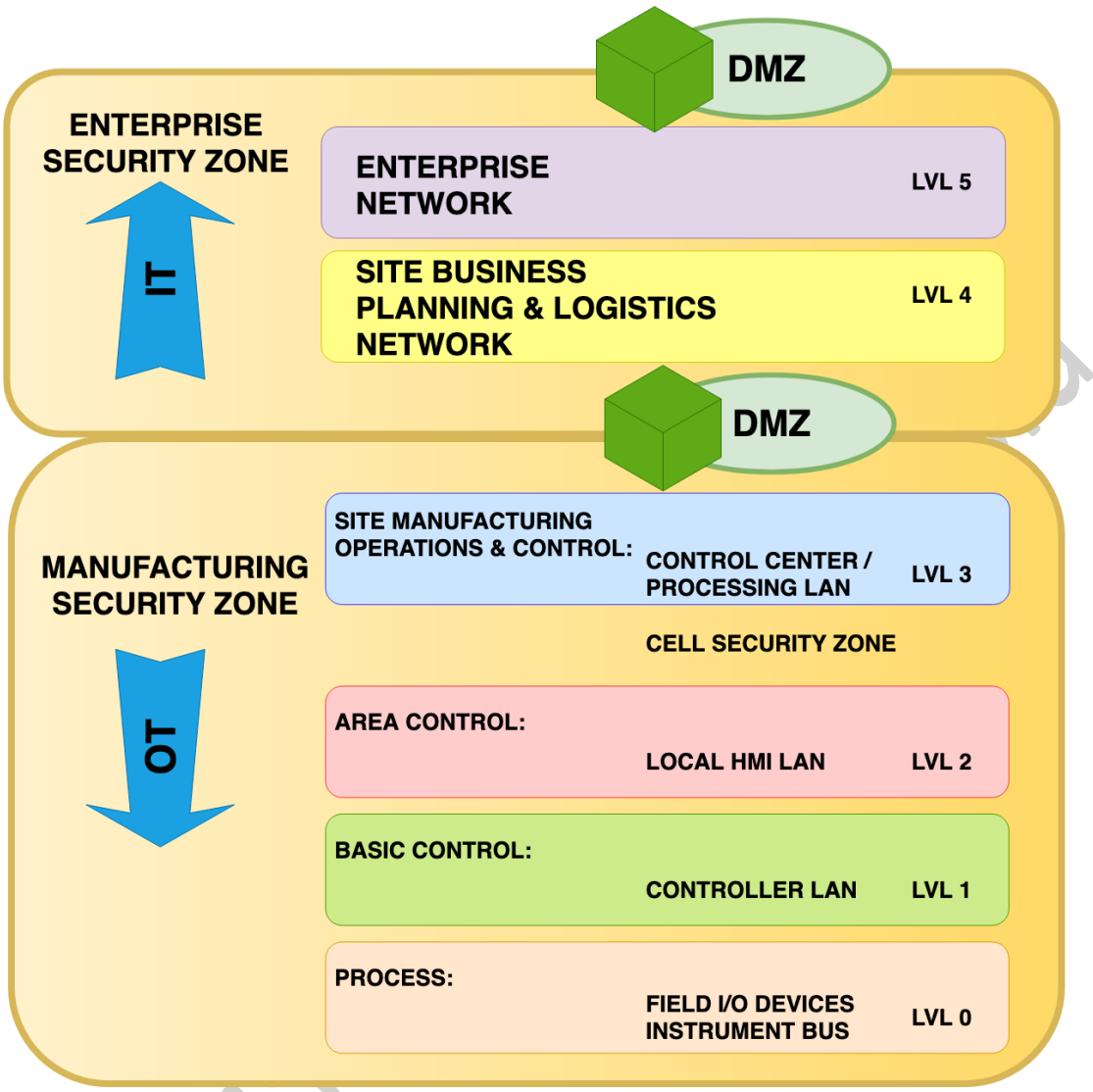
Some of the protocols have been adapted to operate over Ethernet and TCP/IP networks. This enables data from ICS to be transmitted over the public Internet. Example of protocols that operated over Ethernet and TCP/IP are Modbus over TCP/IP, DNP3 over TCP/IP, IEC 60870-5-104. These protocols are treated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

## 5.4 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.




262 **Figure 1: ICS Reference Architecture**




263 **Figure 2: The zone segmentation of business and ICS architecture**

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

### 5.4.1 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). There are many risks exist in this zone due to numerous connectivity and systems involved, hence this zone is considered as untrusted.

