# Guidelines

# Internet of Things (IoT) Cyber Security Guide

## Annex B
## Case Study on Home Control System

In consultation with:

**IMDA IoT Cyber Security Guide Annex B**
**Version 1, Mar 2020**

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 / N | Supporting materials |
|---|---|---|---|
| 1 | Identify the potential targets to be protected<br>a. Define its boundaries and the external systems (including users) that it needs to interact with<br>b. Decompose the target(s) into its subcomponents<br>c. Identify data flows within the target(s), and inputs and outputs from external systems<br>d. Identify sensitive data and where they are handled (at rest, in transit, in use)<br>e. Identify the security needs (based on potential impacts to Confidentiality, Integrity and Availability (CIA) triad) for subcomponents and data flows<br>f. Identify hardware, software and protocols in use | Y | Refer to section 2 |
| 2 | Define the security problem<br>a. Identify system accessibility<br>• Identify attack surfaces<br>• Determine operating environments<br>• Determine system / device lifecycles and supply chain<br>b. Identify system susceptibility (aka vulnerabilities)<br>• Determine known vulnerabilities<br>• Enumerate threats to attack surfaces (using Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege (**STRIDE**) as a guide)<br>• Enumerate threats  to operating environments (using STRIDE as a guide)<br>• Enumerate threats to stages of system / device lifecycles and supply chain (using STRIDE as a guide)<br>c. State any assumptions | Y | Refer to section 3 |
| 3 | Conduct risk assessment<br>• Assess impact of threats and vulnerabilities to CIA triad and match against security needs of assets<br>• Assess attacker capabilities required to realise the threats<br>• Assess the likelihood of the risk<br>• Prioritise the risks for mitigation, including other considerations (e.g. monetary, safety, social and usability impacts) | Y | Refer to section 4 |

| ID | Threat modelling checklist | Y / N | Supporting materials |
|---|---|---|---|
| 4 | Determine the security objectives<br>• 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<br>• 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 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.

