GP-TM codes: ENISA standard  
A-codes: PCI standard   
  
Check: Tamper Security  
  
GP-TM-31: Measures for tamper protection and detection. Detection and reaction to hardware tampering should not rely on network connectivity.

Pass: Case unable to be opened without damaging it. Alternatively, case designed to opened has a seal applied.

A1: The device uses tamper-detection and response mechanisms that cause it to become immediately inoperable and result in the automatic and immediate erasure of any sensitive data that may be stored in the device, such that it becomes infeasible to recover the sensitive data. These mechanisms protect against physical penetration of the device. There is no demonstrable way to disable or defeat the mechanisms and access internal areas containing sensitive information without requiring an attack potential of at least 26 per device for identification and initial exploitation, with a minimum of 13 for initial exploitation.

Description: Check the casing of the device for tamper-evident design, ease of dismantling, and tamper-detection. Best performed while device is running and connected to the network  
  
Potential results: Case easy to open, Lack of tamper-evidence, lack of tamper-detection, tamper-detection  
  
Notes: Tamper-detection can render the device inoperable

Check: Device ports  
GP-TM-33: Ensure that devices only feature the essential physical external ports (such as USB) necessary for them to function and that the test/debug modes are secure, so they cannot be used to maliciously access the devices. In general, lock down physical ports to only trusted connections.

Pass: No ports found of which the function is not immediately clear

GP-TM-32: Ensure that the device cannot be easily disassembled and that the data storage medium is encrypted at rest and cannot be easily removed.

Pass: Unable to access unencrypted data.

Description: look for exposed contacts to wired networks, especially ones that go unused through standard operation.   
  
Potential results: Access to debug channels, access to JTAG

Notes: Attempting to interface with non-JTAG ports will be left to the software team to save time.

## Check: Device IC’s

GP-TM-01: Employ a hardware-based immutable root of trust.

Pass: Unable to determine the location of the firmware. Alternatively, initial firmware located on unwritable storage.  
  
GP-TM-02: Use hardware that incorporates security features to strengthen the protection and integrity of the device – for example, specialised security chips / coprocessors that integrate security at the transistor level, embedded in the processor, providing, among other things, a trusted storage of device identity and authentication means, protection of keys at rest and in use, and preventing unprivileged from accessing to security sensitive code. Protection against local and physical attacks can be covered via functional security.

GP-TM-32: Ensure that the device cannot be easily disassembled and that the data storage medium is encrypted at rest and cannot be easily removed.

Pass: Unable to access unencrypted data.  
  
GP-TM-55: Implement a logging system that records events relating to user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the system. Logs must be preserved on durable storage and retrievable via authenticated connections.

Partial Pass: Presence of durable storage devices. For complete pass: verify the presence of logs.  
  
GP-TM-18: Ensure that the device software/firmware, its configuration and its applications have the ability to update Over-The-Air (OTA), that the update server is secure, that the update file is transmitted via a secure connection, that it does not contain sensitive data (e.g. hardcoded credentials), that it is signed by an authorised trust entity and encrypted using accepted encryption methods, and that the update package has its digital signature, signing certificate and signing certificate chain, verified by the device before the update process begins.

Partial Pass: Presence of mutable storage devices. For complete pass: verify updates.

Description: attempt to glean information from IC’s found on the chips. Almost all IC’s have labels that link to datasheets.  
  
Potential results: Discovery of readable storage IC’s, encryption modules.  
  
Notes: Especially of interest are microcontrollers/processors and storage, encryption and wireless chips. BAG-chips are unable to be probed manually. To fully inspect the device the pcb may need to be removed from the casing entirely.

Step 1: Write down chip labels of all visible chips  
Step 2: Look up written down labels using databases or search engine  
Step 3: categorise IC’s

Test: Scan Chain probing  
GP-TM-33: Ensure that devices only feature the essential physical external ports (such as USB) necessary for them to function and that the test/debug modes are secure, so they cannot be used to maliciously access the devices. In general, lock down physical ports to only trusted connections.

Pass: Test/debug ports unusable to third parties(us)

Description: attempt to control the device through the JTAG TAP, in order the glean information or completely reprogram the device  
  
Requirement: Exposed TAP, Logic analyser/ JTAG software.  
  
Potential results: Discovery of sensitive data, chosen plaintext attacks, device hijacking.  
  
Potential defences: JTAG scrambling, Lock and Key method.  
  
Notes: This test is slow, and the entire electronics research community is focused on it. Perhaps better to focus elsewhere.  
  
Step 0: connect JTAG programmer to TAP. Also   
Test: Power Consumption Monitoring  
A3: There is no feasible way to determine any sensitive information by

monitoring electro-magnetic emissions, power consumption, or any

other internal or external characteristic without an attack potential of

at least 26 for identification and initial exploitation, with a minimum of

13 for initial exploitation.  
  