### 5.4.2 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 high risk and the risks are associated with its direct connectivity to any external systems or networks.

### 5.4.3 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 devices in level 1 support Transmission Control Protocol/ Internet Protocol (TCP/IP) and other common protocols. Whereas level 0 place 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.

### 5.4.4 Demilitarized Zones

This zone which is also known as a perimeter network is a physical and logical sub network that acts as an intermediary for connected security devices so that they evade exposure to a larger 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 [12].

# 6. Chapter 2: ICS Security

This chapter discusses Advanced Persistent Threats (APT) to ICS which may weaken the ICS system. The findings were based on 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 review and network traffic analyses [14].

## 6.1 Top Six Weaknesses in ICS

Table 1 list the top weaknesses and their 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 [13].

**Table 1: Top ICS Weaknesses and Their Security Risks**

| 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<br>2. Weaker boundaries between ICS and enterprise networks. |
| 2. 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<br>2. Increased difficulty in securing accounts as personnel leave the organization, especially |

| | | |
|---|---|---|
| | | sensitive for users with administrator access |
| 3. 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.<br>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 organisation's assets that include data, hardware, software and process. | 1. Unauthorized physical access to field equipment and locations provides increased opportunity to:<br>a. Maliciously modify, delete, or copy device programs and firmware<br>b. Access the ICS network<br>c. Steal or vandalize cyber assets<br>d. Add rogue devices to capture and retransmit network traffic |
| 5. Account Management | Management of access to organisation's particular accounts that maintain relationship between the organization and its users. | 1. Compromised unsecured password communications<br>a. Password compromise could allow trusted unauthorized access to systems. |
| 6. Least Functionality | Controls associated with minimizing the computing resources of systems functions, ports, protocols, and services to only those required to support system essential operations. | 1. Increased vectors for malicious party access to critical systems Rogue internal access established |

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 usually 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 concern issue was the attrition of the skilled staff, which is extremely important in securing the ICS. 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 [14]. The information from Table 1 can be used a reference for organizations to focus their effort in 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.

## 6.2 Possible ICS Security Attacks

Due to the security weaknesses as described in 8.1 above, it is possible for various security attacks to be conducted on ICS. According to 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 scenario are re-presented 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 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 as 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 are 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 | Internal staff and contractors have access to internal systems (including critical |

| | |
|---|---|
| identify the source, which allows them to pass undetected for long periods of time and are also complex to investigate and recover from. | 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 their cease. |

**ASSET 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 centre and installations.
2. The employee with malicious intent to compromise organization's operational facilities, used either own or forged credentials.
3. Equipped with privileged knowledge on organization's network and systems, the employee by passed the defence and performed data theft stealing sensitive information.
4. Organization's operations are disrupted with the access gained to several ICS systems, where employee 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 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, in average, to return to standard operations. | Recommendations:<br>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.

