Guidelines

Internet of Things (IoT) Cyber Security Guide

Annex B
Case Study on Home Control System

In consultation with:

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

CSA SINGAPORE

IMDA IoT Cyber Security Guide Annex B
Version 2, Oct 2025

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 B: Case Study on Home Control System (informative)

1 Overview

This annex introduces a case study on Home Control System (**HCS**) and demonstrates the application of the recommendations in the main document to this case study. While STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) is the model used to help analyse and find threats to the system. It should be noted that other methodologies exist and might be more appropriate for specific use cases. It should also be noted that this case study is not meant to be exhaustive, and the sample application is not definitive of HCS, but for illustrative purposes only.

Table B-1 depicts the threat modelling checklist, defined in the main document, and its application to the case study on HCS.

ID	Threat modelling checklist	Y (yes) / N (no)	Supporting materials
1	Identify the potential target(s) to be protected: i) Define its boundaries and the external systems (including users) that it needs to interact with ii) Decompose the target(s) into its subcomponents iii) Identify data flows within the target(s), and inputs and outputs from external systems iv) Identify sensitive data and where they are handled (at rest, in transit, in use) v) Identify the security needs (based on potential impacts to Confidentiality, Integrity and Availability (CIA triad)) for subcomponents and data flows vi) Identify hardware, software and protocols in use	Y	Refer to section 2
2	Define the security problem: i) Identify system accessibility – Identify attack surfaces – Determine operating environments – Determine system / device lifecycles and supply chain ii) Identify system susceptibility / vulnerabilities (e.g. using STRIDE as a guide) – Determine known vulnerabilities – Enumerate threats to attack surfaces – Enumerate threats to operating environments – Enumerate threats to stages of system / device lifecycles and supply chain iii) State any assumptions	Y	Refer to section 3
3	Conduct risk assessment: i) Assess impact of threats and vulnerabilities to CIA triad and match against security needs of assets ii) Determine the system exploitability (resources required, techniques and tools available) to realise threats. iii) Assess the likelihood of the risk iv) Prioritise risks for mitigation, considering factors such as monetary impacts.	Y	Refer to section 4
4	Determine the security objectives. For example, OT system emphasises safety, where integrity takes precedent over confidentiality.	Y	Refer to section 5

ID	Threat modelling checklist	Y (yes) / N (no)	Supporting materials
5	Define the security requirements needed to address identified security objectives, without specifying their implementation details.	Y	Refer to section 6
6	Design and implement the security capabilities	N	Not cover in this document
7	Validate and verify that the capabilities address the security requirements adequately	N	Not cover in this document

Table B-1: Application of threat modelling checklist

2 Identify the Target of Protection

This section illustrates the guidance provided by item-1 of the threat modelling checklist, which helps to identify the Target Of Protection (**TOP**) for the case study on HCS.

Figure B-1 is the system architecture of the defined case study, which demonstrates the guidance provided by the threat modelling checklist.

