Guidelines

Internet of Things (IoT) Cyber Security Guide

Annex C
Case Study on Smart Buildings

In consultation with:

IMDA IoT Cyber Security Guide Annex C
Version 1, Jul 2022

Info-communications Media Development Authority
10 Pasir Panjang Road
#03-01 Mapletree Business City
Singapore 117438

Content

This Guide is a living document which is subject to review and revision periodically.

Guides are informative documents and voluntary in nature except when it is made mandatory by a regulatory authority. It can also be reference in contracts as mandatory requirements. Users are advised to assess the suitability of this guide for their intended use.

Compliance with this guide does not exempt users from any legal obligations.

NOTICE

THE INFO-COMMUNICATIONS MEDIA DEVELOPMENT AUTHORITY ("IMDA") MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THE MATERIAL PROVIDED HEREIN AND EXCLUDES ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OF NON-INFRINGEMENT, MERCHANTABILITY, SATISFACTORY QUALITY AND FITNESS FOR A PARTICULAR PURPOSE. SUBJECT TO THE MAXIMUM EXTENT PERMITTED UNDER LAW, IMDA SHALL NOT BE LIABLE FOR ANY ERRORS AND/OR OMISSIONS CONTAINED HEREIN OR FOR ANY LOSSES OR DAMAGES (INCLUDING ANY LOSS OF PROFITS, BUSINESS, GOODWILL OR REPUTATION, AND/OR ANY SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES) IN CONNECTION WITH THE USE OF THIS MATERIAL.

IMDA DRAWS ATTENTION TO THE POSSIBILITY THAT THE PRACTICE OR IMPLEMENTATION OF THIS GUIDE MAY INVOLVE THE USE OF INTELLECTUAL PROPERTY RIGHTS AND TAKES NO POSITION CONCERNING THE EXISTENCE, VALIDITY AND/OR APPLICABILITY OF ANY SUCH INTELLECTUAL PROPERTY RIGHTS, WHETHER ASSERTED BY CONTRIBUTORS OF THIS DOCUMENT OR ANY THIRD PARTY.

AS OF THE DATE OF THE ISSUANCE OF THE PUBLIC CONSULTATION OF THIS GUIDE, IMDA HAS NOT RECEIVED WRITTEN NOTICE OF ANY PATENT RIGHTS WHICH MAY BE RELEVANT IN RELATION TO THE IMPLEMENTATION OF THIS GUIDE. HOWEVER, IMPLEMENTERS ARE CAUTIONED THAT THIS MAY NOT REPRESENT THE LATEST INFORMATION AND ARE THEREFORE STRONGLY URGED TO CHECK WITH THE RELEVANT DATABASE IN ITU, ISO, IEC OR THE RELATED STANDARDS DEVELOPMENT ORGANISATION FOR INFORMATION OF PATENT RIGHTS. IMPLEMENTERS ARE ADVISED TO OBTAIN THEIR OWN LEGAL AND/OR TECHNICAL ADVICE IN RELATION TO THE IMPLEMENTATION OF THE GUIDE IF REQUIRED.

Annex C: Case Study on Smart Buildings (informative)

1. Overview

With the proliferation of the Internet, mobile technologies, and ubiquitous connectivity, devices deployed in a commercial building get increasingly connected, and isolation is rarely the case. Data from a traditionally isolated building's Operational Technology (OT) network is now available for use in data-driven decision-making, but it is also exposed to common IoT vulnerabilities, such as weak password, poor device management, insufficient data protection, etc.

The security of data that flows across and between smart Internet of Things (IoT) sensors and building systems in a commercial building is of paramount concern and cannot be overlooked. This case study will show how to implement and enforce cybersecurity and cyber resilience from both Information Technology (IT) and OT perspectives in the built environment for the commercial sector.

This annex is a case study and the guidance provided here is with reference to an example of the IoT application for smart buildings and may not be exhaustive.

1.1 Threat Modelling

One cannot properly secure a commercial building without first performing a threat modelling, understanding the assets that matter and the threats that may surface. STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of service, Elevation of privilege) is a popular model used to help analyse and find threats to systems, in general. It should be noted that other methodologies exist and might be more appropriate for specific use cases. For example, the MITRE Attack framework provides tactics, techniques, and procedures (also known as TTPs) used by threat actors.

It is also worth mentioning that threat modelling should be performed on a frequent and regular basis. For example, it can be performed and reviewed yearly or anytime a new device or asset is added as part of a system or upon appearance of new threats that were not previously modelled.

Table C-1 depicts the threat modelling checklist, defined in the main document ("IMDA IoT Cyber Security Guide"), and its application to this case study.

