SEC Modification Proposal, SECMP0007, DCC CR 211

Firmware Updates to Mandated HAN Devices (PPMIDs and HCALCS)[1]

Full Impact Assessment (FIA)

Version:	**0.76**
Date:	**5th August, 2020**
Author:	**DCC**
Classification:	**DCC PUBLIC**

[1] PPMID = PrePayment Meter user Interface Devices, HCALCS = HAN Connected Auxiliary Load Control Switch

Contents

1 Document History

1.1 Revision History

Revision Date	Revision	Summary of Changes
10/07/2020	0.4	Initial responses with DCC first review
22/07/2020	0.55	Release to Working Group
30/07/2020	0.71	Incorporated feedback from TABASC and Working Group
04/08/2020	0.76	Included overall costs

1.2 Associated Documents

This document is associated with the following documents:

Ref	Title and Originator's Reference	Source	Issue Date
1	SECMP0007 – Solution Design Note 0.7	SECAS	07/08/2018
2	Updated Requirements and Preliminary Impact Assessment (PIA) version 1.21	DCC	05/08/2019
3	SECMP0007 Firmware updates to IHDs and PPMIDs' Business requirements – version 1.31	SECAS	04/02/2020

References are shown in this format, [1].

An initial draft of changes to the Great Britain Companion Specification (GBCS) with changes related to this Modification was shared with the Service Providers by SECAS.

1.3 Document Information and Modification History

The Proposer for this Modification is now Robert Williams, E.ON.

An Early Impact Assessment was requested of DCC in July 2016, after updated requirements were issued by SECAS, with the first Preliminary Impact Assessment (PIA) supplied in July 2018.

A full review of the PIA was carried out based on the expiry of the original design and cost estimates in the original PIA. The second version of the PIA (0.60) submitted in April 2019, includes a full listing of the requirements and two options for a solution approach; solution 1 using Zigbee Over The Air was covered in the previously issued PIA, but a new solution 2 for implementing firmware upgrades using the existing ESME approach was proposed. The document was used by the Service Providers as the basis for a high-level solution design with associated, revised costings.

That document was then reviewed to reflect the findings of the Working Group, and the Refinement Consultation, which included a check on the scope of the Modification.

A first Full Impact Assessment was requested by SECAS on 24th July 2019, but approval to proceed was not issued until 20th August, 2019, and the document was not fully completed.

In December 2019, a streamlining review designed to generate a minimum viable product including the Working Group, Service Providers, and BEIS met. A modified and reduced scope was defined, and the Service Providers were asked to complete a FIA against the new requirements in April 2020.

Note that a section highlighting design decisions made during the development of this solution has been added in Appendix D: Design Decisions.

1.4 Terminology

Note the terms "Device” and "HAN Devices" are used interchangeably with the phrases "PPMID / HCALCS" and "PPMID and HCALCS" in this document. The terms PPMIDS, PPMIDs, and HCALCSs were used in the Business Requirements and may appear in this FIA.

The terms "updates” and "upgrades" relating to firmware updates are used interchangeably in this document.

Additional terms specific to this Modification have been added to Appendix A: Glossary at the end of this document.

2 Introduction

This section gives context to the required solution and includes both the high-level business requirements and detail of the proposed solution. Most of this section is taken verbatim from the business requirements document [3] published by SECAS.

2.1 Context

Over-The-Air (OTA) firmware updates through the DCC Total System are currently supported only for the Communications Hub (CH), Electricity Smart Metering Equipment (ESME) and Gas Smart Metering Equipment (GSME) devices. This modification aims to enable Suppliers to send Manufacturer produced Firmware updates to PPMIDs and HCALCS via the DCC, and for the HAN devices to be able to activate those updates, subject to Manufacturer specific checks that updates are valid (i.e., from the Manufacturer; valid for the Device's current Device Model etc.).

It should be noted there are already a large number of PPMID devices in the field that will require firmware updates, and this number will have increased by the time this Modification is implemented.

2.2 Requirements

Based on the discussions at the Working Group and the Business Requirements as set out in the Solution Design Document [1], DCC understands the outcomes this modification wants to achieve the business requirements that can be summarised as follows.

1.	Manufacturer Image Hashes associated with PPMIDs and HCALCSs to be added to the Central Products List (CPL)
2.	Suppliers to be able to send firmware updates to PPMIDs and HCALCSs over the air (OTA)
3.	The DCC to notify all Responsible Suppliers at certain stages during the processing of firmware updates
4.	The DCC and Responsible Suppliers will check the latest firmware version on PPMIDs and HCALCSs
5.	The Communications Hub will be able to support the prioritisation of firmware Images to all HAN Devices
6.	Upon firmware Image activation, the DCC will update the Smart Metering Inventory (SMI) with the new firmware version for the updated Device
7.	Additional Communications Hub functionality to support the distribution of OTA Upgrade Images to PPMIDs and HCALCSs
8.	Firmware update support capability will need to be mandated on PPMIDs installed after this Modification is implemented

Table 1 High L:evel Business Requirements:

2.3 Detailed Requirements and Business Processes for Firmware Upgrades

A detailed breakdown of the requirements, supporting information, and potential business process solutions for the requirements follows.

2.3.1 Adding PPMID/HCALCS Manufacturer Image Hashes to the CPL

For a Manufacturer Image to be added to the Central Products List (CPL), additional details in relation to that Image will need to be provided to the SEC Panel.

The Supplier will need to confirm to the Panel that the firmware update does not affect how the PPMID or HCALCS communicates using ZigBee.

If the firmware update impacts how the PPMID or HCALCS communicates using ZigBee and requires re-testing, a new ZigBee Assurance Certificate will need to be provided to the Panel before the firmware can be updated.

The CPL Requirements Document specifies the additional details in relation to the Manufacturer Image that must be provided to the Panel:

- the Hash of the Manufacturer Image;
- the identity of the organisation that created that Image; and
- a digital signature created by the creator of the Image across the communication containing the CPL entry details.

The digital signature used to sign the communication between the submitter and the Panel needs to be the same as the one received from a Public Key Infrastructure (PKI) chosen by the Panel to check the signature

A template for submitting CPL entries has been published on behalf of the Panel, which sets out the approach to digital signing taken by the Panel.

In addition to the above, HCALCSs must comply with the Commercial Product Assurance (CPA) Security Characteristics as per the Smart Metering Equipment Technical Specification (SMETS). Changes to HCALCS firmware may require either the inclusion of the new firmware version in the existing CPA certificate or a new CPA certificate. For HCALCSs, this CPA certificate must be submitted to the Panel when adding a new firmware version to the CPL.

2.3.2 Communications Hub Memory Considerations

No additional buffer space on the Communications Hub is being proposed. Only the GSME memory block will be used for storing PPMID and HCALCS Images. The ESME memory block will not be used to store PPMID and HCALCS Images.

PPMID and HCALCS Images will be overwritten by GSME Images if one arrives whilst a PPMID or HCALCS update is in progress. If another PPMID or HCALCS Image arrives whilst a PPMID or HCALCS update is in progress, the newly arrived Image will overwrite the one in process.

Changed requirement: There will be no Service-Level Agreement (SLA) for how long a firmware Image can be stored in the Communications Hub before it is overwritten. The Image will remain on the Communications Hub until it is overwritten.

The Communications Hub shall make the PPMID / HCALCS image available for fourteen (14) days unless a new PPMID / HCALCS / GSME image is available.

If a PPMID / HCALCS / GSME Upgrade Image is discarded or replaced prior to having been successfully transported over the HAN, the Communications Hub shall send an Alert for each target Device Entity Identifier associated with the Upgrade Image File

GBCS drafting places a requirement on the CH to send an Alert for each device associated with an image when the image:

(a) has transferred to the target successfully

(b) failed to transfer after all retries (at ZigBee level) have been exhausted

(c) is discarded.

The Supplier will then know status of the file transfer and whether the image needs resending. If the image is discarded after the mandated storage duration ((c) above) then there is a fair chance that the PPMID isn't operational. A Supplier could send the read firmware version command to the PPMID (after initial upgrade or new installation of a PPMID which supports the feature), but the absence of a response would simply confirm that the PPMID isn't operational; just much quicker.

2.3.3 Dual Supplier Scenarios

Both Responsible Suppliers shall be able carry out firmware updates to PPMIDs in dual Supplier scenarios. The Proposer and the Working Group accept that this may increase the risk of firmware updates being overwritten by each of the Responsible Suppliers in a dual Supplier scenario.

Only the Import Supplier shall be able to carry out firmware updates to the HCALCSs.

2.3.4 Anomaly Detection Thresholds

The Security Sub-Committee (SSC) have stated that Service Requests to update firmware for PPMIDs must be subject to the same Anomaly Detection Threshold (ADT) procedures as ESME and GSME. However, PPMIDs must be counted and reported separately to enable anomalies with the potential to affect energy supply to be detected separately from those for PPMIDs.

The SSC also stated that Service Requests to update firmware for HCALCSs should subject to the same ADT procedures as ESME and GSME since similar risks to the supply of energy apply to HCALCSs.

2.3.5 Activation date-time

Future dated activation of PPMID Manufacturer Images will not be permitted. Upon successful receipt of the OTA Upgrade Image by the PPMID, the Communications Hub will instruct the PPMID to immediately activate the new Manufacturer Image.

Changed requirement: The Communications Hub will no longer be required to record the activation date-time plus [X] minutes. This is due to the decision made at the Working Group meeting held on 19 December 2019, to have the PPMID generate the Device Alert for success/failure of the firmware update. This Alert will go from the PPMID to the Supplier, via the Access Control Broker (ACB).

HCALCS Manufacturer Images are activated using the existing Service Request 11.3, which must be adjusted to include HCALCS as valid target Device Type.

2.4 Sending PPMID Firmware Images

This section outlines how the process will work for PPMIDs if firmware is made up of a single Manufacturer Image or several Manufactures Images. HCALCSs are covered in Section 4 'Sending HCALCS Manufacturer Images' below.

Note: An OTA Upgrade Image must be less than or equal to 750KB in size.

2.4.1 Sending a single Manufacturer Image to a PPMID

This section details the steps that will need to be taken to update PPMID firmware. It is assumed that a Manufacturer provides a Manufacturer Image to the Supplier and a new CPL entry has been created. The resulting OTA Upgrade Image will be less than or equal to 750KB in size.

Sending a Manufacturer Image to a PPMID will require a new Non-Critical Service Request 'Send PPMID Firmware'. Currently the next available and most logical Service Reference Variant for this Service Request will be 11.4.

Supplier Preparations

Before sending the new Service Request to the DCC for a PPMID firmware update, the Supplier will be required to follow several steps. These will be similar in initiating a firmware update to the DCC for a Meter:

Obtain the following information:

1. The Manufacturer Image

2. OTA Header, which should include:

    a. Manufacturer ID;

    b. Model to which it can be applied;

    c. Firmware Version contained in the Image; and

    d. Minimum and maximum hardware version to which it can be applied.

3. A Hash of the Manufacturer Image.

Undertake the following checks on that information:

1. The Hash the Supplier has calculated over the Manufacturer Image is the same as that provided by the person who created the Manufacturer Image (in this case the Manufacturer); and

2. Check that the Manufacturer Image is associated with one or more Device Models on the CPL. The check should include that:

    a. The Hash is recorded on the CPL against one or more entries;

    b. The OTA Header Manufacturer ID, model and Firmware Version fields match identically with one of the entries identified at step (a); and

    c. The hardware version in that CPL entry is between OTA Header minimum and maximum hardware version, inclusively.

Supplier creation of a 'Send PPMID Firmware' Service Request

Having obtained the information and upon the above checks being successful, the Supplier will create a 'Send PPMID Firmware' Service Request. The Service Request will include the following information:

1. Image: The Image to be sent composed of a base64 encoded version of the concatenation:

OTA Header || Manufacturer Image

2. List of Device IDs: Up to 50,000 PPMIDs will be able to be listed within the Service Request.

The DCC checks on the 'Send PPMID Firmware' Service Request

On receipt of the 'Send PPMID Firmware' Service Request, the DCC will follow the following steps:

1. Check whether the OTA Upgrade Image contained within the Service Request is less than or equal to 750KB in size;

2. Calculate the Hash of the Manufacturer Image contained within the Service Request;

3. Check whether the Hash the DCC has calculated is on the CPL, and identify CPL entries with that Hash;

4. For each of the Device IDs in the Service Request:

    a. Check the Device is a PPMID;

    b. From the Smart Metering Inventory (SMI), identify the Device's current Device Model, and ensure that the Manufacturer ID, model and hardware version fields for that current Device Model equate to one of the entries identified at step 3;

    c. Identify, from the SMI, the Communication Hub Function (CHF) ID to which the Device is associated; and

    d. Check that the Supplier is the Responsible Supplier for one of the Smart Meters Associated with that CHF ID.

If this and all preceding checks succeed, the DCC will identify (and temporarily record against the Device ID) the details of all Responsible Suppliers Associated with the CHF ID. This temporary record will be used to populate the DCC Alerts at the next step.

DCC response to the 'Send PPMID Firmware' Service Request

The DCC will be required to notify all Responsible Suppliers at different stages of the Service Request processing. The first notification will happen when the DCC receives the 'Send PPMID Firmware' Service Request:

1. Upon the DCC receipt of the 'Send PPMID Firmware' Service Request, the requesting Supplier will receive a Service Response. If some of the Device IDs in the Service Request failed any of the checks at step 4 under 4.1.3 (above), the DCC will send a Service Response to the requesting Supplier listing all the Device IDs that failed and the reason for the failure in each case. The DCC will carry on processing the firmware distribution for those Device IDs that passed the check.

2. Upon the DCC completing the processing of the 'Send PPMID Firmware' Service Request, each Responsible Supplier identified in 4.1.3 will receive a DCC Alert containing:

a. The Hash of the Manufacturer Image in the Service Request (to identify the CPL entry)

b. A list of Device IDs to which the Image is being sent

DCC Distribution of the 'Send PPMID Firmware' Service Request

If the checks are successful, the DCC will distribute the Image from the Service Request (having decoded from base64 encoding) to the Communications Hub associated with each of the PPMIDs in the List of Device IDs where the Device ID passed the validation.

SEC Schedule 10 'Communication Hub Technical Specifications' (CHTS) 4.4.4 requires that the receiving Communications Hubs can buffer Images intended for ESME and GSME. The Communication Services Provider (CSP) contracts require Communications Hubs to have the capacity to hold two 750KB Images (to support independent distribution of firmware to one of the ESME and the GSME).

Communications Hub notification of Image availability to the PPMID

Once the Image arrives at the Communications Hub, the Communications Hub will need to:

1. Record OTA Header details

2. Notify the PPMID by sending a message to it/them ('the Communications Hub shall send a Zigbee Smart Energy (ZSE) Image Notify command').

PPMID request for the details of the Image

The PPMID will then, in line with the ZigBee OTA specification, send a message (a 'QueryNextImageRequest' ZSE command containing Manufacturer ID (manufacturer code), model (Image type), current Firmware Version, and optionally hardware version) to ask the Communications Hub if there is an Image that may be suitable for it.

Provision of Image details by the Communication Hub to the PPMID

For the Communications Hub to decide that the Image is suitable for the PPMID, the ZigBee OTA specification details a recommended, default policy to determine its response, specifically to:

'send back a response that indicates the availability of an Image that matches the manufacturer code, Image type, and the highest available file version of that Image on the server. However, the server may choose to upgrade, downgrade, or reinstall clients' Image, as its policy dictates. If client's hardware version is included in the command, the server shall examine the value against the minimum and maximum hardware versions included in the OTA file header'

Note that 'server' in the above refers to the Communications Hub and 'client' refers to the PPMID.

The Communications Hub will send back a 'QueryNextImageResponse' accordingly.

PPMID download and authentication of the Image

The PPMID will then download the Image from the Communications Hub, if one is available for it.

When the PPMID has downloaded the Image, it will check the Manufacturer signature (or equivalent) within it. This confirms the Manufacturer Image is as created by the Manufacturer. The PPMID will then store the Manufacturer Image from within the Image sent, so that it is available for activation . The PPMID will then send a 'UpgradeEndRequest' to the Communications Hub.

Activation of the firmware Image

The Communications Hub will then send a 'UpgradeEndResponse' with the activation date-time set to 0x00000000 for immediate activation in line with the ZigBee specifications. The PPMID will immediately activate the Image.

The PPMID will then create a Device Alert containing its firmware version and send it to the DCC. The DCC will update the SMI if the firmware version has changed and forward the Device Alert to the Responsible Suppliers recorded to receive the Alert.

If the Device Alert is not received, the Supplier can send SR11.2 to the DCC. This will result in a Command to the PPMID to respond with its active firmware version. The DCC will forward the Response to the Supplier and update the SMI if the firmware version in the SMI is different. SR11.2 can also be sent at any time by a Responsible Supplier if desired.

Process for updating PPMID Firmware comprised of a single Manufacturer Image

The process described above for processing PPMID firmware updates comprised of a single Manufacturer Image is presented in Figure 1 below.