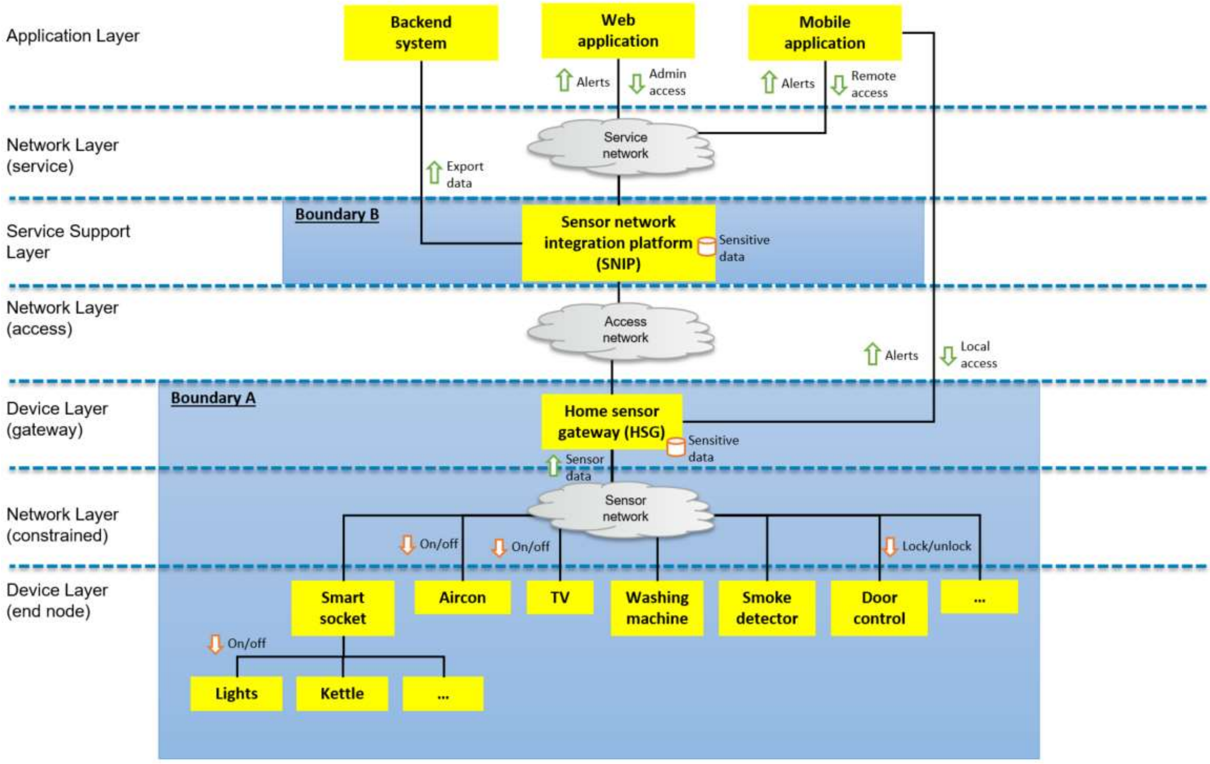


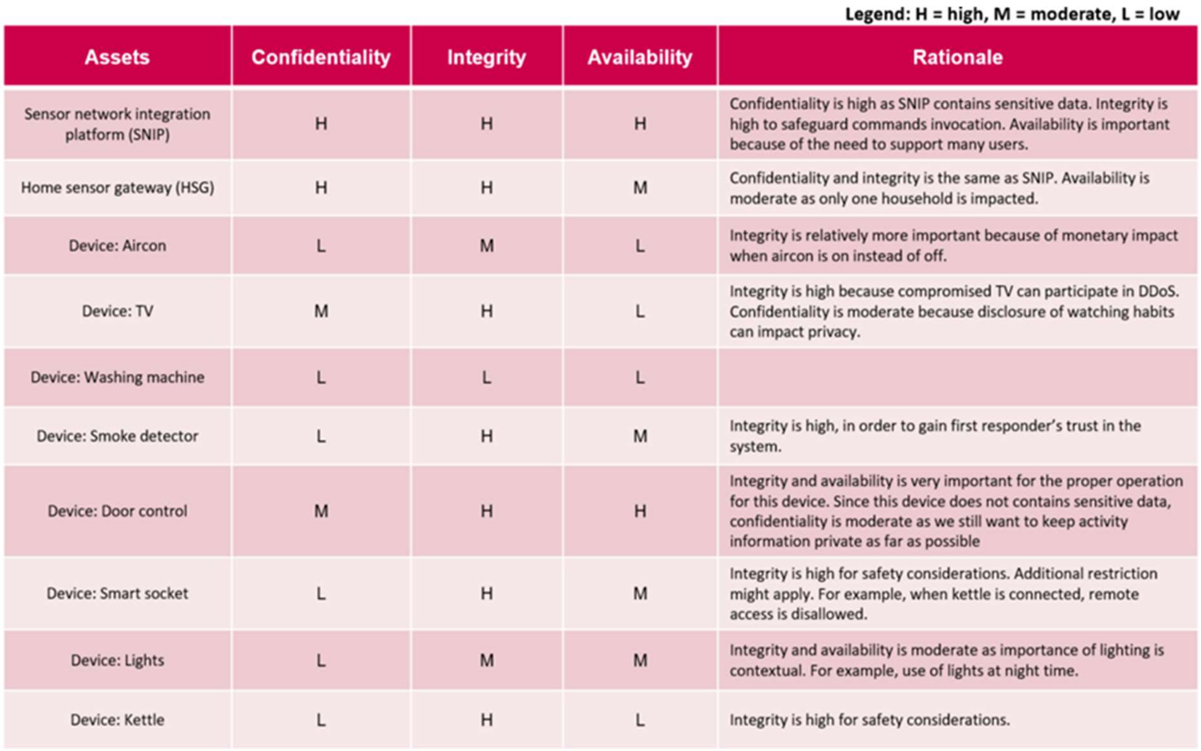
**Figure B-1: System architecture of HCS**

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.