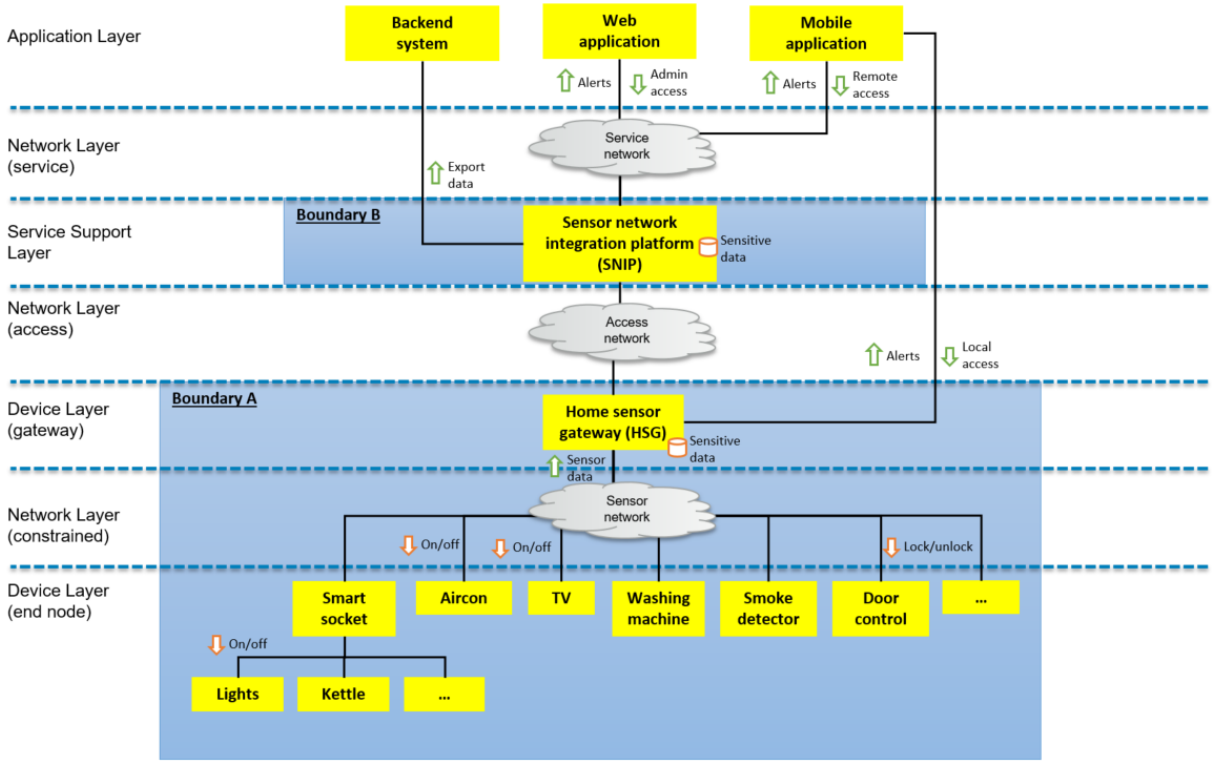

Figure B-1: System architecture of HCS

Two system boundaries for the case study on HCS are defined. Boundary A is defined to cover all the subcomponents within the home setting, while Boundary B is defined to contain the Sensor Network Integration Platform (**SNIP**) hosted on a cloud infrastructure.

Within boundary A, it is defined that the sensor network is based on WiFi connectivity and Home Sensor Gateway (**HSG**) mediate between devices on sensor network and SNIP on access network. HSG can potentially host sensitive data. HSG aggregates sensing data from the connected devices and can also send commands to devices where control is permissible. HSG allows authorised users to access and issue commands for its connected devices, both remotely over the service network (internet or dedicated network) and locally within the home (e.g. using WiFi connectivity). HSG can also operate in local mode, where access network is not available. The devices (lights and kettle) connected to the smart socket are not smart devices. Lights are enabled for control through a pairing mechanism with the smart socket. We defined kettle as not control permissible.

SNIP is a digital platform that aggregates sensing data from multiple gateways of multiple homes and probably host sensitive data. It is connected to the enterprise backend system and may export data in bulk for various purposes, for example, archival. The SNIP supports both web and mobile interfaces for operation and administration purposes.

Table B-2 determines the security needs of the assets, with respect to CIA triad. It helps in prioritising which assets and which aspects to secure.

Legend: H = high, M = moderate, L = low

Assets	Confidentiality	Integrity	Availability	Rationale
Sensor network integration platform (SNIP)	H	H	H	Confidentiality is high as SNIP contains sensitive data. Integrity is high to safeguard commands invocation. Availability is important because of the need to support many users.
Home sensor gateway (HSG)	H	H	M	Confidentiality and integrity is the same as SNIP. Availability is moderate as only one household is impacted.
Device: Aircon	L	M	L	Integrity is relatively more important because of monetary impact when aircon is on instead of off.
Device: TV	M	H	L	Integrity is high because compromised TV can participate in DDoS. Confidentiality is moderate because disclosure of watching habits can impact privacy.
Device: Washing machine	L	L	L	
Device: Smoke detector	L	H	M	Integrity is high, in order to gain first responder's trust in the system.
Device: Door control	M	H	H	Integrity and availability is very important for the proper operation for this device. Since this device does not contains sensitive data, confidentiality is moderate as we still want to keep activity information private as far as possible
Device: Smart socket	L	H	M	Integrity is high for safety considerations. Additional restriction might apply. For example, when kettle is connected, remote access is disallowed.
Device: Lights	L	M	M	Integrity and availability is moderate as importance of lighting is contextual. For example, use of lights at night time.
Device: Kettle	L	H	L	Integrity is high for safety considerations.