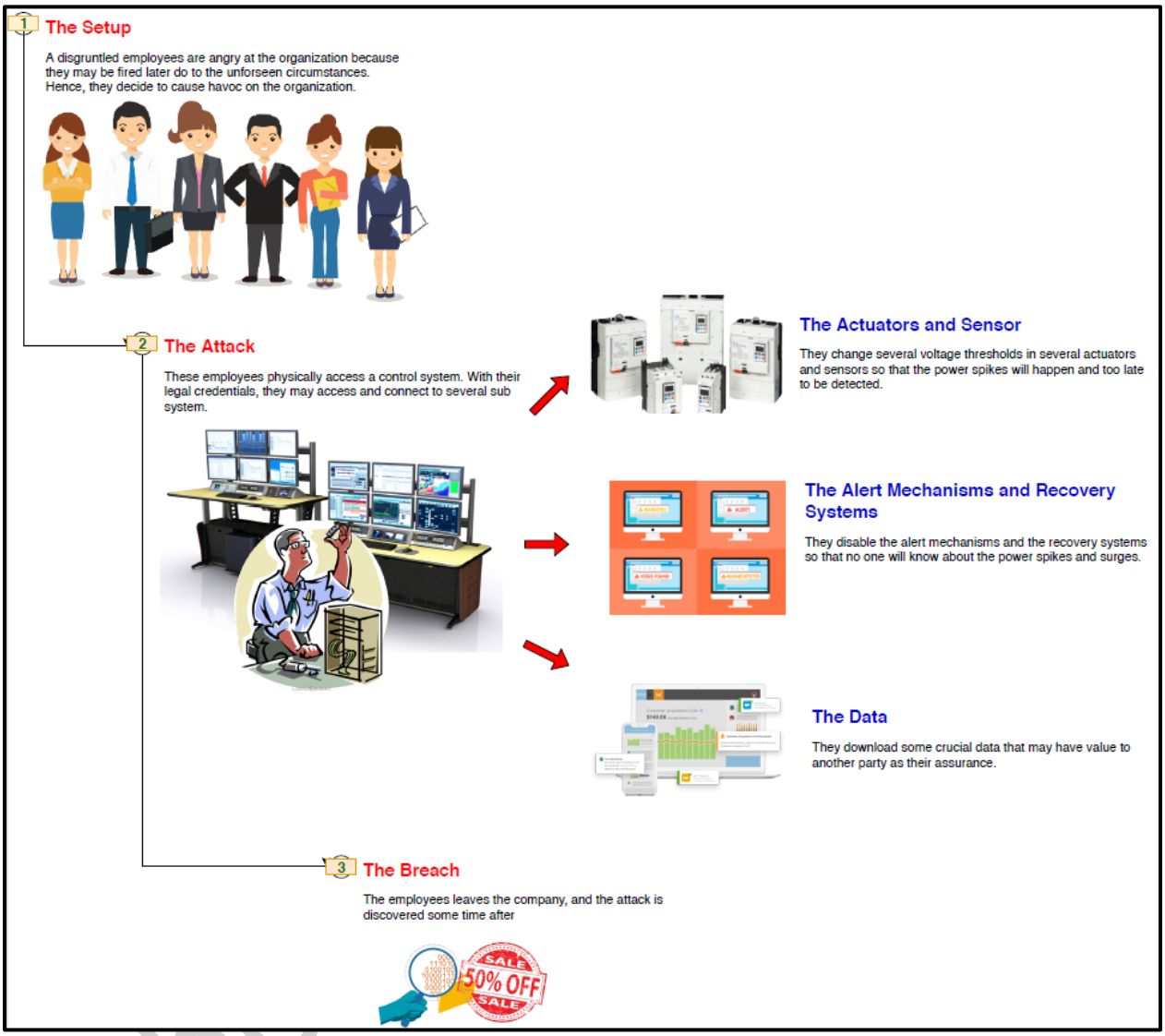


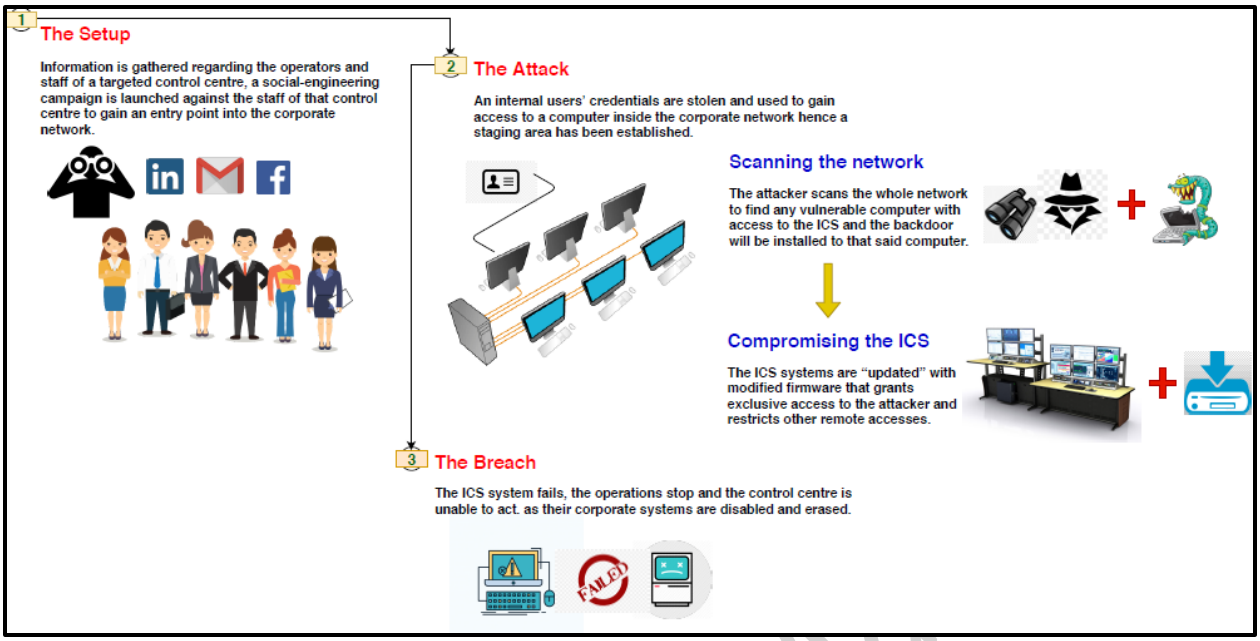

**Figure 3: Attack Scenario 1**

332 **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 cause undesired effects on assets such as malfunction, corruption, or physical damage. This attacks also will affect the overall infrastructure and system. | |
| **IMPACT** | **LIKELIHOOD** |
| **Critical**: The compromise of ICS systems can cause them to 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.). |
| **ASSET AFFECTED** | |
| ICS systems, HMI (Human-Machine Interfaces), Centralised Control System | |

| ATTACK STEPS | |
|---|---|
| 1. The attacker gathers information on the target organization and the relevant, targeted control centre.<br>2. Information regarding the operators and staff of the control centre is gathered, and the attacker will launch a social engineering campaign to gain an entry point into the corporate network.<br>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.<br>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.<br>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.<br>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.<br>7. Once been compromised, the ICS systems are "updated" with modified firmware that permits exclusive access to the attacker and confines other remote accesses.<br>8. This makes the ICS assets to be reconfigured, which make the whole system collapse.<br>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.<br>10. Lastly, when the ICS collapse, the operations stop, and the control centre is unable to act since their corporate systems are deactivated and removed. | |
| **RECOVERY TIME** | **RECOMMENDATIONS** |
| 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). | Recommendations:<br>Need for restricting physical access to ICS networks components in order to reduce the risk of unauthorized access to them. The use of anomalous behaviour detection systems and active system monitoring and logging are good protection measures for this attack. |

