CPA POLICIES AND PROCEDURES

PART 2:

CPA BUILD STANDARD

Document Control

Document Owner	Smart Energy Code Company Ltd
Version	1.2
Date	28 January 2026
Document Status	SSC Approved
Date of Next Review	TBD
Classification	Clear

Change Record

Date	Author	Version	Change Reference
19/08/2024	SECAS	0.1	Draft version created for review by SSC for comment
23/08/2024	SECAS	0.2	Added references
04/09/2024	SSC	0.3	SSC Chair updates reflecting inputs from SSC
30/09/2024	SECCo	0.4	Updated to reflect feedback from SCIRS Members and refers to the Build Standard parts of the Agreed Interpretations - Tracked
24/10/2024	SECCo	0.5	No changes following SSC (09/10/24) and SCIRS (14/10/24). Tracked changes removed. Clean version SSC approved.
30/11/2024	SECCo	0.6	Updated to include a requirement for a CPA Build Standard Certificate.
12/12/2024	SECCo	0.7	Updated to include Agreed Interpretations content for Build Standard: 3.5.1, 3.5.2, 3.5.3, 3.5.4, 3.5.5, 3.5.6, 3.5.7, 3.5.8,3.5.9, 3.5.10. Also deleted out-of-date mappings to CC and CMMI.
23/12/2024	SECCo	0.8	Updated after SCIRS review to add a Build Standard Questionnaire (BSQ) and Assurance Maintenance Questionnaire (AMQ).
09/01/2025	SECCo	0.8.1	Updated after SSC and SOp review to describe potential updates to Build Standard Certificate scope.
13/01/2025	SECCo	0.8.2	Updated after SCIRS to reflect the Build Standard for Triage Tool and Triage System Interface in Section 5.
13/01/2025	SECCo	1.0	Tracked changes removed and version updated for publication
28/05/2025	SECCo	1.1	Parts 1, 2 and 3 updated for changes to: process diagrams; clarifying Assurance Maintenance SIR and SIE; UK Sales base requirement; TLP clarification; CPA Test Lab Operational Requirements; Risk Review outcomes; general accuracy and alignment; and explaining the role of SCIRS.

28/01/2026	SECCo	1.2	Updated to correct incorrect references and add clarification to terms; to clarify the publication of the Build Standard on the SEC website; and to clarify the Build Standard for Triage Tools

Table of Contents

Contents

1. Regulatory Context

The security controls and assurance arrangements for the end-to-end Smart Metering System are defined in the Smart Energy Code (SEC) and aim to provide confidence to all SEC Parties that the systems and Devices supporting smart metering are appropriately secure.

The SEC Sections G7.19 – 7.23 place specific obligations on the Security Sub-Committee (SSC). One such obligation G7.19 (g) requires that:

"The Security Sub-Committee shall: …….

(*g) develop and maintain a document to be known as the* ***"CPA Policies and Procedures"*** *which shall:*

(i) set out the steps that a Manufacturer must follow in order to obtain and maintain a CPA Certificate in respect of a Device Model;

(ii) set out the criteria that a Test Lab must satisfy in order to perform the functions of a CPA Test Lab for the purposes of the CPA Scheme;

(iii) describe the procedures that a CPA Test Lab must apply in evaluating whether a Device Model should be issued with a CPA Certificate;

(iv) make such other provision in relation to the evaluation and assessment of a Device Model for the purposes of the CPA Scheme as the Security Sub-Committee may consider appropriate;

(v) make such other provision in relation to the obligations of Manufacturers and CPA Test Labs for the purposes of the CPA Scheme as the Security Sub-Committee may consider appropriate;

(vi) make such provision relating to the expiry, renewal, suspension, withdrawal and cancellation of CPA Certificates as the Security Sub-Committee may consider appropriate; and

(vii) make such provision in relation to the role of the CPA Scheme Operator as the Security Sub-Committee may consider appropriate;

This '**CPA Policies and Procedures'** documentation is in three parts:

- Part 1 explains the policy, the governance and how the Scheme operates in line with SEC Section G13 together with the formal compliance requirements for Manufacturers and Test Labs including Traffic Light Protocols (TLPs); CPA Test Lab Operational Requirements; and descriptions and templates of the forms and reports that are used;
- Part 2 explains the requirements for Manufacturers to meet the mandatory CPA Build Standard; and
- Part 3 explains the requirements of the Risk Review process that applies when a Device reaches its CPA Certificate expiry date or Risk Review date.

The SSC also has a SEC obligation in Section G7.19(f) in respect of CPA Security Characteristics:

"The SSC shall……..

(f) with respect to the CPA Security Characteristics:

(i) maintain CPA Security Characteristics that set out the levels of security required for Smart Meters, Communications Hubs, SAPCs and HCALCs; and

(ii) where it considers it appropriate from time to time, develop the CPA Security Characteristics so as additionally to set out levels of security required for any other Device, in each case so as to ensure that the required levels of security are proportionate and appropriate taking into consideration the security risks identified in the Security Risk Assessment;

The **CPA Security Characteristics (SCs)** and the **Agreed Interpretations (AIs)** which provide SC and Build Standard clarifications are separate documents provided by the SSC on the SEC website.

This document is Part 2 of the CPA Policies and Procedures and sets out the mandatory development practices that Manufacturers must meet as well as the validation and assurance arrangements performed by CPA Test Labs.

Definitions in this document:

The CPA Policies and Procedures Part 1 contains a section on 'Definitions' that is not repeated in this document. However, the terms 'Manufacturer' (a SEC definition) and 'Developer' (an original CPA term) are used interchangeably throughout the CPA documentation, including SCs, Build Standard, Risk Review Process and Agreed Interpretations etc. Similarly, the term 'Device' (a SEC definition) and 'product' (an original CPA term) are also used interchangeably.

2. The CPA Build Standard

The CPA Build Standard describes the engineering principles and practices that are expected from a Manufacturer creating a good quality, secure product. It covers both development processes and the general security approach taken by the Manufacturer. This includes the development of software, firmware and hardware (electrical and mechanical) components. Validating these aspects of the development approach by a Test Lab will give confidence of a secure and well-understood product throughout the product's lifecycle.

The Security Characteristics (SCs) and Agreed Interpretations (AIs) describe building the right features into the product. The Build Standard describes building the product right and in line with good industry practices. Adherence to the Build Standard alone will not necessarily result in a secure product. However, the absence of key elements of the Build Standard will prevent assurance and CPA Certification.

