CyberSecurity MALAYSIA

First edition
2020-05-05

Guidelines for Secure Industry 4.0

Reference number:
MyVAC-3-GUI-4-IR4-v1

REGISTERED OFFICE:

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

Contents Page

1 Introduction

Industry 4.0 often called "smart factory" and digitalization, is envisioned as an environment of interconnected cyber physical systems with added intelligence and visualisation, in making decentralized decisions, and perform tasks autonomously. It enables real-time data to quickly change how work is organized, how resources are used and scheduling of processes, in producing better products or services, in less time, at greater cost saving.

These functions apply during manufacturing of a product as well as during subsequent handling, up to continuous monitoring of the product lifecycle. This can include intelligent transport and logistics (smart mobility, smart logistics) and resource (electricity, water, oil, etc) utilization.

Industrial machine manufacturers are producing more Industrial Internet of Things (IIoT), with sensors, instruments and devices that are more interconnected. Threat vectors exists within support system such as Heating, Ventilation and Air conditioning system (HVAC), Closed-circuit TV (CCTV), door access systems, that are plagued with default passwords and configurations as well as unencrypted sessions that can easily be exploited. A classic example was the Mirai botnet that turned millions of CCTV into DDoS arsenal. Core systems such as Industrial Control Systems (ICS), Supervisory Control and Data Acquisition System (SCADA) and robotics systems are leveraging on legacy systems that are vulnerable to targeted attacks, given enough motivation, operations can be disrupted and information stolen. Manufacturing production plants that utilizes these machineries are expected to understand the impact of the growing interconnectivity within the plant and the supply chain, and able to establish requirements in safeguarding security in their operations.

Machineries in production plants, including mechanical and engineering facilities, are more connected to the Internet of Things (IoT) and Industrial Internet of Things (IIoT), and at some point, interacting with other office and company networks. Notifications are instantaneously sent out when there is a need for replenishment of supply parts, in order to meet production timeline. Some companies invest in smart products, sending usage and fault data back to company to help improve the performance and stability of its products.

Industry 4.0 will make information available anywhere, anytime. The information will traverse across company boundaries, within product development supply chain. To remain competitive, the operators need to ensure resiliency of production plant operations. Cybersecurity strategies need to be embedded into manufacturing operations from the start, spanning across Information Technology (IT) and Operational Technology (OT). It needs to ensure the security of future manufacturing production operations, throughout its lifecycle.

This document aims to provide security guideline for Industry 4.0 ecosystem leveraging on other related best practices such as ENISA[1] Good Practices for Security of IoT standards that are still at drafting stage under the NIST (Cyber security baseline for Securable IoT Devices) and the CyberSecurity Malaysia's Cyber Security Guideline for Internet of Things (IoT).

[1] https://www.enisa.europa.eu/publications/good-practices-fsor-security-of-iot

1.1 Scope

The guideline serves as a reference for manufacturing companies in Malaysia that are moving towards Industry 4.0, in providing aspects to be considered in technologies and processes that can enhance security of systems within operational plants. The focus is on the manufacturers and system integrators involved in designing, implementing, operating and maintaining the systems. The document identifies specific functions with some depth to enable suppliers of Industry 4.0 technologies to include security measures presently and in future. These security requirements can be included in procurement specification and service contract. Refer to Annex A for a comprehensive list of controls recommended in this guideline.

This guideline uses both the term IoT and IIoT, in which IoT are devices commonly used by consumers while IIoT are devices used largely by industries, since in the Industry 4.0 ecosystem, both elements co-exist.

This guideline provides information security controls that are in conformant to ISO/IEC 27001:2013[2]. It is recommended that organization intending to implement these controls to extend its SOA (statement of applicability) by including the controls stated in this guideline.

1.2 Objective

The objective of the guideline is to enable manufacturers to achieve resiliency in engineering plant operations as well as incorporate cyber security in the manufactured products and services lifecycle that contain cyber mechanisms.

Examples of Industry 4.0 use cases include:

a) Smart Manufacturing (e.g. data driven Quality Control, Augmented Operations)
b) Smart Refinery (e.g. predictive maintenance, information-driven performance)
c) Remote monitoring assistance for control and diagnostic of plant operations (e.g. Energy, Environment)
d) Smart City (e.g. waste management, traffic management, crowd sensing)

1.3 Intended audience

The intended audiences for this document are referred as Key-players throughout this document. The Key-players are categorized as follow:

a) **Manufacturing firms** - embarking in Industry 4.0 for example, in production and plant operations.
b) **Solution provider for Industry 4.0 technologies** - it includes industrial equipment suppliers with IoT and IIoT capability, smart supply chain provider that require vertical and horizontal system integration with plant operations systems.

The security principles and recommendations contained in this document should be applicable to organisations embarking on Smart Manufacturing, Smart Products, Smart Supply Chain and Smart City, adopting base technologies that includes IoT, IIoT, cloud services, big data and analytics and more advanced technologies such as augmented reality, autonomous robotics and simulation in plant operations.

[2] ISO/IEC 27001:2013 Information Security Management Systems — Requirements

This guideline requires the audience to have minimal knowledge in Industry 4.0 ecosystem, good understanding on information security for network, system and application, and information security management.

This document provides a list of cyber security controls to be considered based on relevant risk associated to the asset in use, within companies adopting Industry 4.0 technologies.

2 Terms, definitions, abbreviated terms and acronyms

2.1 Terms and definitions

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

2.1.1
Access control
means to ensure that access to assets is authorized and restricted based on business and security requirements

[ISO/IEC 27000: 2014[3]]

2.1.2
Authentication
provision of assurance that a claimed characteristic of an entity is correct

[ISO/IEC 27000: 2014]

2.1.3
Availability
property of being accessible and usable upon demand by an authorized entity

[ISO/IEC 27000: 2014]

2.1.4
Confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO/IEC 27000: 2014]

2.1.5
Denial of Service
threat aimed to deny access to valid users such as by making a web server temporarily unavailable or unusable

[OWASP Code Review Guide V1.1]

2.1.6
Integrity
property of accuracy and completeness

[ISO/IEC 27000: 2014]

[3] ISO/IEC 27000:2014 Information Security Management Systems — Overview and Vocabulary

2.1.7
Process
set of interrelated or interacting activities which transforms inputs into outputs

[ISO/IEC 27000: 2014]

2.1.8
Risk
effect of uncertainty on objectives

[ISO/IEC 27000: 2014]

2.2 Abbreviated terms and acronyms

AAA	Authentication, authorization and accounting System
BYOD	Bring Your Own Device (BYOD)
CCTV	Closed-circuit TV
CD	Continuous Delivery
CI	Continuous Integration
DDoS	Distributed Denial of Service
DCS	Distributed Control System
DMZ	Demilitarized Zone (DMZ)
GDPR	General Data Protection Regulation (EU)
GRE	Generic Routing Encapsulation
HMI	Human Machine Interface
HVAC	Heating, Ventilation and Air conditioning system
ICS	Industrial Control Systems
IETF	Internet Engineering Task Force
IIoT	Industrial Internet of Things
IoT	Internet of Things
SDN	Software-Defined Networking
MTU	Master Terminal Unit
NFV	Network Functions Virtualization
NIST	National Institute of Standards and Technology
OPC	Open Platform Communications
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition System
e.g.	Exempli Gratia

3 Industry 4.0 ecosystem

An Industry 4.0 ecosystem require integration of office environment as well as field and production systems. In some environment, the coexistence of both office and plant production systems are under one roof. What is more visible is the Industry 4.0 ecosystem is the convergence of the IT and OT components. Industrial control systems (ICS) ceased to be isolated once the incorporation of IT components in the ICS domain become a common practice.