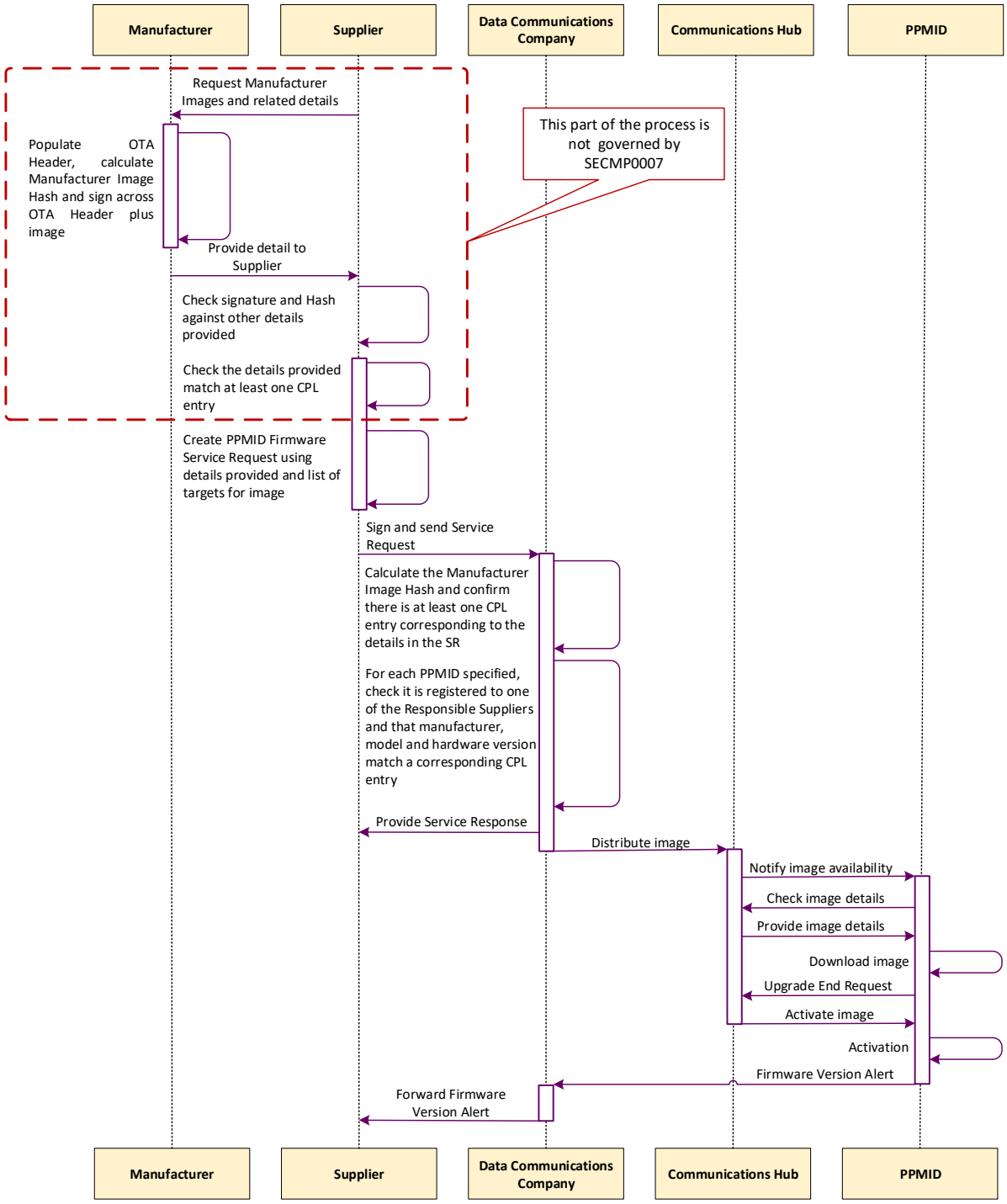

Figure 1 Process for updating a single PPMID Manufacturer Image

2.4.2 Updating PPMID firmware with Multiple Manufacturer Images

This process is for the benefit of Manufacturers and Suppliers, and does not propose any changes to the way in which the DCC manage Manufacturer Images. The DCC simply treats each Image as it would with firmware made up of a singular Manufacturer Image. There is no additional validation for the DCC to carry out compared with firmware made up of a singular Image.

A full description of this process is given in Appendix B: Updating PPMID Firmware with Multiple Manufacturer Images on page 59 below.

2.4.3 Sending HCALCS Manufacturer Images

The process for the OTA upgrade of HCALCSs aligns with the current Technical Specifications and GBCS for the Supplier to distribute and activate firmware on the ESME and GSME. This will be accomplished by adding the HCALCS as a target Device Model to the existing Service Reference Variants.

As with ESME and GSME firmware updates, distribution will be carried out via SR11.1 'Update Firmware' and activation via SR11.3 'Activate Firmware', the latter via a GBCS Critical Command.

The expectation is that HCALCS firmware is typically below 750KB. However, the existing ESME/GSME OTA firmware upgrade mechanisms contained in the GBCS allow manufacturers to split firmware into multiple OTA Upgrade Images less than or equal to 750KB in size; this method can be employed in case HCALCS firmware exceeds the size of 750KB.

2.5 Non-Functional Requirements

PPMID firmware is expected to be typically less than 750KB in size and updates will occur no more than two times per year. Note that there is no requirement for a Change of Supplier (CoS) action to require a PPMID update.

Device manufacturers have advised that their firmware updates are likely to be no larger than 350KB. However, the customisation of PPMIDs with graphics will increase the firmware size; this may happen going forward and require the mechanism for delivering firmware greater than 750KB. In any case, any single OTA Upgrade Image must be less than or equal to 750KB.

In terms of the numbers of PPMIDS installed and requiring updates, DCC has supplied the following information and assumptions. Overall installation numbers are as follows:

SMETS2	Today	At Scale (End 2024)
PPMIDS	2.4million	17.9million
CHF	2.7million	20.3million
%		88%

In the table above, the ratio of PPMIDS to CHF as of July 2020 (about 88%) has been linearly scaled to an "at scale" number of devices. It should be noted that CSP South and Central accounts for approximately 68% of all installations, based on ITSF forecasts.

For network loading and infrastructure augmentation calculations, there is an assumption that the installed base of PPMIDs should be taken as the updateable base. This is almost certainly an overestimate. SECAS have initiated a Request For Information to try and identify the current position.

A further breakdown of the figures to volumes per minute for an example installed base of 15 million PPMIDS looks like this:

- 15 million PPMID updates over 6 months, with two firmware updates per year
- Even Distribution across each of the 6 months
- Equates to an average of 60 firmware downloads per minute

This assumes the sending of single updates to single devices, therefore excluding any batching of updates, any updates rejected for authentication, and does not include resends of data. In previous discussions there has been a variation of +/-10% over the year, and this figure can be applied to system throughput as well.

Volumes associated with HCALCS firmware is expected to be much smaller and with a very low upgrade frequency. It may be possible that HCALCSs do not need updates at all unless changes to the ZigBee version are required.

Following from the discussion with the Security Sub-Committee (SSC) there are no security concerns with regards to firmware upgrades for PPMID or HCALCS.

2.6 Requirements Summary

Based on the discussions at the Working Group and the Business Requirements as set out in the Solution Design Document, DCC consider the requirements for SECMP0007 to be **STABLE**.

3 Solution Architecture

Over-The-Air (OTA) firmware updates through the DCC Total System are currently supported for the Communications Hub (CH), Electricity Smart Metering Equipment (ESME) and Gas Smart Metering Equipment (GSME) devices only.

3.1 Solution Overview

This Modification will allow the Service Users to send firmware images for PPMIDs and HCALCS using the DUIS interface. The DSP will process the received request that contains the firmware image and the list of devices, and forward that to the CSPs along with the corresponding Comms Hub identifiers. DSP will make use of the existing Web Service interface at the two CSP SMWAN Gateways to deliver the firmware image to the CSPs. The OTA firmware image processing by CSPs for PPMID differs slightly from that of the other device types (ESME, GSME or HCALCS) as described below, and the DSP will add a new field to the firmware distribution interface such that CSPs will know the device type.

There will be two different firmware image delivery mechanisms used by Comms Hubs:

- A ZigBee Over-The-Air (OTA) delivery mechanism will be used to deliver firmware to PPMIDs. This method introduces the combined distribution and activation of the Manufacturer Image into one single Service Request. This will be a new Non-Critical Service Request created specifically for the PPMID. The Communications Hub is to manage the activation of PPMID firmware. The PPMID itself will manage the notification to the Service User upon activation of the firmware.
- HCALCS will utilise the existing firmware update procedure used by Electricity Smart Metering Equipment (ESME) and Gas Smart Metering Equipment (GSME). This requires a distinct separation between the distribution and activation of the firmware. As with ESME and GSME firmware updates, distribution will be carried out via SR11.1 ‘Update Firmware’ and activation via SR11.3 ‘Activate Firmware’, the latter via a Great Britain Companion Specification (GBCS) Critical Command.

The CSPs will deliver the firmware image to the corresponding Comms Hubs and the Comms Hubs will in turn deliver it to the target device within the HAN.

The schematic below shows an end-to-end view of the OTA firmware delivery and the mechanisms used to communicate between different systems. The interfaces and message formats used by DSP to communicate with the other parties or devices remain unchanged. The key change is the introduction of a new firmware distribution mechanism (Zigbee OTA as opposed to a combination of Zigbee OTA and GBCS) between the Comms Hub and the PPMID as shown in the schematic below.

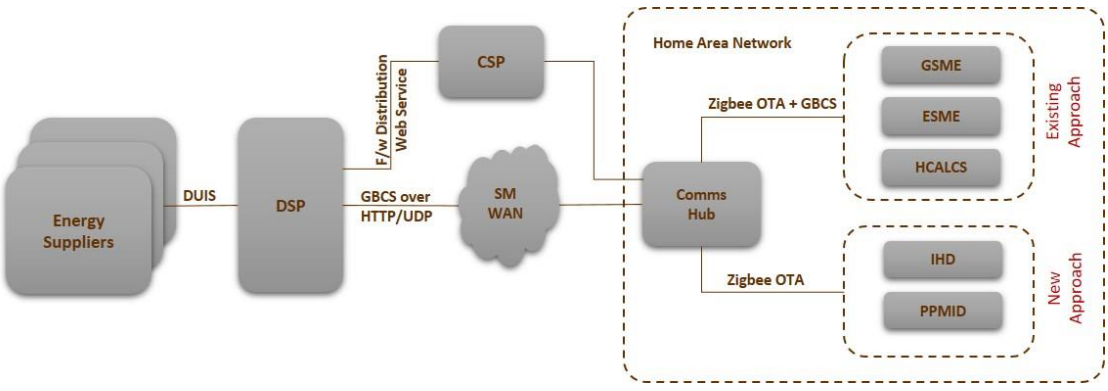

Figure 2 Firmware Delivery Overview

This is a wide-ranging SEC Modification and the impacts across the system actors and components are as follows:

CSP N	H	BIMI	N	CHTS	Y		
CSP S & C	H	GBCS	Y	CH	Y	HCALCS	Y
DSP	H	DUIS, DUGIDS, MMC XML	Y	CPL	Y	PPMID	Y
P & C	H	SMETS	Y	ESME	N		
BT	N	SEC	Y	GSME	N		

Note that SMETS1 devices are not in scope of this Modification, and are covered by a separate DCC programme.

3.2 DSP Solution Overview

The DSP is required to fulfil the following high-level requirements:

- Add support for processing the firmware update requests for PPMID and HCALCS devices within DSP
- Track the progress of the firmware updates and send notifications to the relevant Service Users

The solution is made up of a common component for tracking the firmware distribution progress, and two distinct methods of firmware updating, Zigbee OTA and GBCS Delivery.

The following Service Requests will be enhanced to support the OTA upgrades:

- SR 11.1 ‘Update Firmware’
- SR 11.2 ‘Read Firmware Version’
- SR 11.3 ‘Activate Firmware’

A new Service Request to distribute the firmware images specifically for the PPMIDs, 11.4 Update PPMID Firmware, will be introduced. SRV 11.4 will share its general attributes and validation checks with SRV11.1. Please note that SRV11.4 will be applicable only for SMETS2 PPMIDs.

For HCALCS, the existing Service Requests and the process used for GSME and ESME will be used. These include:

1. Use of the existing SRV 11.1 for distribution of firmware images to HCALCS
2. Use of SRV11.3 for activating the new firmware

The firmware images for both PPMID and HCALCS will be delivered to the CSPs using the existing interfaces.

In the SMETS the HCALCS sections must be updated to reflect the HCALCS capability of receiving and activating new firmware.

3.2.1 CSP Management and CSP SMWAN Gateway

No changes are required within the CSP Management Gateway.

CSP SMWAN Gateway will introduce a new interface for CSPs to notify DSP the status of a firmware image delivery to the Comms Hub.

The existing firmware delivery interface will be updated to include device type as a new attribute. This will help CSPs process the OTA image differently for PPMID device types.

The proposed interface changes are available in the documents attached here.


CR211-Telefonica-SMWAN-Gateway-Ext


CR211-Arqiva-SMWAN-Gateway-Extract

3.2.2 Firmware Distribution Progress Tracking

The DSP will track the progress of the firmware update request at a Device level. This will need to be built as a mechanism common to all device types and the following details will need to be recorded.

Field Name	Notes
Device ID	ID of a Device within the SR 11.1 request
Service Request ID	The Service Request ID
Firmware Version	New firmware version
Processing Status	Indicates the progress of the request (see table below for the status values).
Reason Code	The reason for rejection if the Processing Status indicates a rejection
Last Updated Time	The time at which the latest change in Processing Status was recorded.

Table 2 Firmware Update Tracking

Tracking will allow DSP to block the firmware update request for a device if there is already one in progress. Note there has been a request to change this to a per-Comms Hub basis as described in section 3.2.5 following.

The Service Users will be sent DCC Alerts to notify the different stages of firmware update processing. The input data for these Alerts will be received as notifications from the CSPs or as Device Alerts from the Comms Hubs.

The following diagram illustrates the updates to the firmware distribution flow due to these changes.

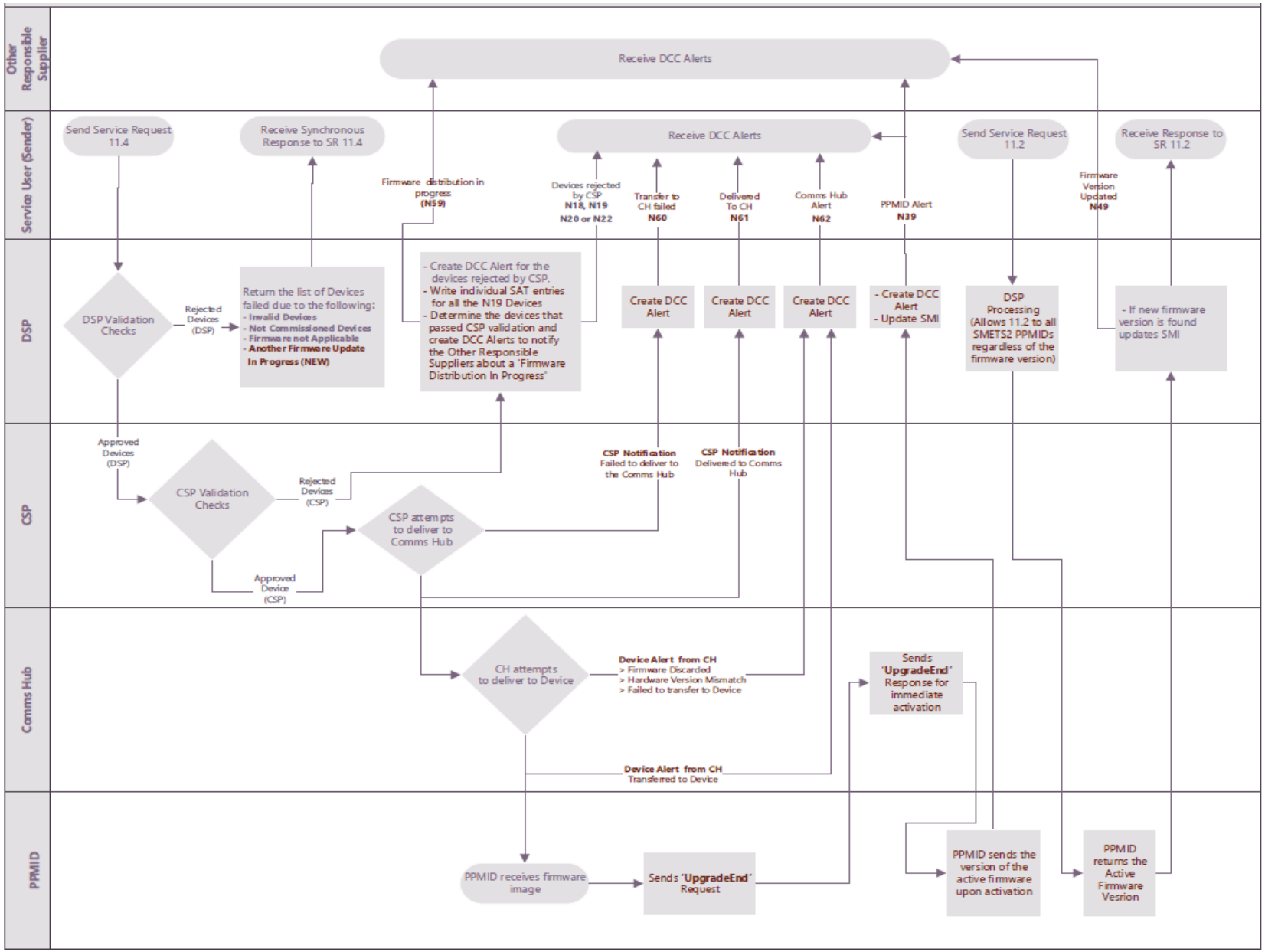

Figure 3: PPMID Firmware Distribution Flow

The first stage of processing by the DSP checks the list of devices included in a Service User request (SR11.1 or 11.4). Devices in the list may be considered as failed as follows:

- Invalid deice
- Not commissioned device
- Firmware not applicable
- Another firmware update in progress

A synchronous response with these device IDs is sent to the Service User that submitted the request.