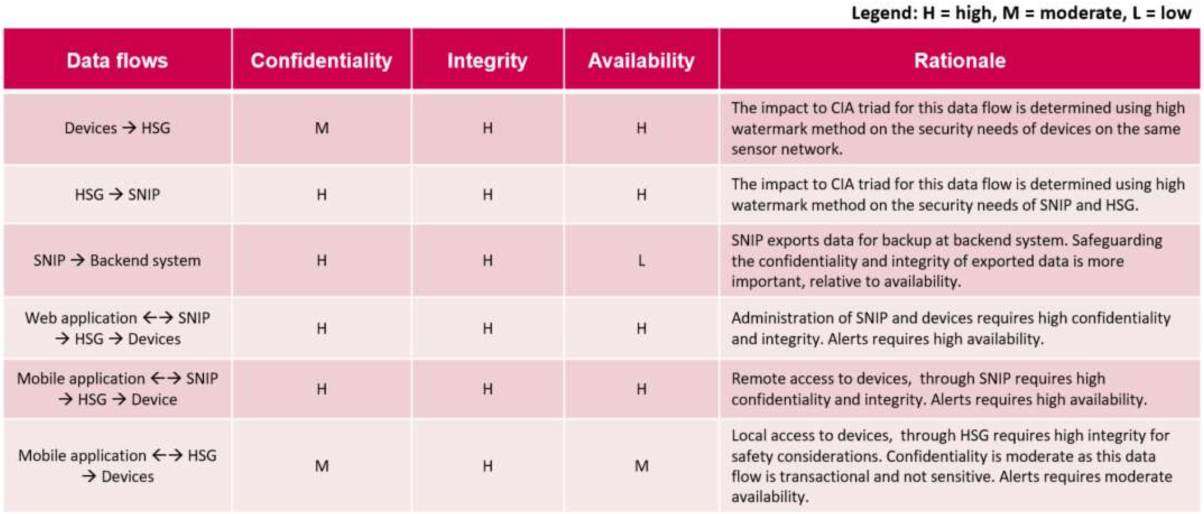


Legend: H = high, M = moderate, L = low

| 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

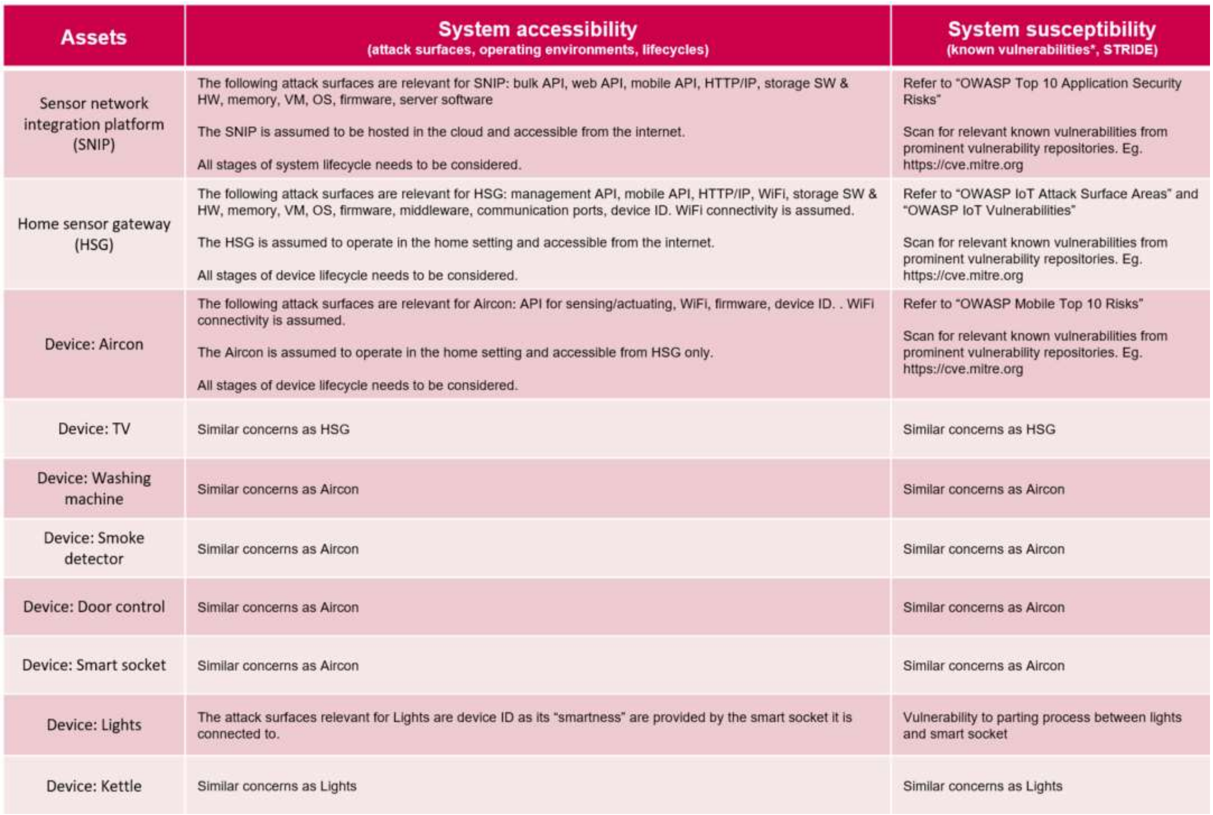
| Data flows | Confidentiality | Integrity | Availability | Rationale |
|---|---|---|---|---|
| Devices → HSG | M | H | H | The impact to CIA triad for this data flow is determined using high watermark method on the security needs of devices on the same sensor network. |
| HSG → SNIP | H | H | H | The 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.