Once accepted, a Build Standard Validation Report is typically valid for 6 years - the same length as a CPA Certificate or Risk Review due date in the case of a lifetime CPA Certificate. A CPA Device Certificate is not valid without a current CPA Build Standard Validation.

The Build Standard expiry date will be confirmed by a CPA Build Standard Certificate. However, the Build Standard expiry date can be different from the CPA Device Certificate expiry date because this is dependent on the evidence that satisfies the Build Standard Requirements remaining unchanged. If, for example, a new manufacturing location or premises is established or the development location changes, or a third-party is appointed to maintain Devices elsewhere or a change of company ownership results in a new location, then the Build Standard will need to be updated to reflect the changes.

Triage Tools and the Triage System Interface that are used for Use Case 004 as set out in the SSC Guidance on Device Security Assurance and Triage, are subject to a separate Build Standard evaluation and Certification process that is explained in the CPA SC "Triage interface updates to GSME, ESME, SAPC & CH SCs and CPA Build Standard Extensions". Note that the Build Standard certification for the Triage Tool and Triage System Interface will expire at the same time as the main Build Standard.

The Manufacturer is responsible for maintaining compliance with the Build Standard and ensuring that it is renewed before the expiry date on the CPA Build Standard Certificate is reached.

An outline of the overall process is provided in CPA Policies and Procedures Part 1 section 7D, Figure 4.

3. CPA Build Standard Roles

The CPA Policies and Procedures Part 1 describes the different roles, responsibilities and governance arrangements of the various parties involved in the CPA Scheme.

The following roles are specifically applicable to the CPA Build Standard,

3.1 Manufacturers:

The Manufacturer is primarily responsible for developing the product being evaluated. Some Manufacturers may use multiple development teams. Each development team may have different approaches to development security. This may be for a number of reasons e.g. geographical or organisational or having different teams for different Device types such as ESME and GSME. The Test Lab must discuss the development approach and the extent to which it is followed across the different development teams. If the Test Lab has reason to believe that the evidence they have observed is only applicable to certain, but not all engineering teams, they should clearly document this in the Build Standard Validation Report (BSVR). This may result in the Manufacturer failing the Build Standard validation process.

The Manufacturer, including any 3rd parties involved in the product development, is expected employ Industry related good working practices, such as ISO/IEC 27000 series, ISO/IEC 18028series, and should have local policy frameworks in place to address the following areas:

a) Leadership and Governance
b) Information Risk Management (IRM)
c) Through-Life Information Assurance and IT security measures
d) Assured Information sharing
e) Quality Assurance and Testing
f) Training, Education and Awareness
g) Audit and Compliance

These areas are not comprehensively examined against the ISO standards mentioned but, it is unlikely a Manufacturer would be able to provide satisfactory evidence for meeting the Build Standard requirements without having such policies and working practices in place.
The Manufacturer is responsible for maintaining compliance with the Build Standard and ensuring that it is renewed before the expiry date on the CPA Build Standard Certificate is reached.

3.1.1 Manufacturer Prerequisites

The Manufacturer must meet the four key requirements listed below before it can be considered for a CPA evaluation. The Manufacturer must provide evidence for each requirement during the evaluation of their product.

a) The Manufacturer must employ a configuration management system.
b) A software-based issue tracker must be used as part of a defined flaws and security vulnerabilities remediation process.
c) The Manufacturer must perform extensive testing of their products.
d) The Manufacturer must employ a flaws and security vulnerabilities-reporting process that enables flaws and security vulnerabilities that are discovered outside the Manufacturer‘s organisation to be reported.

These requirements exist as a simple metric for the Manufacturer’s approach to secure product development – it is unlikely that a Manufacturer routinely creates and maintains a good-quality security-enforcing product if these four key requirements are not met. Therefore, the evaluation must not start unless the Manufacturer can attest that they meet these requirements.

As previously stated, it is the Manufacturer's responsibility to report any changes to the development processes, teams or locations etc.

3.2 CPA Test Labs:

The CPA Test Lab should discuss with the Manufacturer how the Build Standard Requirements map onto the Manufacturer’s development processes and then seek evidence from the Manufacturer to justify the assertion that a requirement is successfully met. This evidence may be in the form of documentation or notes from conversations with relevant members of the Manufacturer’s personnel which may include the lifecycle processes of both the firmware development teams and product manufacturing teams, including third-party contract manufacturing teams. Evidence may also be in the form of training material or witnessed activities. The Test Lab may ask the Manufacturer to acknowledge notes from conversations that are to be used as evidence to confirm that they have been correctly interpreted. Importantly, the CPA Test Lab must ensure that in addition to having a well-documented process, that process is followed in practice.

The CPA Test Lab should submit a Build Standard Questionnaire to the SOp to initiate a Build Standard Validation. This will enable the SOp to log and provide a reference for a subsequent BSVR to be provided by the CPA Test Lab and support the issue of a CPA Build Standard Certificate as appropriate.

It is recommended that members of the CPA Test Lab visit the Manufacturer's engineering premises to gather evidence that the Build Standard requirements have been successfully met – see also section 4 of this document.

If, during the course of evaluation of a product, including Assurance Maintenance, or undertaking a Risk Review, the CPA Test Lab does not believe that the existing Build Standard is still valid, this opinion and the reasons should be documented and provided to the SOp. Subject to consideration by the SOp and SOwn in sections 3.3 and 3.4 below, the CPA Test Lab may need to perform a new validation against the Build Standard as per the normal Build Standard Validation process.

3.3 Scheme Operator (SOp):

Following approval of a Build Standard Questionnaire, the Scheme Operator (SOp) will receive a recommendation from CPA Test Labs with a Build Standard Validation Report (BSVR) and supporting documentation. Where the SOp is satisfied that the required Build Standard has been met, the SOp will confirm the BSVR typically as valid for 6 years – to align with the length of the CPA Certificate or Risk Review due date in the case of a lifetime CPA Certificate.

Where the CPA Test Lab believes that the original Build Standard validation is no longer valid, they will have informed the SOp. It is likely that a reassessment of the Manufacturer's engineering approach will be required. This could cover the existing set of products that are already certified as well as their new product.

Where the SOp is informed by the CPA Test Lab that compliance with the original Build Standard is no longer valid or otherwise has reason to think that the Build Standard is no longer valid, they will inform the Scheme Owner (SOwn).