The DSP then identifies which CSP each device ID is allocated to, and the CSP SM WAN Gateway sends a batched request to the appropriate CSP. The DSP will segregate the PPMIDs based on the region and send them to the relevant CSP using the existing CSP SMWAN Gateway interface to distribute firmware. This interface will be updated to include a new attribute to convey the type of device to the CSPs to help distinguish PPMIDs from the other device types.

The firmware distribution processing statuses maintained by the DSP include associated DCC Alerts as summarised in the table following.

Processing Stage	Processing Step	Processing Status	Notes	Trigger	Outbound Notification Mechanism	Recipients
Processing within DSP	DSP validation checks	REJECTED_BY_DSP	This functionality exists except for the check to see if another firmware update request is in progress for any of the devices.	NA	Synchronous Response	Sender of SR 11.1 or 11.4
Processing within CSP	CSP validation checks failed	REJECTED_BY_CSP	This functionality currently exists.	Notification from CSP	DCC Alerts **N18, N19, N20 or N22**	Sender of SR 11.1 or 11.4
	CSP Validation Checks Successful	APPROVED_ FOR_DISTRIBUTION	Derived by DSP as the inverse of the list of rejected devices. One Alert per Service User.	The above notification from CSP	DCC Alert **N59**	All Responsible Suppliers other than the Sender
	Delivery to Comms Hub Failed	FAILED_CH_TRANSFER	New interface required at CSP SMWAN Gateway to receive this.	Notification from CSP	DCC Alert **N60**	Sender of SR 11.1 or 11.4
	Delivered to Comms Hub	SUCCESSFUL_ CH_TRANSFER		Notification from CSP	DCC Alert **N61**	Sender of SR 11.1 or 11.4
Processing Within HAN	Comms Hub failed to deliver to target Device	FAILED_HAN_ TRANSFER	Device Alert from Comms Hub with Alert Code 0x8F89 and Transfer Response Code 3	Device Alert from Comms Hub	DCC Alert **N62**	Sender of SR 11.1 or 11.4
	Delivered to target Device	SUCCESSFUL_ HAN_TRANSFER	Device Alert from Comms Hub with Alert Code 0x8F8A and Transfer Response Code 0	Device Alert from Comms Hub	DCC Alert **N62**	Sender of SR 11.1 or 11.4
	Firmware discarded by Comms Hub	HAN_DISCARDED	Device Alert from Comms Hub with Alert Code 0x8F89 and Transfer Response Code 1	Device Alert from Comms Hub	DCC Alert **N62**	Sender of SR 11.1 or SR11.4
	Firmware rejected by Comms Hub due to version mismatch of the target hardware	HAN_REJECTED_HW_M ISMATCH	Device Alert from Comms Hub with Alert Code 0x8F89 and Transfer Response Code 2	Device Alert from Comms Hub	DCC Alert **N62**	Sender of SR 11.1 or SR11.4
	Device activates the firmware	FIRMWARE_ACTIVATED	Applicable only for PPMIDs. The Alert Code is 0x8F8B.	Device Alert from PPMIDs	DCC Alert **N39**	All Responsible Suppliers
Service Desk Intervention	Device status reset	RESET_BY_DCC	Changed by the DCC Service Desk via the SSMI interface	NA	NA	NA

Table 3: Firmware distribution statues and DCC Alerts

The status values APPROVED_FOR_DISTRIBUTION, SUCCESSFUL_CH_TRANSFER or SUCCESSFUL_HAN_TRANSFER will be considered as 'In Progress' statuses by the tracking mechanism. If DSP receives a firmware update service request (SR11.1 or SR11.4) for a device, which already has another request with an 'In Progress' status, then the new SR will be rejected. A device will be allowed to stay in the 'In Progress' status only for a limited period of time to avoid any erroneous deadlocks, thus allowing Service Users to send new firmware update requests. The

tracking timeout will be managed as a configurable duration of time and will need to be agreed with DCC.

If there is a need to reset the status of a device manually, the DCC Service Desk will be able to use a new interface provided within the SSMI. This will help reset the status of a device before the tracking timeout expires.

The Service Users will be able to view the last recorded processing status of a device using a SSI screen. Development of the SSI change will be carried out during the design phase.

For the HAN Devices rejected by a CSP due to a Device ID identification failure (DCC Alert N19), individual SAT Log entries will be made.

For the PPMIDs that pass CSP's validation checks, the DCC Alert N59 will be sent to the Responsible Suppliers other than the sender of the SRV 11.4 to notify that a firmware update has been initiated for a given device. DSP derives the list of devices that passed the CSP's validation checks by taking the inverse of the list of devices that fail the validation checks.

In order for DSP to receive notifications from CSP that contain the delivery status of firmware image to the Comms Hub, a new interface will need to be built at the CSP SMWAN Gateway.

Note that a Comms Hub has two slots for firmware upgrades that will also be used for ESME and GSME updates. If several updates are in progress at about the same time then the Comms Hub is expected to prioritise meters upgrades over PPMID upgrades, so a PPMID upgrade may be refused, or an accepted one may be deleted. There will be no retry within CSP or DSP. This situation will be handled by the Comms Hub sending an alert to the DSP as the Access Control Broker, to inform the sender of the firmware update request. It will be the sending supplier's responsibility to re-request the update if required.

A new DCC Alert (N62) will be used for forwarding all the Device Alerts that result from the firmware update processing within a Comms Hub to the Service Users. This will contain a payload with information about any failure messages.

DSP will create SAT log entries for all the Device Alerts. If the Device Alert includes Response Code to indicate a failure, the Response Code will be included in the SAT record. The SAT records for Alerts received from the Comms Hub will contain the Device ID of the relevant device.

Based on the mechanism used by the Comms Hubs to deliver the firmware images to the target devices, the overall solution has been divided into two parts.

3.2.3 Part 1: PPMID Firmware Updates using Zigbee OTA Delivery

The following principles and constraints have been identified for this solution option:

- A Comms Hub needs to be aware of the status of a firmware image download to a HAN device i.e., complete or in progress
- Storage prioritisation for both the Comms Hub and the DSP will be enabled. The DSP will send only one firmware request at a time for a specific device until the Comms Hub indicates the update is complete, and the oldest dated firmware is removed.
- There must be a capability to hold two firmware upgrades in the Comms Hub memory, so there is an ability to queue the upgrades, but there is only one update running at a time

- CHTS changes will be required
- The DSP would reject any request for a firmware upgrade, if there is already one in progress
- There is a requirement for an uplift to any Comms Hub emulator
- Devices remain as Type 2 devices, and communication limited to Zigbee only

A Zigbee OTA delivery mechanism is used for delivering firmware image to a PPMID, the processing of which does not rely on GBCS. The firmware image will be activated automatically after it has been successfully delivered to the PPMID. Therefore, a separate activation request is not needed.

A new Service Request 11.4 Update PPMID Firmware will be introduced to distribute the firmware images specifically for the PPMIDS, and this will enable the DSP to maintain the Anomaly Detection volume thresholds of PPMIDs separate from the other device types. SRV 11.4 will share its general attributes and validation checks with SRV11.1. Note SRV11.4 will be a Non-Critical command and therefore Users aren't obligated to submit ADTs for this. The SSC confirmed this is acceptable as the PPMID devices are not load controlling.

All the Device Alerts from the Comms Hubs will be sent to Service Users as DCC Alerts in relation to the Processing Statuses identified in Table 2. This will help the Service Users to be aware of the progress of the firmware update.

DSP will record the sender's ID of the latest firmware update request (SRV11.4) for the PPMIDs to determine the destination of the DCC Alerts.

Service Users will be able to read the version of the PPMID firmware by using the Service Request 11.2 Read Firmware Version. If the SRV 11.2 is targeted at a PPMID, then the DSP will employ the URP (Unknown Remote Party) pattern to process this. **Note** the correct behaviour relating to 11.2 will only work with PPMIDs where their firmware has been updated using SECMP0007.

If the Response to SRV11.2 contains a version of firmware different to the version in SMI, the SMI will be updated with the new version subject to the rules applicable for the other Devices. Therefore, Service Users could use SRV11.2 also as a vehicle for updating the firmware version of PPMIDs in the SMI.

Summary

- Service Users will be able to use SRV 11.4 to send the firmware update requests for PPMID
- Service Users will receive notifications at different stages of processing across DSP, CSP and the Comms Hubs
- Service Users will be able to use SRV 11.2 to read the firmware version of PPMID as well
- The firmware update mechanism used for PPMID does not require separate activation request as it is activated automatically upon successful distribution

3.2.4 Part 2: HCALCS Firmware Updates using GBCS Commands

The main principles of the alternative approach to implement firmware upgrades is based on a very different approach from the Zigbee OTA delivery.

- This approach treats any device endpoint like an ESME, such that the firmware is pushed to it with credentials
- There is no need for device changes to support keys as HCALCS already have Supplier certificates which can be used to validate security credentials
- There is a requirement to ensure end to end security for the firmware image in the same way as ESMEs
- There is a risk that firmware upgrades could be fired repeatedly at devices with significant impacts on battery life etc. In this case, the required outcome is that the DSP would reject any request for a firmware upgrade, if there is already one in progress
- There is no requirement for any prioritisation of firmware request, which reduces the complexity significantly
- There is no dependency on the ESME device
- CHTS changes will be required to allow the storage of a Firmware update on HCALCS
- GBCS changes are required to support the Read and Activate Firmware Use Case for HCALCS

This option also requires uplift to emulation environments to allow end to end testing of firmware distribution.

The solution to update HCALCS firmware will follow the existing firmware update procedure used for the ESME and GSME. The end-to-end security of the HCALCS will be managed similarly to that of the ESME. The firmware distribution flow for HCALCS is shown following.

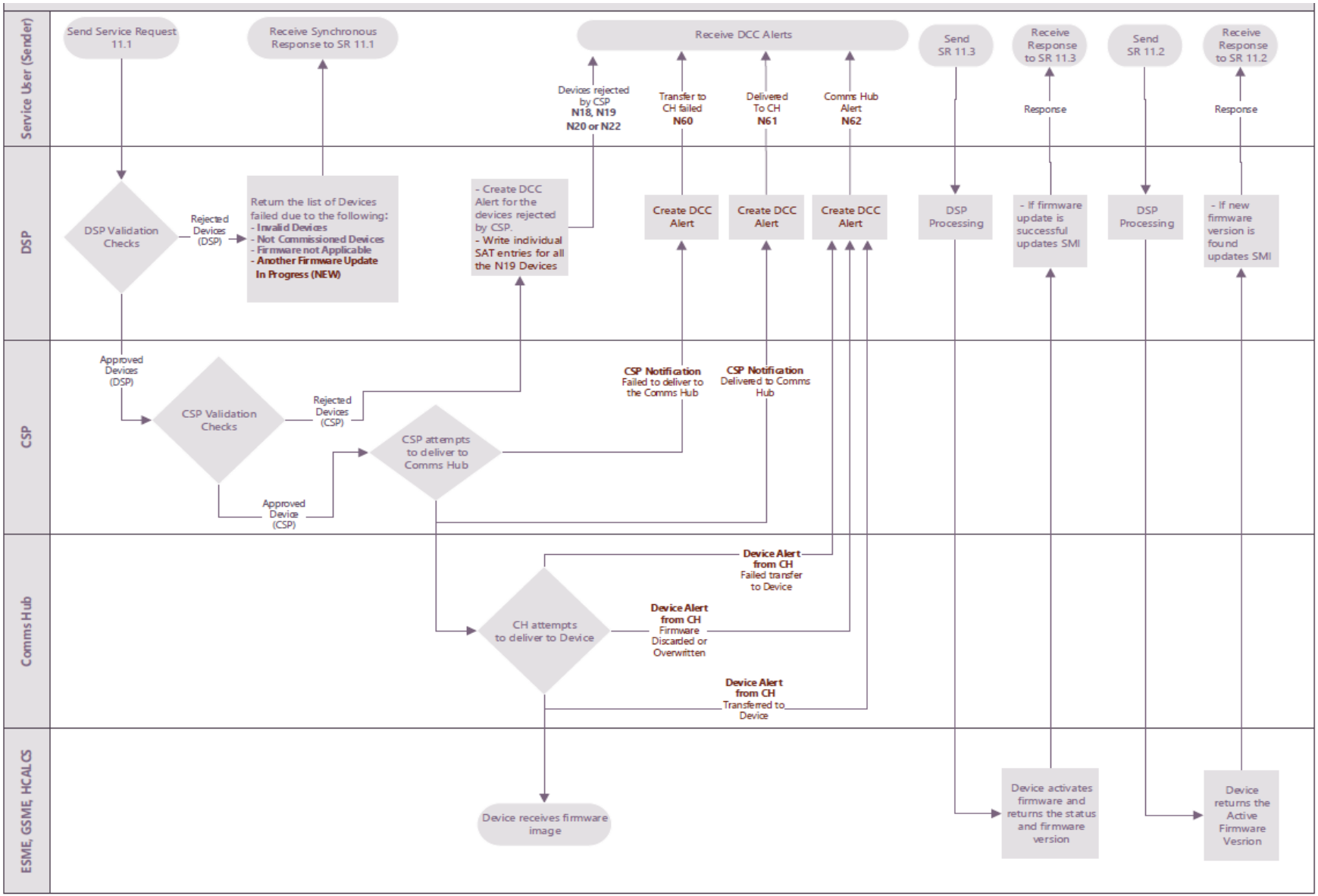

Figure 4: ESME, GSME and HCALCS Firmware Distribution Flow

Service Users will be able to use the following Service Requests for HCALCS firmware updates also.

- SRV 11.1 Update Firmware
- SRV 11.2 Read Firmware Version
- SRV 11.3 Activate Firmware

It is expected that the existing GBCS Use Case for ESME ECS52 (Read Firmware Version) will be implemented for HCALCS and therefore no new Use Case is required. The existing GBCS Use Case CS06 (Activate Firmware) will also need to be extended to HCALCS to support firmware activation.

3.2.5 Control Dependencies on DSP

Controls on firmware Service Requests have been identified as follows.

Note that the DSP implementation of “Firmware Tracking” is a slightly wider scope in that it tracks whether there is a firmware download in progress to the HAN device (i.e. ESME, GSME, PPMID, or HCALCS).

Control 1	Device-Based Control: Recommend a per device check to block any firmware distribution request (ESME / GSME / PPMID / HCALCS) for HAN devices where there is already an update in progress. This will prevent excessive repeated downloads from the CSP to Comms Hub – preventing an “accidental Denial of Service”. Extend the error response on SR11.1/SR11.4 to include an error and a list of devices rejected due to “firmware distribution in progress” to be sent back to the sender of the 11.1 or 11.4. Validation Rule (1) – DSP cannot send another HAN device firmware update to the HAN device until the first update is complete. Return failure code and list of devices Validation Rule (2) - A device can only stay in the ‘In Progress’ status for a limited time to avoid any erroneous deadlocks, thus allowing Service Users to send new firmware update requests. The tracking timeout will be managed as a configurable duration of time.
Control 2	Add a CSP “Too Busy” Response to prevent CSP system overload. The proposal is to modify the existing firmware distribution APIs used for all HAN devices (not just for ESME/GSME) to notify the DSP if the CSP is unable to process the firmware upgrade request. The CSP would return a “Busy” (http 503) with a reason code. DSP currently carries out an immediate web service retry and then carries out a retry every hour for 24 hours followed by a timeout A change the DSP to include provision for an http503 (System Busy) response on the firmware distribution API is required and for this to invoke the “long retry” design pattern. Recommendation is that in all cases the "long retry" design pattern is extended to 4 days.
Control 3	CSP and DSP systems SD 4.4.2 / SD 4.4.1 interface change to notify the status of the firmware download over SMWAN, to support both the individual and batch API status notifications.