Pass: Failure to obtain useful information through power analysis

Description: Map the device’s power consumption to behaviour in order to determine a relation  
  
Requirement: Setup to measure Current consumption, exposed power source.  
  
Potential advanced requirements: Used encryption key and/or user credentials.  
  
Potential results: User enumeration, breaking of encryption through partial information.  
  
Potential defences: Equal-power consumption design.  
  
Notes: Identify as much of the device as possible before doing this, to assist in setting up scenarios to measure. This test will take a long time. Can be combined or replaced with heat mapping.   
  
Specs: Instantaneous IoT device power consumption is unlikely to leave the 0.1-10 Watt range. Depending on input methods this can result in currents ranging from 4 A DC (2.4 V input, 10 W) to 43 mA AC (When plugged into power sockets, 10 W, 230V) to 434µA (230 V, 0.1W). Note that measuring total device input will include actuator power consumption. ARM cortex M7 top clockspeed is 600 MHz. While it is unlikely this speed will be used often, since power consumption scales linearly with clock speed, this seems like a good upper limit to be able to capture in-clock cycle trends. The Nyquist Criterium states that to capture a signal properly, one needs to sample it at twice the rate of the highest frequency component. However, it is better to have some leeway, so the suggested samplerate of the test setup is atleast 1.5 GHz and recommended to be 2 GHz. The test setup will also require a potentiometer to be able to set the resistance value so the voltage drop is never more than 0.2V, a voltage amplifier, and a way to reliably log the measured consumption without consistent active monitoring.  
  
In short: DAC or Oscilloscope: 1.5 Gigasamples per second or higher, ability to be continually read. Amplifier: x100. Potentiometer or other variable resistor: Probably multiple, given resistances range from 50 to 50 million.   
  
Step 0: Perform a power measurement using a wattmeter.  
Step 1: Setup resistance so that voltage drop over the shunt resistor is roughly equal to 0.2 volts  
Step 2: Perform tasks to be measured with the device and measure amplified output with an oscilloscope or DAC.

Step 3: Attempt to correlate timing data from tasks with the output data.  
Test: Heat Mapping  
A3: There is no feasible way to determine any sensitive information by monitoring electro-magnetic emissions, power consumption, or any other internal or external characteristic without an attack potential of at least 26 for identification and initial exploitation, with a minimum of 13 for initial exploitation .

Description: take a recording of the device through thermal imaging to map IC power consumption to behaviour.

Pass: Failure to obtain useful information through thermal imaging  
  
Requirement: High Resolution Thermal imaging capability.  
  
Potential advanced requirements: used encryption key and/or user credentials  
  
Potential defences: Equal-power consumption design.  
  
Notes: Identify as much of the device as possible before doing this, to assist in setting up scenarios to measure. This test will take a long time. Can be combined or replaced with power consumption monitoring. To decrease resolution requirements, consider performing this test in low air-pressure environments or otherwise decreasing cooling effects, though do not overheat the device in doing so.  
Total control system power consumption will never be above 10 watts. This test is Infeasible at room conditions. To make the heating noticeable this test would have to be performed in low air pressure environments.   
  
Step 0: Setup heat camera on low-pressure chamber  
Step 1: Perform tasks with the device  
Step 2: Attempt to correlate the tasks with the thermal image data  
  
Test: Hardware chip probing:  
GP-TM-32: Ensure that the device cannot be easily disassembled and that the data storage medium is encrypted at rest and cannot be easily removed.

Pass: Data at rest encrypted.   
  
Description: physically interface with hardware chips in order to extract information.  
  
Requirement: non-BAG chip, setup to hold probes still/, logic analyser, chip datasheet.  
  
Potential Results: Extraction of firmware, altering of device information, discovery of critical information.  
  
Potential defences: encrypted data storage, required passcodes.  
  
Notes: BAG-chips cannot be probed, tamper-detection could render the device inoperable. Consider extracting the chip from the device entirely.   
  
Test walkthrough:  
Step 0: Investigate datasheet  
Step 1: Setup flying probes on necessary IC pins  
Step 2: Input and read output.

Test: Voltage/Heat stress test  
A2: The security of the device is not compromised by altering environmental conditions or operational conditions (for example, subjecting the device to temperatures or operating voltages outside the stated operating ranges).

Pass: No evidence of security flaws introduced by extreme conditions  
  
Description: operate the device outside of it’s normal operating conditions to attempt to discover additional security flaws  
  
Requirement: climate chamber/oven, heat resistant HV probe setup, Voltage source potentiometer.  
  
Potential results: Unsafe failure of parts of the device, safe failure of device.  
  
Potential defences: Temperature/voltage sensors leading to complete shutdown.  
  
Notes: difficult to plan, will likely lead to inoperability. Alternatively: request test results   
  
Test walkthrough:  
1:Increase or decrease voltage or environmental heat  
2;Perform security tests  
3:If device not failed entirely, back to step 1  
4: attempt to extract any valuable information