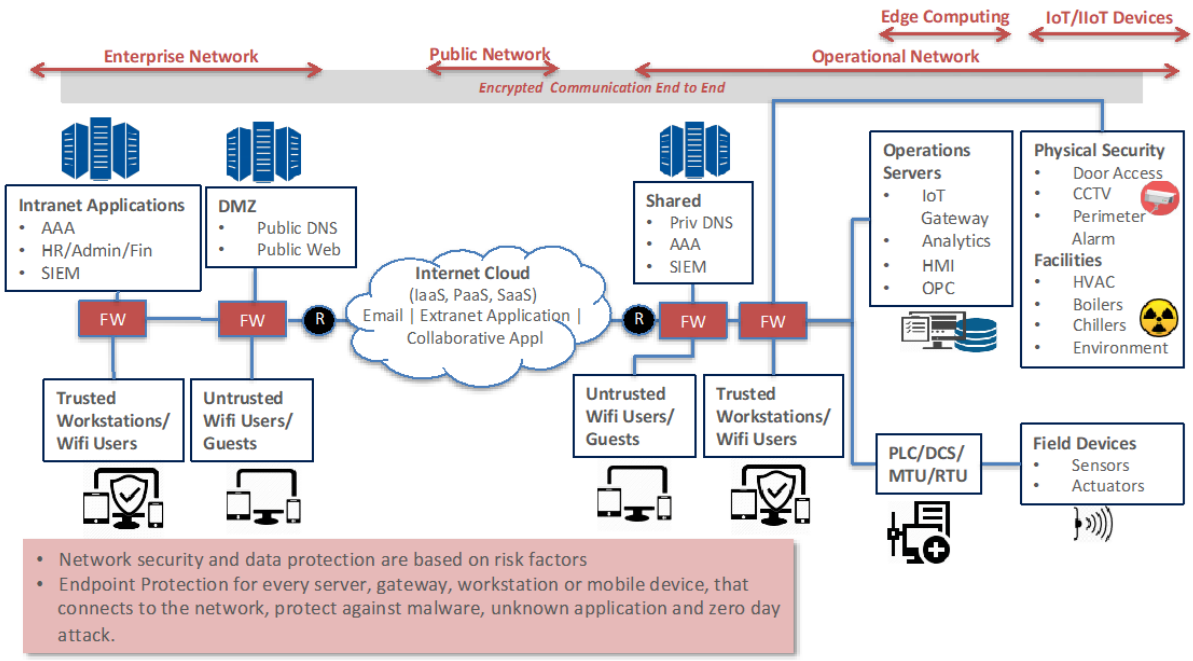

Figure 1: Industry 4.0 High Level Network Architecture

Figure 1 illustrates a high level network architecture of an Industry 4.0 environment which consists of Enterprise Network, Public Network, and the Operational Network. This network architecture may be relevant in Industry 4.0 environment such as Manufacturing plants, Refinery plants or Smart City.

Within the Operational Network, the network is segmented in zones for Untrusted users/devices, Trusted users/devices, Demilitarized Zone (DMZ) for public facing servers, IoT and IIoT devices, Edge Computing and Servers for Analytics. In transition towards industry 4.0, there will be co-existence of sensors and actuators that are IP Address-based and non-IP devices. Non-IP devices send data via fieldbus to PLC or DCS as well as MTU or RTU for SCADA system. IP Address-based IoT and IIoT devices send data to IoT Gateways that performs several critical functions from translating protocols to encrypting, processing, managing and filtering data.

These data are then sent via secure connection to systems that resides in the private or public cloud to conduct further processing utilizing Artificial Intelligence and Machine Learning as part of big data analytics. It is imperative that encryption is applied from the time of data creation, transmission and in storage to preserve data security and privacy. Further guidelines on data security and privacy is deliberated in Section 5.8.3.

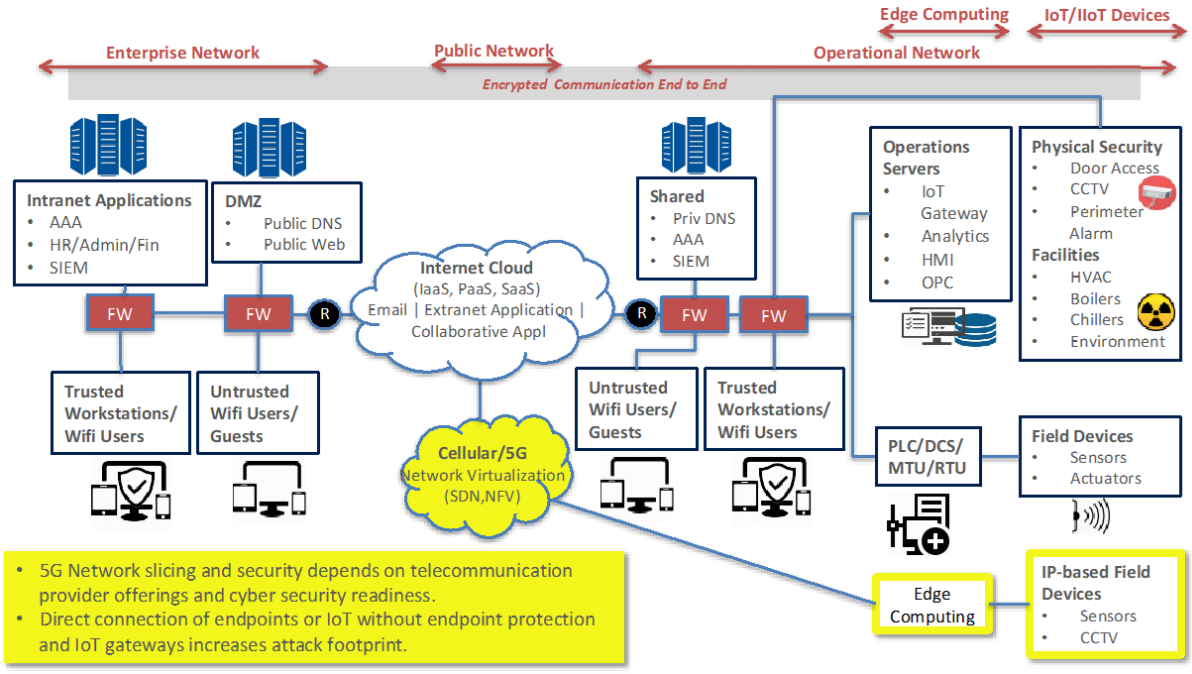

Figure 2: 5G Network Security

On the adoption of the emerging 5G network, the attack method may not be new, but the impact may be multifold higher due to the size of the bandwidth and numbers of devices on the network. The 5G network enables slicing capability which allows the creation of network segments that are completely separated from each other; one segment cannot be attacked from another. However, it does not prevent attacks within the same segment.

In managing 5G network, the security readiness is subject to the security service offerings by the telecommunication service provider, for example ability to detect rogue IoT and IIoT devices and to take automatic action to remove or quarantine them from the network, or authenticate and profile threats on IoT and IIoT devices when joining 5G network. As in Figure 2, any direct connection of endpoints, IoT or IIoT devices to the 5G Network without endpoint protection or IoT gateway will increase the attack footprint.

4 Security threats on Industry 4.0

Companies are constantly faced by risks of cyber attacks and industry espionage. In reality, the external networks are constantly bombarded with malicious traffic, and many successfully penetrate the internal networks effortlessly. Launching targeted attacks is easily camouflaged within noisy traffic. The adoption of Industry 4.0 technologies anticipate threats that impact not only security and privacy, but also safety, when involving cyber physical systems. Potential threats ranges from compromising physical security to production downtimes, spoilage of products to damaging equipment as well as ensuing financial and reputational losses. A company's chances of falling victim to cyber-criminals rise as its size of interconnected devices increases.

Study conducted by Deloitte and MAPI[4] revealed that the top 10 cyber threats facing advanced manufacturing include theft of intellectual property, phishing/pharming malware penetration, as well as mobile devices and mobile network vulnerabilities. These threats are not new, and indeed common

[4] https://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-manu-cyber-risk-in-advanced-manufacturing.pdf

across all industry sectors. However, the security readiness level in each sector varies greatly, subject to technology maturity, regulatory requirements and enforcements.

In 2017, several cases involving WannaCry ransomware hit manufacturing plants such as Honda[5] and service kiosks of LG Electronics[6]. Operations were halted in response to the discovery of the infection. Monetary losses remain unknown.

In other cases, seemingly benign systems can be hacked and used for alternate purposes. For example, a manufacturing company was expanding its global footprint by constructing a production facility in China. In order to keep an eye on the construction progress, the company installed a series of cameras they could control from a remote location. However, it was discovered these connected cameras had been hacked, and the images were being used to covertly monitor the facility.

The adoption of 5G network is expected to increase the level of malicious traffic in multifold. As more vulnerable devices are connected to the 5G network, it is anticipated that larger numbers of botnets with higher bandwidth at their disposal, will result in greater impact of DDoS attacks, based on research[7] findings. Devices connected directly to the 5G network without any gateway or endpoint protection, will become easy targets. Network slicing in 5G network, without security strategies in managing the multiple network domains, business actors, can also become targets of attacks within critical use cases, e.g. smart factories, banking and medical.