3.4 Scheme Owner (SOwn):

Where the SOp informs the SOwn that the original Build Standard validation is no longer valid or they have other information or evidence that to indicate that the Build Standard is no longer valid, the SOwn will consider the next steps. It is likely that a reassessment of the Manufacturer's engineering approach will be required. This could cover the existing set of products that are already certified as well as their new product.

The CPA Scheme Owner may also revoke any existing Build Standard Validation Certificate on the advice of the Scheme Operator e.g. if evidence of noncompliance is discovered. In this case, the SSC will consider the CPA Certification implications for existing CPL entries as set out in the SEC Appendix Z, Section 6.

When the SOp provides a CPA Build Standard Certificate, the SOwn will arrange for it to be published on the SEC website.

4. Application of Build Standard to manufacturing environments

The Build Standard evaluation for smart metering devices includes assessment of the manufacturing environment for the Device, and this environment will in general be the subject of an assessment visit by the evaluators.

All of the Build Standard requirements apply to relevant artefacts and processes that are present in the manufacturing environment as part of achieving the Build Standard goal of giving "confidence of a secure and well-understood product throughout the product's lifecycle" (cf. Section 2 above). However, a number of specific aspects of Build Standard requirements in the manufacturing environment are highlighted and described below.

General extension of configuration items (Requirements 1, 3, 4, 6, & 7)

Build Standard requirements related to configuration management shall be extended to include application to hardware components. They shall also be extended to include artefacts necessary for the manufacturing process, such as:

- Work instructions used in manufacturing processes
- Test programs used in manufacturing equipment to test security-related functionality in the manufacturing environment (e.g. on the manufacturing line or as part of a sampled quality assurance process)
- Associated hardware and software artefacts used for security-related processes on the line, such as setting memory protection states after firmware injection, and disabling debug interfaces a part of the manufacturing process.

Any substitutions of hardware components permitted shall not affect security critical components such as processors, secure elements, or tamper response mechanisms.

Secure transfer of items to manufacturing environment (Requirements 6 & 7)

The evaluators shall examine the developer's processes and procedures for transfer of configuration items from the development (and build) environment to the manufacturing environment, to ensure that the correct versions are picked and that confidentiality, integrity and authenticity (as required according to the item being transferred) are maintained at both ends of the transfer as well as during the transfer itself.

Processes for secure transfer of items shall include secure storage of the items to preserve confidentiality, integrity and authenticity (as required according to the item), and to enable version control of the items, in the manufacturing environment. This therefore includes logical and physical protection (cf. Requirement 6) of relevant systems at the manufacturing site.

Extension of testing to manufacturing environment (Requirement 10)

The developer's processes shall include testing of products on the manufacturing line and sampling of products from manufactured batches, to ensure that security critical actions required on the manufacturing line have been taken (e.g. that relevant interfaces have been disabled).

Security of manufacturing environment processes (Requirement 6)

The evaluators shall examine the developer's processes and procedures for logical and physical protection of assets required to generate and protect security-related data such as keys that may be injected into the product. This may include any requirements on entropy sources or seed generation outside the product identified as part of DEV.*.M134.

Evidence Expected:
Description of processes and procedures covering the security of the manufacturing environment, including the aspects identified above for assessment.

5. Performing Build Standard Validations

During the CPA evaluation, the CPA Test Lab will gather evidence that each of the Build Standard Requirements described in section 6 below has been met. If the Manufacturer believes that a requirement is not relevant to their product or engineering approach they may submit a reasoned argument describing why it does not apply in their circumstances to the CPA Test Lab. In this situation, the CPA Test Lab may wish to discuss the acceptability of the Manufacturer's argument with the SOp to gain an early opinion rather than await the final submission of the BSVR.

The CPA Test Lab must capture and record evidence for each requirement listed. Paper claims by a Manufacturer must be verified by witnessed activities / processes. The CPA Test Lab should look to logs, build script outputs or review session logs, i.e. actual engineering or process artefacts – to get a true picture of whether claimed processes are adhered to in practice. It is also permissible to gather evidence from interviewing members of the development team – again, claims must be verified wherever possible.

Where a Manufacturer provides a Triage System together with a Triage Tool and Triage System Interface to support Triage activities, as described in the *"CPA Security Characteristics, Triage interface updates to GSME, ESME, & SAPC SCs and CPA Build Standard Extensions"* section 3, then these will also be included in the scope of the Build Standard validation. Since the Manufacturer's Triage System is required to be "from a facility that is within the scope of the main Build Standard validation", the Build Standard for the Triage Tool and Triage System Interface will share the same expiry date. For clarity, where the Triage Tool and Triage System Interface have Build Standard Certification added during the course of an existing Build Standard, then the period is limited to the main Build Standard expiry date.

In some cases the procedures used to meet Build Standard requirements will have been defined, but not yet exercised. This might arise, for example, when a developer has defined an external vulnerability reporting and handling process for a new product that has been created but not yet released. Although in this case the procedure can be assessed in principle, evidence of its application cannot yet be observed.

The evaluator should then examine the procedure and confirm that it satisfies the relevant Build Standard requirement(s) in principle. If the same process (or a suitably similar process) has been applied to a similar product in a similar development environment, then it may be possible to observe evidence of the application of that process and to conclude that the Build Standard requirement(s) will indeed be met in practice.

Where there is no suitably similar procedure to observe (e.g. where any alternative procedure uses a different IT system or application, or where it is carried out by staff with different competence or experience, or where it is part of a larger transformation of procedures and environment (such as a future of Industry 4.0 transformation)) then the evaluator shall identify and report any relevant additional supporting evidence (such as a documented trial or test run of the procedure) and shall document the following in their report:

a) Identification of the relevant procedures and the aspects that have not been exercised (or exercised insufficiently to enable a conclusion) in the detailed results table for the affected requirement(s).
b) (Assuming assessment of the procedure in principle concludes that it meets the requirement(s)) identification of the Pass conclusion for the affected requirement(s) as being subject to future confirmation, in both the detailed results table and the Executive Summary table.
c) A recommendation, in the Revalidation Aspects section, for an appropriate evaluation activity to be carried out as part of the next future evaluation work on the product (e.g. assurance maintenance or revalidation). An example evaluation activity might require that the latest version of an identified process specification document should be examined to confirm that it still meets the requirement(s) in principle, and that identified records (or suitable replacement records according to the latest version of the procedure) should be examined to confirm the application in practice. The recommendation should identify whether or not a site visit is expected to be required to complete the evaluation activity (noting that some processes might be suitably assessed via emailed instances of records, screenshots, reports, or logs).