Table B-2: Security needs of assets

Table B-3 determines the security needs of the data flows between assets, with respect to 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 flows	Confidentiality	Integrity	Availability	Rationale
Devices → HSG	M	H	H	The impact to CIA triad for this data flow is determined using high watermark method on the security needs of devices on the same sensor network.
HSG → SNIP	H	H	H	The impact to CIA triad for this data flow is determined using high watermark method on the security needs of SNIP and HSG.
SNIP → Backend system	H	H	L	SNIP exports data for backup at backend system. Safeguarding the confidentiality and integrity of exported data is more important, relative to availability.
Web application ←→ SNIP → HSG → Devices	H	H	H	Administration of SNIP and devices requires high confidentiality and integrity. Alerts requires high availability.
Mobile application ←→ SNIP → HSG → Device	H	H	H	Remote access to devices, through SNIP requires high confidentiality and integrity. Alerts requires high availability.
Mobile application ←→ HSG → Devices	M	H	M	Local access to devices, through HSG requires high integrity for safety considerations. Confidentiality is moderate as this data flow is transactional and not sensitive. Alerts requires moderate availability.

Table B-3: Security needs of data flows

3 Define the security problem

This section illustrates the guidance provided by item-2 of the threat modelling checklist, which helps to define the security problem for the case study on HCS.

Table B-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 (attack surfaces, operating environments, lifecycles)	System susceptibility (known vulnerabilities*, STRIDE)
Sensor network integration platform (SNIP)	The following attack surfaces are relevant for SNIP: bulk API, web API, mobile API, HTTP/IP, storage SW & HW, memory, VM, OS, firmware, server software The SNIP is assumed to be hosted in the cloud and accessible from the internet. All stages of system lifecycle needs to be considered.	Refer to "OWASP Top 10 Application Security Risks" Scan for relevant known vulnerabilities from prominent vulnerability repositories. Eg. https://cve.mitre.org
Home sensor gateway (HSG)	The following attack surfaces are relevant for HSG: management API, mobile API, HTTP/IP, WiFi, storage SW & HW, memory, VM, OS, firmware, middleware, communication ports, device ID. WiFi connectivity is assumed. The HSG is assumed to operate in the home setting and accessible from the internet. All stages of device lifecycle needs to be considered.	Refer to "OWASP IoT Attack Surface Areas" and "OWASP IoT Vulnerabilities" Scan for relevant known vulnerabilities from prominent vulnerability repositories. Eg. https://cve.mitre.org
Device: Aircon	The following attack surfaces are relevant for Aircon: API for sensing/actuating, WiFi, firmware, device ID. . WiFi connectivity is assumed. The Aircon is assumed to operate in the home setting and accessible from HSG only. All stages of device lifecycle needs to be considered.	Refer to "OWASP Mobile Top 10 Risks" Scan for relevant known vulnerabilities from prominent vulnerability repositories. Eg. https://cve.mitre.org
Device: TV	Similar concerns as HSG	Similar concerns as HSG
Device: Washing machine	Similar concerns as Aircon	Similar concerns as Aircon
Device: Smoke detector	Similar concerns as Aircon	Similar concerns as Aircon
Device: Door control	Similar concerns as Aircon	Similar concerns as Aircon
Device: Smart socket	Similar concerns as Aircon	Similar concerns as Aircon
Device: Lights	The attack surfaces relevant for Lights are device ID as its "smartness" are provided by the smart socket it is connected to.	Vulnerability to parting process between lights and smart socket
Device: Kettle	Similar concerns as Lights	Similar concerns as Lights

Table B-4: System accessibility and susceptibility

4 Conduct risk assessment

This section illustrates the guidance provided by item-3 of the threat modelling checklist, which guide how risk assessment is conducted for the case study on HCS.

Table B-5 demonstrates a risk assessment of system accessibility and system susceptibility for each asset. It is useful 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)	Rationale
Sensor network integration platform (SNIP)	H	H	System accessibility of SNIP is high because it is hosted over the internet. System susceptibility is high because there is many known vulnerabilities. Refer to "OWASP Top 10 Application Security Risks"
Home sensor gateway (HSG)	H	H	System accessibility of HSG is determined to be high. HSG is required to support multiple networks and connectivity from diverse devices increasing the attack surfaces. HSG operates in the home setting with risk of physical access. HSG may transfer ownership during its lifecycle. System susceptibility of HSG is determined to be high because there are many known vulnerabilities. Refer to "OWASP IoT Attack Surface Areas" and "OWASP IoT Vulnerabilities".
Device: Aircon	M	M	System accessibility and susceptibility of aircon is determined to be moderate. The assumption is wireless connectivity is used.
Device: TV	H	H	System accessibility and susceptibility of TV is determined to be high. TV hosts web applications which increases its attack surfaces. It operates in home setting with risk of physical access and may transfer ownership during its lifecycle. Refer to "OWASP Mobile Top 10 Risks"
Device: Washing machine	M	M	System accessibility and susceptibility of washing machine is determined to be moderate. The assumption is wireless connectivity is used.
Device: Smoke detector	L	L	System accessibility and susceptibility of smoke detector is determined to be low, when wired connectivity is used.
Device: Door control	M	M	System accessibility and susceptibility of door control is determined to be moderate. The assumption is wireless connectivity is used.
Device: Smart socket	M	M	System accessibility and susceptibility of smart socket is determined to be moderate. The assumption is wireless connectivity is used.
Device: Lights	H	M	System accessibility of light is determined to be high, because it is removable.
Device: Kettle	H	M	System accessibility of kettle is determined to be high, because it is removable.