5 Industry 4.0 cyber security controls

5.1 Risk management

Risk assessment allow companies to prioritize limited resources in meeting business objectives and regulatory compliance. Security risk assessment is conducted whenever there is a change in business process, adoption of new component, or development of new solution. As such, security aspects can be incorporated at the early concept, design or requirement stage, prior to any acquisition, development and implementation of Industry 4.0 technologies.

Integrating risk assessment in any business decision prior to adopting industry 4.0 technologies may appear as a lengthy process, but given the use of readily available methodology, that is repeatable and structured, it will become a norm. By identifying threats and security requirements early, it will reduce the risk of exploit and likelihood of higher unexpected cost implication due to business impact.

Refer to ISO/IEC 27001:2013[8] for the requirements to conduct risk management in information security management systems and refer to ISO/IEC 27005:2018[9] for further guidance on methodology in information security risk management. ISO 31000:2018[10], to which ISO/IEC 27001:2013 and ISO/IEC 27005:2018 conform, can also help general understanding of risk management.

Risk Assessment processes are discussed in the following sub-sections.

5.1.1 Identify assets

The first step in risk assessment is identifying assets, which may include hardware, software and data that is hosted on premise or remotely located. The recommended first step is in identifying the value,

[5] https://www.reuters.com/article/us-honda-cyberattack/honda-halts-japan-car-plant-after-wannacry-virus-hits-computer-network-idUSKBN19C0EI
[6] https://www.zdnet.com/article/wannacry-ransomware-attack-at-lg-electronics-takes-systems-offline/
[7] https://www.computer.org/publications/tech-news/research/botnet-cyberthreat-5g-solution
[8] ISO/IEC 27001:2013 Information Security Management Systems — Requirements
[9] ISO/IEC 27005:2018 Information Security Risk Management
[10] ISO 31000:2018, Risk Management – Guidelines

both tangible and intangible. Assets also need to be classified in terms of its criticality to business operations based on dependencies, availability and other factors that contribute to the value of the asset.

5.1.2 Identify threats and vulnerabilities

The next step is identifying the associated threats to the asset. A list of potential threats can be gathered from past incidents and incidents occurring involving other similar organisation. It involves identifying practical threats expected during machine operation and the impact to the business operations, based on known vulnerabilities. Likelihood of a successful attack or compromise depends on the effectiveness or lack of, control and mitigation measures in place.

5.1.3 Evaluate risk

Ultimately the risk value estimation allows prioritization of the risk treatment plan. Key success factors in ensuring effective risk assessment methodology is to ensure ownership of the treatment plan, as well as commitment from leadership in determining the risk appetite of the organisation. The ISO/IEC 27005:2018 provides guidance on methodology in information security risk management.

5.2 User account, credentials, authentication and authorization

Least privilege is a practice of restricting access rights for users to computing resources and systems that is absolutely required to perform routine and legitimate activities. Production systems used at the plant and office environment should ensure secure access and authorization for each designated user, to avoid abuse, unauthorized access and malicious activities. Restrict privilege access such as administrative account access to designated personnel only.

5.2.1 Individual account for each entity

Production systems should allow creation of individual user account for each entity. “Entities” refer to individual person to machine, as well as machine to machine, both locally and remotely. Each account should be given authorization for relevant and limited function. Administrative privilege access should be limited to designated authorized personnel, and not given to vendors or suppliers. Particular attention must be paid here to the fact that there should be no accounts for groups of users: User accounts should be created individually for every plant user and not based on assigned roles.

5.2.2 Account management

The number of users may change in an operational environment due to change in work shifts, addition of personnel, resignation of personnel or change of departments or job function. The system needs to allow authorized personnel with privilege access to make approved changes in maintaining the user access control. The company should ensure efficient handling in managing the individual user accounts, especially with regard to creating, activating, modifying, deactivating and removing accounts. This can often be done by managing the user accounts centrally. As such, it is recommended that implementation of multiple platform systems allow integration into central identity management systems or directory services.

5.2.3 Management of credentials

Each individual user account should be granted authorization to access certain limited amount of data and function. These credentials or passwords require efficient management process to allow reset of credentials in case of loss, without disrupting the plant operations. When using passwords, it is important that default passwords can be changed upon first login or as and when required, and require strong password verification. Access resetting should not be complex or to cause downtime. Multi-factor or adaptive authentication using security modules protected from physical attack such as pin and

smartcards are recommended. If these are not available, the systems at least should not store passwords in plain text. Access should be limited for that session only.

5.2.4 Public key and symmetric key authentication

In the use of Public Key or Symmetric Key Authentication, the key management need to be efficient and use of secure cryptographic algorithm. The Public Key Infrastructure (PKI) requires additional certificate lifecycle management to avoid systems downtime due to expired certificates.

Create zones and access concepts with corresponding authentication. Users should be subject to authentication via every access, every interface, not only on individual components, but also when crossing network zone boundaries. Use of automation via single sign-on by the use of tokens (such as SAML or OAuth 2.0) with strong encryption and proper input validation is essential.

5.2.5 Authorization verification for every authentication

Each time a user is authenticated on a system, the rights assigned to the user is verified. The systems should allow administrators to change access rights to specific components or services, as environmental requirements change all the time. Systems should allow rights management to be done centrally to ease operation (e.g. support XACML).

5.2.6 Strong authentication for remote access

All remote access to plant operations system and office system should be safeguarded with strong authentication. Where cryptographic authentication mechanisms are used, weak algorithms must be removed. Use of VPN, IPSec and TLS 1.3 offer strong authentication, given secure configuration. Important to note that remote desktop application such as RDP and TeamViewer application, pose threats when installed directly on server systems.

IoT and IIoT components are often supplied with initial default accounts and password. Strong authentication also means that these default accounts should be changed to actual user accounts or removed prior to commissioning. Hard-coded and unchangeable credentials are not only insecure, but also incur cost for hardware replacement if the access is compromised. Any failed repeated access attempts should be forbidden and allowed again after reactivation.

5.2.7 Secure directory service and AAA System

It is very common that attacks on ICS (Industrial Control System) and SCADA system begin with penetration of user endpoints systems for reconnaissance and eventually gaining access to privilege accounts when targeting Directory Services or AAA systems. As such, securing the Directory Service and AAA System includes system lockdown via application whitelisting, hardening of the service, and monitoring of object access.

5.3 Secure remote service

The plant operator should ensure that any requirement for remote service, including those for purposes of maintenance and troubleshooting by vendors are done securely to prevent unauthorized access and ensure accountability. The following subsections discuss the control mechanism for remote service.

5.3.1 Controls in setting up and ending remote session

There should be clear authorization process for initiating and ending a remote session. Prior to any remote service session, it must be determined that the system current workload allow such access, and the account to be used has the necessary rights. The session should be blocked after a specified period of

no activity and any new session should require identification, authentication and authorization. All activities on the system should be logged. Remote access can be further restricted via other filtering method, e.g. limit based on IP Address, trusted device.

5.3.2 Safeguarding through technical and organisational measures

At company level, there should be pre-defined conditions that allow remote service. For example, remote services should not be allowed on systems running highly critical functions, with other dependent machines. Compliance to this pre-defined condition that limit remote service to be conducted, should include technical mechanisms that would automatically prevent and detect any breach of conduct.

5.3.3 Encrypting remote connection

Every session should be encrypted and incorporate strong authentication (refer to Section 5.2.6). Weak cryptographic algorithms should be removed (refer to Section 5.4.3).

5.4 Using secure protocols

When attacking IIoT, due to limited direct access to the machine, the gateway and system that interface with the external user or internal user, will first become a target. As such, secure protocols are required to preserve confidentiality, integrity and authenticity of the data sent, stored and processed. The following subsections discuss the control mechanism in preventing eavesdropping, session hijacking and data alteration.

5.4.1 IP-based protocols on network transmission

When using systems on IP-based network, the confidentiality of data in transit are to be preserved. Use of standard protocols such as TLS 1.3, is highly recommended. If the need for downward compatibility with legacy systems makes encryption impossible, communication should be tunneled through a secure protocol. This is relevant under the assumption that encryption with known standards, any delay due to the encryption will be negligible.

5.4.2 Integrity of data

The integrity of data transmitted, stored and processed between machines need to be ensured. Undetected manipulation of data can have major impact to operations. Open standards such as TLS 1.3 is useful for practical implementation of web applications.