	Anticipate a high volume of such alert status notifications over the interface and recommendation is for the DSP to implement the batch API option, to potentially minimise the load on both the Telefónica and the DSP systems. The notification interface is included in the DSP changes, but will need an upper limit and other non-functional requirements.

3.3 CSP Impacts

This change enables a firmware upgrade to PPMIDs and HCALCS alongside existing HAN devices i.e. ESME and GSME, using a modified DSP-facing CSP hosted API, the SD4.4.1 (CSP North) or SD4.4.2 (CSP South and Central) Firmware Upgrade API. The firmware images will be subject to firmware validation report generation and communication to the DSP via the existing APIs.

Firmware images will be distributed to Comms Hubs with a priority lower than existing ESME or GSME firmware images such that if an ESME or GSME firmware request is received, they will be prioritised and scheduled for distribution of firmware image ahead of PPMIDS and HCALCS. The image activation instructions for PPMID will be embedded within the firmware image, image activation for HCALCS is separate to the distribute firmware request and follows the existing ESME/GSME firmware service.

The PPMID firmware version is to be read via a new GBCS use case targeting the Communications Hub as defined in GBCS, while the HCALCS firmware version to be read via a change to the existing SR11.2 DUIS command and associated GBCS use case.

Firmware distribution alerts will be sent to understand the device type and transfer success notification will be added. Two new alerts for all HAN device upgrades to indicate success or failure criteria of a firmware download.

This Modification also impacts the CSP Support applications, and will require expansion of environment compute and storage capacity. Whilst the nature of the changes to both the CSP Comms Hubs and support systems are similar, they are broken out and described in the following sections.

3.4 CSP South and Central Solution Overview

CSP South and Central's scope of delivery for this Modification includes the introduction of a new service to support the distribution of firmware images to additional HAN devices, i.e. PPMIDs and HCALCS. The features of this service include the Modification of the existing CS06 meter firmware service and newly introduced service including:

- Introduction of the HAN firmware transfer status alerts from the CSP to the DSP. The business rules with regards to the usage of the new API would be designed in the Design stage, as CSP South and Central anticipates a potential increase to the volume of such SMWAN firmware distribution notification alerts, which will be seen in the DSP hosted API in the SD 4.4.2 SMWAN Gateway interface.

- Confirmation of a failure to transfer a firmware image to the appropriate HAN device.

- Introduction of new service busy alerting to temporarily defer the DSP service request until the CSP platform is able to service the firmware upgrade request.

3.4.1 Impact to CSP South and Central Communication Hubs

The CSP South and Central Comms Hub impacts to deliver this Modification are outlined below.

Change Category	Description of Change
New	Implement new GBCS Use case CS05c Distribute Firmware to PPMID including immediate activation of PPMID as a new command Implement new GBCS Use case CCS08 Firmware Transfer Alert to notify the DSP with the firmware download status alerts in-line with GBCS alert structure (0x8F8A/ 0x8F89) Implement GBCS Use Case CS08 Read PPMID / HCALCS Firmware Version Business Rules in Comms Hub to prioritise GSME over PPMID, HCALCS firmware OTA New alerts relating to error cases relating to Firmware storage prioritisation issues.
Modified	Firmware download status alerts to include HAN device type; GBCS Use Case CS05b Distribute Firmware to include HCALCS in the ESME, GSME device list.

3.4.2 Impact to the Smart m2m Solution Components

The CSP South and Central Smart m2m solution is the core solution component responsible for the scheduling, prioritisation and distribution of the firmware update to the target end HAN devices. The changes proposed in Smart m2m & Networks as part of this Modification include:

SD4.4.2 FirmwareUpgrade API	This is the firmware distribution API is used for all HAN devices not just ESME/GSME. The API specification will be modified to identify the HAN device type in the API request so that CSP South and Central can distinguish between ESME/GSME firmware and PPMID/HCALCs requests to distribute the images and permit the Comms Hub to differentiate and prioritise the images. This interface will also be modified to notify the DSP if Smart m2m is unable to process the firmware upgrade request at the time when the request was received. It is expected that this will be via a HTTP 503 status code however this will be agreed during design.
Modification of existing OTA firmware download alerts	This change requires that Smart m2m process any alerts generated by the Communication Hub with the HAN device “type” corresponding to the firmware image downloaded to the Communication Hub. This change allows CSP South and Central systems & administrators to identify the type of HAN device that a firmware upgrade request was intended for and for use in downstream reporting processes.
Notification of Firmware Download Status to DSP	This new function requires that Smart m2m notifies the DSP of the status of the firmware download to target Communications Hub(s) with a status: • Download Successful • Download Failed • Other • Reason Code (root cause of a failure, for example) Smart m2m will send the notification directly to the DSP using the new notification API hosted by the DSP, via the Access Gateway. This interface will be agreed with the DSP during the design phase.
HAN Device Firmware Upgrade	A new function which, upon receiving an SD4.4.2 firmware update request, will assess service load on Smart m2m. Currently, CSP South and Central has no means by which to protect the CSP South and Central Firmware delivery service. This is covered in section 3.2.5, Control 4 following.

Admission Control	When CSP receives an SD4.4.2 firmware update request, if the Smart m2m cannot accept the DSP request, then Smart m2m will send a synchronous response to the DSP notifying the DSP to defer the firmware upgrade service request until the CSP platform is able to service at a later point in time.
Billing Report	All HAN device firmware upgrades including those to the new HAN devices be represented as separate transactions on the Smart m2m DMM Billing Report i.e. requests to upgrade the Meter and a PPMID device connected to the same CH be represented as separate transactions on the current interface. Additionally, to manage scenarios which could result in such requests showing up as duplicates on a file i.e. same Job Id, same date time etc., add an additional synthetic key (representing a sequence id) to the interface. This is to ensure Netcracker doesn't reject requests against the same Comms Hub under the same Job and the same date-time as duplicates. Additional Billing Report content will include, for each operation: • HAN Device Type • DSP Job ID • Firmware ID
CHF <-> HAN Device Firmware Upgrade Status	This new function provides CSP South and Central Service Management with some visibility of the transfer of HAN device firmware image transfers between the CHF and HAN devices. Also it will provide an indication of the success or failure of the activation of the image on the target HAN device. The Communications Hub will send an alert containing the following HAN device firmware upgrade status to Smart m2m:which will map the alerts received from the Communication Hubs to a corresponding Simple Network Management Protocol (SNMP) trap.
Smart m2m Day 0 & Day 4 Reports	These reports are used by CSP South and Central IT systems to calculate the PM2 performance measures for each HAN Device firmware upgrade request. The reports will identify the device type that the report relates to. This information is required so that the IT systems can identify which target device data needs to be used in the PM2 calculations. Smart m2m will include all Firmware requests which have passed the validation report stage in a SLA Day 0 & Day 4 Report

3.5 CSP North Solution Overview

The Modification will impact the components shaded in the following diagram.

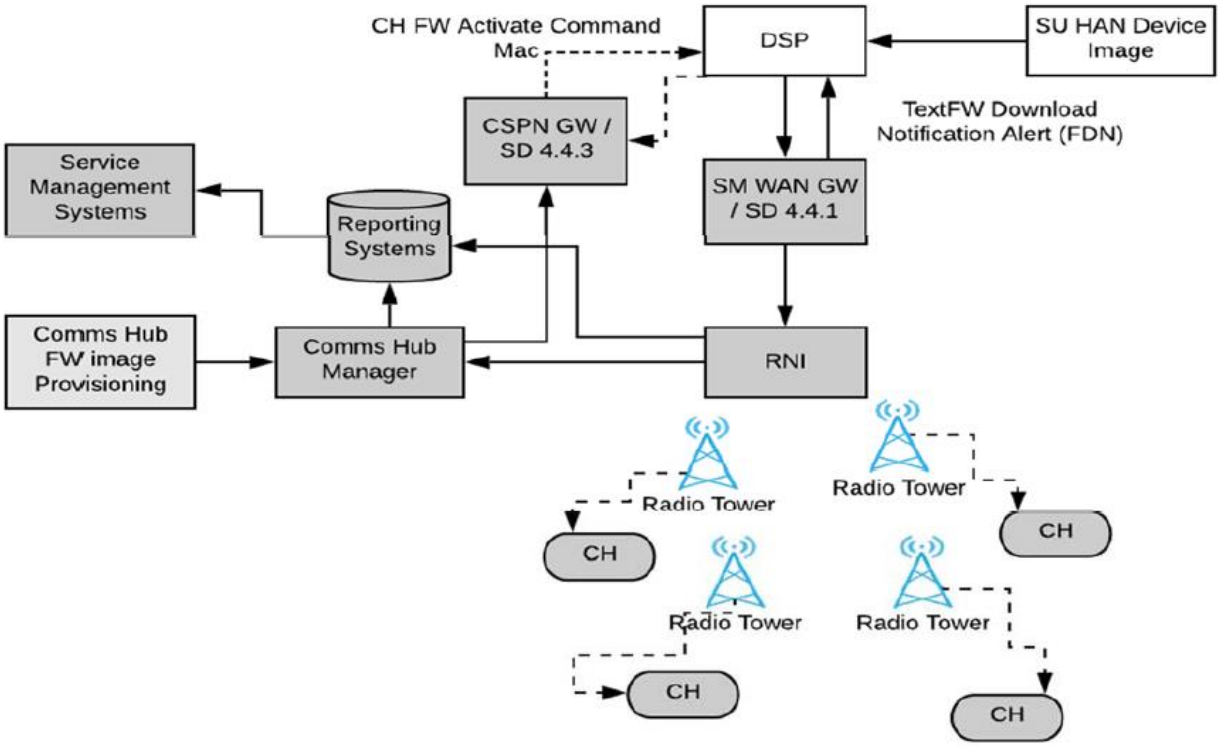

Figure 5: Impacted CSP North Components

Changes specific to the CSP North solution are described following.

3.5.1 Communications Hub Development

Changes to the Communications Hub will be required to:

- support the download of the FW upgrade image to the HCALCS and PPMID and offer it over the HAN
- support the Alerts generated
- update the WAN SDK (Sensus development) with a new API, which will need to be integrated into the Communications Hub
- support the handling of the new API to transfer the new alerts.
- store the update images in the GSME block using the image storage and replacement rules in GBCS. The image will be stored in the GSME memory block for a minimum of 2 (two) weeks before deletion

Alerts

The CHF shall support the generation of new GBCS 8F8A and 8F89 alerts with the option of enhancing the 'Transfer Response Code' or adding 'additional bytes' to the payload defined in GBCS. The exact detail to be agreed during the detailed solution design.

New CHF alerts shall also be generated for the ESME / GSME but not the CHF. The table below provides a breakdown of the image removal triggers and the corresponding GBCS alert code.

Trigger	Action	Alert Code	Transfer Response Code
End device sends an Upgrade End Request with Status of Success	Discard image	8F8A	0 – Success
End device sends a Query Next Image request with a hardware version out of range of the image's min and max hardware versions	Discard image	8F89	2 - hardwareVersionMismatch
Higher priority GSME image received	Discard image	8F89	1 - imageDiscarded
New PPMID/HCALCS image received for the same device model	Abort active download Discard image	8F89	1 - imageDiscarded
End device sends an Upgrade End Request with Status other than Success	Discard image	8F89	3 - fileTransferFailure
End device stopped downloading for 24hrs	Discard image	8F89	3 - fileTransferFailure
End device does not initiate download for 14 days	Discard image	8F89	1 - imageDiscarded

Table 4: Image Removal Triggers and Alerts

3.5.2 SMWAN to SMWAN Gateway Interface

The RNI (Regional Network Interface) is the core server stack that routes traffic from the DSP to the (CSP North) CH. It presents a web services layer to the DSP, to which Service Requests are posted via the relevant API. It also provides the head end control of FWDL jobs and manages routing information for contacting CHs.

There are 4 main impacts to the FlexNet service in the RNI as part of this Modification:

1. FlexNet protocol change to move CHs independently off the FWDL channel when complete.[2]

2. Update to the Distribute Firmware API to handle an additional end point type parameter.

3. New Firmware Delivery Notification in SD4.4.1 to be created and sent to DSP.

[2] While not part of this Modification's objectives, the FlexNet Protocol change has potential future applications for recovery of diagnostic data relating to the HAN, without increasing network bandwidth requirements. This provides potential for much greater insight into the 'last mile' at scale, should it be decided to develop this capability further. This would enable the Service Desk and other support functions to not only provide granular details of the status of the HAN FWDL to their devices but also add such functionality for any other critical services.

4. SDK, FlexNet protocol and RNI changes for logging triage (Service Management) metadata

The CSP North SM WAN Gateway Interface, SD4.4.1, will be impacted by changes required by the DSP.

3.5.3 Access Network – TK Basestation & Network Management System

As a result of increased demand on the network capacity, there will be a requirement to increase the radio channels within the overall CSP North solution from 16 channels to 32 channels. **Note** updated volumetrics information has been provided to all Service Providers to review all infrastructure-based statements.

The Network Management System (NMS) will also change to support the auto tuning of the Communications Hub, which will indicate the conclusion of the FWDL job, instigating a switch to the Communications Hub's normal channel. The Basestations will have to be updated to support the additional radio channels.

3.5.4 Communications Hub Manager

Comms Hub Manager (CHM) is the Device Manager which provides key functions such as providing default credentials to the CH manufacturer by interfacing with BT SMKI, sending CH Install Alerts to DSP, managing CH Firmware download and activation, refreshing credentials following the Install & Commission process, managing credentials during expiry and compromise and getting Unlock command from DSP for returned CH's, including supporting remote CH Diagnostic by Service Users.

This Modification impacts the CHM Console, Middleware and Reporting functions to support the following changes:

- The updated Distribute Firmware API requires an additional end point type mandatory parameter to specify the device type to which FWDL is initiated to, and thus requires changes to CH FWDL capability

- The CHM will provide functionality for Comms Hub Image Provisioning and Activation, support any Comms Hub alerts, and will also provide provisioning of HAN FWDL in test systems.

The CHM – CHF interface will be updated to define the following new messages:

- Alert 1: 0x8F89 - OTA Firmware Image Delivery to HAN Device – Failure (Generic Alert applicable for all HAN Devices)

- Alert 2: 0x8F8A - OTA Firmware Image Delivery to HAN Device – Success (Generic Alert applicable for all HAN Devices)

- Alert 3: 0x8F8B - Firmware Activation PPMID (Applicable for PPMID only)

The Firmware Distribution CH/CHM process flow is as follows.

Step	Event	Process
1	Reception of the Upgrade End Request Command	Communications Hub shall: set transferResponseCode to fileTransferSuccess if the transfer of the Manufacturer Image has completed successfully and process from step 2; and set transferResponseCode to fileTransferFailure if

		the transfer of the Manufacturer Image has failed and process from step 3;
2	[Success] Communications Hub shall create an Alert	Alert with the Alert Code field set to 0x8F8A Set firmwareVersion to the OTA Upgrade Image File version, Include the transferResponseCode from the previous step and process from step 4;
3	[Fail] Communications Hub shall create an Alert	Alert with the Alert Code field set to 0x8F89 Set firmwareVersion to the OTA Upgrade Image File version, Include the transferResponseCode from the previous step and process from step 4;
4	Communications Hub shall send the Alert created in the previous step	CHM to ingest alert 0x8F8A or 0x8F89

Table 5: CHF behaviour and process steps

In the case of the PPMID Firmware Image update, the final step in the process flow includes the PPMID activating the firmware and sending an Alert message with Alert Code 0x8F8B.

3.5.5 Business Support System

The Business Support System (BSS) provides the key functions such as Comms Hub Lifecycle Management that includes Forecast & Ordering, Delivery, Acceptance, Rejection, Installation, Return, Refurbishment and Disposal, maintains Comms Hub Logistical and Operational status, provides Postcode Coverage, supports Performance Measurement & Reporting, and Comms Hub Billing.

This Modification impacts the BSS Integration and Reporting functions to support the following changes and functionalities:

- Updated FW Download and SMWAN Gateway logs to support reporting, analysis and triage activities
- New log for newly supported Alerts to support reporting, analysis and triage activities
- Impact on infrastructure (compute, storage and licensing) due to increased volumes of firmware downloads and Alerts.

4 Impact on DCC Systems, Processes and People

This section describes the impact of SECMP0007 on DCC's Services and Interfaces that impact Users and/or Parties. These impact both solution options.

4.1 Technical Specifications

The legal text for all technical specification has been developed as part of the Working Group and SECAS-related activities for this Modification. The intention is that they will be baselined as part of the Modification Refinement process, and released to all parties when this Modification is approved for implementation to commence.

Notes on the applicability of the Zigbee OTA specifications and Smart Metering Technical Specifications are covered in Appendix C: Technical Specifications Changes.

4.1.1 SMETS and CHTS

SMETS and CHTS will be updated as part of this Modification.