ID	Threat modelling checklist	Y / N	Supporting materials
1	Identify the potential targets to be protected a. Define its boundaries and the external systems (including users) that it needs to interact with b. Decompose the target(s) into its subcomponents c. Identify data flows within the target(s), and inputs and outputs from external systems d. Identify sensitive data and where they are handled (at rest, in transit, in use) e. Identify the security needs (based on potential impacts to Confidentiality, Integrity and Availability (CIA) triad) for subcomponents and data flows f. Identify hardware, software and protocols in use	Y	Refer to section 2

ID	Threat modelling checklist	Y / N	Supporting materials
2	Define the security problem a. Identify system accessibility • Identify attack surfaces • Determine operating environments • Determine system / device lifecycles and supply chain b. Identify system susceptibility (aka vulnerabilities) • Determine known vulnerabilities • Enumerate threats to attack surfaces (using Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege (**STRIDE**) as a guide) • Enumerate threats to operating environments (using STRIDE as a guide) • Enumerate threats to stages of system / device lifecycles and supply chain (using STRIDE as a guide) c. State any assumptions	Y	Refer to section 3
3	Conduct risk assessment • Assess impact of threats and vulnerabilities to CIA triad and match against security needs of assets • Assess attacker capabilities required to realise the threats • Assess the likelihood of the risk • Prioritise the risks for mitigation, including other considerations (e.g. monetary, safety, social and usability impacts)	Y	Refer to section 4
4	Determine the security objectives • State the security objectives. For example, OT systems emphasize safety, where system integrity takes precedence over data confidentiality	Y	Refer to section 5
5	Define the security requirements • State the necessary requirements to address the identified security objectives without going into their specific implementation	Y	Refer to section 6
6	Design and implement the capabilities	N	Not covered by this document
7	Validate and verify that the capabilities address the security requirements adequately	N	Not covered by this document

Table C-1: Application of threat modelling checklist

1.2 Security Frameworks

This case study was written with guidance provided by the main document ("IMDA IoT Cyber Security Guide"). Robust controls defined in frameworks such as NIST 800-53 and ISO 27001, as well as industrial security requirements such as IEC 62443 and NERC CIP can also be referenced to complement the various security controls and best practices mentioned inside this document. IEC 62443 should be referenced when formal evaluation and certification is required, for example industrial automation subsystems, such as lifts and escalators.

It is recommended that the IoT device vendor reviews and adapts its security framework and policies regularly. This is crucial because it allows the company to adapt to ever-changing threats

and ensure comprehensiveness and effectiveness. Additional guidance on IoT security controls could also be found in the document "IoT security reference architecture - an ANT-centric study"[1].

2. Identify the Target of Protection

This section illustrates the guidance provided in item-1 of Table C-1, which helps identify the Target Of Protection (TOP) for this case study.

The TOP contains two system boundaries – the Proximity Network (PN) and the Commercial Building Network (CBN).

1.3 Proximity Network

The PN consists of two critical components – the IoT Cloud and IoT Edge Gateway. The IoT Cloud, essentially is an operating system on the cloud, built on open standards to allow management, monitoring and control of IoT devices in a smart building and spans across the buildings, cities or countries. Such IoT clouds must ensure extensive connectivity while operating in a secure and open ecosystem to help organizations efficiently and agilely innovate and develop their ecosystems.

IoT Edge Gateway, as the data ingestion end of IoT Cloud, acts as a lightweight building management system (BMS) and adapts thousands of devices and systems within the CBN to connect to the cloud. It extends the intelligence of the IoT Cloud to the edge, by providing device management, device control, and edge computing through the integration and inheritance of traditional OT technologies, such as Modbus, BACnet, and IEC-104, and deep coordination with IoT Cloud Platform.

1.4 Commercial Building Network

The CBN contains the backend components deployed in a typical commercial building. End devices, such as power meters, water meters, air-conditioning, and solar, are connected to the IoT Edge Gateway, which now also acts as a lightweight BMS to work with direct digital controller (DDC) used to manage, monitor, and control equipment in a commercial building. Typically, the IoT Edge Gateway is interconnected to the end devices via OT protocols such as BACnet, OPC-UA, Modbus TCP or Modbus RTU. These protocols allow communication between the devices in a commercial building.

From a security perspective, these protocols tend to be unencrypted and without integrity checks, and it leaves them susceptible to cybersecurity attacks that include but are not limited to replay and manipulation attacks. A breach to a building network will simply open up to attackers to everything they can access.

Figure C-1 shows the system architecture of an example case study, which will help to demonstrate the guidance provided by Table C-1. Note that in the case of a Smart Building scenario, it is not uncommon to find a BMS. In this case, it is appropriate to include the BMS in between the IoT Edge Gateway and the device layer. There can be more granularity in terms of zones definition but for the purpose of the illustration of the case study, we will define the zones as described in Figure C-1.