This applies to use of the Build Standard for both development and manufacturing (cf. Section 4 above) environments.

Where a Manufacturer uses their own or commercial tools to satisfy a requirement, these should be listed in the Build Standard Validation Report.

If the CPA Test Lab is satisfied that each of the requirements has been fulfilled, they submit their findings to the SOp in a Build Standard Validation Report and the SOp will then review the findings and, when satisfied, recommend to the CPA Scheme Owner that a CPA Build Standard Certificate should be awarded.

6. Renewing Build Standard Validations

A Build Standard validation is an assessment of a Manufacturer's engineering processes and does not necessarily apply only to a single product i.e. a Build Standard validation may apply to more than one product. The CPA Test Lab should note where there is evidence to suggest that the scope of the Build Standard validation is unlikely to apply to more than one product. A Manufacturer may have multiple product evaluations covered by a single Build Standard Validation Report. A Build Standard Validation Report is typically valid for a six year period as for a CPA Certificate or Risk Review date in the case of a lifetime CPA Certificate. When the expiry date is reached, a renewal of the Build Standard validation will be required. The Manufacturer is responsible for ensuring the validity of the Build Standard is maintained at all times when a CPA Certificate is current. This includes providing notification of significant changes affecting previous Build Standard evidence to the SOp via a CPA Test Lab (as described below). Examples of significant changes could be a change in site (e.g. affecting physical security evidence for Requirement 6), configuration management system (affecting evidence for Requirement 3 and Requirement 4), assurance tools (e.g. static analysis or fuzzing tools for Requirement 8), build environment (e.g. affecting evidence for Requirement 7), vulnerability handling process (affecting evidence for Requirements 10 and/or 12), addition or change of a manufacturing subcontractor (affecting evidence for the Manufacturing extensions in Section 4 above)).

There are several situations in which changes to a Manufacturer's processes mean that a CPA Test Lab would need to perform additional actions to maintain a Build Standard validation:

a) The Manufacturer starts evaluation of a new product that requires changes to the scope of the original Build Standard validation (e.g. adding a new team, or process, or site)
b) The Manufacturer declares a change (e.g. a new site, addition of support for Triage Activities, or new build system/test tools) outside of an evaluation or Assurance Maintenance task
c) A change is identified during Assurance Maintenance.

In all of these cases the process is essentially the same: the CPA Test Lab will assess the changes and determine (in consultation with the SOp) whether:

a) they require a new full Build Standard validation, which would then result in a new BSVR and a new Build Standard Certificate with a new 6 year expiry date; or
b) whether the changes are suitable to be assessed in isolation, which would result in an update to the Build Standard Validation report to document the changes and the evaluator conclusions, a change to the description of scope on the Build Standard Certificate (if required by the changes), but no change to the expiry date on the Build Standard Certificate. The situations are described in more detail under sub-headings below: for a) and b) above see '*Renewing the Build Standard after a notified change or during a new evaluation*' below; for c) see '*Renewing the Build Standard during Assurance Maintenance*'.

For clarity: even where a change is suitable for Build Standard refresh or for reissuing the BSVR, the Manufacturer may nonetheless ask for a new full Build Standard validation to be carried out (resulting in a new 6 year expiry date).

Renewing the Build Standard after a notified change or during a new evaluation

If a new product evaluation is to be started and the Build Standard expiry date has not been reached, the CPA Test Lab must determine whether the product being assessed is still relevant to the existing Build Standard validation report, and whether the evidence in the report is still valid. The CPA Test Lab must consider the scope of the existing Build Standard Validation Report and confirm that the new product has been developed using the same process. If the original Build Standard is still valid, the CPA Test Lab should continue with the evaluation as normal and a new validation of the Build Standard is not required.

At the conclusion of the new product evaluation, the CPA Test Lab should consider whether the Manufacturer's processes are still as described in the existing Build Standard validation report and whether they still achieve the requirements listed in the Build Standard. If the CPA Test Lab believes that the Build Standard is still valid, and that the new product is covered by the validated processes, then the CPA Test Lab must record this finding in their test report and no further action is necessary regarding the Build Standard. The Build Standard remains valid and the existing CPA Build Standard Certificate expiry date is unchanged.

If the CPA Test Lab does not believe that the existing Build Standard is still valid, this opinion and the reasons should be documented and provided to the SOp. Subject to consideration by the SOp and SOwn in sections 3.3 and

3.4 above, the CPA Test Lab may need to perform a new validation against the Build Standard as per the normal Build Standard Validation process.

Renewing the Build Standard during Assurance Maintenance

A Build Standard update carried out during Assurance Maintenance is referred to as a 'Build Standard refresh'. A Build Standard refresh is required if the date of the latest Build Standard validation (including any formal updates to the validation), and the date of the latest Build Standard refresh are both more than 1 year from the date of completion of the Assurance Maintenance activity.

The following questions should be asked if a Build Standard refresh is required:

1. Have any of the processes and procedures assessed in the last Build Standard or Build Standard refresh (including any Device refurbishment activities as in [Refurb] covered by a Build Standard extension in [Triage]) [Note: the extended Build Standard requirements for Triage System, Triage Tool and Triage System Interface are specified in [Triage, section 3]. Have these changed in terms of:
   - the assurance-generating activities carried out
   - the responsibilities for the activities or their oversight
   - the tools or IT products and systems used to implement the processes and procedures?

   Note that changes would include cases where a defined process or procedure was no longer being carried out, or where relevant inputs were no longer available (e.g. vulnerability information for third-party products). Assurance-generating activities are those that implement a critical check or control under the scope of the Build Standard – an example of a change in such an activity would be a change to the definition of flaw categorisations, or to test stages or their completion criteria.
2. Have any new processes or procedures been defined in the areas of:
   - Configuration management
   - Test processes and pass/fail criteria
   - Product build
   - Flaw remediation (including notification of flaws in the product, or monitoring of flaws in third-party components)
   - Use of platform security procedures?
3. Have any changes been made in the physical scope of the processes covered by the Build Standard, e.g. additional sites becoming involved, or movement of an activity outside the original secure area in which it was carried out (even where equivalent security measures apply)?
4. Have there been any notifications of security vulnerabilities in the product or in any of its third-party components since the last Build Standard validation or Build Standard refresh (whichever is the later)?
5. Have you issued any notifications of vulnerabilities in the product to customers since the last Build Standard validation or Build Standard refresh (whichever is the later), or are any currently in preparation?
6. Have any activities related to refurbishment as in [Refurb] been added since the last Build Standard or Build Standard refresh?