Table B-5: Assessment of system accessibility and susceptibility

Table B-6 demonstrates a risk assessment of system exploitability. It determines a list of attacker types (script kiddies, criminals, hacktivist, terrorists, state sponsored, etc) that have 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	System exploitability	Rationale
Sensor network integration platform (SNIP)	H	The asset is valuable to a range of attackers (script kiddies, criminals, hacktivist, terrorists, state sponsored),including some with high capabilities and resources.
Home sensor gateway (HSG)	H	The asset is valuable to a range of attackers (script kiddies, criminals, hacktivist, terrorists, state sponsored),including some with high capabilities and resources.
Device: Aircon	L	The asset is valuable to script kiddies only.
Device: TV	M	The asset is valuable to a range of attackers (script kiddies, criminals, hacktivist) with moderate capabilities and resources.
Device: Washing machine	L	The asset is valuable to script kiddies only.
Device: Smoke detector	M	The asset is valuable to script kiddies and criminals with moderate capabilities and resources.
Device: Door control	M	The asset is valuable to script kiddies and criminals with moderate capabilities and resources.
Device: Smart socket	M	The asset is valuable to script kiddies and criminals with moderate capabilities and resources.
Device: Lights	M	The asset is valuable to criminals with moderate capabilities and resources.
Device: Kettle	L	The asset is not valuable to attacker.

Table B-6: Assessment of system exploitability

Table B-7 determines the priority for mitigation of the threats for each asset, with holistic considerations for risks of system accessibility, system susceptibility and system exploitability. For illustrative purposes, our case study will only elaborate on the high priority items for mitigation in subsequent sections.

Legend: H = high, M = moderate, L = low

Assets	System accessibility (attack surfaces, operating environments, lifecycles)	System susceptibility (known vulnerabilities, STRIDE)	System exploitability	Priority
Sensor network integration platform (SNIP)	H	H	H	H
Home sensor gateway (HSG)	H	H	H	H
Device: Aircon	M	M	L	
Device: TV	H	H	M	H
Device: Washing machine	M	M	L	
Device: Smoke detector	L	L	M	
Device: Door control	M	M	M	H
Device: Smart socket	M	M	M	H
Device: Lights	H	M	M	
Device: Kettle	H	M	L	

Table B-7: Assessment of priority

5 Determine the security objectives

This section illustrates the guidance provided by item-4 of the threat modelling checklist, which guide how security objectives is determined for the case study on HCS.

Table B-8 demonstrates the definition of security objectives for the threat modelling process. For illustrative purposes, we limit the assets to those identify as high priority in Table B-7. The needs of CIA triad for the assets are identified in Table B-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
Sensor network integration platform (SNIP)	H	H	H	1. Ensure confidentiality of sensitive data. 2. Ensure confidentiality and integrity of data and commands. 3. Provide proper access control 4. Ensure integrity of system 5. Resilience against DOS. 6. Prevent multitenancy from compromising security
Home sensor gateway (HSG)	H	H	M	1. Ensure confidentiality of sensitive data. 2. Ensure confidentiality and integrity of data and commands. 3. Provide proper access control 4. Ensure integrity of HSG 5. Fail safely 6. Prevent multitenancy from compromising security
Device: TV	M	H	L	1. Ensure confidentiality and integrity of data and commands. 2. Ensure integrity of TV 3. Prevent multitenancy from compromising security
Device: Door control	M	H	H	1. Ensure confidentiality and integrity of data and commands. 2. Provide proper access control 3. Ensure integrity of door control 4. Ensure availability
Device: Smart socket	L	H	M	1. Fail safely 2. Ensure integrity of data and commands. 3. Provide proper access control, including verifying connected devices 4. Ensure integrity of smart socket

Table B-8: Security objectives

In addition, Table B-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 the threat modelling checklist, which help definition of security requirements for the case study on HCS. It should be noted that the checklist is only a template of common security considerations. Users are required to determine the appropriateness and applicability of the checklist items so as to add on, remove, and/or adjust them according to the uses and businesses' needs.