[1] https://www.ntu.edu.sg/ntc/support-from-the-entrepreneurship-ecosystem/developing-the-technopreneurship-ecosystem/internet-of-things-(iot)-security-reference-architecture

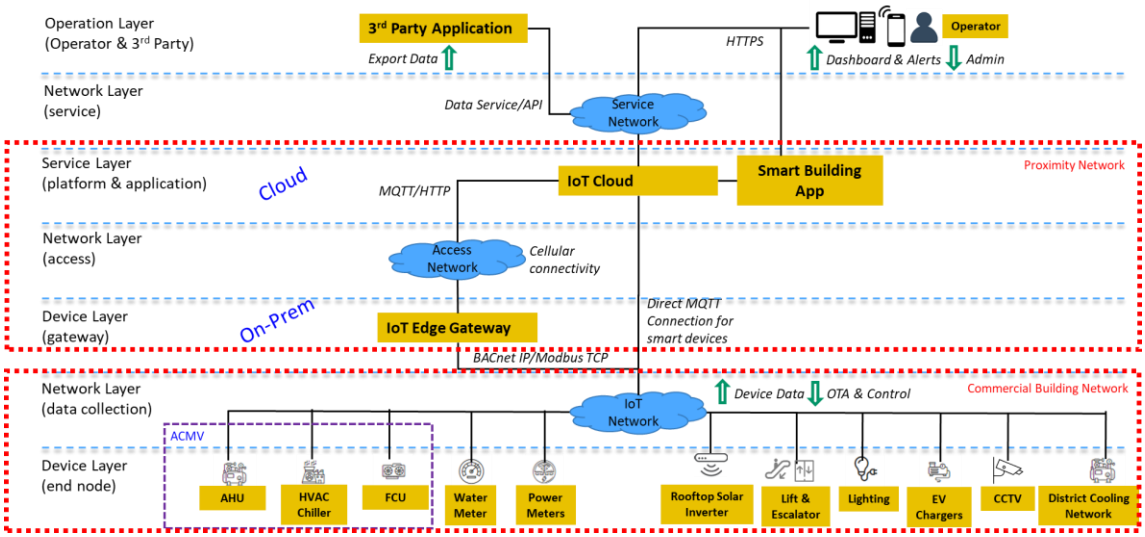

Figure C-1: General architecture of Smart Building

Through the threat model, assets under the TOP are being identified. Table C-2 determines the security needs of the assets with respect to the CIA triad. It helps in prioritising which assets and which aspects to secure.

Note that several end devices are interconnected to IoT Edge Gateway. For illustration, we will simply pick a few end devices to support the case study. The reader is free to extend the threat modelling to other connected devices.

Legend: H = High, M = Moderate, L = Low

Assets	Confidentiality	Integrity	Availability	Rationale
IoT Cloud	H	H	H	Confidentiality is high because of customers' information on the cloud and access to the backend. Integrity is high to safeguard commands invocation, and availability needs to be high to maintain the ability to access and control the backend.
IoT Edge Gateway	H	H	H	Confidentiality is high because of customers' information on the Edge Gateway and access to the cloud. Integrity is high to safeguard commands invocation, and availability needs to be high to maintainability access and control the backend at all times.
Device – Water Meter	L	H	H	Confidentiality is not an issue, but rather readings must be true, and availability must be present.
Device – Power Meter	L	H	H	Confidentiality is not an issue, but rather readings must be true, and availability must be present.
Device - Rooftop Solar Inverter	L	H	H	Confidentiality is not an issue, but controls must not be modified, and availability must be present.
Device – Lift and Escalator	L	H	M	Confidentiality is not an issue, but controls and readings must not be modified. Availability may/may not be an issue because downtime can be afforded.

Table C-2: Security Needs of Assets

Table C-3 determines the security needs of the data flows between assets with respect to the CIA triad. It provides information on which data flows required attention and the type of security required.

Legend: H = High, M = Moderate, L = Low

Data flow	Confidentiality	Integrity	Availability	Rationale
Devices -> IoT Edge Gateway	M	H	H	Raw sensor data collection requires high integrity and availability. Confidentiality is not as important for raw data. Integrity and availability are high to ensure the information communicated is correct and available.
IoT Edge Gateway -> IoT Cloud	H	H	H	Confidentiality is high as communication is over the Internet. Integrity and availability are high to ensure the information communicated is correct and available.
IoT Cloud -> 3rd party application	H	H	M	Analysis of data by 3rd party applications requires high data integrity. Confidentiality is high to protect the data collected. Availability may/may not be an issue because downtime can be afforded.
IoT Cloud -> Operator	H	H	H	Data analysis reporting requires high confidentiality, integrity, and availability for operators/users.
Operator -> IoT Cloud -> IoT Edge Gateway -> Devices	H	H	M	Management of devices by users requires high confidentiality and integrity. Some downtime can be afforded.
3rd party Application -> IoT Cloud -> IoT Edge Gateway -> Devices	H	H	M	Management of devices by 3rd party applications requires high confidentiality and integrity. Some downtime can be afforded.

Table C-3: Security Needs of Data Flows

1.5 Extending assets' CIA assessment to OT's Safety, Resilience and Reliability

Equally important to the security well-being of a Smart Building eco-system are the 3 attributes of OT, i.e. Safety, Resilience and Reliability. For more information, please refer to Annex A ("Foundational Concepts").