Where changes are identified, the evaluator shall then assess (in consultation with the SOp) whether:

- the changes require a full re-validation of the Build Standard, resulting in a new BSVR, and a new Build Standard Certificate with a new 6-year expiry date; or
- the changes can be dealt with in isolation (i.e. without revalidating *all* of the Build Standard requirements) as part of the assurance maintenance process, resulting in a formal update to the previous BSVR, a change to the description of scope on the Build Standard Certificate (if applicable because of the changes), but no change to the Build Standard Certificate expiry date.

The records of responses to questions and any other resulting Build Standard activity during a Build Standard refresh (along with the BSVR itself) will be made available to evaluators in future for the purposes of evaluating other products or for other Assurance Maintenance activities.

7. Build Standard Validation Requirements

The tables below describe the mandatory Build Standard Requirements. The CPA Test Lab should gather evidence as to whether each requirement has been met.

The assurance activities listed are recommendations and are provided as guidance to the amount of assessment that might reasonably be performed. The CPA Test Lab may modify the assurance activities as they wish, as long as they are still able to make a case for why each requirement has been successfully met by the Manufacturer.

Some requirements also include 'Notes' under the main table: the Notes contain additional details arising from interpreting the generic Build Standard requirements for smart metering Devices. These Notes are also part of the requirement (as indicated by the use of 'shall'/'must'/'will').

Requirement 1: *Released versions of the Manufacturer's products must be uniquely identified. Released versions must be able to be completely recreated at a later date, with traceability provided by the identifier(s).*	
Description:	Customers and the Manufacturer should be able to uniquely identify released versions of products. It must be possible to recreate a released version of a security product (i.e. one that will have an entry on the CPL). If a product has changed since release, the Manufacturer should be able to identify all the changes that have been made as well as the individual developer that made the change. A record of such changes will also be needed to populate the Security Analysis Template (SAT) for a Risk Review.
Assurance Activity:	The Test Lab must ensure that a unique identifier is assigned to released versions of products. The Manufacturer should be able to associate these identifiers to specific builds of their products. The Test Lab must be confident that the Manufacturer reliably follows a process that achieves this. The Test Lab must seek evidence that the development team can later reproduce new instances of released builds.

Notes

Assessment of preparation of OTA updates

(See also Requirement 6 & Requirement 7)

As part of the Build Standard assessment the evaluator shall check the processes and procedures used by the developer to prepare software/firmware updates in a secure manner (linking to the examination of the update process examined in DEV.*.M866, DEV.*.M902 and VER.*.M347). The scope for this check is up to the point at which the update leaves the developer's control.

In particular the evaluator shall confirm the process for correct build of the update, application of any security mechanisms to the update, and the protection of those security mechanisms against unauthorised use or tampering (e.g. management of any keys used to protect the updates).

Evidence Expected:

Documentation of the firmware update process in terms of the development environment and manufacturing environment assets involved.

Requirement 2: *Updates that fix security flaws and security vulnerabilities must be actively advertised to supported customers and categorised according to the severity of the flaws and security vulnerabilities.*	
Description:	It should be straightforward for customers to establish whether a particular version of a product has known issues, and to establish if they have the most up-to-date version. Remediation procedures should be available to customers where security flaws and security vulnerabilities are discovered.
Assurance Activity:	The Test Lab must examine the Manufacturer's processes for informing customers of security issues discovered in their product, and ensure that these will ensure an effective and timely distribution of information. (Suggested methods could be using metrics i.e. 75% of customers made aware of issue within 2 working days. 95% within 7 days. Another approach may be to alert customers of a flaws and security vulnerabilities within 1 working day via a website, regularly update customers and provide information on the solution).

Notes

Notifying vulnerabilities to SSC

The SEC Section G3.21A requires "*Where a CPL Manufacturer becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on, the security of any Device Model in respect of which it is the CPL Manufacturer, it shall comply with the requirements of Section G3.18(b) and (c).*"

SEC Sections G3.18 (b) and (c) state:

"G3.18(b) take reasonable steps to ensure that the cause of the vulnerability or likely cause of the material adverse effect is rectified, or its potential impact is mitigated, as soon as is reasonably practicable;

and (c) ensure that the Security Sub-Committee is promptly notified of the steps being taken to rectify the cause of the vulnerability or likely cause of the material adverse effect, or to mitigate its potential impact (as the case may be), and the time within which those steps are intended to be completed."

- For these purposes the following definition of "Material Security Vulnerability", applies:

  "Material Security Vulnerability" means a weakness or exposure in (or in connection with) a Relevant Metering System which:

  (i) renders the Metering System (and/or the data stored thereon) materially vulnerable to unauthorised access or operation, or unauthorised interference causing theft or corruption of data; and/or

  (ii) is likely to have a material adverse effect on the security of any hardware, software or firmware which forms part of the Metering System.

Evidence Expected:

Documented evidence from the Manufacturer that their process includes SSC as a customer for the purposes of distributing vulnerability information that meets the definition of Material Security Vulnerability.

Documented evidence from the Manufacturer that if there are any actual vulnerabilities meeting the definition then they have in fact been notified to SSC.

Confirming Flaw Severity Categorisation

As part of the Build Standard assessment the evaluator shall check that the developer's flaw remediation process categorises flaws according to their severity, and implements a prioritisation that takes account of this severity.

Evidence Expected:

Documentation identifying the severity categories, process for categorisation, and process for prioritisation based on the severity categorisation.

Requirement 3: *All configuration items used in the Manufacturer's products must be uniquely identified.*	
Description:	All constituent components that are used to create the finished product must be uniquely identified. Any change made to these components must be attributed to the individual Developer making the change. This ensures that configuration management can properly occur, and that changes are properly managed. Without this, it would be extremely challenging for a Manufacturer to state with certainty precisely which components made up a given build of their product. The development and build environment must also be considered as configuration items.
Assurance Activity:	The Test Lab must ensure that all configuration items are uniquely identified. The Test Lab must also seek evidence by taking a sample of 10 to 20 configuration items and checking that they can be uniquely identified as defined by their process.