333 The illustration of this attack is depicted in Figure 4.



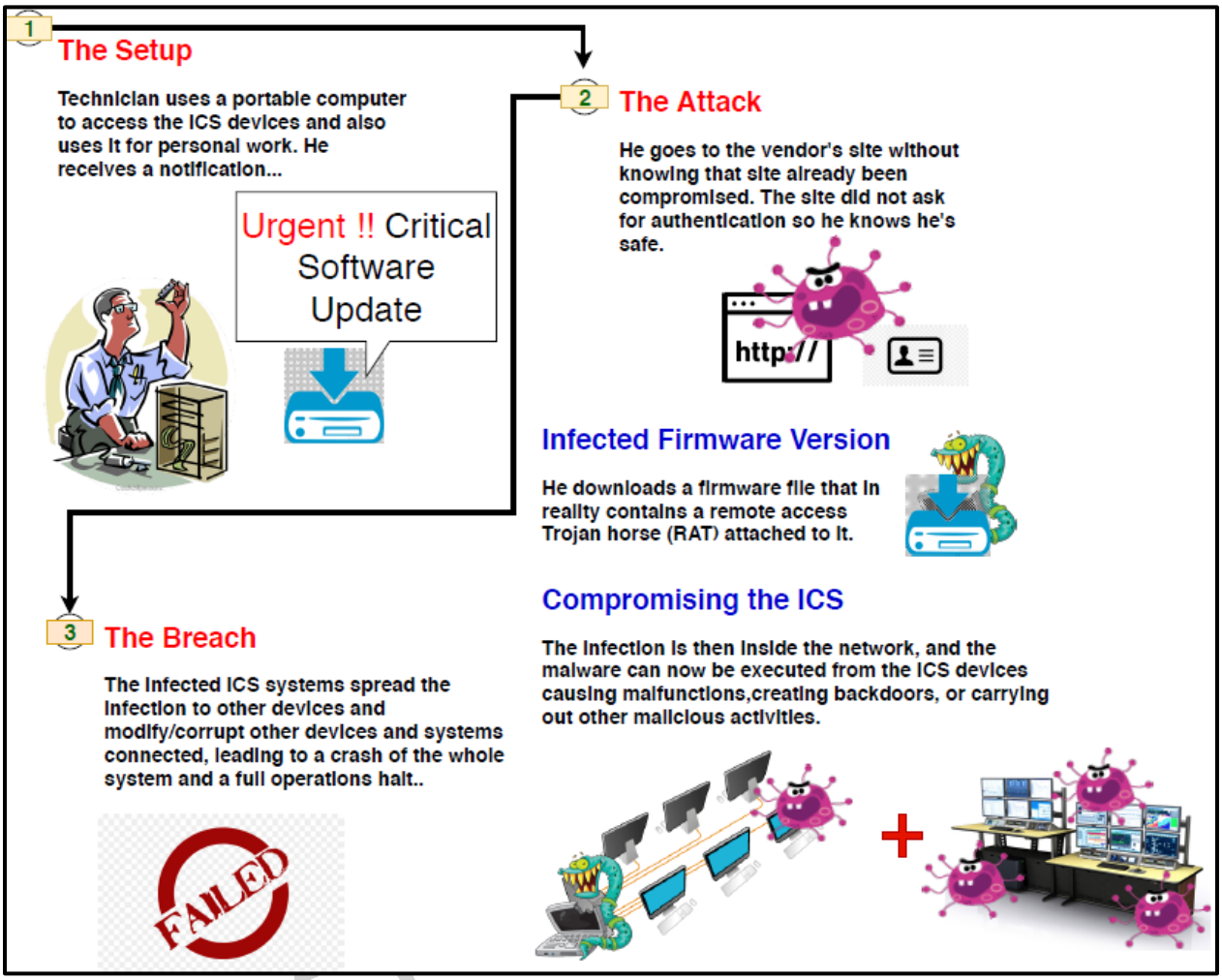

334 **Figure 4: Attack Scenario 2**

335 **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.<br><br>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 directly connect a laptop to the ICS devices. The risk is further increased due to the fact that most technicians would use standard corporate laptop 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.<br><br>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 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 on a regular basis in order 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** |
| 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. |
| **ASSET AFFECTED** | |
| ICS assets, HMI, data historian, PLCs, Common systems | |

| ATTACK STEPS | |
|---|---|
| 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.<br>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.<br>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 the ICS devices to be infected with the malware.<br>4. The malware infection may cause the ICS devices malfunction, create backdoors, or carry out other malicious activities.<br>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.<br>6. At the same time, the infected files downloaded by technician may also infect the laptop used to download them. That malware running on the laptop may perform the following malicious activities:<br>a. Connects to a C&C server to enable remote access to the attackers.<br>b. Search for information on the infected laptop to find other potential victims and steal business information.<br>c. Use the laptop as a staging point for further infection of other systems.<br>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**. | Recommendations:<br>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. |

336 The illustration of this attack is depicted in Figure 5.




337 **Figure 5: Attack Scenario 3**

### 6.3 A Holistic Approach to ICS Security - People, Process and Technology

For cybersecurity to be effective, organizations must take a holistic approach in managing cybersecurity. A systematic approach used in ISMS is to consider these three aspects: people, process and technology. People refers to individuals who directly or indirectly interact with any of the ICS components, regardless of whether they are employees or vendors. Most of the times, people are the weakest link in the organization with respect to security. Ensuring that people are able to behave securely would definitely increase the security of the whole system. Process addresses the gap between people and technology. To address the security of an organization, first things to do is 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) [17]. Risk assessment needs to be conducted at least annually or as and when required or whichever is earlier due to critical changes in 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 need to be yearly reviewed to address the current security threats. Technology refers to technical solutions that be used as countermeasures to address the security risks in ICS whether it is intentional or due to human errors.