Support for the Modifications changes would be mandated through the SMETS for all newly installed PPMIDs, and through the CHTS for installed Communications Hubs. The changes would result in new obligations on the DCC, and Suppliers would be required to demonstrate that they are able to support the sending of the new Service Request and receiving the Service Response and DCC Alerts by way of testing obligations. However, Suppliers would not be required to upgrade Firmware on PPMIDs, unless there were changes to the SEC or a SEC governance mandated upgrade.

4.1.2 DUIS, DUGIDS, MMC, GBCS, CHDS

There will be a new Service Request 11.4 Update PPMID Firmware for the purpose of distributing and activating the firmware image to the PPMIDs.

The existing SRV 11.2 Read Firmware Version will be extended to support PPMID device type.

Unlike the firmware upgrade mechanism for the other device types, there will not be a separate activation SRV for PPMID.

The proposed GBCS changes for this Modification introduces the following GBCS Use Cases:

- CS08 Read PPMID/HCALCS Firmware Version
- CS05c Distribute Firmware to PPMID
- CCS08 Firmware Transfer Alert

The Comms Hubs and PPMIDs will use the following Device Alert Codes to report the firmware distribution statuses.

- Alert 1: 0x8F89 - OTA Firmware Image Delivery to PPMID - Failure
- Alert 2: 0x8F8A - OTA Firmware Image Delivery to PPMID - Success
- Alert 3: 0x8F8B - Firmware Activation PPMID

DUGIDS will need to explain the behaviour of a new DCC Alerts introduced as part of this change. DUGIDS will also need to explain the changes to the behaviour of existing DCC Alerts due to the introduction of PPMID.

The DUIS and MMC schemas will need updates to support the new Service Request.

For the HCALCS solution, DUGIDS documentation will be updated to describe that SRV 11.1, SRV11.2 and SRV 11.3 will be used for HCALCS firmware update. Since this does not involve any changes to the input Service Request format or new GBCS Use Cases, the DUIS and MMC schemas do not require any changes.

The CH2 Communications Hub Detailed Specification (CHDS) will be updated as part of this Modification.

4.1.3 Transform

DSP Transform will need to implement the libraries for the GBCS Use Case CS08 (Read PPMID/HCALCS Firmware Version) and to parse the new Device Alerts.

Configuration updates will be applied to the Transform component to support the GBCS Use Cases for Read Firmware Version and Activate Firmware on HCALCS.

4.1.4 CPL

Implementation of this change will commence with the recording of a firmware hash against a PPMID device.

No change is expected to the structure of the CPL due to this Modification, but the permitted data types and validations may require updates.

4.2 Security

In terms of the DSP, there are no perceived security impacts, and there is no need for additional Penetration Testing or Protective Monitoring specific to this Modification. A penetration test might be required based on any other Modifications or Change Requests that make up a release.

The HCALCS update method would include security related effort for the CSP security certification bodies, to review the design and for full CPA certification.

4.3 Implementation Approach

Within the Smart Meter Implementation Programme (SMIP), the Implementation Approach is referred to as Transition to Operations (TTO).

This change will be implemented as part of a larger release. It is assumed that the activities required for TTO will be minimal following completion of contractual test phases. Some updated service procedures have been implemented and take part in some form of service role playing in advance of go live.

Any required environment uplifts will take place outside of business hours.

4.4 Application Support

The DSP Application Management Support team are responsible for the provision of application level support for the DSP. This Modification provides additional functionality that will be subject to support following its deployment to the Production environment, and it is expected that the added functionality and processing logic to existing SRVs will lead to the raising of additional incidents to cover for OTA firmware upgrades to include PPMIDs and HCALCS. As a result, DSP has made a conservative estimate that the change will result in five medium complexity calls that need to be assimilated, investigated, resolved and monitored per month over the support term.

The DSP team will need to be prepared to support the change from the day it goes into live operation. As such, the team must review the functional solution and its technical implementation. The team must understand any configurable options and develop procedures to support the implantation.

For the CSPs:

- The CSP Service Desks will require coordination for CH Specialists and will need to understand timings and frequency of downloads

- There is a requirement to plan and schedule such that the system can avoid Network conflicts and saturation when trying to push out CH firmware downloads at the same time

Specific **CSP South and Central** Service Management impacts from this Modification include the introduction of:

- New Service User facing functionality that is expected to result in modifications to incident scripts and introduce new incident scenarios that require triage

- New firmware image types whilst retaining the current Communication Hub firmware storage capacity, driving additional new edge cases related to delivering firmware images to HAN devices

Specific **CSP North** Service Management impacts include:

- Updated FW Download and SMWAN Gateway logs from RNI to CSP North support relating to reporting, analysis and triage activities.

- New log for newly supported Alerts from RNI

- Impact on infrastructure (compute, storage and licensing) due to increased volumes of FW downloads and Alerts.

- Modifications to the Incident Management process, Service Desk resourcing and related systems to support additional incidents relating to firmware update failures for PPMID and HCALCS devices. An Additional FTE allowance will be used only in relation to the triage of non-contractor related incidents which occurred as a result of firmware download attempts to PPMID or HCALCS.

- Implementation of monitoring for the new network Service Requests and device alerts.

- Development, integration and assurance activities to include firmware updates to PPMIDs and HCALCSs in monthly Performance Measure reporting. Includes set up and reporting of new exclusions.

4.5 Infrastructure Impact

This Modification does not materially increase processing, data storage or data exchange within the DSP solution. No specific infrastructure requirements or changes have been identified, but there will be an increase in Service Request volumes as a result of this Modification.

The Modification will lead to additional data processing at the DSP. One instance of the new firmware upgrade SR message will trigger a lot more processing effort than typical SRs, since one containing 50,000 device IDs would trigger validation of all of them, the need to generate files, interact with both CSPs and the sending of approximately 100,000 alerts. Assuming the messages are billed appropriately, any additional hardware required would be handled through normal capacity planning processes.

Note that the aggregated impact of many such changes to the DSP solution will ultimately result in a reduction of the available headroom assumed as part of the original DSP agreement. There may be a need to raise a Change Request against the DCC to cover additional compute and storage capabilities to cover this aggregated impact in the future.

For both CSPs, there is a quoted need to increase the capacity, rather the capability of their networks. In both cases, the activity to execute the Production Environment capacity expansion requirement shall be conducted under the business-as usual operational change process, but not before the date that CSP completes the migration of the Production Environment to the technically refreshed platform.

CSP South and Central will provide a quote to provision additional hardware required uplift for the Production Infrastructure in order to meet the firmware upgrade demand once the Modification is Live.

CSP North note the Smart Metering Wide Area radio Access Network (SMWAN) uses dedicated multicast/broadcast radio channels and is technically the same as the mechanism to provide firmware updates to Communications Hubs and ESME/GSME. The use of this mechanism, whilst being efficient, will result in additional traffic to be carried by SMWAN radio channels. This impact assessment includes estimates on the price related to this additional traffic, the additional channels required and the functionality to support these new channels.

Initially, the FWDL system was designed to support small numbers of large multi-cast FWDL Jobs containing upwards of tens of thousands of devices in each Job. Currently, the FWDL system has been expanded from one to three FWDL channels, at ASML cost, to support the usage of Service Users, i.e. a very large numbers of FWDL Jobs containing small numbers of devices, often a single device. *With no change* to Service User behaviour, it is anticipated that further FWDL channels will be required in the system as the numbers of Communication Hubs increase and to support FWDL Jobs introduced by new types of devices.

Note DCC have reviewed this assumption, and will prepare DUIS Guidance notes for changes to procedures for handling all HAN device firmware updates as described in section 4.13 following.

Further information regarding the CSP North infrastructure augmentation is given in Appendix E.

4.6 Non Functional Impacts

DSP does not expect that there will be a material impact on system performance as a result of this change. DSP will validate this with some specific regression tests during the implementation phase.

There will be no change to the system resilience solution as a result of this change.

There will be no change to the Disaster Recovery solution or BCDR procedures as a result of this change.

4.7 Safety Impact

There are indirect but foreseeable systems safety risks associated with the management of device firmware updates. Functional failures could adversely impact communications with a device or render the device inoperable and impact the supply of energy to consumers. Such failures might include:

- device not added to the Central Products List
- device's firmware version not maintained in the Smart Meter Inventory
- failure to validate firmware update request
- firmware is not activated when scheduled
- failure to alert Supplier on failure
- failure of Supplier to re-request update following a delivery failure
- Supplier attempts to update firmware on incompatible device

These types of risk are subject to software Failure Modes, Effects and Criticality Assessment (FMECA) as part of the DSP System Hazard Analysis Report, based on the DSP Use Case level functional design, with any risks to data confidentiality, integrity and availability also addressed by the DSP information security programme.

No new types of hardware infrastructure are required to be procured or installed as a result of this change and, therefore, there is no foreseeable health and safety impact.

4.8 Request Management

The DSP Request Management will implement a mechanism to track the progress of the firmware update process at a Device Level. The DSP will block a firmware update request for a device if there is already one in progress and will return the list of such devices as part of the synchronous response. If the firmware update request for a Device stays in the ‘In Progress’ status longer than a defined duration the Device will be released from tracking so that new requests can be accepted.

The status records held by the firmware update tracking mechanism are expected to be available only for a short-term (up to a week). The housekeeping of these records will be managed by way of configurable parameters.

Request Management needs to amend the processing of all the affected Service Requests and implement the newly introduced Service Request. It also needs to implement the scenarios related to the new Alerts.

Request management needs to validate the firmware image as with existing firmware upgrades (e.g. active according to the CPL and the supplied hash matches the CPL entry) and the list of device IDs (e.g. the sending Service User is the responsible supplier for the device).

Request management will need to look up the appropriate CHF in order to indicate to the CSP to which CHF the request will be directed. For devices which pass validation, Request Management will form a request to send over the new CSP SMWAN Gateway interfaces for the purpose (similar to existing ones), segregated by CSP.

When DSP receives a Device Alert from a PPMID indicating a successful activation of firmware, DSP will update the SMI and notify all the Responsible Suppliers using the DCC Alert N39.

An Electricity Import Supplier (EIS) or Gas Import Supplier (GIS) responsible for the PPMID will be allowed to send a firmware update using the SRV 11.4.

The processing of SRV11.1, SRV11.2 and SRV11.3 will be updated to support HCALCS. The existing validations for the ESME will be applicable for the HCALCS as well. CSP SMWAN Interface documentation will be updated to describe the use of existing ESME/GSME Firmware Update interface for HCALCS.

4.9 Data Management and Data Model

This change does not materially increase processing, data storage or data exchange within the DSP solution, as such, this change on its own does not warrant the procurement of additional infrastructure.

The Data Model will need changes to support the firmware update tracking.

In addition, there is a need to add mappings for the new GBCS Use Cases, for the alerts between the DUIS version and the SRV, and to the GBCS version against the Use Case where applicable.

There will be a new web service interface for SSMI to reset the firmware delivery status of a Device.

Reference data updates will be applied to Data Management related to SRV11.1, SRV11.2, SRV11.3 and SRV11.4.

4.10 Anomaly Detection

No changes are required within the Anomaly Detection component.

Anomaly Detection volume thresholds will need to be applied for SR11.4.

4.11 SSI

SSI will feature a ‘Firmware Update Status’ screen to allow the Service Users to view the last recorded status of a firmware update request against a single device.

SSMI will also feature the ‘Firmware Update Status’ screen, with an additional functionality to reset the status of a device. The data presented in the new SSI/SSMI screens will be applicable to all device types and will be served by the Reporting Database instance and the data synchronisation would take place at an interval of about 15 minutes.

The SSI report RSAT_004 Firmware Activations Service Request Report will be updated to include HCALCS.

4.12 ESI Inventory Extract

No changes are required to Enterprise Systems Interface (ESI).

4.13 SEC Changes and Usage Limitation

Although not directly impacting the Service Providers, DCC have requested that some form of obligation be added to the SEC or in guidance to users to limit the initial take up and general usage of the firmware download channels to "reasonable". While this is not something that has been in place before, it is something that will have a significant impact on additional infrastructure and resources allocated by the Service Providers to firmware downloads. The changes should include:

- DUIS Guidance to Service Users for all firmware downloads that after an initial Service Request that they should wait until they get an alert for a successful or discarded transfer before they resend or send a subsequent SR.

- The Guidance will show that after sending a firmware image, the supplier should wait for an activation alert or failure message from the PPMID before re-sending the image update.

- A managed schedule should be agreed between the DCC and the appropriate parties.

- The guidance should include a statement that firmware updates must be limited to a gap of at least 5 days between attempts.

DCC does not believe Anomaly Detection Thresholds (ADTs) would be an appropriate or valid method of limiting the usage**.**

5 Implementation Timescales

Implementation of this change is assumed to follow a waterfall methodology. For the purposes of this FIA, it is assumed that this change will be implemented alongside other Modifications and change requests.

5.1 Approach

Details of a release plan including all the Service Providers with potentially different release dates and content will be negotiated and evaluated separately, led by DCC. The timelines in the rest of this section are indicative only for each Service Provider, and are based on a standalone Modification release for comparison only.

The **DSP** timeline reflects a start around December 2020 and a subsequent completion in November 2021.

Generic November 2021 Release Phases	**Start**	**End**
DCC confirmation of required November 2021 scope in agreement with SECAS	December 2020	
PIT Phase	January 2021	May 2021
SIT Phase (limited to functional changes only)	June 2021	August 2021
UIT Phase (limited to functional changes only)	September 2021	October 2021
Transition to Operations and Go Live	October 2021	November 2021

Table 6: Potential DSP Release Phases and Dates

Note that the implementation lifecycle is expected to fit into this schedule, but the timescales shown as part of the Price Breakdown run over a shorter elapsed period for the purposes of costing. As additional CRs are applied to the release, timescales are expected to expand to fill the schedule set out above.

In order to achieve this timescale and implement changes alongside other releases such as SMETS1 and the DSP aspect of the Central Switching Programme it may be necessary to align some activities with those programmes of work. Where required, changes will be implemented using feature switches to enable functionality to be only switched on for testing when it is required.

The **CSP South and Central** proposed delivery timeline indicates that after the DCC approval to start project mobilisation, it would take approximately 14 months to exit the PIT phase for this CR, with SIT planned for a duration of 3 months and UIT planned for 2 months. As part of the proposed delivery plan supporting the IA, CSP South and Central anticipates that it would take in total 20 months (approx.) prior to UIT exit as shown in the following plan on a page.

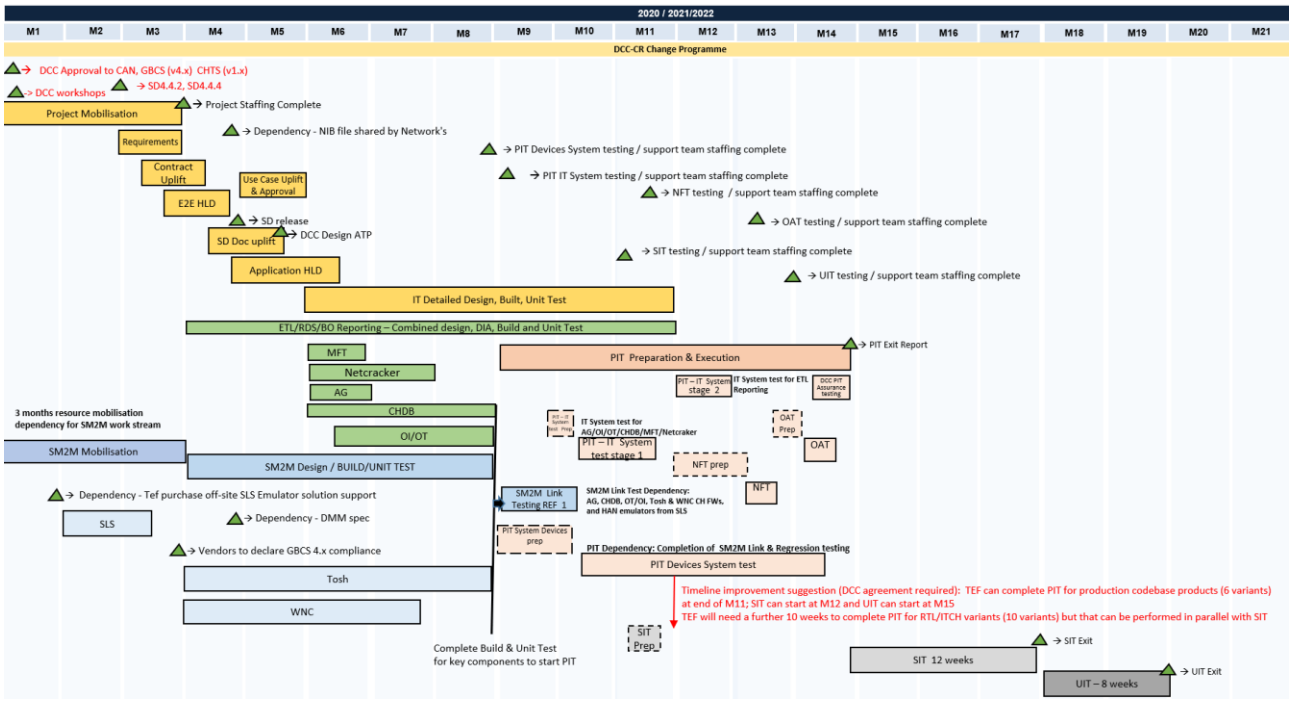

Figure 6: CSP South and Central Indicative Plan

This plan includes the following stages:

- A period of two (2) months to undertake in-depth analysis work to construct technical requirements and high-level design
- A period of three (3) to five (5) months of detailed design across different work streams.
- A period of 5 months to build and unit test Smart m2m changes
- A period of 8-9 months to build & unit test all IT (back office) components
- A period of 1 month required to uplift and link test the PIT B environment for PIT system testing
- A period of 5 month required to deliver the Communications Hub firmware before being made available for PIT testing.
- CSP South and Central PIT testing with the Production codebase Communication Hub variants will take approx.7 weeks while testing with non-Production codebase variants will take approx. 10 weeks to complete. All other phases of PIT i.e. PIT IT System testing and NFT can be executed in parallel and all major defects uncovered during PIT testing can be fixed within the PIT window.
- Around 2 months of Non-Functional Testing which includes performance testing of the new functionality on existing service demand.