Requirement 4: *The Manufacturer must use an audit mechanism that identifies the author of any change to a configuration item.*	
Description:	Any change to a component of the product must be attributed to an individual Developer. This audit mechanism must use time stamping with a reliable time source to enable root-cause analysis to be performed easily should problems arise. Authorised users should be aware of this audit mechanism.
Assurance Activity:	The Test Lab must ensure that all changes to configuration items are uniquely identified. The audit mechanism must also identify the individual Developer making the change. Changes must only be made by authorised Manufacturer personnel. All authors of changes must be uniquely identified within all systems used to hold and process configuration items. The Test Lab must seek evidence by selecting a random sample of changes to configuration items and check that they have been uniquely identified as required from a defined process. The Test Lab must seek evidence that the Manufacturer's configuration management processes enable them to answer simple questions about their product. The granularity of the audit logs must enable the Test Lab to identify who originally authored a function and who made the last change to this file. It must also enable them to identify the purpose of any given change as well as the files to which the change applied. It must also identify the approver of a change.

Requirement 5: *The Manufacturer must use defined processes for remediation of flaws and security vulnerabilities and show that Manufacturers are trained in these processes. The Manufacturer must also show that mechanisms are in place to ensure that this process cannot be bypassed.*	
Description:	All but the very simplest products will contain incorrect behaviour or functionality. The Manufacturer is expected to have a well-defined process for triaging flaws and security vulnerabilities. This process should identify a resolution (if any) and make necessary changes to the product where appropriate. It is important that all staff that work in software, firmware and hardware development and product engineering are trained in the relevant process, and understand how to apply it to the products they work with, to ensure that the quality of the product improves as flaws and / or security vulnerabilities are discovered and remediated over time. Likewise, it is also important that Manufacturers are not able to "game" any flaws and / or security vulnerabilities remediation system, and that discovered issues really are resolved, rather than being hidden.
Assurance Activity:	The Test Lab must investigate the Manufacturer's flaws and / or security vulnerabilities remediation processes and ensure that they are applicable to any realistic problems which the Test Lab can hypothesise may occur in the future. The remediation processes must not be limited to security flaws and / or security vulnerabilities only. The Test Lab should perform a paper-based test of the process with the Manufacturer – walking through some hypothetical problems and understanding how the Manufacturer believes these would be captured and resolved. The Test Lab must investigate internal training that is provided to product engineering staff on these processes and determine whether it appears likely that the process will be understood and applied in practice. The Test Lab must then discuss the flaws and / or security vulnerabilities remediation processes with engineering staff and determine whether the processes appear to be understood and followed by staff.

Notes

Confirmation of external vulnerability monitoring

As a particular example of the developer's flaw remediation process the evaluators shall confirm that the developer:

- monitors publicly announced flaws in products and protocols that are used in the product (including any 3rd party components), e.g. Zigbee;
- determines their implications for the product under evaluation; and
- takes appropriate action in accordance with their flaw remediation process.

Note: it is not intended that the assessment of the developer's flaw remediation process will be confined to considering Zigbee flaws, but Zigbee flaws should always be included in the types of flaws examined and reported in the BSVR.

Evidence Expected:

Developer flaw remediation process documentation and examples illustrating its application.

Requirement 6: *The Manufacturer's configuration management system(s) must be protected from malfeasance from both internal and external sources. All configuration items must be protected at all times.*	
Description:	The configuration management system by necessity contains the sensitive information comprising of the Manufacturer's products. It is therefore vital that the confidentiality and integrity of this system is robust against malfeasance and improper use at all times. The protection of the configuration management system is not limited to the security of the system itself. This protection must also extend to the systems where development effort is regularly performed, and should include physical, personnel and procedural security measures enacted around the development and configuration management environments. Manufacturers are expected to be able to demonstrate that their site, network, and full development environment is given the protections deserved by the product. These protections must follow commercial good practice for network security.
Assurance Activity:	The Test Lab must investigate the Manufacturer's physical and logical protection of their configuration management system. The Test Lab must verify that the physical protection prevents unauthorised access to development systems, both during working hours and out-of-hours. The Test Lab should investigate the logical protection of the development environment and configuration management system, to ensure that the integrity of the product is maintained. They should consider the architecture of the systems and ensure they follow commercial good practice and relevant SSC guidance. The Test Lab review the incident reporting and disaster recovery procedures and interview Manufacturers to gain assurance that the procedures are implemented in practice.

Notes

Assessment of preparation of OTA updates

(See also Requirement 1 & Requirement 7)

As part of the Build Standard assessment the evaluator shall check the processes and procedures used by the developer to prepare software/firmware updates in a secure manner (linking to the examination of the update process examined in DEV.*.M866, DEV.*.M902 and VER.*.M347). The scope for this check is up to the point at which the update leaves the developer's control.

In particular the evaluator shall confirm the process for correct build of the update, application of any security mechanisms to the update, and the protection of those security mechanisms against unauthorised use or tampering (e.g. management of any keys used to protect the updates).

Evidence Expected:

Documentation of the firmware update process in terms of the development environment and manufacturing environment assets involved.

Requirement 7: *The way that products are assembled must be consistent and repeatable i.e., the build process should be automated.*	
Description:	Automation of regularly repeated activities helps to ensure that mistakes are limited. Assembly of the product from its constituent components as described in the Manufacturer's configuration management system is one such automatable process. Automation in this context can help ensure that new instances of the same build can easily be recreated, and that changes to the build environment are controlled and understood. This helps to ensure that changes that may have a poorly understood security impact are minimised, and that the Manufacturer has control over the product creation process.
Assurance Activity:	The Test Lab must ensure that there is an automated process for assembling the product from items held under configuration control. The Test Lab must ensure that this process is routinely followed in practice. The Test Lab must ensure that changes to the assembly process are controlled and audited by the Manufacturer.

Notes

Assessment of preparation of OTA updates

(See also Requirement 1 & Requirement 6)

As part of the Build Standard assessment the evaluator shall check the processes and procedures used by the developer to prepare software/firmware updates in a secure manner (linking to the examination of the update process examined in DEV.*.M866, DEV.*.M902 and VER.*.M347). The scope for this check is up to the point at which the update leaves the developer's control.

In particular the evaluator shall confirm the process for correct build of the update, application of any security mechanisms to the update, and the protection of those security mechanisms against unauthorised use or tampering (e.g. management of any keys used to protect the updates).

Evidence Expected:

Documentation of the firmware update process in terms of the development environment and manufacturing environment assets involved.