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

Vendor disclosure checklist	**Y (yes) / N (no) / NA (not applicable)**	**Supporting materials**
1. Cryptographic support		
CHECK-CS-01: Do your devices and system employ industry-accepted cryptography and best practices? Examples include the use of: a) Accepted algorithms and their correct implementation and application. b) Accepted entropy sources and approved random number generator(s). c) Sufficient key length. d) Sufficient crypto-period. e) Use of updatable cryptography.	Y	The strength of cryptography is fundamental to safeguard the objectives of confidentiality and integrity. In particular, the cryptography must be approved for the lifetime of the devices. Recommended for: SNIP, HSG, TV, Door control, Smart socket
CHECK-CS-02: Do you define and implement proper key management practices (generation, exchange, storage, use, destruction and replacement) accordingly to industry-accepted best practices and recommendations?	Y	Proper key management is required to prevent the disclosure of keys through the system/device lifecycles. Recommended for: SNIP, HSG, TV, Door control, Smart socket
2. Security function protection		
CHECK-FP-01: Do you employ and properly implement a trusted computing base (TCB) according to industry-accepted recommendations and best practices? The TCB should include: a) policies; b) hardware; c) firmware; d) operating systems; e) virtualisation; f) software; g) basic input/output system; h) system services; i) device drivers;	Y	Recommended for: SNIP, HSG

Vendor disclosure checklist	Y (yes) / N (no) / NA (not applicable)	Supporting materials
j) protocols; k) RoT; and l) trust anchor.		
CHECK-FP-02: Do you establish RoT for your devices and system, according to industry-accepted best practices and recommendations?	Y	To safeguard the confidentiality and integrity of sensitive data (e.g. keys) at rest and in use. Recommended for: SNIP, HSG, TV Optional for: Door control, Smart socket
CHECK-FP-03: Do you employ secure boot mechanisms to protect and verify software according to industry-accepted best practices and recommendations? If an unauthorised change to the software is detected, the device should alert the user and/or administrator to the issue and should not connect to wider networks than those necessary to perform the alerting function.	Y	To safeguard integrity of the boot process. Recommended for: SNIP, HSG, TV
CHECK-FP-04: Do you protect security data elements, such as credentials, keys, and tokens, from unauthorised disclosure and modification according to industry-accepted best practices and recommendations?	Y	Recommended for: SNIP, HSG
3. Identification and authentication		
CHECK-IA-01: Do you establish unique, non-modifiable, and verifiable identities for IoT entities (i.e., users, platforms, gateways, devices)?	Y	To safeguard the integrity of identification to mitigate against threats of spoofing. Recommended for: SNIP, HSG, TV, Door control, Smart socket
CHECK-IA-02: Do you securely provision and manage the credentials of IoT entities (i.e., users, platforms, gateways, devices)? For example, by being salted, hashed, or encrypted.	Y	
CHECK-IA-03: Do you employ secure authentication mechanisms according to industry-accepted best practices and recommendations?	Y	
CHECK-IA-04: Do you establish mutual authentication before any interactions between clients (users, devices, gateways, applications) and servers?	Y	To safeguard the integrity of connections to prevent unauthorised remote access. Recommended for: SNIP, HSG, TV, Door control, Smart socket
4. Network protection		
CHECK-NP-01: Do you employ proven transport protocols and recommended network services with properly activated security controls? Examples of best practices for transport protocols include using the following: a) TLS for TCP payloads. b) DTLS for UDP payloads.	Y	To safeguard the confidentiality and integrity of the payloads. Recommended for: SNIP, HSG, TV, Door control, Smart socket