Safety refers to the ability of the asset to operate in a safe manner that will not be detrimental to the safety of users at all times. A very classic example is that of a smart escalator. It should fail gracefully in a case of a fault and not be able to cause any harm to the vulnerable.

Resilience refers to the asset's ability to maintain functioning state while reliability refers to the ability of the asset to perform a specific function as it is expected to. In the same manner, Table C-3 can be extended to identify the security needs to ensure safety, resilience as well as reliability of the assets.

To focus and illustrate how the security requirements can be defined for Smart Building, we will focus on the CIA triad.

3. Define the security problem

This section illustrates the guidance provided by item-2 of Table C-1, which helps define the security problem for this case study.

Table C-4 identifies the concerns that contribute to system accessibility and system susceptibility for assets under TOP. It provides the information (threats, vulnerabilities, operating environments, assumptions, etc.) required to define the security problem.

Assets	System accessibility	System susceptibility
IoT Cloud	The following attack surfaces are relevant for the IoT Cloud: API calls, HTTPS traffic, storage SW, memory, VM, OS, firmware, middleware, server software The IoT Cloud is hosted in the cloud and is accessible from the Internet. All stages of the system lifecycle need to be considered.	OWASP Top 10 Application Security Risks Scan for relevant known vulnerabilities from prominent vulnerability repositories such as https://www.cve.org/
IoT Edge Gateway	The following attack surfaces are relevant for IoT Edge Gateway: MQTT/HTTP traffic, storage SW and HW, memory, OS, firmware, communication ports, WIFI, 4G IoT Edge Gateway is hosted in the commercial building network and is accessible via the Internet. All stages of the device lifecycle need to be considered.	OWASP IoT Attack Surface Areas and OWASP IoT Vulnerabilities Scan for relevant known vulnerabilities from prominent vulnerability repositories such as https://www.cve.org/
Device – Water Meter	The following attack surfaces are relevant for Water Meter: Modbus traffic, firmware Water Meter is hosted in the commercial building network and is accessible from the IoT Edge Gateway (or BMS connected in between) only. All stages of the device lifecycle need to be considered.	OWASP IoT Attack Surface Areas and OWASP IoT Vulnerabilities Scan for relevant known vulnerabilities from prominent vulnerability repositories such as https://www.cve.org/
Device – Power Meter	Similar concerns as Water Meter	Similar concerns as Water Meter
Device – Rooftop Solar Inverter	Similar concerns as Water Meter	Similar concerns as Water Meter
Device – Lift and Escalator	Similar concerns as Water Meter	Similar concerns as Water Meter

Table C-4: System accessibility and susceptibility

4. Conduct risk assessment

This section illustrates the guidance provided by item-3 of Table C-1, which guides how risk assessment is conducted for this case study.

Table C-5 demonstrates a risk assessment of system accessibility and system susceptibility for each asset. This is for illustration purposes only as risks are context-sensitive to the real world. In the table, risks are classified as high, moderate, and low, according to the given rationale.

Legend: H = High, M = Moderate, L = Low

Assets	System accessibility (attack surfaces, operating environments, lifecycles)	System susceptibility (known vulnerabilities, STRIDE)	Rationales
IoT Cloud	H	H	System accessibility is high because it is hosted in the public cloud. System susceptibility is high because it may contain some vulnerabilities. Refer to OWASP Top 10 Application Security Risks
IoT Edge Gateway	M	H	System accessibility is medium because it "sits" within the CBN. System susceptibility is high because it may contain some vulnerabilities and can be connected to the IoT Cloud. Refer to OWASP IoT Attack Surface areas.
Device – Water Meter	M	M	System accessibility and susceptibility of water meters are determined to be moderate. The assumption is that the device "sits" within the CBN while the Modbus protocol is insecure.
Device – Power Meter	M	M	System accessibility and susceptibility of the power meter are determined to be moderate. The assumption is that the device "sits" within the CBN while the Modbus protocol is insecure.
Device – Rooftop Solar Inverter	M	M	System accessibility and susceptibility of the rooftop solar inverter are determined to be moderate. The assumption is that the device "sits" within the CBN while the Modbus protocol is insecure.
Device – Lift and Escalator	M	M	System accessibility and susceptibility of lift and escalator are determined to be moderate. The assumption is that the device "sits" within the CBN while the Modbus protocol is insecure.

Table C-5: Assessment of system accessibility and susceptibility

Table C-6 demonstrates a risk assessment of attacker capability for each asset, for illustrative purposes only. It determines a list of attacker types (script kiddies, criminals, hacktivists, terrorists, state-sponsored, etc.) that have an interest in the assets. The risks are defined by the capability of the most sophisticated attacker in the list, which can compromise the assets. Similarly, risks are classified as high, moderate, and low, according to the given rationale.