# 7. Chapter 3: Practical Guides for Securing ICS

This chapter provides guidelines to specifically secure OT, while ISO/IEC 27001 [7] 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<br><br>PS – Personnel Security | CM – Configuration Management<br><br>CP – Contingency Planning<br><br>IR – Incident Response<br><br>MA – Maintenance<br><br>MP – Media Protection<br><br>PE – Physical and Environment Protection<br><br>CA – Security Assessment and Authorization<br><br>SI – System and Information Integrity<br><br>PL – Planning<br><br>SA – System and Services Acquisition<br><br>PM – Program Management | AC – Access Control<br><br>AU – Audit and Accountability<br><br>IA – Identification and Authentication<br><br>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. The Technology contains Security Control Families that describe technical security controls to be implemented on the ICS.

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, application of the Technology Security Control Families can be specified based on the ICS levels.

## 7.1 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**

| 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.<br>2. Need to include awareness on control system specific information and training for ICS applications.<br>3. Awareness and training must cover the physical process being controlled as well as the ICS. |
| 2. Personnel Security | 1. Categorize positions with a risk designation and screening criteria.<br>2. Ensure that each employee has received training relevant and necessary to his job functions.<br>3. Ensure that the employees have demonstrated their competence in their job functions. |
| 3. Configuration Management | 1. Document current ICS network and device configuration.<br>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.<br>3. Perform 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.<br>2. Periodically review contingency plans with employees responsible for restoration of the ICS, and test the plans to ensure that they continue to meet their objectives. |
| 5. Incident Response | 1. Establish an incident response plan that includes the following items:<br>a) Classification of incidents<br>b) Response actions<br>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:<br><br>a) NIST SP 800-63 [8]<br>b) NIST SP 800-100 [9] |
| 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.<br>2. Implement access control systems to ensure only authorized people have access to controlled spaces.<br>3. Implement access monitoring systems which include still and video cameras, sensors, and various types of identification systems.<br>4. Use asset location technologies to track the movement of people and vehicles within the plant.<br>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.<br>6. Ensure ICS devices to have current antivirus and security patches.<br>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.<br>8. Remove or lock removable media drives and disable the USB ports.<br>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.<br>2. Deploy network-based IDS (or IPS) between the control network and the corporate network in conjunction with a firewall.<br>3. Deploy host-based IDS on computers that use general-purpose operating systems.<br>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.<br>5. Separate the automated process for ICS patch management from 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 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:<br><br>1. NIST SP 800-53A [10]<br>2. NIST SP 800-37 [11]<br>3. NIST SP 800-100 [9] |
| 11. Planning | 1. 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 | 1. 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 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. |

## 7.2 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 9.2.1 until 9.2.4, respectively. The security controls guidance given in these sub-chapters are explained in NIST SP 800-82r2 but has 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.

### 7.2.1 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 infrastructure under management to the control device at Level 1. This is where the actual physical process occurs. 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 discreet and wireless. However, the processes remain almost the same with possibly efficiency and other capabilities/features are further improved with the advanced of technology.

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

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

| 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 are 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 Industrial Internet of Things (IIoT) environment, even Level 0 devices may have their own 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 requirement, remote access from external users should only be allowed through VPN in the enterprise zone. From the enterprise zone, access to these Level 0 devices must be done through a remote access server located in the DMZ. |

### 7.2.2 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. Level 1 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 include 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.

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

| 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 are allowed to enter the area.<br>2. Identify the users who have access to the data, as well as make changes to the configuration of Level 1 devices.<br>3. Implement Role-based Access Control (RBAC).<br>4. If the device has 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).<br>5. If VLAN is used, assign each automation cell to a single VLAN.<br>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.<br>2. If password is used, make sure the factory set password is changed.<br>3. Use secure password that follows the best-practice of password usage.<br>4. Multi-factor authentication, if supported, can optionally be implemented for improved security.<br>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 requirement, 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 must be done through a |

| | |
|---|---|
| | remote access server located in the DMZ.<br>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.<br>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. |

### 7.2.3 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 is the highest level where the ICS availability requirement dominates over confidentiality requirements of typical IT systems. 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 level 2 and 3 contain general purpose computers, and therefore from security standpoint, may have the same security risks. The only difference is the scope of work done by computers in these two levels.