Vendor disclosure checklist	Y (yes) / N (no) / NA (not applicable)	Supporting materials
c) TLS for MQTT. d) HTTPS.		
CHECK-NP-02: Do you establish secure connectivity according to industry-accepted best practices and recommendations? Examples include: a) Use of VPN. b) Use of private mobile access point names (APN) from telecommunication operators when using a public mobile carrier network. c) Use of secure DNS to prevent DNS spoofing. d) Use of traffic filtering based on type, port, and destination. e) Use of mutual TLS (mTLS). f) Use whitelisting to establish or deny connections from non-trusted sources. Additionally, IETF Request for Comments (RFC) 8520 Manufacturer Usage Description (MUD) can be a mechanism for devices to provide this information to the network.	Y	Applicable to safeguard the data flows highlighted in Table B.3 Recommended for: SNIP, HSG, TV, Door control, Smart socket
CHECK-NP-03: Do you employ segregation of communication channels for endpoints with varying trust-levels according to industry-accepted best practices and recommendations? Examples include using VLAN, firewalls for DMZ, unidirectional security gateway, network segmentation or micro-segmentation, and physical isolation.	Y	Applicable to safeguard the data flows highlighted in Table B.3 SNIP and HSG can segregate communication channels for administration purposes from normal operations. SNIP should establish DMZ, using firewalls, against remote connections from devices and users. HSG should safeguard the devices within home, from connections outside the home. Recommended for: SNIP, HSG, TV, Door control, Smart socket
CHECK-NP-04: Do you implement network monitoring and access control according to organisational information flow control policy? Examples of access control include: a) Use of secure authorisation mechanisms for each connection to join a network. b) Use of secure de-authorisation mechanisms for each connection to disconnect and forget a network.	Y	Proper access control is required to limit access to the system networks. Recommended for: SNIP, HSG, TV, Door control, Smart socket
5. Data protection		
CHECK-DP-01: Do you protect data in transit, in use, and at rest, from unauthorised disclosure and modification according to industry-accepted best practices and recommendations? Examples of data include, but are not limited to, security data, personal data, sensing data, metadata, event logs, software, and their configurations.	Y	To safeguard the confidentiality and integrity of sensitive data. Sensitive data includes cryptographic keys and user credentials. Recommended for: SNIP, HSG, TV, Door control, Smart socket

Vendor disclosure checklist	Y (yes) / N (no) / NA (not applicable)	Supporting materials
CHECK-DP-02: Do you provide evidence and means to attest the authenticity and integrity of data-in-transit, data-in-use, and data-at-rest according to industry-accepted best practices and recommendations? Examples include using hashing and digital signatures. These data include sensing data, software, and its configurations.	Y	To safeguard the software and firmware in SNIP, HSG and devices, including transportation of updates. Recommended for: SNIP, HSG, TV, Door control, Smart socket
CHECK-DP-03: Do you implement input validation to safeguard input data, which includes commands and sensing data? Examples of input validation include: a) Validating incoming content types. b) Validating response types. c) Validating the HTTP methods against authorisation credentials. d) Whitelisting allowable HTTP methods. e) Defining the acceptable character set, e.g., Unicode Transformation Format-8 (UTF-8). f) Validating that input characters are acceptable. g) Encoding/escaping input and output. h) Checking for anomalies.	Y	To safeguard the data in SNIP, HSG and devices, including inputs and commands. Recommended for: SNIP, HSG, TV, Door control, Smart socket
CHECK-DP-04: Do you enforce access control to detect and prevent unauthorised data access and data exfiltration? Additionally, do you verify and filter independently data output, including commands and processed sensing data?	Y	To safeguard aggregated data in SNIP and HSG from unauthorised access. Recommended for: SNIP, HSG
6. Access protection		
CHECK-AP-01: Do you employ session management to secure interactions for different clients according to industry-accepted best practices and recommendations? Examples include: a) Verify and protect the integrity of sessions. b) Restrict access by client types. c) Restrict data transfer and file transfer by clients.	Y	
CHECK-AP-02: Do you implement lock-out mechanism to protect against repeated unauthorised attempts by any user (human, software or device)? Examples of mechanisms include delay in between login attempts, lock-out for repeated unauthorised attempts, and forced reauthorisation.	Y	To safeguard SNIP and HSG from unauthorised access, both locally and remotely, including physical access. Recommended for: SNIP, HSG
CHECK-AP-03: Do you employ multi-factor authentication (for user access) and timely notifications?	Y	To safeguard impactful operations by requiring higher level of authentication. Recommended for: SNIP, HSG, TV, Door control, Smart socket
CHECK-AP-04: Do you enforce physical and remote access restriction to safeguard against unauthorised access to assets, equipment, user devices, removable media, and interfaces?	Y	To safeguard against physical access to system/device interfaces.