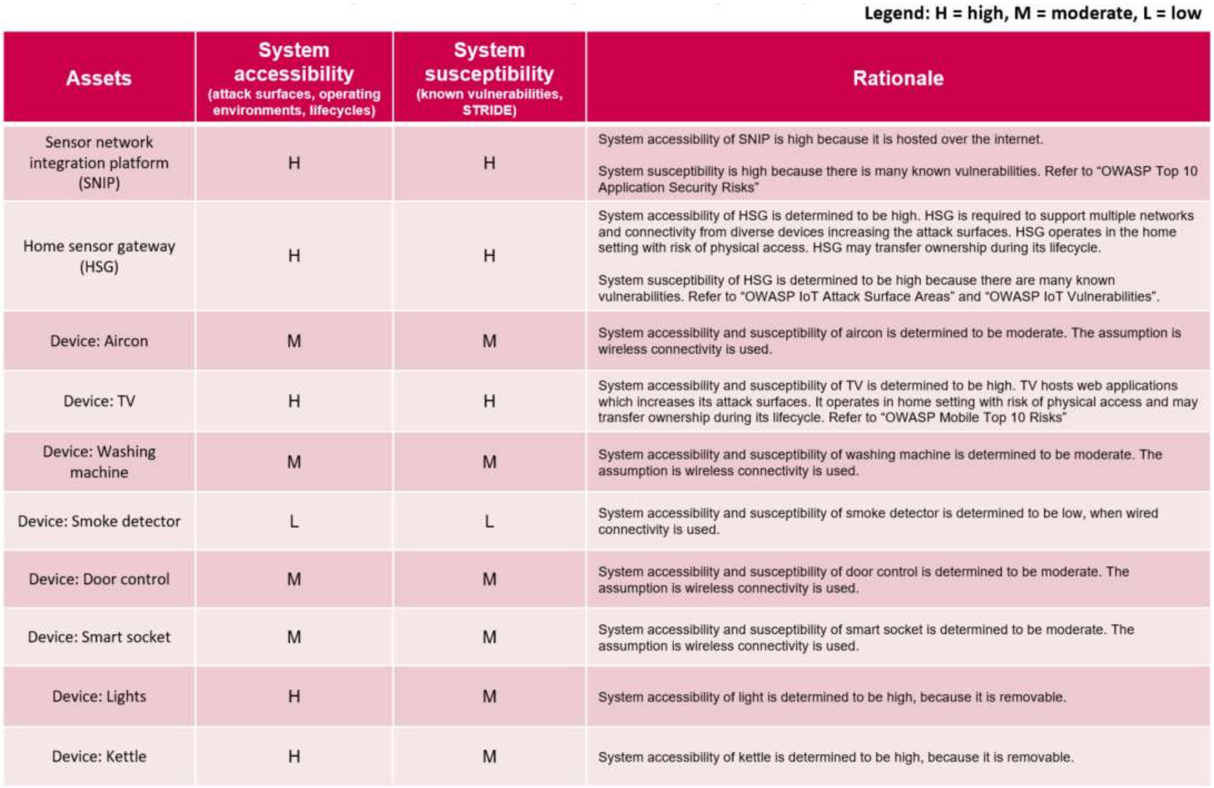
| Assets | System accessibility<br>(attack surfaces, operating environments, lifecycles) | System susceptibility<br>(known vulnerabilities*, STRIDE) |
|---|---|---|
| Sensor network integration platform (SNIP) | The following attack surfaces are relevant for SNIP: bulk API, web API, mobile API, HTTP/IP, storage SW & HW, memory, VM, OS, firmware, server software<br>The SNIP is assumed to be hosted in the cloud and accessible from the internet.<br>All stages of system lifecycle needs to be considered. | Refer to "OWASP Top 10 Application Security Risks"<br>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.<br>The HSG is assumed to operate in the home setting and accessible from the internet.<br>All stages of device lifecycle needs to be considered. | Refer to "OWASP IoT Attack Surface Areas" and "OWASP IoT Vulnerabilities"<br>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.<br>The Aircon is assumed to operate in the home setting and accessible from HSG only.<br>All stages of device lifecycle needs to be considered. | Refer to "OWASP Mobile Top 10 Risks"<br>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.

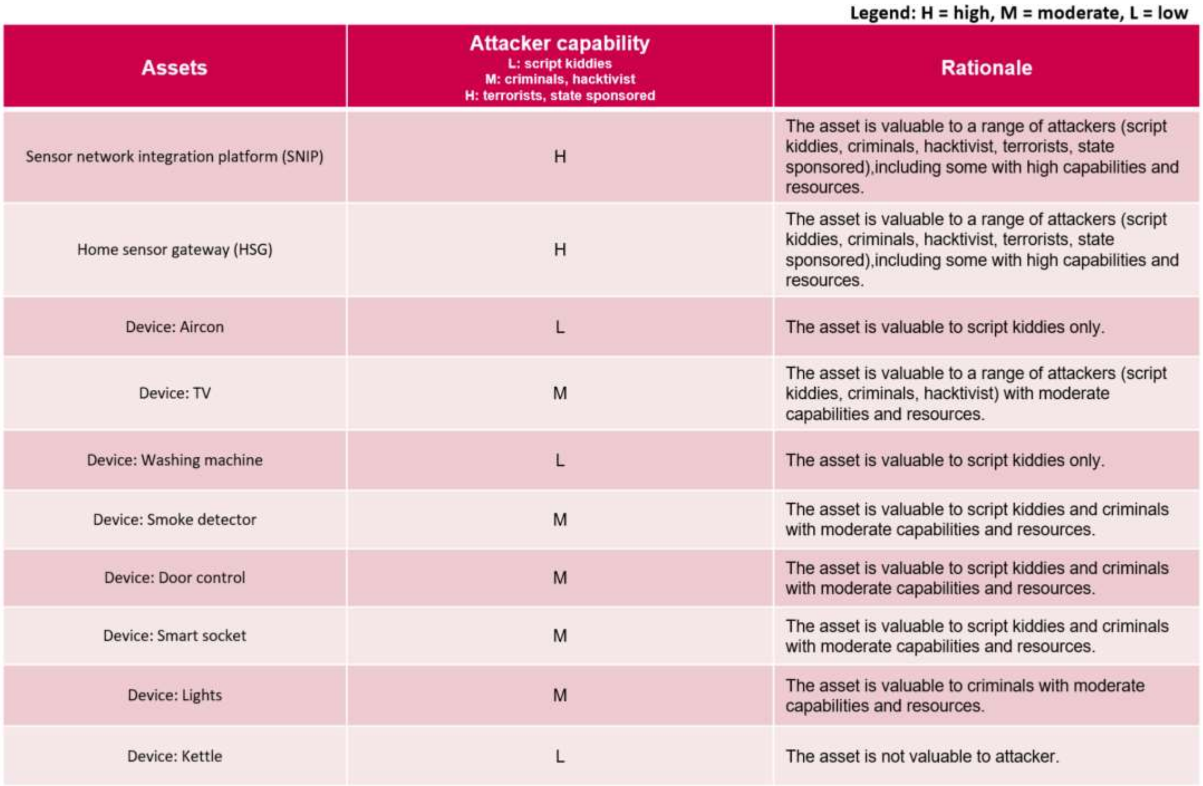


**Legend: H = high, M = moderate, L = low**

| 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.<br>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.<br>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 attacker capability for each asset. 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.