Indicative PIT entry and PIT exit, SIT entry and SIT exit dates as shown in the indicative delivery plan.

The **CSP North** proposed delivery timeline indicates that after the DCC approval to start project mobilisation, it would take approximately 14 months to exit the PIT phase for this CR, with SIT planned for a duration of 3 months and UIT planned for 2 months. As part of the proposed delivery plan supporting the IA, CSP South and Central anticipates that it would take in total 20 months (approx.) prior to UIT exit as shown in the following plan on a page.

- A period of two (2) months to undertake in-depth analysis work to construct technical requirements and high-level design

- A period of three (3) to five (5) months of mobilisation, requirement analysis and detailed design across different work streams.
- A period of 3 months to build and unit test the application and consequential Comms Hub firmware changes
- A separate workstream to build and unit test all back office components
- CSP North PIT and SIT will requires two cycles of PIT and two cycles of SIT testing. The combined PIT testing would take approximately 18 weeks to complete, with SIT taking approximately 20 weeks.
- These timelines do not include environment uplift and preparation.

The WAN and Production environment expansion are two separate programmes of work as follows:

- WAN Capacity Expansion Development and Coding, 12.5 months
- WAN Capacity Expansion Deploy, test and go Live, 10 weeks
- Production Environment infrastructure Expansion, 6 months

The **System Integrator** will be responsible for managing and leading the SIT and UIT phases of testing.

6 Testing Considerations

This Full Impact Assessment includes the cost to develop, fully test and deliver this SEC Modification as a standalone change. Costs were submitted by the Service Providers on a per-Application Phase basis, including Development and Build, PIT, SIT, UIT, Implementation (sometimes referred to as TTO), and Application Support.

PIT System testing may, at the discretion of the SP, consist of two cycles of testing of the new functionality delivered by this Modification, plus two cycles of regression testing. A repeat of a subset of PIT System test cases will be conducted for DCC Test Assurance witnessing.

Testing costs for SIT and UIT have been built on the following assumptions:

- Go live in November 2021 (although this will have no impact on costs)
- SIT testing 12 weeks
- UIT testing 8 weeks
- 10 test sets per Comms Hub type. This means 10 for CSP North (5 Single Band CH, 5 Dual Band CH), 20 for CSP South and Central (same split per band, but two meter manufacturers).
- Risk-based regression testing

Note that CSP activities include “Production Uplift” or “environment uplift” which covers the CSPs getting their backend systems up to scratch so that they support the new way of working for SEC MOD 7. As you say the new versions of firmware would be developed but based on experience would be initial cuts and would take a number of iterations before genuine production ready versions can be accepted.

6.1 Pre-Integration Testing (PIT)

For the DSP, System Testing, Performance Testing and the Factory Acceptance Testing (FAT) phase will operate as a single phase of PIT activity with a single drop.

For the CSPs, the Communications Hub change testing will be limited to PIT testing of the new functionality outlined in this Modification as well as PIT regression testing.

Note that DCC are currently leading an initiative to introduce "real" devices in the testing regime, and this is expected to have a positive impact on testing durations and cost.

6.1.1 The CSP South and Central PIT Approach

The CSP South and Central PIT Approach will include:

- Design, build and system test modifications to the CSP South and Central solution to support the delivery of the functionality for the PPMID and HCALCS firmware service within the PIT environment
- Execution of NFT of the uplifted solution in accordance with a defined non-functional test approach. Note this has not been included in the CSP South and Central plan at this stage.
- Provision of a fixed number of ITCH variant Communication Hubs to the meter Test Stub provider to support the meter Test Stub provider develop any meter emulator updates to support PIT testing

Note CSP South and Central indicated that testing with real devices in PIT is currently out of scope, as well as any uplift or use of NXP based emulator in PIT.

Due to the DUIS changes as part of this Modification, existing Test Stubs would be uplifted for to be able to PIT test the firmware upgrade to PPMIDS and HCALCS. PIT device testing will validate using the Test Stubs with added capability to test firmware OTA over the HAN to PPMIDS and HCALCS.

Updated versions of the wired ITCH variant Communication Hubs will be provided to the Test Stub provider for use in developing and testing the uplifted Test Stub as follows.

	Changes
Modified	Modification to test stubs to support new GBCS alert definition; Modification to the test stubs to include the additional attributes including additional value in the enumeration for error code; Modification to the PIT test stubs required to validate the new API developed regarding the status of the firmware download status notifications over SMWAN to the DSP.

The following System Test activities are required for PIT:

- Modification to existing test scripts to support updates to functionality within the CSP solution
- To support assurance of the new functionality within the PIT environment
- Regression testing of existing System Test scripts
- Documentation of the testing artefacts as per the existing PIT approach

The system test activities described in the following table:

Use Case	Title	Activity	Description
UC4.01	Meter firmware distribution.	Test Script Uplift & Regression	Updated functionality test case to include the new functionality being introduced as part of this CR and also confirm that meter firmware operation has not been impacted by software changes to the Communications Hub
UC4.02	Communications Hub firmware distribution and activation.	Test Script Regression	Test case to confirm that CH firmware operation has not been impacted by software changes to the Communications Hub
UC8.01	Input Billing Data (Auto)	Test script regression	Test to prove the Netcracker Billing interface for firmware downloads being extended to additional HAN devices.
UC8.0	Create DCC Bills and Invoices	Test script regression	Test to validate the Netcracker Billing process and validation of invoices generated as part of tests.

UC12.08	Test Messages	Test script regression	Regression of the test case to confirm that the test message processing has not been impacted by software changes to the Communications Hub
UC13.01	GBCS commands, responses and alerts	Test script uplift and regression	Regression of the test case to confirm that the test message processing has not been impacted by software changes to the Communications Hub
UC13.05	Power Alerts	Test script regression	Regression of test case to confirm that power outage alert transmission and processing has not been impacted by software changes to the Communications Hub.
UC14.01	Smart m2m DMM management	Test script regression	Regression of test case to confirm that device management and monitoring firmware operation has not been impacted by software changes to the Communications Hub.
UC14.02	DSP Diagnostics.	Test script regression	Regression of test case to confirm that device management and monitoring firmware operation has not been impacted by software changes to the Communications Hub.
UC23.01	Communications Hub Installation	Test script regression	Regression of test case to confirm that installation and CSP commissioning and processing has not been impacted by software changes to the Communications Hub.

Table 7: CSP South and Central System Test Activities

A defined non-functional test cycle on the functionality in this Modification will include:

- Testing approach and scope
- testing may occur during the Release PIT timeframe however this is not on the critical path for exit from PIT;
- Test volumes will reflect a scaled view of service demand with some consideration for new functionality within this demand

6.1.2 CSP North PIT Approach

It is assumed that all testing in PIT will be performed with meter emulators and real PPMIDs and HCALCS and that both CH variants (SBCH and DBCH) will be tested in a near parallel approach.

The upgraded applications RNI, CHM and BSS will be regression tested prior to commencing CH testing. NMS and TK testing will be performed separately, treated as a maintenance release (environment A path first).

CH firmware changes will be verified primarily in two variants, SBCH and DBCH, and the full regression test suite will be shared between both CH firmware variants, with regression targeted on modified firmware sections.

The PIT Test Approach will be to test DBCH and SBCH in near parallel when execution commences and DBCH –F will be verified following DBCH completion, as per the Plan on a Page above.

The PIT Test Team will perform Targeted regression in DBCH – F, SBCH ITCH, DBCH ITCH, W-ITCH firmware and in the CHM application, and the Test Team will verify all changes for the Modification in the CH FW, RNI, BSS and CHM firmware in parallel.

Note that CSP North will implement a multi-phase PIT testing approach, essentially with a cycle sequence of PIT -> SIT -> PIT > SIT, because of the large number of defects that are not detected in PIT that only become apparent in SIT. This clearly has a significant impact on testing costs and durations.

Also it should be noted that CSP North currently only has the capability to execute two sets of Comms Hub firmware PIT testing in parallel. If PIT testing of other changes are not complete, and this capability is not increased, before the Modification release is received from their supplier, this Modification's SBCH PIT testing may have to be prioritised over DBCH PIT testing.

6.2 System Integration Testing (SIT)

CSP test lab support will be required to permit the System Integrator (SI) to execute the SI regression test pack for System Integration Testing. The same support will provide triage and defect resolution activities during any SI managed integrated testing.

6.2.1 DSP System Integration Testing

Tests described in this section are specific to this change and independent of any release-based testing.

New scenarios and scripts will be created as follows:

Firmware update for PPMID	Create new scenario and script for new SRV11.4 – Update PPMID Firmware (which should be very similar to the existing SRV 11.1 scenarios and scripts). The scenario and script will include the relevant DCC Alerts indicating the progress of the firmware through the different stages of distribution, update and activation processing, including N59, N61, N62 and N39. This SRV will share its general attributes and validation checks with SRV11.1. The firmware will be distributed OTA and the PPMID will activate the firmware update. Update the SRV11.2 existing scenario and scripts to include support for Firmware Reads and Updates for PPMID.
Firmware update for HCALCS	Will follow the existing procedure currently used for ESME and GSME: • Update existing SRV11.1 scenario and script to include the relevant DCC Alerts indicating the progress of the firmware through the different

	stages of distribution and update processing. DCC Alerts include N59, N61 and N62. • Update existing scenarios and scripts for the following SRVs to include support for Firmware Updates for HCALCS: o SRV 11.1 Update Firmware; o SRV 11.2 Read Firmware Version; o SRV 11.3 Activate Firmware. • Update scenario and script for SSI Report RSAT 004 Firmware Activation Report to include HCALCS.
Negative Scenarios of SRV11.1 for HCALCS and for SRV11.4 for PPMID Firmware	Four existing negative DCC Alert Test Scenarios and scripts to be updated to include PPMID and HCALCS devices for the following DCC Alerts: N18, N19, N20 and N22. SAT entry for N19 defines entry for each rejected device. • Three new negative DCC Alert scenarios and scripts to be created and executed for N49, N50 and N51 covering PPMIDs and HCALCS when executing SRV11.2. • New Negative scenario for Hash on CPL for PPMID and HCALCS to verify if Firmware Update can be applied or not.
Applicable to ESME, GSME, HCALCS and PPMID	Two new negative DCC Alert scenarios and scripts to be created for the following new DCC Alerts to be tested for ESME, GSME, HCALCS and PPMID: o N60: Delivery to Comms Hub failed o N62: Failed to deliver firmware image to device o N62: Firmware image rejected/overwritten at Comms Hub Creation of one new negative scenario and script for ESME, GSME, CHF, HCALCS and PPMID where another Firmware Update is in progress. New scenario and SSI script for users to access a 'Firmware Update Status' screen to allow the Service Users to view the last recorded status of a firmware update request against a single device. New scenario and SSMI script for users to access a 'Firmware Update Status' screen, to view the last recorded status of a firmware update with additional functionality to reset the firmware status of a device. An update to the Business Scenario for Change of Mode and Firmware: o Additional Alerts to be added o Additional scenario for PPMIDs o Update to Interaction diagram required

SIT Execution Approach	The SIT execution approach will be: 1. Validation performed by CSPs and within HAN with DCC Alert Codes generated will be tested against all three CHFs including SBCH and DBCH 2. The validation performed by DSP with DCC Alert Codes generated to be tested against a single CHF 3. The Firmware Update, Read and Activation of Firmware updates for PPMID will be tested against all three CHFs including SBCH and DBCH 4. The Firmware Update, Read and Activation for HCALCS will be performed against all three CHFs including SBCH and DBCH
SIT Execution	**Happy Path Test Execution** Execute SRV 11.4 and SRV11.2; Update and Read Firmware for PPMID, verifying DCC Alert Codes N59, N61, N62 and N39 through the three CHFs; Execute SRV11.1, SRV11.2 and SRV11.3 Update and Read Firmware for ESME, GSME and HCALCS through the three CHFs, verifying DCC Alerts N59, N61 and N62. Verify users can access new SSI and SSMI screens “Firmware Status Update” to query the status of firmware updates and reset firmware status. Generate SSI Report RSAT 004 Firmware Activation Report to verify HCALCS are included. **Negative Scenarios Test Execution** Negative DCC Alert Codes N49, N50 and N51 to be executed for PPMID and HCALCS are validated by DSP. Only to be executed against single CHF (SRV11.2). The three DCC Alert Codes will be spread across the three CHFs. Negative DCC Alert Codes N18, N19, N20 and N22 are validated by CSPs therefore, tested for PPMID and HCALCS against all three CHFs. Negative DCC Alert Codes N60 and N62 are validated by CSP/HAN area therefore, to be tested for ESME, GSME, HCALCS and PPMID against all three CHFs; Negative validation tests for ESME, GSME, CHF, HCALCS and PPMID where another Firmware Update is in progress (spread across the three CHFs) Negative test for hash on CPL. Verify the hash for PPMID and HCALCS to determine if firmware update can be applied

6.2.2 CSP South and Central SIT

There will be provision of an agreed amount of CSP test lab support including:

- Support the SI for the testing of scenarios within SIT

- Support the SI for the installation of the provided meter equipment within the CSP Test Lab to support the testing with physical devices.

- Provide 20 existing SIT Communication Hub sets (10 Toshiba, 10 WNC) during the SIT execution period for a period of 12 weeks; CSP South and Central will re-allocate its existing SIT Communication Hub (20) to support the SIT. Charges do include the required associated equipment (debug boards, ZigBee sniffers).

CSP South and Central assumes that the following devices will be made available by the DCC-L for testing in SIT:

- 2.4GHz and sub-GHz ESME and GSME compatible with a specified version of GBCS

- PPMID and HCALCS devices operating on 2.4GHz and sub-GHz from two separate manufacturers with firmware revisions comparable to those available in Production at the time of SIT entry

- PPMID and HCALCS devices operating on 2.4GHz and sub-GHz from two separate manufacturers with compliance to a specified version of GBCS

- DCC provided device emulators for that operate as a specified version of GBCS compliant PPMID and HCALCS devices on 2.4GHz and sub-GHz

  CSP South and Central will support the SI during System Integration Testing (SIT) including defect triage and resolution Including the following System Test activities:

  - Modification to the existing test scripts to support updates to the functionality within the CSP solution

  - Device set-up

  - Execution of the tests with support from the DSP

  - Test execution monitoring as required

  - Collection of logs

6.2.3 CSP North SIT

PIT and SIT will be performed using Debug and Non-debug CH variants.

Other activities are essentially the same as those for CSP South and Central.

6.2.4 User Integration Testing (UIT)

UIT will comprise the preparation and execution stages for the relevant UIT environment, and will take place following completion of PIT and SIT.

The overall UIT project window is scheduled to run for approximately eight calendar weeks and will cover three separate testing elements:

- Firmware Tracking (2 weeks)
- PPMID Firmware Updates using Zigbee OTA Delivery (3 weeks)
- HCALCS Firmware Updates using the GBCS Commands (3 weeks)

Real ESME, GSME, and PPMID devices will be used. HCALCS emulators will be used.

Specific UIT test activities will include the following:

- Planning and preparation of the tests
- Testing of the OTA process for ESME and GMSE devices on meter sets covering all three CHF manufacturers, both single and dual band, to ensure that tracking of the firmware process is working as expected in the UIT environment
- Testing of both the OTA process for PPMID and separately HCALCS devices on meter sets covering all three CHF manufacturers, both SBCH and DBCH, to ensure:
    - Tracking of the firmware process is working as expected in UIT
    - Firmware is updated on the devices and device alerts are received
    - DSP returns details of the firmware for the applicable device in response to SR8.2
    - (PPMID only) The CHF returns the current firmware version of the PPMID in response to SR11.2 when sent to the applicable device
- Preparing, presenting and agreeing a test completion report on the testing results
- Providing a summary of defects raised during testing

6.2.5 Support for Integration Testing

DSP Effort will be required from the Implementation and Triage teams to support the additional testing. This consists of issue investigation, resolution and deployments to the environments.