5.4.3 Cryptographic strength and quality

Cryptographic algorithms continue to evolve. The use of standardized encryption processes approved by public bodies such as the National Trusted Cryptographic Algorithm List (MySEAL)[11] and corresponding recommended key lengths under NIST 800-131A[12], is highly recommended. As new threats are discovered and computing capability expand, these lists are subject to regular revision by the respective entities maintaining the list. Thus, machines used in plants should support the ability to update the cryptographic module, if need be. One of the ways to determine the cryptographic strength on a system or application, is by using vulnerability scanning tools with latest signatures. Vulnerability management is described in Section 5.10.2.

[11] MySEAL - https://myseal.cybersecurity.my/en/aksa.html
[12] NIST Special Publication 800-131A - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf

5.4.4 Special consideration for fieldbus

At ICS, the fieldbus links the programmable logic controllers (PLC) to the physical components such as actuators, sensors, electric motors, switches, valves and console lights. There are limitations in applying security controls at the fieldbus level to ensure authenticity and integrity of communication. Given the real-time requirements, decisions as to whether it is necessary or even possible to encrypt the data at fieldbus level should be taken based on what the plant is used for.

However, once the data reaches the Control System (e.g. DCS, PLC, RTU, MTU), security controls such as data encryption, endpoint protection and secure application are applicable. Technology forecast of the ICS technology indicates that there will be more production of IP-based sensors and actuators, and IoTs, as the technology move towards eventual phasing out of Non-IP devices.

5.5 Network segmentation

The plant should be divided into zones based on individual security requirements of the systems. Technical measures are used to separate individual segments. The approach to network segmentation is described in this section.

5.5.1 Risk-based security requirements for network segmentation

Risk assessments enables the identification of security requirements associated to each asset associated to the plant operations. The risk analysis approach, as described in Section 5.1, will determine the security controls required for each asset component. External facing servers and internal servers have different risk level, however, when internal systems are accessible via VPN and other form of remote access, that increases the risk of threat exposure. Network segmentation is required to reduce threat exposure.

5.5.2 Zoning of services

Shared network services, such as domain name servers (DNS), Directory Servers for authentication, should be located within the same zone with relevant controls to protect against internal and external threat. Data flows into and out of a machine should be identified. Plant operational systems, such as SCADA, PLC, Manufacturing Execution System (MES) networks, should be located within specific zoning. It is important to ensure the failure of one zone affects as few as possible, of the other zones. Trusted and untrusted users are segregated in separate segments with tighter policy for untrusted users' segment. IoT devices segment require connection to only designated IoT gateway or edge computing.

5.5.3 BYOD in industry

Modern office-based businesses support the idea of Bring Your Own Device (BYOD). This can be a great option for businesses that rely upon remote workers, because BYOD allows each employee to use devices with which they are comfortable, increasing productivity and improving morale.

However, devices should be vetted and approved to access network. Limit access to pre-approved devices, and configure firewall and VPN to allow access only to designated essential devices.

5.5.4 Zoning network access controls

Within every zone, there are controls limiting access across zones based on static controls such as IP Addresses, MAC Addresses, port services, or Network Access Control system that profiles and authenticate user and devices. Perimeter and machine controls include firewalls (application and network), filtering outgoing and incoming communication, as well as within the machine itself. Changes to the machine location may require update and changes to these static zone perimeter controls.

Monitoring of network traffic across zones may reveal early onset of malware outbreak or malicious activities.

5.5.5 Internet access within ICS (Industrial Control Systems) network

It is important to determine the need for access from and to Internet within the plant network that hosts the ICS components. The Internet access, if any, should not contradict the defined security functionality of the plant and that critical systems are appropriately isolated to reduce the risks of unauthorized access.

5.6 Safeguarding wireless technology

All use of wireless technologies should comply with latest wireless technology standards. In the context of this document, wireless includes WiFi, cellular, bluetooth, and other wireless technology. However, it is common knowledge that most wireless technology installed with default configurations can be compromised using publicly available tools. This section provides safeguards to secure wireless technology implementation.

5.6.1 Secure configuration

Security requirements for wireless technology includes changing default configurations, removing weak encryption and reduce range of wireless signals. Cryptographic algorithm supported by devices will evolve as new vulnerabilities discovered. Considering wireless devices are exposed to threats for long term periods, security configurations and firmware need to be updated as new security advisories are published.

5.6.2 Wireless access management

Wireless access requires strong authentication and complex passphrase. Additional controls include allowing only authorized device connection based on registered device, for example with the use of Network Access Control (NAC) or MAC Address filtering.

5.6.3 5G network

5G network provides strong authentication and encryption for connectivity and transmission. It allows large bandwidth and high number of device connection. However, it also creates high visibility of devices in a public network, creating a large footprint for attacks depending on the vulnerabilities residing within the application, systems and weak configurations on the IoT devices or endpoints. The majority of threats that exists over decades such as vulnerability scanning and botnet infection are still relevant in the 5G environment, at an even higher rate.

Prior to decisions on connecting organisation assets, IoT or endpoints, to any 5G network, it is pertinent to ensure that the IoT or endpoint devices comply to Endpoint protection (refer to Section 5.7).

IoT or endpoints, should be connected to 5G network via secure gateway or edge computing that provides security and privacy, without compromising performance.

Any IoT devices or endpoints that are connected to 3rd party network service provider should not be simultaneously connected to the organisation internal network, to avoid unauthorized connection.

It is essential that 5G network service provider implement security measures such as ability to detect and quarantine rogue IoT devices, as well as mitigate botnets, before it compromises other devices. However, the security of the 5G Network Service Provider largely depends on the regulatory requirements set by the telecommunication regulator.

5.7 Endpoint protection

Protect the last mile. Endpoints, including shared terminals, servers and computers in general, within operational environment are target of compromise. Cyber attacks target weak endpoints, which penetrates via storage media, file downloads, as well as email links and attachments. Operational physical industrial system such as SCADA, PLC, MES consists of computer consoles that manage data from and to sensors and actuators, and are highly targeted.

5.7.1 Application whitelisting

Application whitelisting reduce the risk of malicious software and unauthorized programs from executing on the endpoints. A correctly configured application whitelisting prevents execution of unapproved software, regardless downloaded from websites, email attachment or introduced via storage media.

Implementing application whitelisting in Directory Servers, email servers and file sharing servers will prevent adversaries from running malware to steal credentials and contents.

For legacy systems that are lacking in patches in response to latest attacks, will benefit from the implementation of application whitelisting, to reduce attack footprint.

5.7.2 Privilege account management on endpoints

Apply least privilege rule in account creation. This is a practice of restricting access rights for users to computing resources and systems that is absolutely required to perform routine and legitimate activities only.

In addition to that, restrict administrative or privilege access to operating systems or firmware and applications to only designated authorized personnel. Any use of endpoints should not be running on privilege access. Any such default implementation needs to be changed. Admin accounts are 'keys to the kingdom', and used by adversaries to gain full control of information and systems. Regularly revalidate the need for privileges, and assign users based on the principle of least privilege.

5.7.3 Patch management and firmware update

Patching of software (such as web browsers, Microsoft Office) and operating systems or firmware vulnerabilities are part of cyber hygiene. Challenges with industrial system is that proprietary software have dependencies on legacy systems, that prevent operators from applying patches in fear of disrupting operations. The approach to any update, upgrade or patch management is to conduct tests prior to implementation on production wide systems.

Firmware or software updates on IoT devices should be limited to authorized user and devices, authenticated firmware or software (digitally signed) and conducted over encrypted communication; regardless wired or wireless connection, as well as via middleware, API or direct connection. There are about 300 middleware IoT platforms that can perform firmware updates, however, the connection should be tunneled over encrypted channel such as HTTPS, IPSec or VPN. Most middleware supports encrypted transport via HTTPS to be secure and firewall-friendly. Protocols such as Generic Routing Encapsulation (GRE) provide encapsulation, but not encryption. Thus, such use should be tunneled over encrypted communication.

Having an integrated console for device monitoring and management will enable verification of successful or failure of updates of firmware or software on IoT devices. Failure of update can be due to storage space, corrupted file or incompatibility issues. The monitoring and management system should also maintain secure connection with IoT devices. There are variety of commercial and opensource

solution such as the OMA Lightweight M2M that provides security for IoT device management. At the time this paper is written, the IETF working group is still drafting a standard for firmware update architecture suitable for IoT devices[13].

5.7.4 Hardening configuration

Endpoint hardening also includes disabling unwanted port services, network interfaces, enabling host-based firewall to ensure connections are allowed from trusted sources only, disabling password retention, removing development tools and library, and more. Hardening procedures are specific to the type of applications and operating systems or firmware.