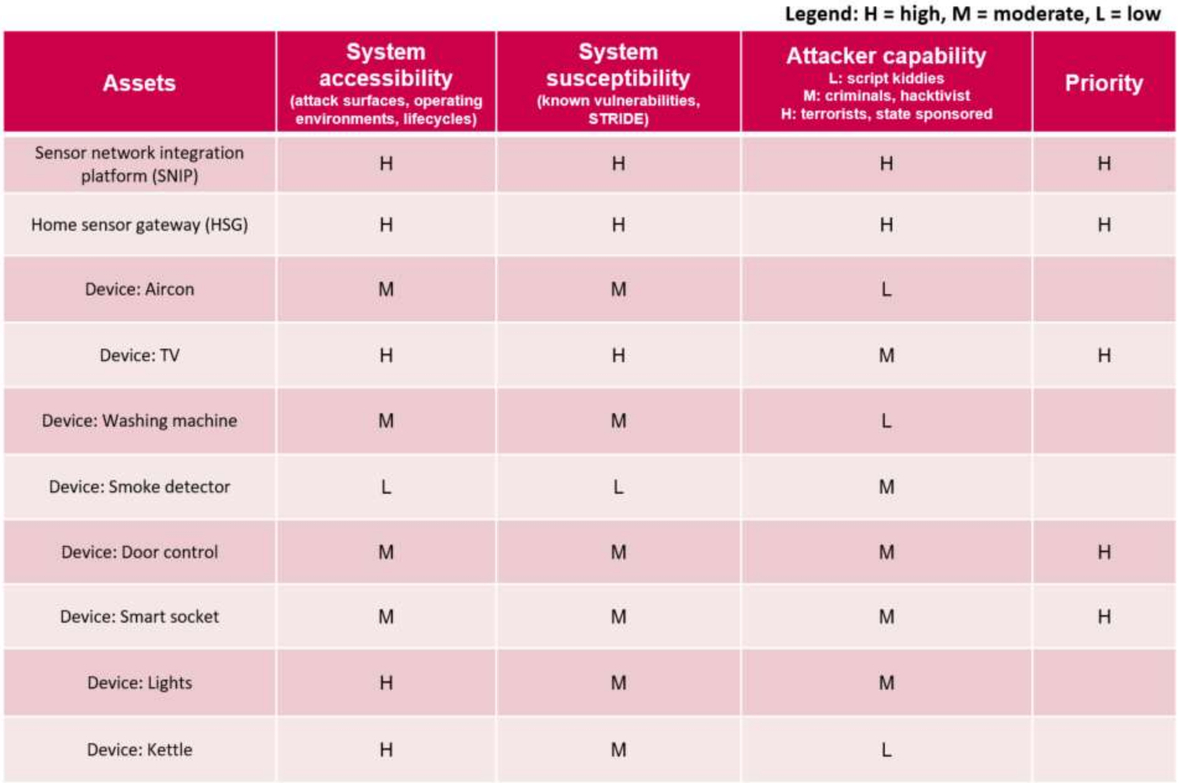


Legend: H = high, M = moderate, L = low

| Assets | Attacker capability<br>L: script kiddies<br>M: criminals, hacktivist<br>H: terrorists, state sponsored | 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 attacker capability**

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 attacker capability. 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