Legend: H = High, M = Moderate, L = Low

Assets	Attacker Capability	Rationale
IoT Cloud	H	The asset is valuable to a range of attackers (script kiddies, criminals, hacktivists, terrorists, state-sponsored), including some with high capabilities and resources.
IoT Edge Gateway	H	The asset is valuable to a range of attackers (script kiddies, criminals, hacktivists, terrorists, state-sponsored), including some with high capabilities and resources.
Device – Water Meter	L	The asset is valuable to script kiddies only.
Device – Power Meter	L	The asset is valuable to script kiddies only.
Device – Rooftop Solar Inverter	M	The asset is valuable to script kiddies, criminals, and hacktivists with moderate capabilities and resources.
Device – Lift and Escalator	M	The asset is valuable to script kiddies, criminals, and hacktivists with moderate capabilities and resources.

Table C-6: Assessment of attacker capability

Table C-7 determines the priority for mitigation of the threats for each asset, with holistic considerations for risks of system accessibility, system susceptibility, and attacker capability, for illustration purposes only. Our case study will only elaborate on the high priority items for mitigation in subsequent sections for illustrative purposes.

Legend: H = High, M = Moderate, L = Low

Assets	**System accessibility** (attack surfaces, operating environments, lifecycles)	System susceptibility (known vulnerabilities, STRIDE)	Attacker Capability	Priority
IoT Cloud	H	H	H	H
IoT Edge Gateway	M	H	H	H
Device – Water Meter	M	M	L	
Device – Power Meter	M	M	L	
Device – Rooftop Solar Inverter	M	M	M	
Device – Lift and Escalator	M	M	M	

Table C-7: Assessment of priority

5. Determine the security objectives

This section illustrates the guidance provided by item-4 of Table C-1, which guides how security objectives are determined for this case study.

Table C-8 demonstrates the definition of security objectives for the threat modelling process. For illustrative purposes, we limit the assets to those identified as high priority in Table C-7. The needs of the CIA triad for the assets are identified in Table C-2 and defined in this table as principal objectives to safeguard. This table also identified a list of possible security objectives.

Legend: H = High, M = Moderate, L = Low

Assets	Confidentiality	Integrity	Availability	Security objectives
IoT Cloud	H	H	H	1. Ensure confidentiality of sensitive data 2. Provide proper access control 3. Ensure integrity of the system 4. Prevent multitenancy from compromising security 5. Ensure confidentiality and integrity of data and commands 6. Resilience against DOS
IoT Edge Gateway	H	H	H	1. Ensure confidentiality of sensitive data 2. Provide proper access control 3. Ensure integrity of the system 4. Fail safely 5. Ensure confidentiality and integrity of data and commands 6. Resilience against DOS

Table C-8: Security Objectives

In addition, Table C-3 guides the identification of security requirements under network protection and data protection categories.

6. Define the security requirements

This section illustrates the guidance provided by item-5 of Table C-1, which helps define the security requirements for this case study. It should be noted that the checklist is only a template of common security considerations. Users must determine the appropriateness and applicability of the checklist items to add on, remove, and/or adjust according to the uses and businesses' needs. This checklist alone is not a substitute for formal evaluation and certification.

Table C-9 suggests the application of the vendor disclosure checklist for assets highlighted in Table C-8. In practice, the technology solution provider would have to further elaborate on how they address the security requirements listed.

Legend: Y = Yes, N = No, NA = Not Applicable

ID	Vendor disclosure checklist	Y / N / NA	Supporting materials
1. Cryptographic support			
CK-CS-01	Do your devices and system properly utilize industry-accepted cryptographic techniques and best practices? Examples of best practices include: · use of approved algorithms and their correct implementation and application · sufficient key length · use of approved random number generator(s) · recommended crypto-period · recommended entropy sources · use of updatable cryptography	Y	The strength of cryptography is fundamental to safeguard the objectives of confidentiality and integrity. In particular, cryptography must be approved for the lifetime of the devices. Recommended for IoT Cloud and IoT Edge Gateway to maintain confidentiality and integrity of the information.
CK-CS-02	Do you employ proper key management (generation, exchange, storage, use, destruction, replacement, etc.)?	Y	Proper key management is required to prevent the disclosure of keys through the system/device lifecycles. Recommended for IoT Cloud and IoT Edge Gateway to ensure that keys used to establish confidentiality and integrity are supported with proper key management.
2. Security function protection			
CK-FP-01	Do you establish Root-of-Trust?	Y	To safeguard the confidentiality and integrity of sensitive data (e.g., keys) at rest and in use. Recommended for IoT Cloud and IoT Edge Gateway
CK-FP-02	Do you employ secure boot?	Y	To safeguard the integrity of the boot process. Recommended for IoT Edge Gateway since it is an on-prem physical device with the necessary resources to support Secure Boot.
3. Identification and authentication			
CK-IA-01	Do you employ unique, non-modifiable, and verifiable identities for clients (user, device, gateway, application) and servers?	Y	To safeguard the integrity of identification to mitigate threats of spoofing. Recommended for IoT Cloud and IoT Edge Gateway
CK-IA-02	Do you employ mutual authentication? For example, before establishing connections and after pre-defined intervals	Y	To safeguard the integrity of connections to prevent unauthorized remote access. Recommended for IoT Cloud and IoT Edge Gateway