Requirement 8: All *Changes to the Manufacturer's products must be purposeful, necessary and be demonstrated to have very little impact or no negative impact on the overall quality of the product.*	
Description:	Manufacturers should be able to demonstrate testing and acceptance procedures for all new versions of the product. This applies particularly to the maintenance of security requirements. The Manufacturer should also be able to demonstrate how security flaws and security vulnerabilities are resolved and prevented from being reintroduced. The Manufacturer should also be able to demonstrate how regressions in security components are detected. This requirement is necessary to ensure that the quality of the product does not diminish over time.
Assurance Activity:	The Test Lab must ensure that the Manufacturer has a process for managing changes to the product. The Test Lab must ensure that an acceptance procedure exists for new versions of the product. The acceptance criteria should be determined using a documented quality standard. The Test Lab must ensure that this procedure is routinely followed in practice. The Test Lab must select a security flaws and security vulnerabilities that existed in the product[1] and determine how the Manufacturer identified the cause of the problem and the measures that have been put in place that prevent it from being reintroduced. The Test Lab should investigate whether the measures are successful in practice.

[1] If this is a genuinely new product from a Manufacturer who has never previously produced a product, then it is acceptable to review of their intended processes and procedures. The Test Lab must ensure there is reason to be confident that the procedures will be followed in practice.

Notes

Assessment of IRP & CRP handling

(See also Requirement 10)

As part of the Build Standard assessment the evaluator shall confirm that the developer:

- Identifies the versions of SMETS and GBCS that each version of the product implements
- identifies the IRPs and CRPs that each version of the product implements (where these have not been incorporated into the SMETS/GBCS versions implemented)
- defines tests applicable to each IRP and CRP that are to be carried out in order to test the implementation of each IRP and CRP
- carries out the IRP and CRP tests on each relevant version of the product.

(The intention of this interpretation is to confirm that any IRP and CRP changes that affect security and that are implemented separately from their inclusion in SMETS/GBCS have been tested appropriately.)

Evidence Expected:

Documentation of the process for managing IRPs and CRPs and ensuring that they are tested in the product.

Requirement 9: *Flaws and security vulnerabilities remediation is performed in practice.*	
Description:	The existence of plans for flaws and security vulnerabilities remediation alone is insufficient to meet this requirement. The Manufacturer must be able to show how problems in the product are discovered, analysed, corrected, tested, regression tested and managed in the configuration system in practice. This is to ensure that the product's overall quality improves over time as problems are discovered and rectified. The Manufacturer should also be able to show how their development teams have learnt from problems discovered in the product. The Manufacturer should have performed root cause analysis, and learnt from each issue. Flaws and security vulnerabilities are not limited to coding errors and implementation mistakes. They also include problems in the documentation of specifications and design.
Assurance Activity:	The Test Lab must seek evidence that the Manufacturer's flaws and security vulnerabilities remediation procedures are routinely followed in practice. They should pay particular attention to points in the development cycle where Developers and engineers are likely to be under significant pressures (e.g. in the run-up to the release of a new version of a product), to ensure that processes are not discarded at such times. The Test Lab should seek evidence from the Manufacturer as to how they actively seek out problems in products throughout the product's life cycle. The Manufacturer must also be able show to the Test Lab how a random sample of issues discovered (from minor to major) at all points in the product's lifecycle have been managed from discovery, through analysis, correction, testing and ultimate resolution.

Requirement 10: *The Manufacturer's products must behave as designed. i.e. they should have reason to believe that they are correct. Using non-trivial test cases, Manufacturers should be able to demonstrate evidence of security and functional testing. This testing should cover the whole scope of the product.*	
Description:	The Manufacturer's engineering processes must ensure that the products they supply do what they intended them to do – from the initial concept, all the way through to the implementation, it is vital that whichever engineering approach is taken, it ensures a quality product. Products with good overall quality do not directly imply high security, but low overall product quality is a certain indicator of potential problems. Regardless of the development style that the development and engineering teams employ, it is important that in practice the Manufacturer has a good understanding of what it is their product actually does. Evaluated CPA products will necessarily be security enforcing, and thus the Manufacturer must have reason to believe that they are secure; this confidence must be founded on the activities they have undertaken to develop it.
Assurance Activity:	The Test Lab must ensure that there is a good testing regime for products, and that tests are non-trivial, and are likely to exercise the product in practice. The Manufacturer must be able to explain to the Test Lab how they ensure good test coverage (i.e. that a sizeable percentage of each product's functionality and implementation is routinely tested). The Test Lab must seek evidence that the Manufacturer engages in security testing of their products. This must include positive (the product does what it is designed to), negative (the product doesn't do certain things it ought not to) and penetration (edge cases in the product's design or implementation do not cause unexpected behaviour, and perturbation of the product's environment does not interfere with its secure functioning). The Test Lab must also ensure that issues, which are discovered through such testing, are treated via the Manufacturer's flaws and security vulnerabilities remediation processes.

Notes

Assessment of negative testing

As part of assessing the developer's testing regime, the evaluators shall briefly describe the developer's policies for negative tests in the BSVR, shall comment on their suitability (e.g. in terms of whether they include typically useful tests such as boundary extremes, values outside the expected range, or instances of each distinct type of failure of a security check), and shall describe their conclusion as to consistent application of the policy based on a set of evaluator observations of evidence provided by the developer.

Evidence Expected:

Developer policies for negative testing, indicating what types of negative tests are required in each stage of testing, giving examples of negative tests, and indicating how sufficiency of negative tests is to be judged.

Examples of the application of the policy to the product under evaluation, and rationale for how the developer confirms that the policy is being routinely applied.

Assessment of developer reviews

(See also Requirement 13)

As part of assessing the effectiveness of the developer's reviews of product design and implementation, the evaluators shall comment on whether the developer's processes are likely to detect undeclared functionality in the product. Examples of relevant measures might include combinations of detailed code reviews by an independent coder (e.g. pair programming or other peer review of design/code), or use of analysis tools to detect untested code (which is then independently reviewed), and manual/automated reviews of code against aspects of the developer's coding standard that are designed to prevent vulnerabilities.

Evidence Expected:

Description of reviewing and analysis processes as part of Build Standard evidence.

Assessment of IRP & CRP handling

(See also Requirement 8)

As part of the Build Standard assessment the evaluator shall confirm that the developer:

- Identifies the versions of SMETS and GBCS that each version of the product implements
- identifies the IRPs and CRPs that each version of the product implements (where these have not been incorporated into the SMETS/GBCS versions implemented)
- defines tests applicable to each IRP and CRP that are to be carried out in order to test the implementation of each IRP and CRP
- carries out the IRP and CRP tests on each relevant version of the product.