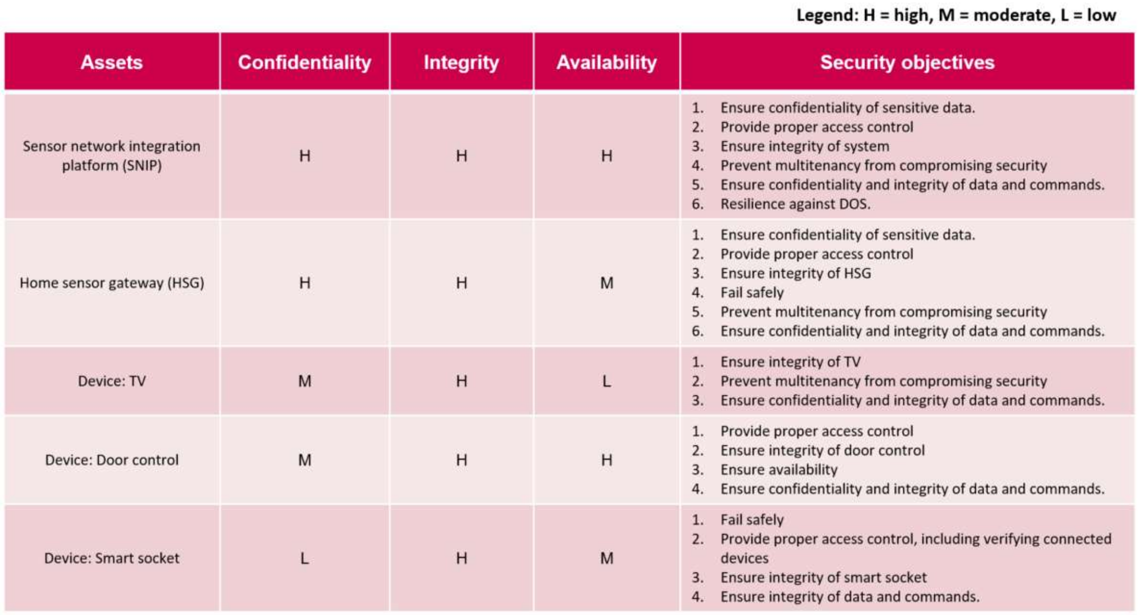
| Assets | System accessibility<br>(attack surfaces, operating environments, lifecycles) | System susceptibility<br>(known vulnerabilities, STRIDE) | Attacker capability<br>L: script kiddies<br>M: criminals, hacktivist<br>H: terrorists, state sponsored | Priority |
|---|---|---|---|---|
| Sensor network 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 principle 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.<br>2. Provide proper access control<br>3. Ensure integrity of system<br>4. Prevent multitenancy from compromising security<br>5. Ensure confidentiality and integrity of data and commands.<br>6. Resilience against DOS. |
| Home sensor gateway (HSG) | H | H | M | 1. Ensure confidentiality of sensitive data.<br>2. Provide proper access control<br>3. Ensure integrity of HSG<br>4. Fail safely<br>5. Prevent multitenancy from compromising security<br>6. Ensure confidentiality and integrity of data and commands. |
| Device: TV | M | H | L | 1. Ensure integrity of TV<br>2. Prevent multitenancy from compromising security<br>3. Ensure confidentiality and integrity of data and commands. |
| Device: Door control | M | H | H | 1. Provide proper access control<br>2. Ensure integrity of door control<br>3. Ensure availability<br>4. Ensure confidentiality and integrity of data and commands. |
| Device: Smart socket | L | H | M | 1. Fail safely<br>2. Provide proper access control, including verifying connected devices<br>3. Ensure integrity of smart socket<br>4. Ensure integrity of data and commands. |

**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.

**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 utilise industry accepted cryptographic techniques and best practices? Examples of best practices include:<br>· use of approved algorithms and their correct implementation and application<br>· sufficient key length<br>· use of approved random number generator(s)<br>· recommended crypto-period<br>· recommended entropy sources<br>· use of updatable cryptography | Y | The strength of cryptography is fundamental to safeguard the objectives of confidentiality and integrity.<br>In particular, the cryptography must be approved for the lifetime of the devices.<br>Recommended for: SNIP, HSG, TV, Door control, Smart socket |
| CK-CS-02 | Do you employ proper key management (generation, exchange, storage, use, destruction, replacement, etc.) techniques? | Y | Proper key management is required to prevent the disclosure of keys through the system/device lifecycles.<br>Recommended for: SNIP, HSG, TV, Door control, Smart socket |
| **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.<br>Recommended for: SNIP, HSG, TV<br>Optional for: Door control, Smart socket |
| CK-FP-02 | Do you employ secure boot? | Y | To safeguard integrity of the boot process.<br>Recommended for: SNIP, HSG, TV |
| **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 against threats of spoofing.<br>Recommended for: SNIP, HSG, TV, Door control, Smart socket |
| 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 unauthorised remote access.<br>Recommended for: SNIP, HSG, TV, Door control, Smart socket |
| **4. Network protection** | | | |
| CK-NP-01 | Do you enforce network access control?<br>For example, ensure explicit authorisation to join a new network and/or allow remote access. | Y | Proper access control is required to limit access to the system networks.<br>Recommended for: SNIP, HSG, TV, Door control, Smart socket |
| CK-NP-02 | Do you employ proven transport protocols with security controls properly activated? | Y | To safeguard the confidentiality and integrity of the payloads. |

| ID | Vendor disclosure checklist | Y / N / NA | Supporting materials |
|---|---|---|---|
| | Examples include:<br>· Use of TLS for TCP payloads.<br>· Use of DTLS for UDP payloads. | | Recommended for: SNIP, HSG, TV, Door control, Smart socket |
| CK-NP-03 | Do you employ industry best practices for secure connectivity?<br>Examples of industry best practices:<br>· Use of VPN or leased lines.<br>· Use of private mobile APNs from telecommunication operators when using a public mobile carrier network.<br>· Use of DNS pinning to prevent DNS spoofing.<br>· Use of traffic filtering based on type, port and destination.<br>· Use of certificate pinning.<br>· Employ TLS when using MQTT.<br>· Scan for open network ports.<br>· 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 B.3<br>Recommended for: SNIP, HSG, TV, Door control, Smart socket |
| CK-NP-04 | Do you segregate communication channels for trusted end points from non-trusted?<br>Examples include:<br>· Use of VLAN.<br>· Use of firewalls for DMZ.<br>· Use of unidirectional security gateway.<br>· Use of network segmentation or micro segmentation.<br>· Physical isolation. | Y | Applicable to safeguard the data flows highlighted in Table B.3<br>SNIP and HSG can segregate communication channels for administration purposes from normal operations.<br>SNIP should establish DMZ, using firewalls, against remote connections from devices and users.<br>HSG should safeguard the devices within home, from connections outside the home.<br>Recommended for: SNIP, HSG, TV, Door control, Smart socket |
| **5. Data protection** | | | |
| CK-DP-01 | Do you protect the confidentiality and integrity of your sensitive data?<br>· in transit<br>· in use<br>· at rest | Y | To safeguard the confidentiality and integrity of sensitive data. Sensitive data includes cryptographic keys and user credentials.<br>Recommended for: SNIP, HSG, TV, Door control, Smart socket |
| CK-DP-02 | Do you protect the authenticity and integrity your codes and firmware?<br>· in transit<br>· in use<br>· at rest | Y | To safeguard the software and firmware in SNIP, HSG and devices, including transportation of updates.<br>Recommended for: SNIP, HSG, TV, Door control, Smart socket |
| CK-DP-03 | Do you ensure the authenticity and integrity of your data (e.g. inputs, commands and sensing data)?<br>· in transit<br>· in use<br>· at rest<br>Examples include:<br>· Validate incoming content-types.<br>· Validate response types.<br>· Validate the HTTP methods against authorisation credentials.<br>· Whitelist allowable HTTP methods. | Y | To safeguard the data in SNIP, HSG and devices, including inputs and commands.<br>Recommended for: SNIP, HSG, TV, Door control, Smart socket |

