

This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

Paper Reference:	TABASC_90_0106_09
Action:	For Discussion

MP231 Proposed Solution

1. Purpose

[MP231 'Firmware upgrade pathways'](#) is currently undergoing the Refinement Process. The purpose of this paper is to update the Technical Architecture and Business Architecture Sub-Committee (TABASC) on the Proposed Solution to this modification and ask for its views.

2. Summary of MP231

This section summarises the key points of this Modification Proposal. More information is available in the Modification Report in Appendix A.

2.1 What is the issue?

Certain Device models need to have a firmware upgrade applied in a specific order. Failure to follow the specific order can result in unintended consequences. Investigation of the issue indicates that it is not an uncommon requirement for firmware updates to be implemented in a specific order.

There is currently no location where this information relating to certain dependencies for each Device is publicised as a reliable source. The information may be able to be found within the Release Notes for that particular Device and firmware version. However, that information may either not be available to a Supplier as they could contain commercially sensitive information or the Supplier may have inherited the Device as the consumer changed Supplier. Also, the Release Notes could be difficult to interpret as they can be very complex. The Release Notes by themselves without specialist Device Manufacturer or engineer knowledge may not provide the clarity required to inform a Supplier.

The information required to ensure each Device has its firmware upgrade applied in the correct order is not included within the Firmware Information Repository (FIR), nor is there a requirement in the Smart Energy Code (SEC) for that information to be provided.

2.2 What is the solution?

The solution will place an obligation on Device Manufacturers to provide additional information with their Central Products List (CPL) submissions. This information will then be included in the FIR so that it is accessible for Suppliers, through the SEC website.

The additional information will be:

1. CPL Entry ID(s) of the previous firmware version that can be upgraded to the new version on their CPL submission. This could be one or many versions depending on their firmware. If there is no previous version, then 'N/A' should be used to populate the field.
2. ZigBee chipset vendor of the chipset that is included on that version of the Device Model
3. ZigBee stack version that is included on that version of the Device Model
4. ZigBee band information with regards Device behaviour when joining the Home Area Network (HAN). This will be a drop-down field within the CPL submission.

This information will be requested on a best endeavours basis for existing entries on the CPL. If it is not possible to source the information for some Device Models then these fields will be left empty.

3. What are the options?

3.1 CPL Entry ID or Firmware Version?

The TABASC discussed this issue at meeting 73, in January 2022. TABASC members stressed that they were more comfortable using the firmware version itself to denote the upgrade path as opposed to a CPL row reference as it was thought this would introduce unnecessary complexity. The benefit of using a firmware version name relates to user experience as that is the terminology they are already familiar with. TABASC members agreed that the commonly known name for firmware versions should be included in the FIR entries.

Since these discussions, SECAS has reviewed the current CPL entries more fully and noted that the same firmware versions are used by multiple manufacturers for Device Models. Therefore, to remove ambiguity the manufacturer code would also be needed as a minimum along with the firmware version to become part of the Firmware Upgrade Path. It might also be required to add the Device Model identifier, and possibly the Device hardware version and revision, to ensure uniqueness.

The CPL Entry ID would already provide this unique reference and therefore SECAS recommends that the CPL Entry ID be used.

The Firmware Upgrade Path is deemed to be only available to SEC Parties, this is why it is added to the FIR instead of the CPL. For ease of use the FIR and CPL can be combined by means of a standard Excel Xlookup using the CPL Entry Number as a key. This allows the creation of a single list which can be filtered to identify the firmware version.

3.2 Provision of Zigbee information

The Security Sub-Committee (SSC) has requested that in addition the firmware upgrade pathway, Device Manufacturers also provide three pieces of ZigBee information: ZigBee band, ZigBee chipset vendor and ZigBee stack certificate. Respondents to the Refinement Consultation either supported the provision, or did not provide a view. More information on responses to the Refinement Consultation can be found in Appendix B. However, some Device Manufacturers have indicated outside of the consultation that they are not comfortable having this information available to all SEC Parties. The SSC is therefore considering whether this information should be provided directly to the SSC, separately to the CPL submission process. This would be via an encrypted format that is restricted to the SSC, using a similar on-line reporting form that is used to report security vulnerabilities.

4. Questions for the TABASC

We seek the TABASC's view on the following questions to feed into the Modification Report:

- Does the TABASC share the view of using CPL Entry ID as the identifier, rather than firmware version?
- Should ZigBee information be included as part of the FIR, and therefore viewable to SEC Parties, or as separate process and viewed solely by the SSC.

5. Next steps

Once this modification has been discussed with the TABASC and the Working Group, the Proposer will confirm their Proposed Solution and it will be presented to the Change Sub-Committee (CSC) for approval to proceed to the Report Phase.

6. Recommendations

The TABASC is asked to:

- **PROVIDE VIEWS** that the Proposed Solution should use the CPL Entry ID as the identifier for firmware sequencing information; and
- **PROVIDE VIEWS** whether the ZigBee information should be provided to the SSC only as part of a separate process.

Kev Duddy

SECAS Team

24 May 2023

Attachments:

- **Appendix A:** MP231 Modification Report
- **Appendix B:** MP231 Refinement Consultation responses