5.8 Virtualization and cloud security

Security first approach. Although there are limited views that virtualization should reduce the risk of security breach, and that cloud solution would save costs, the key factor would be assessing the risk and embedding security requirements at the early onset.

5.8.1 Security principles

Industry 4.0 infrastructure may include IoT gateway and data analytics function in the cloud. The cloud and virtualisation environment require similar security principles to be applied at network, operating systems, applications and data levels in mitigating cyber threats. It is critical to pick cloud provider based on their security credentials and offerings. The ISO/IEC 27017:2015[14] provides the code of practice for information security controls for cloud services.

5.8.2 Secure cloud infrastructure and edge computing

Most current cloud implementation for industrial system involves industrial machine monitoring, asset tracking or shipping monitoring. However, study indicates more decentralized approach of edge computing, in which data is processed closer to its source should be more efficient. For cloud computing to effectively be implemented in industrial setting, edge computing would be required, in order to reduce the streaming of information to the cloud at all times. Edge computing, such as IoT gateway, can function at endpoints, gateway servers or micro datacenters. IoT devices send data to IoT Gateways that performs several critical functions from translating protocols to encrypting, processing, managing and filtering data before the data is sent or retrieved by the Cloud applications. Connection between edge computing and the cloud should be encrypted, as well as preserving data integrity and privacy (refer to Section 5.8.3).

As such at every component involved in the data handling, require security principles to be applied, as this exponentially increases the area of footprint for attacks. As new IIoT proliferate, secure design of the network and application infrastructure becomes important in order to enable scalability without resulting more cost implications (refer to Section 3 on network architecture).

5.8.3 Data protection and privacy

As more data is being collected at edge computing and transmitted to cloud for big data and analytics, in public as well as on-premise infrastructure, data privacy needs to be preserved. This can be achieved via methods such as data pseudonymization (reversible) and anonymization (non-reversible). Larger aspects on data protection and privacy in the big data ecosystem require compliance with local (e.g. Personal Data Protection Act 2010) and global laws (e.g. GDPR) depending on the geo location of the

[13] https://datatracker.ietf.org/doc/draft-ietf-suit-architecture/
[14] ISO/IEC 27017:2015 Code of Practice for information Security Controls based on ISO/IEC 27002 for Cloud Services https://www.iso.org/standard/43757.html

business. Guidelines on data protection and privacy for big data includes those by ENISA[15] which covers privacy by design in big data detailing eight strategies on "Privacy by Design in Big Data", as well as a handbook on compilation of best practices by Cloud Security Alliance[16] entitled "Big Data Security and Privacy Handbook".

5.9 Monitoring and threat detection

No absolute security knowing that cyber threat prevails at all times, and protection mechanisms may not be effective in all instances, monitoring mechanisms are necessary to detect anomalies. There are several approaches to monitoring and threat detection as described in this section.

5.9.1 Monitoring all access

All access to machines should be logged, including access from external network, and a copy of the log is kept in a central logger. Information that needs to be logged include identity of user/system, time, duration and type of access, that need to be kept for further evaluation. The monitoring system, such as Security information and event monitoring (SIEM), should be located in a separate network segment than the segment for IIoT devices and user devices.

5.9.2 Integration of monitoring console

Monitoring of incidents and SIEM should be centralized at control centers. Security-related events include incorrect password entry, exhaustion of resources, attempts at unauthorized access and changes to security-related configuration files (refer to Clause 12.4.1 Event Logging, ISO/IEC 27002:2013). SIEM can be deployed to detect known incidents and correlating logs across devices.

5.9.3 Anomaly detection and prevention

Detection of new and unknown attacks often require additional methods such as data analytics and intelligence. The challenges include reducing false positives and avoiding faults that can disrupt operations. In a plant environment, where machine activities are more mundane and significantly more uniform, it allows easier characterization on what is normal.

It should be further noted that there are only limited solutions currently that allow analysis of ICS/SCADA protocols. More effort is underway to secure ICS/SCADA protocols as well as having more alternatives for threat detection and prevention.

5.10 Components and integrated testing

Equipment and software tests are not limited to functional tests, but also performance and security tests. Security tests is part of regression tests, this is to avoid major overhaul on codes when major security findings are discovered only at the end of software development cycle. Other tests to provide high level of security assurance are also discussed in this section.

5.10.1 Security tests as integral part of development and integration

As part of Secure software development practice, security tests for software applications can identify vulnerabilities at early stage in software development. Security tests should be an integral part of development and integration. Various method includes tests on invalid input will reveal vulnerability in input validation. Static code review will reveal common programming issues such as hardcoded

[15] https://www.enisa.europa.eu/publications/big-data-protection
[16] https://iapp.org/media/pdf/resource_center/BigData_Security_and_Privacy_Handbook.pdf

password in clear text, buffer overflow vulnerabilities and lack of encryption. This can be done using tools by developer throughout key milestones in software component development and integration.

5.10.2 Vulnerability test and penetration testing

Part of software testing towards the end of software development cycle is to conduct vulnerability assessment and penetration testing. These can be done by independent third party or other departments that had not been involved in the software development.

5.10.3 Functional safety and stress testing

In Industry 4.0, where physical systems are involved, it is pertinent to include functional safety in operations. The industry 4.0 has implications in the requirements for network, security, robots/cobots, software and semiconductors used in operations. There is existing basic functional safety standard IEC 61508, first published in 1998, and now undergoing 3rd revision for release in 2020.

The standard series are still undergoing development and there is a need to align safety and security requirements for the Industry 4.0. Many of the techniques from IEC 61508[17] can be used to meet industrial security requirements in software. These techniques include doing design reviews, having coding standard, planning the use of tools, verification at the unit level, requirements, traceability, independent verification and assessment.

Stress test is a means to determine breaking points in terms of capacity management. At the same time, any random or systematic failure of hardware or software should not threaten life, or weaken security controls. The ISA/IEC 62443[18] series standard specifies security requirements for industrial control covering design, implementation and management of IACS (industrial automation and control systems).

5.11 Recovery

Define a recovery plan that resets the plant to trustworthy state in the event of malfunction or an attack.

5.11.1 Creating a backup system regularly

Integrate backup of systems, firmware, configurations and critical data at regular intervals, or when changes occur. Ensure restoration can be performed in the event of any incident of malfunction or an attack. If central systems are used for backup, the system should include secure data exchange, or encryption.

5.11.2 Restoring a trustworthy state after a malfunction or attack

Backups allow a machine to be restored to a trustworthy state in the event of attack or malfunction. Test restoration procedures periodically. This includes restoring system, firmware, configuration and data that are critical for the operations.

5.12 Determining security requirements for vendors and suppliers

When supplied goods do not meet minimum security requirements, it becomes the weakest link in the plant environment, becoming an easy target. Thus, security requirements should be defined and determined at the very early stage of the process, such as procurement process where the requirements are determined for vendors and suppliers.

[17] IEC 61508 Functional Safety – Standards https://www.iec.ch/functionalsafety/explained/
[18] https://www.isa.org/intech/201810standards/

5.12.1 Checking security requirements

For every system in the plant, there is a need to ensure the system meets the security requirements of the supplied components. Security requirements can be verified by going through documentations and verifying the security functions. For highly sensitive operations, the integrator and plant operators need to review the security requirements jointly.

5.12.2 Outsourced software development

In the Industry 4.0 ecosystem, there are continuous integration (CI) and continuous delivery (CD) involving front-end application, middleware or APIs and back-end big data engine, across products used in the field. Where software is provided and maintained by third parties, security requirements should be included in software development process or DevSecOps[19].

Basic controls such as input validation, encryption, strong authentication, should be part of security requirements and automated. Standard secure software development process or Secure SDLC as described in Figure 3 provides an approach ideal during the first four are development stages and the 5th stage is pre-production stage.