ID	Vendor disclosure checklist	Y / N / NA	Supporting materials
4. Network protection			
CK-NP-01	Do you enforce network access control? For example, ensure explicit authorization to join a new network and/or allow remote access.	Y	Proper access control is required to limit access to the system networks. Recommended for IoT Cloud and IoT Edge Gateway
CK-NP-02	Do you employ proven transport protocols with security controls properly activated? Examples include: - Use of TLS for TCP Payloads - Use of DTLS for UDP Payloads	Y	To safeguard the confidentiality and integrity of the payloads. Recommended for IoT Cloud and IoT Edge Gateway
CK-NP-03	Do you employ industry best practices for secure connectivity? Examples of industry best practices: · Use of VPN or leased lines. · Use of private mobile APNs from telecommunication operators when using a public mobile carrier network. · Use of DNS pinning to prevent DNS spoofing. · Use of traffic filtering based on type, port, and destination. · Use of certificate pinning. · Employ TLS when using MQTT. · Scan for open network ports. Use whitelisting to establish or deny connections from non-trusted sources. In addition, IETF RFC 8520 Manufacturer Usage Description (MUD) can be a standard mechanism for devices to provide this information to the network.	Y	Applicable to safeguard the data flows highlighted in Table C.3 Recommended for IoT Cloud and IoT Edge Gateway For cellular communications (i.e. 4G, NB-IoT), certain security enhancement considerations include providing a private APN provisioned together with dedicated VPN channel between telecommunication's network infrastructure to cloud platform infrastructure. Inter-device connectivity should be disabled at the telecommunications level to prevent malicious attack at one location to gain access to other location through cellular network. Static IPs can also be assigned for each device over cellular communications to identify each device.
CK-NP-04	Do you segregate communication channels for trusted endpoints from non-trusted? Examples include: · Use of VLAN. · Use of firewalls for DMZ. · Use of unidirectional security gateway. · Use of network segmentation or micro-segmentation. Physical isolation.	Y	Applicable to safeguard the data flows highlighted in Table C.3 Recommended for IoT Cloud and IoT Edge Gateway Commercial Building Network is physically isolated from the enterprise network. DMZ is designed to restrict external access without exposing the internal network and system. The network traffic is safeguarded by web proxy and firewall with strict rules.
5. Data protection			
CK-DP-01	Do you protect the confidentiality and integrity of your sensitive data? · in transit · in use at rest	Y	To safeguard the confidentiality and integrity of sensitive data. Sensitive data includes cryptographic keys and user credentials. Recommended for IoT Cloud and IoT Edge Gateway This is optional for devices such as Lift and Escalator and Rooftop Solar Inverter and where the protocols can support.
CK-DP-02	Do you protect the authenticity and integrity your codes and firmware? · in transit · in use at rest	Y	To safeguard the software and firmware in IoT Cloud, IoT Edge Gateway, including updates. Recommended for IoT Cloud and IoT Edge Gateway

ID	Vendor disclosure checklist	Y / N / NA	Supporting materials
CK-DP-03	Do you ensure the authenticity and integrity of your data (e.g., inputs, commands, and sensing data)? · in transit · in use · at rest Examples include: · Validate incoming content types. · Validate response types. · Validate the HTTP methods against authorization credentials. · Whitelist acceptable HTTP methods. · Define the acceptable character set (e.g., UTF-8). · Validate that input characters are acceptable. · Encode/escape input and output.	Y	To safeguard the data in IoT Cloud, IoT Edge Gateway, and devices, including inputs and commands. Recommended for IoT Cloud and IoT Edge Gateway This may apply to Lift and Escalator, and Rooftop Solar Inverter devices and where the protocols can support.
CK-DP-04	Do you enforce access control to detect and prevent unauthorized data access and exfiltration and filter your outputs?	Y	To safeguard aggregated data in IoT Cloud and IoT Edge Gateway from unauthorized access. Recommended for IoT Cloud and IoT Edge Gateway
6. Access protection			
CK-AP-01	Do you employ mechanisms to manage and secure local and/or remote access? Examples of mechanisms include: · auto logoff. · Screen lock. · Delay in between login attempts and lock-out for repeated unauthorized attempts. Forced re-authorization.	Y	To safeguard IoT Cloud and IoT Edge Gateway from unauthorized access, both locally and remotely, including physical access. Recommended for IoT Cloud and IoT Edge Gateway
CK-AP-02	Do you send out-of-band notifications on impactful operations and/or alerts (e.g., credential reset, security update failures)?	Y	To enable users to detect unauthorized attempts from alerts. Recommended for IoT Cloud and IoT Edge Gateway
CK-AP-03	Do you enforce access control to prevent unauthorized access to system interfaces, system files, and removable media?	Y	To safeguard against physical access to system/device interfaces. Recommended for IoT Cloud and IoT Edge Gateway
CK-AP-04	Do you employ anti-tamper mechanisms for resistance, evidence, detection, and/or response?	Y	To prevent and detect physical tampering. Recommended for: IoT Cloud and IoT Edge Gateway
CK-AP-05	Do you support multi-factor authentication for impactful operations (e.g., credential reset)?	Y	To safeguard impactful operations by requiring a higher level of authentication. Recommended for: IoT Cloud and IoT Edge Gateway