| ID | Vendor disclosure checklist | Y / N / NA | Supporting materials |
|---|---|---|---|
| | · Define the acceptable character set (e.g. UTF-8).<br>· Validate that input characters are acceptable.<br>· Encode/escape input and output. | | |
| CK-DP-04 | Do you enforce access control to detect and prevent unauthorised data access and exfiltration, and filter your outputs? | Y | To safeguard aggregated data in SNIP and HSG from unauthorised access.<br>Recommended for: SNIP, HSG |
| **6. Access protection** | | | |
| CK-AP-01 | Do you employ mechanisms to manage and secure local and/or remote access?<br>Example of mechanisms include:<br>· auto logoff.<br>· screen lock.<br>· delay in between login attempts and lock-out for repeated unauthorised attempts.<br>· forced re-authorisation. | Y | To safeguard SNIP and HSG from unauthorised access, both locally and remotely, including physical access.<br>Recommended for: SNIP, HSG |
| CK-AP-02 | Do you send out-of-band notifications on impactful operations and/or alerts (eg. credential reset, security update failures)? | Y | To enable users to detect unauthorised attempts from alerts.<br>Recommended for: SNIP, HSG |
| CK-AP-03 | Do you enforce access control to prevent unauthorised access to system interfaces, system files and removable media? | Y | To safeguard against physical access to system/device interfaces.<br>Recommended for: SNIP, HSG, TV, Door control, Smart socket |
| CK-AP-04 | Do you employ anti-tamper mechanisms for resistance, evidence, detection and/or response? | Y | To prevent and detect physical tampering.<br>Recommended for: HSG, TV, Door control, Smart socket |
| CK-AP-05 | Do you support multi-factor authentication for impactful operations (eg. credential reset)? | Y | To safeguard impactful operations by requiring higher level of authentication.<br>Recommended for: SNIP, HSG, TV, Door control, Smart socket |
| **7. Security management** | | | |
| CK-MT-01 | Do you employ proper user and password management?<br>Examples include:<br>· Enforce strong password policy.<br>· Enforce no default passwords.<br>· Specify password expiration.<br>· Ensure that password recovery and reset mechanism are secure. | Y | To safeguard access to SNIP, HSG and TV (device with mobile operating system)<br>Recommended for: SNIP, HSG, TV |
| CK-MT-02 | Do you enforce proper access control to management functions?<br>Examples include:<br>· Enforce least privilege policy.<br>· Use of attribute-based access control (ABAC) or role-based access control (RBAC).<br>· Implement dual control for key management protection to prevent a single bad actor's compromise to the key materials.<br>· Support granular access permissions per user and per application.<br>· Implement separation of duties to key management system to prevent a single bad actor/administrator from compromising the system. | Y | To safeguard the administration functions of SNIP and HSG from normal operations.<br>Recommended for: SNIP, HSG |
| CK-MT-03 | Do you employ malware mitigation mechanism?<br>Examples include:<br>· Ensure file integrity using cryptographic hash. | Y | To safeguard the integrity of the software.<br>Recommended for: SNIP, HSG, TV |