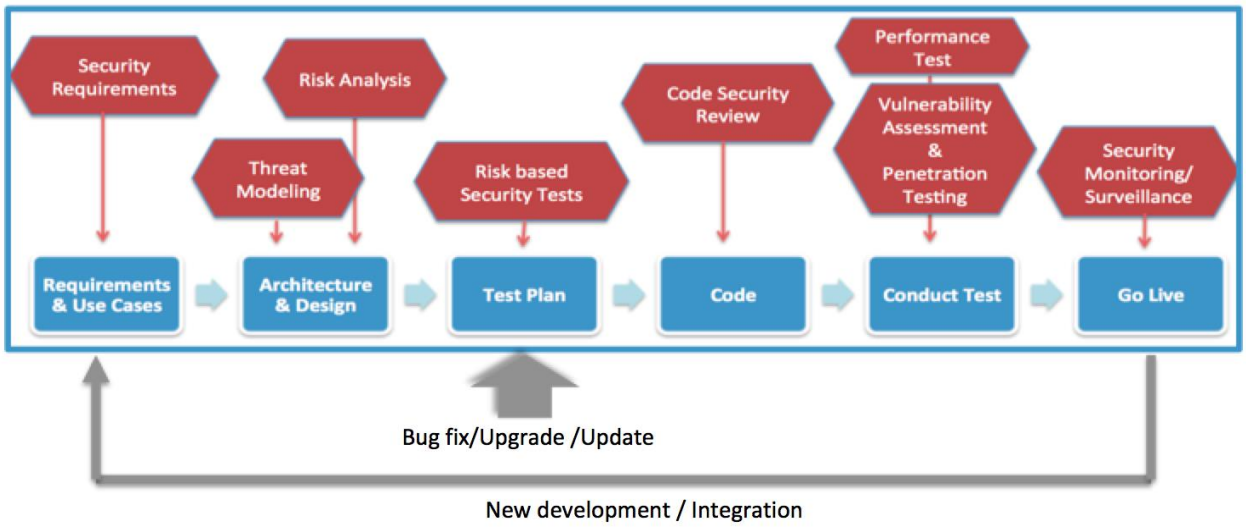

Figure 3: Security Assurance in DevSecOps

However, upon software production, where big data involves constant CI/CD of new code, due to changes in data source and data formats, changes to analytics method, the code require automated security testing, as well as live tracking and traceability, which is relevant to DevSecOps approach. There are several guidelines available on DevSecOps, and it requires the platform to be built and integrated with test tools for on-demand, and automated test for security assurance (refer to DevSecOps Best Practices[20]). Tools include IDE integration plugin, Static Application Security Testing (SAST), Dynamic Application Scanning Tool (DAST), Vulnerability Management Tools and other pre-defined custom test tools.

[19] Development Security Operations (DevSecOps)
[20] https://www.devseccon.com/wp-content/uploads/2017/07/DevSecOps-whitepaper.pdf

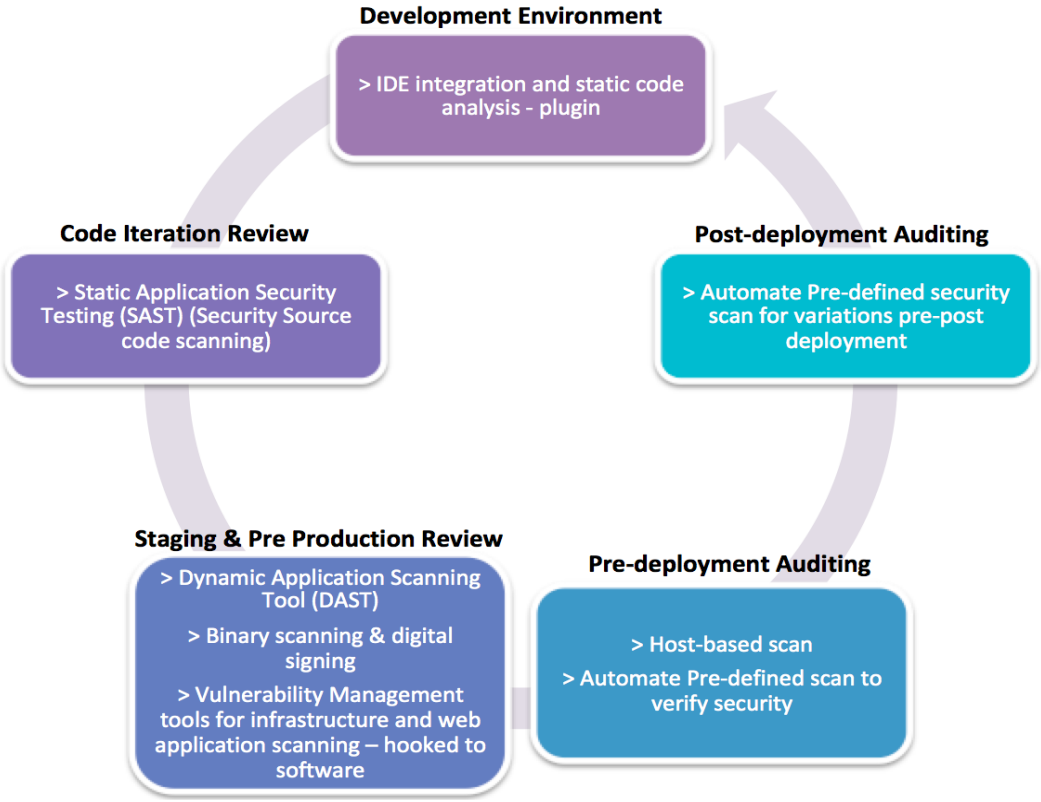

Figure 4: Automation in DevSecOps

Ensure software maintenance coverage includes bug fixes and security fixes. It is also recommended to include requirement to review the security of the source code in contractual agreement. Any big data implementation require inclusion of DevSecOps platform for customer's security monitoring and reporting.

5.13 Documentation

One of the means to communicate security effectively and ensuring compliance to standards is by documentation. However, documentation need to reflect actual practice in order to be relevant.

5.13.1 Establish process

Security requirements of organisational and technical process identified in this document should be documented. Organisational procedure and responsible roles should be derived from the documentation. Standard operating procedures and guidelines should provide steps to be taken in a given situation.

5.13.2 Documentation of risk analysis

Risk analysis should be documented to enable traceability on threats coverage, vulnerabilities, controls and countermeasures, risk treatment and ownership as well as tracking progress of implementation. The documentation should show the methods on how risk analysis was based on.

5.13.3 Security incidents

Security incidents should be recorded and archived, using ticketing system or equivalent, for tracking and for future references. This includes incidents within the organisation and, security incidents that have been observed in machines already in use within the organisation. The records should be internal, however, in the event there are impact to **third** parties, the organisation should report the incidents to

relevant entities. These requirements are included in Clause 16.1 of the ISO/IEC 27001:2013.

5.13.4 Security specification in service level agreements from vendors and suppliers

In ensuring security across the ICT Supply Chain, acquisition requirements and service level agreements should include relevant security requirements. These requirements are included in Clause 15.1.2 of the ISO/IEC 27001:2013[21].

5.14 Operational security training

Continuous training in IT security, network security and IT, in plant environment is essential in ensuring a reliable and resilient plant operations in the age of Industry 4.0. It demands that new requirements be added to job profiles to compel compliant conduct.

Due to the fact that safety approvals prevent plants from modifying their operational environment, as such security measures such as applying software patches require prior test and approval. It is pertinent that endpoints and network security are implemented effectively.

5.14.1 Awareness

Security is strongest as its weakest link; inattention, ignorance and negligence can result in critical gaps. Every personnel need to understand their role and contribution in influencing the level of security at the plant. All personnel should be made aware on security requirements for the plant, product and the entire company, and taught on compliant conduct.

5.14.2 Plant planners and project designers

In any plant for any new deployment it is essential that the planners and designers establish security requirements for any new implementation. These requirements include operating systems or firmware being used, network technologies, protocols and interfaces. Training includes coverage in the following areas:

a) Risk analysis and risk management
b) Basics of directory services/databases and authentication
c) Basics of TCP/IP and bus networks
d) Security related specifications for plant documentation
e) Important security protocols and how they work (cryptographic basics)
f) Operating systems and security management of OS
g) Basics of asset, patch and vulnerability management
h) Security hardening of IT systems
i) Basics of virtualization
j) Computer emergency response and incident management in plant networks
k) Statutory framework

Although the content above focuses on technical issues, governance and sociological aspects are just as important. Training needs to be coupled with strong support from decision makers and company management at operative level, in order to make security effective.

5.14.3 Training approach

Considering the diverse level of knowledge amongst plant operators, plant planners and project managers, the training will vary based on background and current job scope. To build understanding in network security for example, there are trainings on firewalls and secure network architecture. For

[21] https://www.iso.org/standard/54534.html

application developers, there are, for example, web application security trainings. For more specialized trainings for operational environment, there are hands-on trainings covering topics such as ICS/SCADA security training and IoT security training, for industry professionals which are available worldwide.