ID	Vendor disclosure checklist	Y / N / NA	Supporting materials
7. Security management			
CK-MT-01	Do you employ proper user and password management? Examples include: · Enforce a strong password policy. · Enforce no default passwords. · Specify password expiration. · Ensure that password recovery and reset mechanisms are secure.	Y	To safeguard access to IoT Platform Recommended for IoT Cloud and IoT Edge Gateway It is worth mentioning in certain cases/project deployment, disabling password login and using certificate based authentication is implemented.
CK-MT-02	Do you enforce proper access control to management functions? Examples include: · Enforce the least privilege policy. · Use of attribute-based access control (ABAC) or role-based access control (RBAC). · Implement dual control for key management protection to prevent a single bad actor's compromise to the key materials. · Support granular access permissions per user and per application. · Implement separation of duties to the key management system to prevent a single bad actor/administrator from compromising the system.	Y	To safeguard the administration functions of IoT Platform. Recommended for IoT Cloud and IoT Edge Gateway
CK-MT-03	Do you employ a malware mitigation mechanism? Examples include: · Ensure file integrity using a cryptographic hash. · Baseline "normal"behavior. · Detect unauthorized software. · Monitor devices and traffic flows. · Scan backup images. · Prohibit insecure bootloaders.	Y	To safeguard the integrity of the software. Recommended for: IoT Cloud and IoT Edge Gateway It will be useful to add if you have/deployed any threat detection/monitoring services, for example, endpoint detection and response?
CK-MT-04	Do you secure remote management of devices, including sensor gateways? Examples include: · Support secure Over-The-Air (OTA) updates of device applications and configurations. · Support software and/or firmware updates using cryptographically secure methods. · Support platform integrity checking, such as the measured boot mechanism or verifying the firmware integrity. Restrict remote management to secure networks.	Y	To safeguard the remote management function of Edge and devices, including remote updates. Recommended for: IoT Edge Gateway

ID	Vendor disclosure checklist	Y / N / NA	Supporting materials
8. Resiliency support			
CK-RS-01	Does your device support integrity self-test, error detection, and correction for critical functions and return to a safe state?	Y	To safeguard the integrity and availability of the system, devices are monitored and attested periodically. Recommended for: IoT Cloud and IoT Edge Gateway
CK-RS-02	Do you safeguard against a compromised device from compromising the system? Examples include: · Use of Perfect Forward Secrecy (PFS) for secure communication. · Use of distinct secret keys for an individual device.	Y	To safeguard the availability of the system in the event devices are compromised. For example, it is allowed for compromised devices to be disconnected manually. Recommended for: IoT Cloud and IoT Edge Gateway
CK-RS-03	Do you employ mechanisms against failures from resource exhaustion and/or malicious attacks such as DDoS? Examples include: · Monitor to ensure that cloud resources are sufficient to sustain services. · Detect resource exhaustion for early preventive or corrective actions · Control the execution of resource-intensive software. · Enforce power thresholds. · Limit the number of concurrent sessions. · Operate with excess capacity.	Y	To safeguard the availability of the system by detecting and preventing resource exhaustion. Recommended for: IoT Cloud
CK-RS-04	Do you conduct regular backups of system data (including settings)?	Y	To safeguard the availability of the system, ensuring the ability to recover from a compromised state. Recommended for: IoT Cloud
9. Security audit			
CK-AU-01	Do your devices and system record enough information (e.g., who does what and when) in audit logs and flag significant events? Examples of events include: · User logins, logouts, and unsuccessful authentication attempts. · Connection, disconnection attempts and unsuccessful connection attempts. · Unsuccessful authorization attempts. · Access to sensitive data. · Import and export of data from removable media. · Any change in access privileges. · Creation, modification, and deletion of data by user. · Impactful operations. · Remote operations. · Security update failures. · Physical access attempts where possible. · Emergency access where possible.	Y	To safeguard the system by having the ability to detect and analyze when attacks are realised. Recommended for: IoT Cloud and IoT Edge Gateway