7 Service Operation and Transition

This section contains information about the transition to a live environment.

7.1 PPMID Numbers and Functionality at Go Live

Once implemented this Modification will ensure that a PPMID-related SR11.2 would send the firmware activation Alert directly to the Supplier. The Alert would be directed to the Access Control Broker (ACB) on the Device. The ACB, using registration data, would then validate that the Supplier the Alert is addressed to is the Supplier for the Device. However, no existing devices could support this functionality, namely the redirected firmware alert, until after a successful PPMID firmware update had been applied by this Modification, because until then, existing devices do not send any Firmware Activation Alerts today and they would need a SECMP0007 driven firmware update in order to do that.

If an existing, deployed PPMID supports the standard Zigbee OTA process today then there's no reason why the (new) Comms Hub can't use the Zigbee OTA process to get the new firmware onto the PPMID.

Note that SECAS have issued a Request for Information to get an idea of the number of Transition to Operations (TTO) Approach

CSP South and Central will provide costs and durations to deploy the CSP changes in Production.

CSP North costs have been provided. Note the switch of the Communication Hub manufacturing line to the new firmware version shall be decided under business-as-usual process.

8 Costs and Charges

8.1 Application Development and Support Costs

This section indicates the total quote for each application development stage for this modification. Note these costs assume a standalone release of just this SEC Modification without any other Modifications or Change Requests, which may not be truly reflective of what the test costs or programme duration might look like. A calculation of those costs will be carried out when the contents of the future Release is determined through a "Grouping CR" also referred to as a "Release CR".

£ (million)	Design and Build	PIT	SIT	UIT	TTO	App. Support	SP Total
Phase Total	9.4m	4.2m	3.8m	1.6m	0.7m	1.1m	20.8m

Design	The production of detailed System and Service designs to deliver all new requirements.
Build	The development of the designed Systems and Services to create a solution (e.g. code, systems, or products) that can be tested and implemented. It includes Unit Testing (also referred to as System Testing), Performance Testing and Factory Acceptance Testing by the Service Provider or supplier.
Pre-Integration Testing (PIT)	Each Service Provider tests its own solution to agreed standards in isolation of other Service Providers. This is assured by DCC. This phase also includes regression testing across all Comms Hub products
Systems Integration Testing (SIT)	The PIT-complete solutions are brought together and tested as an integrated solution, ensuring all SP solutions align and operate as an end-to-end solution. The System Integrator is responsible for leading this phase with the SPs offering testing support services.
User Integration Testing (UIT)	Users are provided with an opportunity to run a range of pre-specified tests in relation to the relevant change. The DCC is responsible for leading this phase with the SPs offering testing support services.
Implementation to Live (TTO)	The solution is implemented into production environments and ready for use by Users as part of a live service.
Application Support	Any costs associated with supporting the new functionality.

8.2 Impact on Contracts and Schedules

Schedules will require modification for the Service Providees to reflect the changes under this Modification. The contract schedules will be updated as part of a CAN which combines schedules updates from other relevant Modifications

8.2.1 DSP

Expected contract schedules to be amended include:

- Schedule 2.1 – Review to determine whether updates are required as a result of the new functional requirements outlined within this Full Impact Assessment
- Schedule 6.1 - Inclusion of three new milestones referencing completion of PIT,SIT and go live for this change
- Schedule 7.1 – Update to include a payment against the Schedule 6.1 milestones and the Operational charge uplift

There will be no updates to SLAs as a result of this change.

8.2.2 CSP South and Central

CSP South and Central has asked for Introduction of the new Service exemptions in the PM2 Category 1 Firmware Payload Service Measure. **DCC** are reviewing this and all the following requests.

- Review SMWAN transaction billing approach with the DCC, due to the potential increase in the number of SMWAN transactions. The billing process will aim to reduce the complexity and operational cost whilst permitting a charge for increased SMWAN transactions.
- Review of the PM2 Category 1 Firmware Payload success rate including:
    - Revision to the PM2 Target Service Level and Minimum Service Level
    - Introduction of the relief on the application of Service Credits and associated escalation mechanisms for the early period of implementation
    - Extension to the current 4-day Distribute Firmware window. DCC do not believe this should be adopted.

8.2.3 CSP North

CSP North has indicated the following changes:

- Schedule 2.1 – to reflect additional requirements related to the delivery of new firmware image types
- Schedule 2.2 - Modification to the existing PM2 Category 1 Firmware Payload Service Measure
- Schedule 3 - to include the DCC responsibilities i.e. to monitor and confirm that minimum PPMID endpoints i.e. 2.5M PPMID firmware requests has been achieved in Production, ensure that there are process controls in place in the upstream DCC

systems i.e. service request throttling, manage backlog /pent up demand in a controlled manner, availability of physical devices in SIT.

- Schedule 6.1 – to include delivery Milestones in relation to this CR
- Schedule 7.1 – to reflect any payments under this Change Request and to include payment milestones
- Schedule 11 – to reflect an uplift to the CH specifications
- Schedule 12 – to reflect the uplifted technical specification versions (such as GBCS and CHTS)

Note The DCC is reviewing the above changes and charges.

Appendix A: Glossary

The table below provides definitions of the acronyms and terms used in this document.

ACB	Access Control Broker	ITCH	Instrumented Test Comms Hub
API	Application Programming Interface	ITSF	Intention to Submit Final Tender
BEIS	Department for Business, Energy & Industrial Strategy	Manufacturer image	a full firmware Image or one part of a firmware Image as defined in the GBCS.
BSS	Business Support System	MMC	Message Mapping Catalogue
CAN	Contract Amendment Note	NFT	Non-Functional Testing
CH, Comms Hub	Communications Hub	NMS	Network Management System
CHDS	CH2 Communications Hub Detailed Specification	OTA	Over The Air
CHF	Comms Hub Function	OTA Upgrade Image	the concatenation of the OTA Header and the Upgrade Image that is equal to or less than 750KB. This is defined in GBCS and DUIS
CHTS	Communication Hubs Technical Specification	PIA	Preliminary Impact Assessment
CHM	Comms Hub Manager	PIT	Pre-Integration Testing
CoS	Change of Supplier	PM2	Performance Measurement 2
CPA	Commercial Product Assurance	PPMID	PrePayment Meter user Interface Device
CPL	Central Products List	RNI	Regional Network Interface
CR, CRP	Change Request, BEIS Change Request	ROM	Rough Order of Magnitude
CSP	Communication Service Provider	SAT	Service Audit Trail
CSP N, CSP S&C	CSP North, CSP South and Central	SEC	Smart Energy Code
DCC	Data Communications Company	SECAS	Smart Energy Code Administrator and Secretariat
DSP	Data Service Provider	SI	System Integrator
DUGIDS	DCC User Gateway Interface Design Specification	SIT	Systems Integration Testing
DUIS	DCC User Interface Specification	SMETS	Smart Metering Equipment Technical Specification
DSMS	DCC Service Management System	SMI	Smart Metering Inventory
DUGIDS	DCC User Gateway Interface Design Specification	SMIP	Smart Meter Implementation Programme
EIS	Electricity Import Supplier	SMKI	Smart Meter Key Infrastructure
ES	Electricity Supplier	SMWAN	Smart Meter Wide Area Network
ESI	Enterprise Systems Interface	SNMP	Simple Network Management

			Protocol
ESME	Electricity Smart Metering Equipment	SP	Service Provider
FAT	[DSP] Factory Acceptance Testing	SR	Service Request
FIA	Full Impact Assessment	SRV	Service Request Variant
firmware	A package of firmware which can be made up of a single or several Manufacturer Images. This term will NOT be capitalised.	SSC	Security Sub-Committee
FWDL	firmware download (delivery)	SSMI	Self Service Management Interface
GBCS	Great Britain Companion Specification	SSI	Self Service Inventory
GFI	GBCS Integration Test for Industry	TK	Transceiver Kit (CSP North)
GPF	Gas Proxy Function	TSIRS	Technical Specification Issue Resolution Sub-Group
GS	Gas Supplier	TTO	Transition to Operations
GSME	Gas Smart Metering Equipment	UIT	User Integration Testing
HAN	Home Area Network	Upgrade Image	The Manufacturer Image concatenated with additional information as defined in the GBCS.
HCALCS	HAN Connected Auxiliary Load Control Switch	WAN	Wide Area Network
IHD	In Home Display	W-ITCH	Wireless ITCH
		ZSE	Zigbee Smart Energy

Appendix B: Updating PPMID Firmware with Multiple Manufacturer Images

The process set out in this section is for the benefit of Manufacturers and Suppliers. This process does not propose any changes to the way in which the DCC currently manage Manufacturer Images. The DCC simply treats each Image as it would with firmware made up of a singular Manufacturer Image. There is no additional validation for the DCC to carry out compared with firmware made up of a singular Image.

The expectation is that PPMID firmware is typically below 750KB. However, it may be possible for PPMID firmware to exceed this in the future. This section illustrates how to activate firmware comprised of multiple OTA Upgrade Images that are less than or equal 750KB in size.

The operating firmware version in this example is 0x10, which is reflected in the CPL entry example in Table 8 below.

A PPMID is to be updated to firmware version 0x20. This requires two Images to be sent to the PPMID, to provide all the changed firmware/configuration data required for firmware version 0x20.

The Manufacturer has split this upgrade data into two Images:

- Image 0x15: this contains the first part of the upgrade data and contains Manufacturer instructions for the PPMID to only store this first part on activation
- Image 0x20: this contains the second part of the upgrade data and contains Manufacturer instructions for the PPMID to check that Image 0x15 has already been activated. Activating this Image causes the functionality of the PPMID to be upgraded to firmware version 0x20.

The new CPL entry will look like this.

Manufacturer identifier	Model identifier	Hardware version	Hardware version revision	Firmware version	Hash
FF: FE	AA:BB	01	01	00:00:00:10	(Hash of Image 10)
FF: FE	AA:BB	01	01	00:00:00:15	(Hash of Image 15)
FF: FE	AA:BB	01	01	00:00:00:20	(Hash of Image 20)

Table 8: Example New CPL Entry for firmware comprised of multiple Manufacturer Images

To upgrade firmware for a PPMID, the Supplier will follow the following process:

1. Having undertaken the necessary checks, the Supplier will create a ‘Send PPMID Firmware’ Service Request to distribute Image 0x15.

2. The DCC will distribute Image 0x15 to the Communications Hub and the PPMID will download the Image. The PPMID will then send a Device Alert containing its firmware version. Note that this value will still be 0x10 (in line with the Technical Specification Issue Resolution Sub-Group (TSIRS) decision). Therefore, the Device Alert will only indicate delivery of the Image. It will NOT indicate that the PPMID has successfully validated the Image. The DCC will update the SMI if

the firmware version has changed and forward the Device Alert to the Responsible Suppliers recorded to receive the Alert.

3. On receipt of the Device Alert from the DCC containing the PPMID's firmware version, the sending Supplier will send Image 0x20. If this Device Alert was not received the Supplier can only resend Image 0x15 (since the TSIRS decision means, there is no mechanisms to discover if the PPMID had that Image).

4. The DCC will distribute Image 0x20 to the Communications Hub. When the PPMID has downloaded the Image, the PPMID will send a Device Alert containing its firmware version. Note that this value will, if activation was successful, now be 0x20 (in line with the TSIRS decision). Therefore, this Device Alert will indicate delivery of the Image and that the PPMID successfully activated the Image. The DCC will update the SMI if the firmware version has changed and forward the Device Alert to the Responsible Suppliers recorded to receive the Alert.

5. The Supplier can only resend Image 0x20 if this Device Alert is not received. However, the Supplier should verify this first by sending SR11.2 to the PPMID. The DCC will then update the SMI if the firmware version has changed and forward the Device Response for SR11.2 to the Supplier.

The result is that the PPMID (excluding where the OTA firmware upgrade process cannot be completed e.g. where there is no Wider Area Network (WAN) connectivity), will be operating firmware version 0x20.

The above process is explained in detail in Figure 7 and Figure 8, Process for upgrading PPMID firmware comprised of multiple Manufacturer Images, Part 2 (parts 1 and 2 respectively) below.

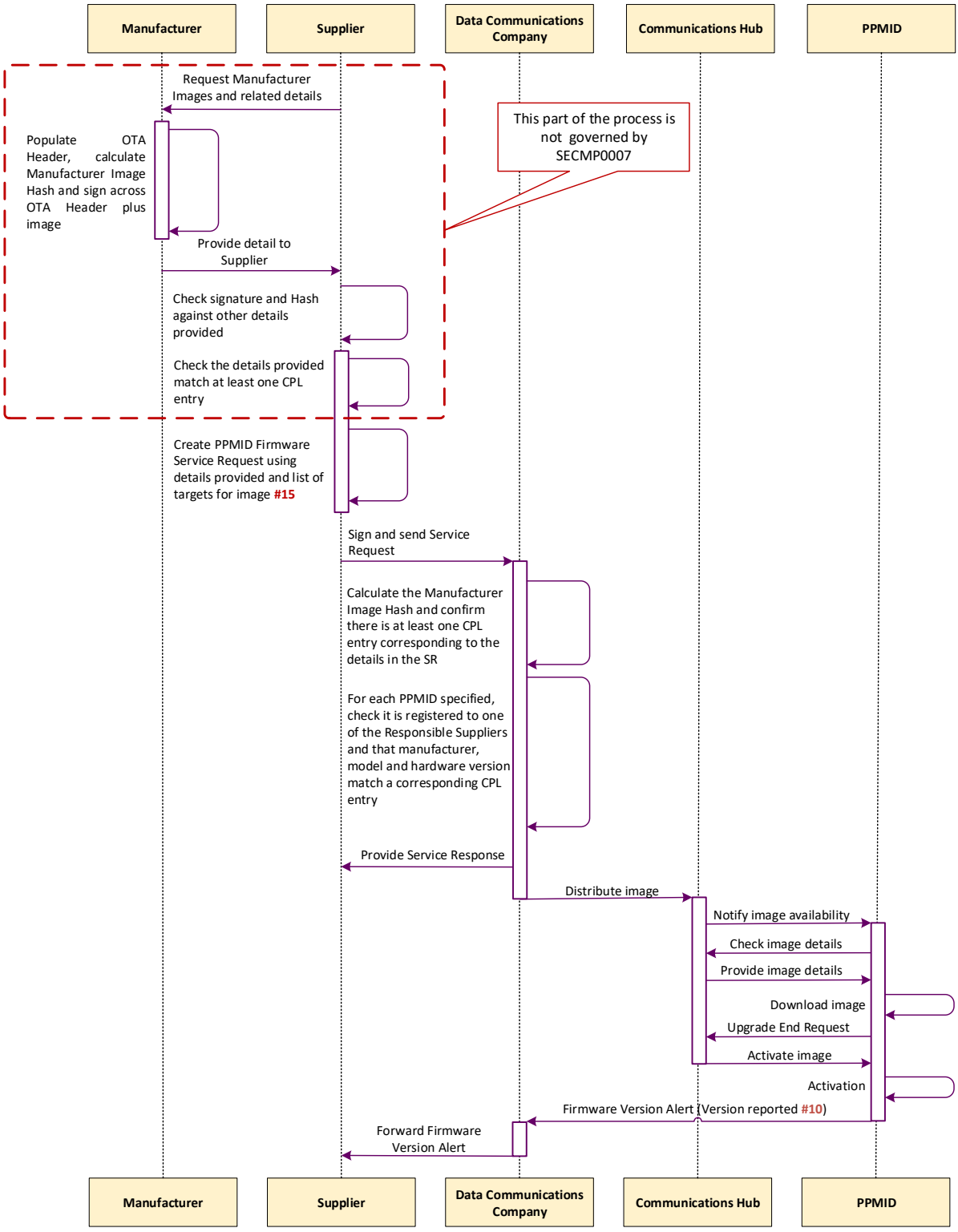

Figure 7: Process for upgrading PPMID firmware comprised of multiple Manufacturer Images, Part 1