Annex A

Industry 4.0 cyber security controls summary

The control objectives and controls listed in Table A.1 are directly derived from this guideline and may be used in context with Clause 6.1.3 (information security risk treatment) of ISO/IEC 27001:2013.

Table A.: Control Objectives and Controls

Overview on cyber security requirements for Industry 4.0		
5.1	Risk management	
5.1.1	Identify assets	Identifying assets includes hardware, software and data hosted on premise or remotely. Assets to be classified based on criticality to business operations, dependencies, availability and other factors that contribute to the value of the asset.
5.1.2	Identify threats and vulnerability	List potential threats associated to each asset, based on past incidents and incidents involving other similar organisation, and impact to the business operations. Likelihood of a successful attack or compromise depends on the effectiveness or lack of, control and mitigation measures.
5.1.3	Evaluate risk	Refer to ISO/IEC 27005:2018 for guidance on methodology in information security risk evaluation.
5.2	User account, credentials, authentication and authorization	
5.2.1	Individual account for each entity	Production systems allow creation individual user account for each entity. "Entities" refer to individual person to machine and machine to machine, both locally and remotely. Group or role-based accounts are not allowed. Each individual user account is granted authorization for relevant and limited function. Administrative privilege access should be limited to dedicated authorized personnel, and not given to vendors or suppliers.
5.2.2	Account management	Allow users access based on respective work shifts. Integrated system to manage individual user accounts with regard to creating, activating, modifying, deactivating and removing accounts via identity management systems or directory services for authentication, authorization and accounting (AAA).
5.2.3	Management of credentials	Allow efficient management of credentials to allow reset of credentials in case of loss, without disrupting the plant operations. When using passwords, default passwords should require change upon first login or on-demand, with strong password verification and not stored in plain text. Multi-factor or adaptive authentication using security modules protected from physical attack such as pin and smartcards are recommended.
5.2.4	Public Key and Symmetric Key authentication	Key management need to be efficient and use of secure cryptographic algorithm. Public Key Infrastructure (PKI) requires certificate lifecycle management to avoid systems downtime due to expired certificates.

5.2.5	Authorization verification for every authentication	Each user authentication is verified and rights assigned to the user. The systems should allow administrators to change access rights to specific components or services when required.
5.2.6	Strong authentication for remote access	Remote access to plant operations system and office system require strong authentication. Cryptographic authentication mechanisms to be used and weak algorithms should be removed. Use of VPN, IPSec and TLS 1.3 offer strong authentication, given secure configuration. Remote desktop application such as RDP and TeamViewer, pose threats when installed directly on server systems. Default accounts to be changed or removed. Hard-coded and unchangeable credentials not allowed. Failed repeated access attempts should require reactivation of account.
5.2.7	Secure Directory Service and AAA System	Secure the Directory Service and AAA System including system lockdown via application whitelisting, hardening of the service, and monitoring of object access.
5.3	Secure remote service	
5.3.1	Controls in setting up and ending remote session	Establish clear process for initiating, authorization and ending a remote session. Session to be blocked after a period of no activity. Log all activities on the system.
5 .3.2	Safeguarding through technical and organisational measures	Pre-define conditions that allow remote service. For example, remote services should not be allowed on systems running highly critical functions, with other dependent machines.
5.3.3	Encrypting remote connection	Encrypt every session and incorporate strong authentication. Weak cryptographic algorithms should be removed. Refer to the National Trusted Cryptographic Algorithm List (MySEAL) and corresponding recommended key lengths under NIST 800-131A.
5.4	Using secure protocols	
5.4.1	IP-based protocols on network transmission	Preserve confidentiality of data in transit. Use of standard protocols such as TLS 1.3, is highly recommended. Legacy systems which do not support encryption, should tunnel communication through a secure protocol.
5.4.2	Integrity of data	Integrity of data transmitted, stored and processed between machines need to be preserved. Open standards such as TLS 1.3 is recommended.
5.4.3	Cryptographic strength and quality	System should allow update of cryptographic module. Encryption algorithm approved by the National Trusted Cryptographic Algorithm List (MySEAL) and corresponding key lengths under NIST 800-131A, is recommended.
5.4.4	Special consideration for fieldbus	Fieldbus level do not ensure authenticity and integrity of communication. However, once the data reaches the Control System (e.g. DCS, PLC, RTU, MTU), security controls such as data encryption, endpoint protection and secure application are applicable.
5.5	Network segmentation	

5.5.1	Risk-based security requirements	External facing servers and internal servers accessible via remote access has higher risk of threat exposure.
5.5.2	Zoning of services	Establish network segment for common shared services such as DNS, AAA and SIEM. Another separate network segment for operational system such as SCADA, PLC, Manufacturing Execution System (MES) networks. Trusted and untrusted users are segregated in separate segments, with tighter policy for untrusted users' segment. IoT devices segment require connection to only designated IoT gateway or edge computing.
5.5.3	BYOD in industry	Personal devices should be vetted and approved to access network.
5.5.4	Zoning network access controls	Apply controls limiting access across zones based on static controls such as IP Addresses, MAC Addresses, port services or Network Access Control system that profiles and authenticate user and devices, primarily in the operational network.
5.5.5	Internet access within ICS (Industrial Control Systems) network	Internet access, should not contradict the security functionality of the plant and that critical systems are appropriately isolated to reduce the risks of unauthorized access.
5.6	Safeguarding wireless technology	
5.6.1	Secure configuration	Change default configurations, remove weak encryption and reduce range of wireless signals. Update security configurations and firmware as new security vulnerabilities are discovered.
5.6.2	Wireless access management	Use strong authentication and complex passphrase for wireless access. Additional controls include restricting to only authorized devices, such as use of Network Access Control (NAC) or MAC Address filtering.
5.6.3	5G network	IoT or endpoints connection to 5G network, should be via secure gateway or edge computing that provides security and privacy. The IoT devices or endpoints connected to 3rd party network service provider should not be simultaneously connected to the organisation internal network.
5.7	Endpoint protection	
5.7.1	Application whitelisting	Reduce the risk of malicious software and unauthorized programs from executing on the endpoints. For legacy systems lacking in patches in response to latest attacks, application whitelisting reduces the attack footprint.
5.7.2	Privilege account management on endpoints	Apply least privilege rule in account creation by restricting access rights for users to computing resources and systems that is absolutely required to perform routine and legitimate activities only. Restrict administrative or privilege access to operating systems or firmware and applications to only designated authorized personnel. Any use of endpoints should not be running on privilege access. Regularly revalidate the need for privileges, and assign users based on the principle of least privilege.

5.7.3	Patch management and firmware update	Firmware or software updates on IoT devices should be limited to authorized user and devices, authenticated firmware or software (digitally signed) and conducted over encrypted communication; regardless wired or wireless connection, as well as via middleware, API or direct connection. Use device monitoring and management to verify successful or failed updates of firmware or software on IoT devices.
5.7.4	Hardening configuration	Includes but not limited to disabling unwanted port services, network interfaces, enable host-based firewall to ensure connections are allowed from trusted sources only, disable password retention, remove development tools and library.
5.8	Virtualization and cloud security	
5.8.1	Security principles	Refer to ISO/IEC 27017:2015 Code of practice for information security controls based on ISO/IEC 27002 for cloud services.
5.8.2	Secure cloud infrastructure and edge computing	Edge computing can be performed at endpoints, gateway servers or micro data centers. IoT devices send data to IoT Gateways that performs several critical functions from translating protocols to encrypting, processing, managing and filtering data, before the data is sent or retrieved by the applications in the Cloud. Connection between edge computing and the cloud should be encrypted, as well as preserving data integrity and privacy.
5.8.3	Data protection and privacy	Data collected at edge computing and transmitted to cloud for big data and analytics, in public as well as on-premise infrastructure, require data protection and privacy. Method for privacy protection includes data anonymization. Data protection and privacy in big data ecosystem require compliance with local (e.g. Data Protection Act Malaysia) and global laws (e.g. GDPR) depending on the geo location of the business. Guidelines on data protection and privacy for big data includes ENISA "Privacy by Design in Big Data" detailing eight strategies, as well as Cloud Security Alliance "Big Data Security and Privacy Handbook".
5.9	Monitoring and threat detection	
5.9.1	Monitoring all access	Access to all machines and systems should be logged, including access from external network, and a copy of the log is kept in a central logger. Information that needs to be logged include, but not limited to, identity of user/system, time, duration and type of access. Monitoring system, such as security information and event monitoring (SIEM), should be located in a separate network segment than the segment for IIoT devices and user devices.
5.9.2	Integration of monitoring console	Monitoring of incidents and SIEM should be centralized at control centers. Security-related events include incorrect password entry, exhaustion of resources, attempts at unauthorized access and changes to security-related configuration files (refer to Clause 12.4.1 Event Logging, ISO/IEC 27002:2013).
5.9.3	Anomaly detection and prevention	Effective anomaly detection and prevention require reduction of false positives and avoid faults that can disrupt plant operations. However, limited solutions that support ICS/SCADA protocols.
5.10	Components and integrated testing	