ID	Vendor disclosure checklist	Y / N / NA	Supporting materials
CK-AU-02	Are your audit logs protected from modification, deletion, physical tampering, and sensitive data disclosure?	Y	To safeguard the confidentiality and integrity of audit logs. Recommended for: IoT Cloud and IoT Edge Gateway
10. Lifecycle protection			
CK-LP-01	Have you conducted threat modelling to identify, analyze and mitigate threats to the system?	Y	To understand and focus limited resources on what needs protection. Recommended for: IoT Cloud and IoT Edge Gateway
CK-LP-02	Did you design and develop the system using a secure systems engineering approach?	Y	To employ the "security by design" principle and develop a system/design using security best practices. Recommended for: IoT Cloud and IoT Edge Gateway
CK-LP-03	Do you implement and maintain the system with components from a secure supply chain with no known unmitigated vulnerabilities?	Y	To safeguard the supply chain of system components. In this case, maintain a list of suppliers for the components. Recommended for: IoT Cloud and IoT Edge Gateway
CK-LP-04	Do you provide, communicate and update security information (terms of service, features, guidelines, instructions, and notifications, etc.) in simple language and timely manner? Examples of security information include: · Security policies · Security updates · Instructions for device/media sanitization · End-of-life notifications · Phase-out plan.	Y	Ensure that there is an ownership and commitment to providing security information promptly so that known vulnerabilities can be mitigated. Recommended for: IoT Cloud and IoT Edge Gateway
CK-LP-05	Do you ensure that the system is hardened before the "Operational" lifecycle phase? Examples of system hardening include: · Remove all backdoors. · Remove all debug codes from the released version. · Change default configuration and disable unnecessary services. · Remove or tamper-covered JTAG, unneeded serial and ports before deployment. · Harden VM host properly, including disabling memory sharing between VM. · Remove default and hardcoded passwords.	Y	Employ the "security by defaults" principle and ensure the system is configured securely before operation. Recommended for: IoT Cloud and IoT Edge Gateway To minimize potential attack surfaces, if the product has unused features such as DHCP or Wi-Fi, it is also suggested to disable them.
CK-LP-06	Do you maintain an inventory of connected devices, software, firmware versions, applied patches, and updates throughout the "Operational" lifecycle stage?	Y	Employ the "accountability" principle to keep track that only authorized and patched devices are in use. Recommended for: IoT Cloud and IoT Edge Gateway
CK-LP-07	Do you conduct penetration testing and/or vulnerability assessment periodically and before each major release?	Y	Conduct periodic testing on the integrated system to detect vulnerabilities due to improper integration. For example, by going through Cyber Security Agency (CSA) Cybersecurity Labelling Scheme (CLS). Please send any enquiries on the Cybersecurity Labelling Scheme to certification@csa.gov.sg.

ID	Vendor disclosure checklist	Y / N / NA	Supporting materials
			Recommended for: IoT Cloud and IoT Edge Gateway and devices
CK-LP-08	Do you establish proper vulnerability disclosure and management? Examples include: · Ensure the supply chain's capability to provide upgrades and patches. · Provide vulnerability disclosure and processes to track and respond promptly. · Provide firmware and software patches/updates for vulnerabilities discovered on time. · Employ proper change management processes to manage security patches or updates. · Notify and/or allow the user to approve/reject updates, patches, and changes to user settings, where appropriate. · Disclose minimum support period.	Y	Build resilience by establishing ownership and standard operating procedures (SOPs) to disclosure, manage and resolve the vulnerability. Recommended for: IoT Cloud and IoT Edge Gateway Further to vulnerability disclosure, it is also recommended the vendor implement/establish both a threat & vulnerability management system as well as cybersecurity incident and response plan with playbooks and workflow process. This will help the organization to respond to cybersecurity incidents in a more organized and responsive manner.
CK-LP-09	Do you ensure that identities, certificates, and secrets are secured throughout the lifecycle (e.g., creation, provisioning, renewal, and revocation)?	Y	By the "accountability" principle, the identities and secrets should be safeguarded throughout their lifecycles. Recommended for: IoT Cloud and IoT Edge Gateway
CK-LP-10	Do you sanitize devices and systems of security data and sensitive user data before the "Reuse or Dispose of" lifecycle stages?	Y	The "accountability" principle should safeguard sensitive data throughout the system/device's lifecycles. Recommended for: IoT Cloud and IoT Edge Gateway

Table C-9: Usage of Vendor disclosure checklist

7. Additional resources

Readers, who are also interested in the implementations of specific vendors, can refer to the following non-exhaustive list of online resources:

- "Case Study on Smart Facilities Security through Envision EnOS" whitepaper by Envision: https://developer.envisioniot.com/contactus/
- "Building resilience, through visibility." whitepaper by Honeywell: https://buildings.honeywell.com/content/dam/hbtbt/en/documents/downloads/Cybersecurity%20-%20Building%20Resilience,%20Through%20Visibility.pdf
- "A Practical Framework for Cyber Secure, Cloud Connected Smart Building Control Systems" whitepaper by Schneider Electric: https://download.schneider-electric.com/files?p_enDocType=Brochure&p_File_Name=998-20437895+A+Practical+Framework+for+Cyber+Secure+Cloud+Connected+Smart+Building+Control+Systems+-+White+Paper.pdf