(The intention of this interpretation is to confirm that any IRP and CRP changes that affect security and that are implemented separately from their inclusion in SMETS/GBCS have been tested appropriately.)

Evidence Expected:

Documentation of the process for managing IRPs and CRPs and ensuring that they are tested in the product.

Requirement 11: *Security enhancing features of the underlying platform, implementation language and tool chain should have been considered and used unless evidence is presented as to why this is not necessary or possible.*	
Description:	Modern platforms, development languages, libraries and development tools regularly offer security enhancing technologies to both minimise the occurrence of security defects, and to minimise their impact should they occur by mistake. The Manufacturer is expected to understand the security enhancing technologies offered by their chosen platform, language, libraries and tools and to have made an informed decision about whether to employ them. Security enhancing features are expected to be used unless there is a strong rationale to not do so[2].
Assurance Activity:	The Test Lab should discuss how the Manufacturer uses security-enhancing technologies, and determine their approach to these. The Test Lab should also assess whether the Manufacturer understands the security enhancing technologies available to them. The Test Lab should assess the development team's selected tool chain and development environment to determine whether the whole set of available security enhancing technologies have been used. Where this is not the case, the Test Lab must discuss this with the Manufacturer and understand the rationale for why specific technologies have not been selected. The Test Lab must then determine whether these represent consistent and well-reasoned arguments for the omission of such technologies. The Test Lab must clearly record these reasons in the report. The Test Lab must ensure that this requirement is not solely applied to the Manufacturer's own software, but also to third-party components they may employ.

[2]An example of this *might* be a new feature on the platform that has been widely proven as unreliable in practice.

Requirement 12: *Externally reported flaws and security vulnerabilities in the Manufacturer's products must be handed appropriately.*	
Description:	Flaws and security vulnerabilities in security products that are found externally must be treated with appropriate severity. These flaws and security vulnerabilities must be investigated and resolved as appropriate. This is particularly important in a smart metering context where numerous penetration tests and vulnerability assessments may be conducted on networks where these products may feature. The Manufacturer must be proactive in responding to externally reported issues in their products.
Assurance Activity:	The Test Lab must seek evidence that the Manufacturer has a process for receiving externally discovered flaws and security vulnerabilities that are reported. This process must be routinely followed in practice. The Test Lab should investigate whether externally reported flaws and security vulnerabilities are passed into the Manufacturer's standard flaws and security vulnerabilities remediation processes. Manufacturers should demonstrate that they monitor publicly announced security flaws and security vulnerabilities for their products and that they respond to issues identified in their products as appropriate.

Requirement 13: *The Manufacturer should use a coding standard that is applied to all code in their finished products (including third-party components). The coding standard and associated processes must ensure that common software defects and easily avoided security weaknesses are not introduced into the product's code.*	
Description:	Regardless of the development language selected, there are both good and bad practices for secure coding. Coding standards can cover many aspects of development – from "house styles" through to lists of prohibited library APIs. This requirement is intended to help ensure that all code contributing to the product is developed with security in mind, and that development processes (such as code review and check-in gates) help to keep the software quality as high as possible from a security perspective. This requirement intends to ensure that simple mistakes are not accepted into code that is used in the final product, and that development staff are made aware of secure development practices. It is also vital that the Manufacturer's use of third-party components does not introduce weaknesses in their products. The Manufacturer should have a process to determine code quality before a third-party component is used. The third-party component must be kept up-to-date as security issues are discovered and resolved.
Assurance Activity:	The Test Lab must ensure the Manufacturer has a coding standard[3], and that this coding standard addresses both software quality and security issues. The Test Lab should ensure that the coding standard covers all languages that the Manufacturer uses, and that it covers good practice for common security errors made in these languages. These should also be up-to-date and based on industry-standard good practice – as an example, the SANS Institute and the Mitre Corporation publish a list [CWE25] of what they consider the "most dangerous" coding errors, so a good coding standard should seek to minimise the occurrence of these errors. The Manufacturer is responsible for maintaining and renewing the Build Standard. The Test Lab must ensure that the Build standard is maintained and kept up-to-date by the Manufacturer. The Test Lab should determine what secure development training is provided to Developers and engineers to ensure that Manufacturers are informed about the importance of adhering to the coding standard. Engineers should be provided with sufficient information about the contents of the coding standard. The Test Lab may test the Manufacturer's personnel's understanding of the coding standards at an interview. The Test Lab must also ensure that there is a process in place for individual Manufacturers to be notified of changes to the Manufacturer's Coding Standard.

Assurance Activity (continued)	The Test Lab must seek evidence that the Manufacturer's engineering process uses the coding standard and ensure that code that does not meet the coding standard cannot reach the product. They should seek evidence that the process is routinely followed. The Test Lab must ensure that the Manufacturer has an on- boarding process for third party components (including open- source or the public-domain components). This process should ensure that these components follow the in-house coding standard, or an equivalent level of quality. The Test Lab must ensure that there is a maintenance process for all third-party code and components, ensuring that they remain current and secure, and that this process is routinely followed.

[3]It is acceptable for the Manufacturer to employ a third-party coding standard, as long as it applies to their environment and their engineers make use of it in practice.

Notes

Assessment of developer reviews

(See also Requirement 10)

As part of assessing the effectiveness of the developer's reviews of product design and implementation, the evaluators shall comment on whether the developer's processes are likely to detect undeclared functionality in the product. Examples of relevant measures might include combinations of detailed code reviews by an independent coder (e.g. pair programming or other peer review of design/code), or use of analysis tools to detect untested code (which is then independently reviewed), and manual/automated reviews of code against aspects of the developer's coding standard that are designed to prevent vulnerabilities.

Evidence Expected:

Description of reviewing and analysis processes as part of Build Standard evidence.

8. References

[CWE25] M. Howard *Improving Software Security by Eliminating the CWE Top 25 Vulnerabilities*, IEEE Security and Privacy, vol. 7, no.3, pp. 68-71, May/June 2009.

See also https://cwe.mitre.org/top25/

[Refurb] SSC Guidance for Device Refurbishment & Security Controls, Part 2, v1.3 (in general the latest version should be used), available at https://smartenergycodecompany.co.uk/ssc-guidance-on-device-security-assurance-and-triage/

[Triage] Triage interface updates to GSME, ESME, SAPC & 4G CH SCs and CPA Build Standard Extensions, v2.1, https://smartenergycodecompany.co.uk/