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

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

| 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 are allowed to enter the area.<br>2. Identify users who have access to Layer 2/3 devices and data.<br>3. Implement Role-based Access Control (RBAC).<br>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).<br>a. 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. Authentication mechanism needs to be enabled in all Layer 2/3 devices.<br>2. If the device comes with factory set password, the password needs to be changed.<br>3. Use secure password that follows the best-practice of password usage.<br>4. Multi-factor authentication, if supported, can optionally be implemented for improved security.<br>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.<br>2. Monitor of sensors, logs, IDS, antivirus, patch management, policy management software and other security mechanisms in real-time basis where feasible.<br>3. Incorporate system auditing utilities.<br>4. Perform periodic audits to validate:<br>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.<br>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 VPN in the enterprise zone. From the enterprise zone, access to Level 2/3 devices must be done through a remote access server located in the DMZ.<br>2. If encryption is required, encryption at OSI Layer 2 (instead of Layer 3) should be considered, if possible.<br>3. Use cryptographic system approved by an authorized body, such as NIST/ Communications Security Establishment (CSE) through Cryptographic Module Validation Program (CMVP).<br>4. Cryptographic protection should be selected based on a risk assessment and the identified value of the information being protected and ICS operating constraints.<br>5. Encryption hardware should be temper resistant and uncontrolled electronic connections.<br>6. Use remote key management.<br>7. Use separate plaintext and ciphertext ports. |

### 7.2.4 Security Controls for ICS DMZ

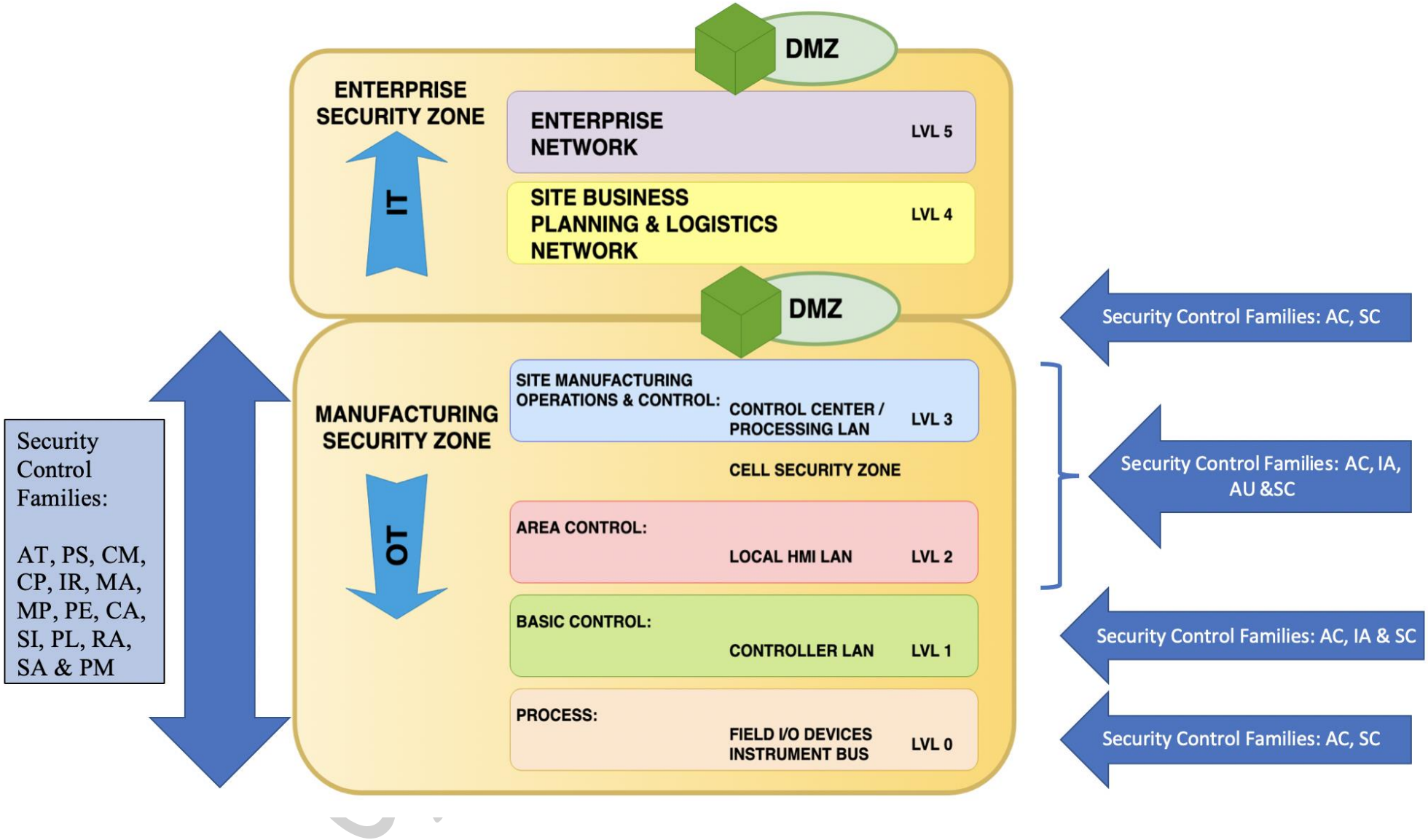
A DMZ refers to a perimeter network segment that typically connects two or more networks. For ICS, the DMZ locates servers that contains data from the ICS in which the data can be accessed from the corporate network. However, the ICS information or data exchange from external domain is restricted and can only be through 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.