| ID | Vendor disclosure checklist | Y / N / NA | Supporting materials |
|---|---|---|---|
| | · Baseline “normal” behaviour.<br>· Detect unauthorised software.<br>· Monitor devices and traffic flows.<br>· Scan backup images.<br>· Prohibit insecure bootloaders. | | |
| CK-MT-04 | Do you secure remote management of devices, including sensor gateways?<br>Examples include:<br>· Support secure Over-The-Air (OTA) updates of device applications and configurations.<br>· Support software and/or firmware updates using cryptographically secure methods.<br>· Support platform integrity checking, such as the measured boot mechanism or verifying the firmware integrity.<br>· Restrict remote management to secure networks. | Y | To safeguard the remote management function of HSG and devices, including remote updates.<br>Recommended for: SNIP, HSG, TV<br>Optional for: Door control, Smart socket |
| **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 integrity and availability of the system, devices are monitored and attested periodically.<br>Recommended for: HSG, TV, Door control, Smart socket |
| CK-RS-02 | Do you safeguard against a compromised device from compromising the system?<br>Examples include:<br>· Use of Perfect Forward Secrecy (PFS) for secure communication.<br>· Use of distinct secret keys for individual device. | Y | To safeguard availability of the system, in the event devices are compromised.<br>For example, allowed for compromised devices to be disconnected manually.<br>Recommended for: HSG, TV, Door control, Smart socket |
| CK-RS-03 | Do you employ mechanisms against failures from resource exhaustion and/or malicious attacks such as DDoS?<br>Examples include:<br>· Monitor to ensure that cloud resources are sufficient to sustain services.<br>· Detect resource exhaustion, for early preventive or corrective actions<br>· Control the execution of resource-intensive software.<br>· Enforce power thresholds.<br>· Limit the number of concurrent sessions.<br>· Operate with excess capacity. | Y | To safeguard availability of the system by detecting and preventing resource exhaustion.<br>Recommended for: SNIP |
| CK-RS-04 | Do you conduct regular backups of system data (including settings)? | Y | To safeguard availability of the system ensuring the ability to recover from a compromised state.<br>Recommended for: SNIP, HSG |
| **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?<br>Example of events include:<br>· User logins, logouts and unsuccessful authentication attempts.<br>· Connection, disconnection attempts and unsuccessful connection attempts.<br>· Unsuccessful authorisation attempts.<br>· Access to sensitive data.<br>· Import and export of data from removable media.<br>· Any change in access privileges. | Y | To safeguard the system by having the ability to detect and analyse when attacks are realised.<br>Recommended for: SNIP, HSG, TV |

| ID | Vendor disclosure checklist | Y / N / NA | Supporting materials |
|---|---|---|---|
| | · Creation, modification and deletion of data by user.<br>· Impactful operations.<br>· Remote operations.<br>· Security update failures.<br>· Physical access attempts where possible.<br>· Emergency access where possible. | | |
| 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.<br>Recommended for: SNIP, HSG |
| **10. Lifecycle protection** | | | |
| CK-LP-01 | Have you conducted threat modelling to identify, analyse and mitigate threats to the system? | Y | To understand and focus limited resources to what needs protection.<br>Recommended for: SNIP, HSG, TV, Door control, Smart socket |
| CK-LP-02 | Did you design and develop the system using a secure systems engineering approach? | Y | To employ “security by design” principle and develop system/design using secure best practices.<br>Recommended for: SNIP, HSG, TV, Door control, Smart socket |
| 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.<br>In this case, maintain a list of suppliers for the components.<br>Recommended for: SNIP, HSG, TV, Door control, Smart socket |
| 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?<br>Examples of security information include:<br>· Security polices<br>· Security updates<br>· Instructions for device/media sanitisation<br>· End-of-life notifications<br>· Phase out plan. | 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.<br>Recommended for: SNIP, HSG, TV, Door control, Smart socket |
| CK-LP-05 | Do you ensure that the system is hardened before the "Operational" lifecycle phase?<br>Examples of system hardening include:<br>· Remove all backdoors.<br>· Remove all debug codes from the released version.<br>· Change default configuration and disable unnecessary services.<br>· Remove or tamper-covered JTAG, unneeded serial and ports before deployment.<br>· Harden VM host properly, including disabling memory sharing between VM.<br>· Remove default and hardcoded passwords. | Y | Employ “security by defaults” principle and ensure the system is configure securely before operation.<br>Recommended for: SNIP, HSG, TV, Door control, Smart socket |
| CK-LP-06 | Do you maintain an inventory of connected devices, software and firmware versions, applied patches and updates throughout the “Operational” lifecycle stage? | Y | Employ the “accountability” principle to keep track that only authorised and patched devices are in use.<br>Recommended for: SNIP, HSG, TV, Door control, Smart socket |
| 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. |

| ID | Vendor disclosure checklist | Y / N / NA | Supporting materials |
|---|---|---|---|
| | | | Recommended for: SNIP, HSG, TV, Door control, Smart socket |
| CK-LP-08 | Do you establish proper vulnerability disclosure and management?<br>Examples include:<br>· Ensure the supply chain's capability to provide upgrades and patches.<br>· Provide vulnerability disclosure and processes to track and response promptly.<br>· Provide firmware and software patches/updates for vulnerabilities discovered, in a timely manner.<br>· Employ proper change management processes to manage security patches or updates.<br>· Notify and/or allow user to approve/reject updates, patches and changes to user settings, where appropriate.<br>· Disclose minimum support period. | Y | Build resilience by establishing ownership and standard operating procedures (SOPs) to disclosure, manage and resolve vulnerability.<br>Recommended for: SNIP, HSG, TV, Door control, Smart socket |
| 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 safeguard throughout their lifecycles.<br>Recommended for: SNIP, HSG, TV, Door control, Smart socket |
| CK-LP-10 | Do you sanitise devices and systems of security data and sensitive user data, before the "Reuse or Dispose" lifecycle stages? | Y | By the “accountability” principle, the sensitive data should be safeguard throughout the system/device’s lifecycles.<br>Recommended for: SNIP, HSG, TV, Door control, Smart socket |

**Table B-9: Usage of Vendor disclosure checklist**