Vendor disclosure checklist	Y (yes) / N (no) / NA (not applicable)	Supporting materials
		Recommended for: SNIP, HSG, TV, Door control, Smart socket
CHECK-AP-05: Do you employ anti-tampering mechanisms to detect, prevent, make evident and/or respond to physical attacks?	Y	To prevent and detect physical tampering. Recommended for: HSG, TV, Door control, Smart socket
7. Security audit		
CHECK-AU-01: Do you synchronise your clocks to authoritative time sources to provide timestamps for audit records?	Y	Recommended for: SNIP, HSG
CHECK-AU-02: Do you record security events to facilitate monitoring, analysis, and timely alerts raised (e.g., who does what and when) regarding activities performed? Examples of security events include the following: a) User logins, logouts, and unsuccessful authentication attempts. b) Connection, disconnection attempts and unsuccessful connection attempts. c) Unsuccessful authorisation attempts. d) Access to sensitive data. e) Import and export of data from removable media. f) Any change in access privileges. g) Creation, modification, and deletion of data by user. h) Remote operations. i) Security update failures. j) Physical access attempts where possible. k) Emergency access where possible. l) Configuration changes.	Y	To safeguard the system by having the ability to detect and analyse when attacks are realised. Recommended for: SNIP, HSG, TV
CHECK-AU-03: Do you protect audit records from unauthorised operations (create, read, update and delete)? Do you allocate sufficient record storage, and raise timely alerts before records are overwritten?	Y	To safeguard the confidentiality and integrity of audit logs. Recommended for: SNIP, HSG
8. Security management		
CHECK-SM-01: Do you employ strong credential management according to industry-accepted best practices and recommendations? Examples include: a) Enforcing a strong password policy. b) Enforcing no default passwords. c) Specifying password expiration periods. d) Ensuring that password recovery and reset mechanisms are secure. e) Randomising pre-loaded login credentials.	Y	To safeguard access to SNIP, HSG and TV (device with mobile operating system) Recommended for: SNIP, HSG, TV

Vendor disclosure checklist	Y (yes) / N (no) / NA (not applicable)	Supporting materials
f) Use of FIDO2 security tokens.		
CHECK-SM-02: Do you employ access control policies and mechanisms to manage system, networks, and devices according to industry-accepted best practices and recommendations. Examples include: a) Use of attribute-based access control (ABAC) or role-based access control (RBAC). b) Enforce a least privilege policy. c) Restrict and manage privilege access rights.	Y	To safeguard the administration functions of SNIP and HSG from normal operations. Recommended for: SNIP, HSG
CHECK-SM-03: Do you employ protection mechanisms to detect and mitigate the effects of unauthorised and malicious software and hardware? Examples include the following: a) Ensuring file integrity using cryptographic hash. b) Baselining normal behaviour. c) Detecting unauthorised software. d) Monitoring devices and traffic flows. e) Scanning software and backup images. f) Prohibiting insecure bootloaders.	Y	To safeguard the integrity of the software. Recommended for: SNIP, HSG, TV
CHECK-SM-04: Do you employ protection mechanisms to secure the remote management of devices and gateways? Examples include: a) Supporting secure OTA updates of device applications and configurations. b) Supporting software and/or firmware updates using secure processes and cryptographically secure methods. c) Supporting platform integrity checking such as the measured boot mechanism or verifying the firmware integrity. d) Restricting remote management to secure networks.	Y	To safeguard the remote management function of HSG and devices, including remote updates. Recommended for: SNIP, HSG, TV Optional for: Door control, Smart socket
9. Resiliency support		
CHECK-RS-01: Do you employ mechanisms to support integrity self-test, error detection, correction for critical functions, and return to a safe state? For example, leaving the device in a state that minimises potential for harm during an unexpected interruption of an update, taking into account the risks of the IoT device not functioning as expected.	Y	To safeguard integrity and availability of the system, devices are monitored and attested periodically. Recommended for: HSG, TV, Door control, Smart socket
CHECK-RS-02: Do you implement measures to protect against failures from outages, resource exhaustion, and/or malicious DoS attacks? Examples include the following:	Y	To safeguard availability of the system by detecting and preventing resource exhaustion. Recommended for: SNIP