5.10.1	Security tests as integral part of development and integration	Method of security tests for software applications that can identify vulnerabilities at earlier stage of software development, includes but not limited to, tests on input validation and static code review on detection of common programming issues such as hardcoded password or credentials in clear text, buffer overflow vulnerabilities and lack of encryption. This is to ensure security framework is embedded in the software design.
5.10.2	Vulnerability test and penetration testing	Software testing towards the end of software development cycle includes vulnerability assessment and penetration testing.
5.10.3	Functional safety and stress testing	Functional safety standard IEC 61508 with 3rd revision for release in 2020.Verify software compliance with IEC 61508 to meet industrial security requirements.
5.11	Recovery	
5.11.1	Creating a backup system regularly	Integrate backup of systems, firmware, configurations and critical data at regular intervals, or when changes occur. For central backup storage, include secure data exchange, or encryption.
5.11.2	Restoring a trustworthy state after a malfunction or attack.	Test restoration procedures periodically. This includes restoring system, firmware, configurations and data that are critical for the operations.
5.12	Determining security requirements for vendors and suppliers	
5.12.1	Checking security requirements	Verify security requirements by going through documentations and verifying the security functions. For highly sensitive operations, the integrator and plant operators need to review the security requirements jointly.
5.12.2	Outsourced software development	Implement Secure SDLC methodology for one off software development, while DevSecOps is used for Cloud based application. Include requirement for source code review in contractual agreement. Ensure maintenance contract includes bug fixes and security fixes and DevSecOps platform for monitoring and reporting.
5.13	Documentation	
5.13.1	Establish process	Security requirements of organisational and technical process should be documented, including organisational procedure, roles and responsibilities, standard operating procedures and guidelines.
5.13.2	Documentation of risk analysis	Document risk analysis to enable traceability on threats coverage, vulnerabilities, controls and countermeasures, risk treatment and ownership as well as tracking progress of implementation.
5.13.3	Security incidents	Security incidents should be recorded and archived, using ticketing system or equivalent, for tracking and for future references.
5.13.4	Security specification in service level agreements from	Include security requirements across ICT Supply Chain, acquisition requirements and service level agreements. Refer to Clause 15.1.2 of the ISO/IEC 27001:2013.

	vendors and suppliers	
5.14	Operational security training	
5.14.1	Awareness	All personnel should be made aware on security requirements for the plant, product and the entire company, and taught on compliant conduct.
5.14.2	Plant planners and project designers	Planners and designers need to establish security requirements for any new implementation including operating systems or firmware being used, network technologies, protocols and interfaces. Training includes coverage in the following areas: a) Risk analysis and risk management b) Basics of directory services/databases and authentication c) Basics of TCP/IP and bus networks d) Security related specifications for plant documentation e) Important security protocols and how they work (cryptographic basics) f) Operating systems and security management of OS g) Basics of asset, patch and vulnerability management h) Security hardening of IT systems i) Basics of virtualization j) Computer emergency response and incident management in plant networks Statutory framework
5.14.3	Training approach	Provide security training relevant to the background and job scope. For network security for example, there are trainings on firewalls and secure network architecture. For application developers, there are, for example, web application security trainings. More specialized trainings for operational environment covering topics such as ICS/SCADA security training and IoT security training are also available.

Bibliography

[1] Good Practices for Security of Internet of Things in the context of Smart Manufacturing available at <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot>

[2] ISO/IEC 27001:2013 Information Security Management Systems — Requirements

[3] ISO/IEC 27000:2014 Information Security Management Systems — Overview and Vocabulary

[4] Cyber risk in advanced manufacturing available at <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-manu-cyber-risk-in-advanced-manufacturing.pdf>

[5] Honda halts Japan car plant after WannaCry virus hits computer network available at <https://www.reuters.com/article/us-honda-cyberattack/honda-halts-japan-car-plant-after-wannacry-virus-hits-computer-network-idUSKBN19C0EI>

[6] WannaCry ransomware attack at LG Electronics takes systems offline available at <https://www.zdnet.com/article/wannacry-ransomware-attack-at-lg-electronics-takes-systems-offline/>

[7] As Mobile Users Near 5G, Cybersecurity Experts Prepare for Next Face-Off with Saboteurs' Botnets available at <https://www.computer.org/publications/tech-news/research/botnet-cyberthreat-5g-solution>

[8] ISO/IEC 27005:2018 Information Security Risk Management

[9] ISO 31000:2018, Risk Management – Guidelines

[10] MySEAL available at <https://myseal.cybersecurity.my/en/aksa.html>

[11] NIST Special Publication 800-131A available at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf>

[12] A Firmware Update Architecture for Internet of Things available at <https://datatracker.ietf.org/doc/draft-ietf-suit-architecture/>

[13] ISO/IEC 27017:2015 Code of Practice for information Security Controls based on ISO/IEC 27002 for Cloud Services

[14] Privacy by design in big data available at <https://www.enisa.europa.eu/publications/big-data-protection>

[15] Big Data Security and Privacy Handbook available at <https://iapp.org/media/pdf/resource_center/BigData_Security_and_Privacy_Handbook.pdf>

[16] IEC 61508 Functional Safety – Standards available at <https://www.iec.ch/functionalsafety/explained/>

[17] New ISA/IEC 62443 standard specifies security capabilities for control system components available at <https://www.isa.org/intech/201810standards/>

[18] DevSecOps Whitepaper- The business benefits and best practices of DevSecOps implementation available at <https://www.devseccon.com/wp-content/uploads/2017/07/DevSecOps-whitepaper.pdf>

Acknowledgements

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 Guideline for Secure Industry 4.0 are as follows:

Ts. Dr. Zahri Yunos/ Ts. Dr. Solahuddin Shamsuddin/ Ts. Dr. Maslina Daud/ Mr Abdul Fuad Abdul Rahman/ Ms Fateen Nazwa Yusof/ Mr Mohamad Nasrul Taufiq Salleh/ Mr Muhamad Izzat Yahood/ Mrs Nurul Syazwani Kamarulzaman/ Mrs Shazwani Salleh/ Mr Syamsul Syafiq Syamsul Kamal	CyberSecurity Malaysia
Mrs Noraishah Binti Awaludin	Bank Negara Malaysia
Mr Saiful Bahry M.Hissham	Dell Global Business Center Sdn Bhd
Mrs Raja Azrina Raja Othman	Expert
Dr Gopinath Rao	Favoriot
Mr Ahmad Hafiz Mohd	German-Malaysian Institute (GMI)
Mr Abdul Fattah Mohd Yatim	Independent Expert IEM
Mrs Siti Mariam Mohd Din	Jabatan Standard Malaysia
Mrs Suhara Abdul Rahman	Jabatan Peguam Negara (AGC)
Mrrs Lyana Shohaima	Kementerian Komunikasi dan Multimedia Malaysia (KKMM)
Ms Vimala Murugan	Kementerian Perdagangan Antarabangsa dan Industri (MITI)
Mrs Nur Hidayah Abdullah	MAMPU
Mrs Nas Fatehah Mahadi	Malaysia Digital Economy Corporation Sdn Bhd (MDEC)
Mrs Paul Ng	Malaysia IOT Association (MyIoTA)
Mrs Shahrulniza Musa	Malaysian Software Testing Board (MSTB)
Mrs Shariffah Rashidah Syed Othman	National Cyber Security Agency (NACSA)
Mr Kamaruzaman Abdol Rahim	Perbadanan Putrajaya (PPJ)
Prof. Dr. Raha Abdul Rahman	Pusat Perubatan Universiti Kebangsaan Malaysia (PPUKM)
Ms Hafizah Mansur	Universiti Islam Antarabangsa Malaysia (UIA)
Mrs Azleyna Ariffin	Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM)
Dr. Dzaharuddin Mansor	The National Tech Association of Malaysia (PIKOM)
Mr Thaib Mustapa	TM Applied Business Sdn Bhd