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

| 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.<br>2. The DMZ connects to the firewall that restrict communication between corporate network and DMZ, and ICS network and DMZ. Most importantly that the corporate network and ICS network do not communicate directly with each other. No transit traffic is allowed across servers in DMZ.<br>3. Implement continuous ingress and egress traffic monitoring on the DMZ is recommended. |
| 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 is tailored to the specific needs of ICS environment.<br>2. It is recommended that the system such as antivirus product is not the same as that used for the corporate network to avoid any unforeseen risk.<br>3. Harden and actively patch all the servers in DMZ. |

443 **7.2.5 Summary of Security Controls for ICS Architecture**

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




446 **Figure 6: Security Controls Families for ICS Architecture**

# References


[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] 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).

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

[10] 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)

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

[12] 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)

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

[14] 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)

[15] 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

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

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

## Appendix A

Impact Level

| 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, 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)[15].

## Appendix B

Likelihood Level

| 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 with respect to 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 a 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 for the threat [16].

# FEEDBACK FORM

## CYBER SECURITY GUIDELINE FOR INDUSTRIAL CONTROL SYSTEM

File name: MYVAC-3-FRM-1-ICS-V1

Document classification: Confidential

| | |
|---|---|
| **Name** | |
| **Organization** | |

Please return this document to:
ics@cybersecurity.my

Instruction to fill out this feedback form are as follows:

| Field | Description |
|---|---|
| **Section** | Indicate the section to which your comment refers.<br><br>Please choose ***General*** in this column if your comment:<br>i. refers to the whole document, or<br>ii. does not refer to any section of the document. |
| **Line number** | Indicates the line number to which your comment refers. |
| **Figure/Table** | Indicate the figure or table to which your comment refers. |
| **Type of comment** | Choose the type most relevant for your comment.<br><br>The following types are available:<br>- general (ge)<br>- technical (te)<br>- editorial (ed)<br><br>Only enter the short form for the type: **ge**, **te** or **ed**. |
| **Comment** | Enter your comment in this column and explain the reason for the comment.<br><br>If you wish to submit figures or complex objects in addition to the textual comments on the particular section, insert them as separate pages. |
| **Proposed change** | If appropriate, enter a modified version of the section or sentence in this column. |

| **Section** (e.g. 3.1) | **Line number** (e.g. 17) | **Figure/ Table** (e.g. Table 1) | **Type of comment** **ge** = general **te** = technical **ed** = editorial | **Comments** | **Proposed changes** |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |

| |
|---|
| **Other comments (if any):** |
| **By signing this form, I hereby acknowledge that I have read and understand the "Cyber Security Guideline for Industrial Control System". My comments towards this document are as mentioned above.**<br><br>**Signature:**<br><br>……<br>**Name:**<br><br>**Date:** |



**THANK YOU FOR YOUR TIME HAVE A PLEASANT DAY**

**---END OF DOCUMENT---**