Vendor disclosure checklist	Y (yes) / N (no) / NA (not applicable)	Supporting materials
a) Monitoring to ensure that cloud resources are sufficient to sustain services. b) Detecting resource exhaustion for early preventive or corrective actions. c) Controlling the execution of resource-intensive software. d) Enforcing power thresholds. e) Limiting the number of concurrent sessions. f) Having the capacity to operate during resource outages (e.g., power, network) or the ability to operate in a degraded mode.		
CHECK-RS-03: Do you employ mechanisms to periodically back up system data, including their settings? Do you conduct disaster recovery exercises to verify the backup and recovery mechanisms?	Y	To safeguard availability of the system ensuring the ability to recover from a compromised state. Recommended for: SNIP, HSG
CHECK-RS-04: Do you maintain or degrade the IoT system and devices to a safe and expected state on encountering errors/failures? Do you provide timely alerts, with sufficient information, to relevant authorised users to support effective remediation?	Y	Recommended for: Door
10. Lifecycle support		
CHECK-LP-01: Do you conduct threat modelling to identify, analyse, assess, and document threats to the IoT system?	Y	To understand and focus limited resources to what needs protection. Recommended for: SNIP, HSG, TV, Door control, Smart socket
CHECK-LP-02: Do you design and develop your IoT solution according to industry-accepted secure systems engineering approaches, best practices, and recommendations?	Y	To employ "security by design" principle and develop system/design using secure best practices. Recommended for: SNIP, HSG, TV, Door control, Smart socket
CHECK-LP-03: Do you construct and maintain your IoT solution using components 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: SNIP, HSG, TV, Door control, Smart socket
CHECK-LP-04: Do you identify and manage supply chain risks with defined processes and procedures, including risks from the use of opensource software?	Y	
CHECK-LP-05: Do you harden your IoT solution before putting it into operation? Examples of system hardening include the following: a) Removing all backdoors; b) Removing all debug codes from the released version; c) Enabling secure configuration and settings;	Y	Employ "security by defaults" principle and ensure the system is configure securely before operation. Recommended for: SNIP, HSG, TV, Door control, Smart socket

Vendor disclosure checklist	Y (yes) / N (no) / NA (not applicable)	Supporting materials
d) Removing unnecessary software and services; e) Removing or tamper-covered JTAG; f) Removing unnecessary serial ports and other ports before deployment; g) Appropriate hardening of VM host, including disabling memory sharing between VMs; h) Removing default and hardcoded passwords; and i) Removing unused networks and interfaces.		
CHECK-LP-06: Do you provide, communicate, and update security information in a timely manner? Examples of security information include the following: a) Terms of service. b) Support policies. c) Security guidelines, instructions, and educational materials. d) Security notifications and updates. e) Instructions for device/media sanitisation. f) Phase out plan and end-of-life notifications.	Y	To ensure that there is an ownership and commitment to provide security information in a timely manner so that known vulnerabilities can be mitigated. Recommended for: SNIP, HSG, TV, Door control, Smart socket
CHECK-LP-07: Do you maintain an information inventory of system components and assets throughout the IoT system operation? Examples include the following: a) Supplier information. b) Hardware models and versions, including physical locations. c) Software and firmware versions, including applied patches and updates. d) Configurations and settings, including IP addresses, ports, protocols, and services. e) Maintenance status.	Y	Employ the “accountability” principle to keep track that only authorised and patched devices are in use. Recommended for: SNIP, HSG, TV, Door control, Smart socket
CHECK-LP-08: Do you conduct penetration testing and vulnerability scanning as part of the security assessment, before commissioning, periodically, and before each major release? Do you enable and test all optional, non-default features of the IoT devices for security?	Y	Conduct periodic testing on the integrated system to detect vulnerabilities due to improper integration. Recommended for: SNIP, HSG, TV, Door control, Smart socket
CHECK-LP-09: Do you establish vulnerability management and disclosure according to industry-accepted best practices and recommendations? Examples include the following: a) Ensuring the supply chain's capability to provide upgrades and patches. b) Providing vulnerability disclosure and processes to track and respond promptly.	Y	Build resilience by establishing ownership and standard operating procedures (SOPs) to disclosure, manage and resolve vulnerability. Recommended for: SNIP, HSG, TV, Door control, Smart socket

Vendor disclosure checklist	**Y (yes) / N (no) / NA (not applicable)**	**Supporting materials**
c) Providing firmware and software patches/updates for discovered vulnerabilities in a timely manner. d) Employing proper change management processes to manage security patches or updates. e) Notifying and/or allowing users to approve/reject updates, patches, and changes to user settings, where appropriate. f) Disclosing minimum support period.		
CHECK-LP-10: Do you manage identities, certificates, and secrets securely throughout their lifecycles, including creation, provisioning, renewal, and revocation?	Y	By the "accountability" principle, the identities and secrets should be safeguard throughout their lifecycles. Recommended for: SNIP, HSG, TV, Door control, Smart socket
CHECK-LP-11: Do you employ mechanisms for the proper disposal of devices and systems, and for resetting or sanitising sensitive data by authorised users when feasible, according to industrial best practices? Examples include the option to factory reset, erase and zeroise both security data and user data.	Y	By the "accountability" principle, the sensitive data should be safeguard throughout the system/device's lifecycles. Recommended for: SNIP, HSG, TV, Door control, Smart socket

Table B-9: Usage of Vendor disclosure checklist