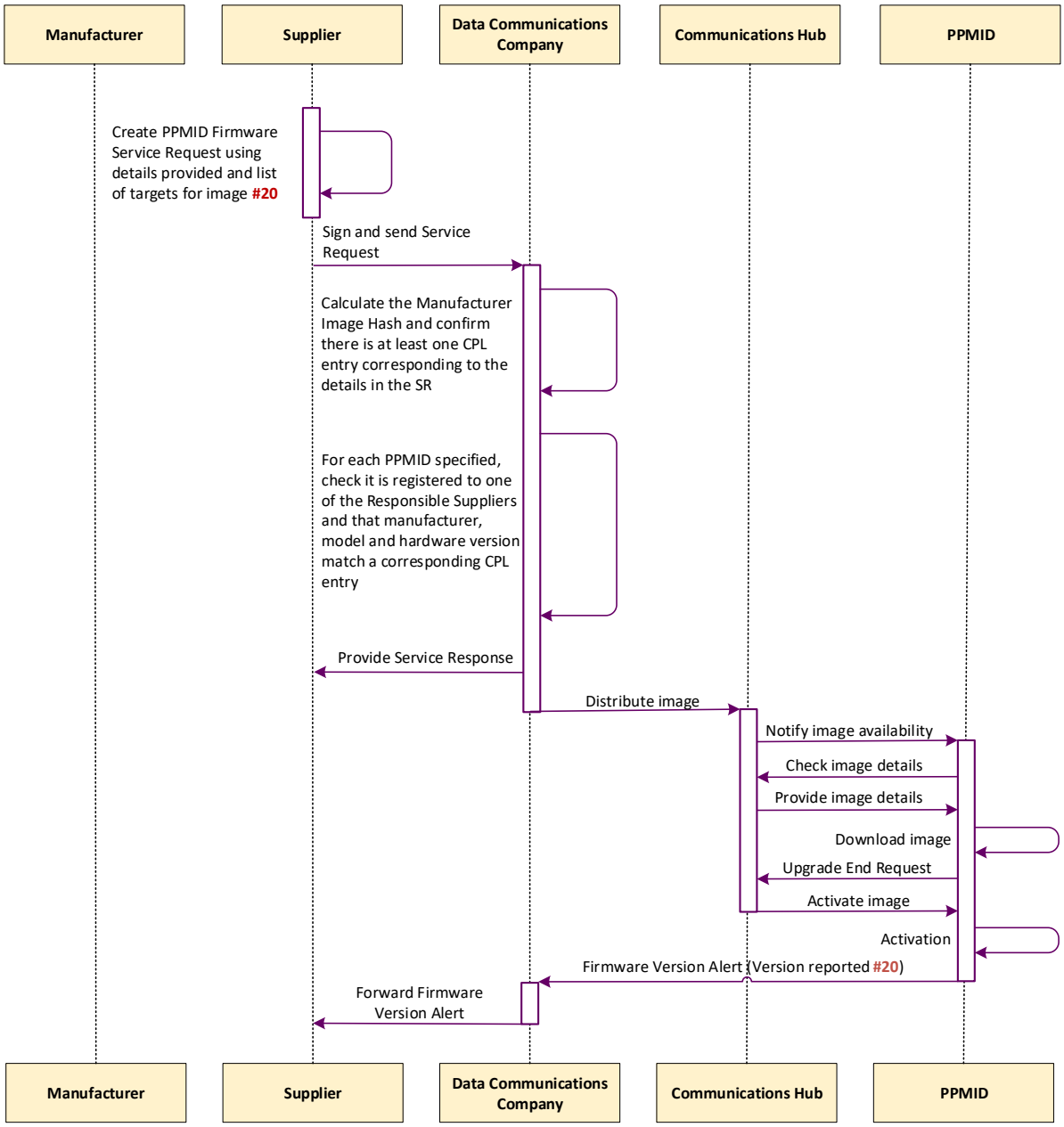

Figure 8: Process for upgrading PPMID firmware comprised of multiple Manufacturer Images, Part 2

Appendix C: Technical Specifications Changes

In the case of PPMID firmware updates, the GBCS, SMETS and CHTS technical specifications, as noted in section 4.1, mandate the use of ZigBee specifications but do not repeat the details of the ZigBee specifications. There are a few exceptions where functionality differs from the ZigBee specification. The manufacturer specific ZigBee implementation may differ between chipset vendors and device manufacturers and this must be considered by manufacturers when designing devices based on the ZigBee specifications.

With regards to the ZigBee OTA specifications GBCS doesn't deviate from the ZigBee standard except for the activation command where for ESME and GSME no activation is allowed by the server (CH) and for PPMID and HCALCS only immediate activation by the server (CH) is allowed.

The ZigBee OTA specifications allow for different timings e.g. for clients (PPMID) to send the Upgrade End Request and the server (CH) must be able to handle these different timings and the possibly different content of the Upgrade End Request. The ZigBee OTA specifications are clear about the communication between the server (CH) and the client (device). To be on the safe side only mandated attributes and commands should be relied upon; optional commands and attributes may or may not work and this needs to be addressed in the server firmware.

Currently the CH must be able to handle the OTA upgrade for different ESME makes and models and up to four ESMEs in parallel. The OTA upgrade to the PPMID and HCALCS follows the exact same set of specifications at the ZigBee level as the ESME OTA upgrade with the exception of the activation at the end of a successful transfer (see above).

Appendix D: Design Decisions

This section contains design decisions agreed by the DCC and Working Group during the development of this SEC modification.

July 2018, First Preliminary Assessment sent to Working Group, scope extended to HCALCS

February 2019, DCC and Service Provider review of requirements with two solutions proposed:

1. Original Approach, No GBCS Changes

2. Extend Proven OTA Firmware Method; create a type 1 IHD and extending PPMID's, HCALCS, and the new type 1 IHD to support firmware distribution in a manner that would be similar to ESME firmware distribution and activation

July 2019, Working Group agrees to two solutions:

Option 1; for PPMIDs and IHDs, ZigBee Over-The-Air (OTA) delivery mechanism

Option 2; for HCALCS, OTA firmware update procedure used by Electricity Smart Metering Equipment (ESME) and Gas Smart Metering Equipment (GSME)

Expense of adding PPMIDs and IHDs to CPL was cited as a major cost, and the reason for not using Option 2 for PPMIDs and IHDs.

September 2019, DCC and SP Design Review 1

Rather than use new DUIS Service Requests 11.4 Download Firmware and 11.5 Read Firmware specifically for PPMIDs and IHDs, SPs recommended extending SR11.1 to support SMETS2 PPMIDs and IHDs.

New API to the CSPs for Distribute Firmware to PPMID/IHDs. Although the Modification suggested a new API from DSP to CSP for distribution of Firmware to PPMID or IHD, SPs can see no reason why a new API is required. The content to be sent between DSP and CSP is exactly the same as the current API for ESME/GSME firmware and therefore it is proposed that the existing DSP -> CSP API is used. To ensure that Service Users get feedback of the firmware download to the Comms Hubs, there needs to be a notification from the CSP's central systems back to the DSP through a custom API, with settings of Success and Fail. This notification will then trigger a new DCC Alert to be sent to the Service User informing them of the status of the download to the Comms Hub. It is suggested that this notification should apply to all firmware download activities, not just PPMID/IHD but also ESME, GSME, and HCALCS. This is more than current SECMP0007 scope, but would help users.

Notifications of delivery to PPMID/IHD: In order to track delivery of Firmware from the Comms Hub to the PPMID/IHD, further notifications are needed from the Comms Hub. This gives information of Activations and confirmation that it is Activated (as this needs to be logged). Using the Zigbee OTA the Comms Hub issues an "Upgrade End Request", on behalf of the Comms Hub as a mandated command on the Zigbee cluster with translation in the CHF.

Map SR11.2 to new GBCS Use Case with new GBCS Use Case required for the CHF, allowing Service Users to be able to read the firmware version with a Service Request.

HCALCS to implement the GBCS Use Cases 11.1., 11.2, and 11.3, using the Use Case for activation in the same way as an ESME. Assume the ESME buffer gets overwritten so there is no need for an additional buffer.

September 2019, DCC and SP Design Review 2

Activate Firmware Date and Time: In cases where the PPMID or IHD updates are sent to the Comms Hub, the activation date and time isn't set as currently SR11.1 doesn't contain the date and time of when a firmware activation is required. Suggestion is that rather than updating 11.1 with a date and time value, we assume the firmware implementation should be immediate. We noted that storing updates which would be activated at a later date or time would take up both network and Comms Hub capacity, and potentially would add risk to the stored image. SPs suggested removing option completely to reduce testing, SSC mandated that the maximum delay for activation will be 30 days.

Business Rules for Firmware Updates on Comms Hub Storage:

- If the firmware is downloaded, then the images should be offered to all related ESMEs on the SM HAN.
- If some of the ESMEs on the SM HAN are still updating, then the ESME buffer space must not be overwritten until all downloads are complete.

DSP will add functionality for validation of the firmware image, tracking of progress including the notification of a valid download to the Comms Hub, and to reject any potential downloads when an update is already in place. As Service Users don't have visibility of the firmware management, there is a proposal to make this functionality available for all types of device. This is based on discussions with the DAB. The CSP systems would have this information in a report, and there would be an added call in the DSP to retrieve the relevant information. Tracking and other pieces are included in SECMP0007.

Firmware scheduling and rules for rejection if a pre-existing download is still active:

- If a CSP receives a firmware request for an end device (i.e. ESME, HCALC, PPMID/IHD) that targets a Comms Hub, where a prior firmware download request has already been received and is being actioned within the SLA window, then the CSP can reject the second firmware request, and it will not count as a failure from a Service Measure perspective. It will be deemed an allowable exception. Feedback from SECAS: "Existing Firmware Update functionality uses the Extended Unique Identifier (EUI) to identify the individual target device, updates to the PPMID/EUI use the same concept; in this context “offering” the image to all related ESMEs doesn’t seem to fit in." However, if the CSP can complete the download for the first image and still complete the second download within the four day SLA period, then it should be allowed to schedule it.
- If the firmware download is rejected, the CSP should send a Firmware Download Delivery alert, with the status code set to an error code indicating that an existing download was

already in place. The view of the working group was that ESME and GSME firmware updates have priority, to the extent that it is allowed to purge a PPMID/IHD update from the CH memory. Such a mechanism is desirable since PPMID/IHD may be removed by the consumer at any time (even when the transfer from the CH to the PPMID/IHD has been started) and pending upgrade images could block the memory in the CH.

The transfer of ESME and GSME images to the CH has been estimated to take about half a day. The transfer of the image from the CH to an ESME should be reasonably fast to free up the memory in the CH to support PPMID/IHD/HCALCS images in a short time; the GSME image will remain much longer in the CH memory and may take at least one day to transfer over the HAN

October 2019, requirement for new SR 11.4 relating to PPMIDs:

The Security Sub-Committee (SSC) have stated that Service Requests to update firmware for PPMIDs must be subject to the same Anomaly Detection Threshold (ADT) procedures as ESME and GSME. However, PPMIDs must be counted and reported separately to enable anomalies with the potential to affect energy supply to be detected separately from those for PPMIDs.

The SSC also stated that Service Requests to update firmware for HCALCS should be subject to the same ADT procedures as ESME and GSME since similar risks to the supply of energy apply to HCALCS.

December 2019, streamlining review with Working Group, Service Providers, and BEIS results in reduced scope.

1. In-Home Displays (IHDs): remove IHDs from scope
2. Local firmware updates: allow local firmware updates to PPMIDs only
3. Communications Hub memory block rules: restrict PPMID and HCALCS firmware Images to GSME block of Comms Hub
4. Comms Hub SLA: remove the requirement for a two-day SLA for an Image to stay on the Comms Hub. The Image will remain until it is overwritten
5. Comms Hub logging of updates: remove the requirement for the Comms Hub to log the progress of up to 15 Devices in the Upgrade Image list
6. Firmware updates over 750KB: any firmware updates over 750KB in size must be split into separate Images. Each Image can be no larger than 750KB in size. The Service User must then request distribution of each Image separately.
7. Future-dated Update Activation: limit firmware updates to immediate activation only.
8. Service Request for PPMID firmware updates: new SR to distribute and activate PPMID firmware, to facilitate separate Anomaly Detection Thresholds (ADTs) required for PPMIDs.
9. Alerts and notifications remain unchanged
10. Dual Supplier Scenarios: in a dual Supplier scenario, both Responsible Suppliers shall be able carry out firmware updates to PPMIDs and HCALCS
11. The PPMID generates the success/failure Alert to the DCC. This removes the following Communications Hub requirements:
    - to record the activation date-time plus [X] minutes
    - to subsequently read the firmware version on the Device

June 2020, GBCS Change to reflect new requirements:

> The Communications Hub shall make the GSME image available for fourteen (14) days and, after this period, replace the GSME image with an image for the PPMID / HCALCS, if one becomes available. If the transfer of a GSME image to the GSME is in process, the Communications Hub shall only replace this GSME image with an image for the PPMID / HCALCS once the GSME image transfer has completed.
>
> The Communications Hub shall make the PPMID / HCALCS image available for fourteen (14) days unless a new PPMID / HCALCS / GSME image is available.
>
> If a PPMID / HCALCS / GSME Upgrade Image is discarded or replaced prior to having been successfully transported over the HAN, the Communications Hub shall send an Alert for each target Device Entity Identifier associated with the Upgrade Image File with the Alert Code 0x8F89 as specified in Section 11.7 by setting firmwareVersion to the Upgrade Image File version and transferResponseCode to imageDiscarded.

Note 1: there is no requirement specifying the time for the new image to live on Comms Hub in the GBCS legal drafting.

Note 2: This is a divergence from the design proposal previously discussed with DCC. Analysis of the previous design proposal has highlighted a constraint with the way memory protection is implemented that means the use of RAM as an alternative storage area for OTA images is no longer considered a viable option.

Appendix E: CSP North Hardware Augmentation Details

The capacity of the CSP North firmware download solution is very high. Each base station transceiver kit (TK) currently supports 3 FWDL channels that together will support 3 FWDL jobs running concurrently. There are approximately 1,350 macro TKs in the radio network, each supporting 3 FWDL channels. The system will accept up to 400 FWDL Jobs simultaneously, each of which can contain 10k devices and be spread across a large number of TKs in the network. The success of the FWDL process in a large capacity network is dependent upon the efficient creation of large FWDL jobs in relatively small geographic areas that then utilise only a small number of TKs and subsequently a small number of FWDL channel resources at the TKs. Currently there is almost no management of FWDL jobs by Service Users and as a result there have been occasions where the system has become overloaded and FWDL jobs have either been rejected by the system or timed out due to lack of channel resources at a TK.

The system is currently set up with 3 FWDL channels per TK, which can be increased to 6. Six FWDL channels per TK is the current system maximum, without further extensive changes being made to the system operation.

This channel expansion is currently available to provide more FWDL capacity as Communications Hub numbers increase and assuming Service Users continue to submit FWDL jobs with limited management processes in place. However, there is a limit to the FWDL system capacity available and at it has been stated by CSP North that some FWDL management process is required in order to support the FWDL requirements to all devices, once numbers scale to multiple millions of Communications Hubs. For example, several Service Users have been submitting large numbers of FWDL jobs containing only a single device to be upgraded. Whilst this is sometimes unavoidable, it should be done by exception and not as standard practice.

The proposal within this Modification is to increase the FWDL channels to the maximum of 6 per TK in order to support the additional FWDL jobs that will be generated for the additional HAN devices. All FWDL jobs to any device type will be transmitted on these FWDL channels and therefore it should be noted that jobs to PPMIDS and HCALCS will potentially use FWDL capacity that would otherwise have been available as spare capacity for CH, ESME and GSME FWDL jobs. Therefore, it is important to also note that in the longer term, in order to support the additional FWDL capacity, a process must be put in place that allows Service Users to manage FWDL job in a more efficient manner. Without a change in Service User behaviour in creating FWDL jobs, there will potentially be some capacity bottlenecks in the FWDL system as Comms Hub numbers scale to multiple millions.

There are three significant changes required to support the FWDL channel expansion:

- New FWDL radio channels allocated to base stations to support additional traffic from new devices

- Modification to functionality within the Network Management System (NMS) CH tuning process to allow for dynamic automated updates to the Communications Hub default embedded channel tables to allow all Communications Hubs to be able to operate on newly defined FWDL channels.

- Modification to the Transceiver Kit (TK) firmware to increase the number of radio channels that the TK is programmed to transmit on from 16 to a new upper limit of 32 channels.

New Radio Channels required to support Firmware Downloads to HAN Devices

The number of dedicated broadcast radio channels allocated to support FWDL Jobs at each macro TK (radio cell) shall be increased by 3 new channels from 3 to 6. After this upgrade, each TK will be able to support firmware upgrades to devices that are contained in 6 separate FWDL Jobs simultaneously. The process to upgrade all Production Environment Base Station Transceiver Kits (TK) with the new channel plan requires a period of up to 4 weeks, as each individual base station must be upgraded individually in a serial process.

The current FWDL Broadcast channels support all FW upgrades to ESME, GSME and Communications Hubs (CH). The FWDL Jobs to upgrade CHs use only a very small proportion of the available FWDL channel resource because these jobs can be managed in large groups very efficiently by ASML.

The majority of the current available FWDL channel resource is allocated to FWDL jobs for ESME and GSME. These FWDL Jobs are created by the Service Users and tend to be many Jobs daily, typically containing small numbers of devices. It is the expectation that this type of usage of the FWDL system will continue once HAN devices are included until a process for optimisation of FWDL Job management is agreed with Service Users. The estimates for the numbers of PPMIDs and HCALCS to be included in the sizing for this CR leads to an expectation that the number of device upgrades and subsequently the number of FWDL Jobs submitted to the system will approximately double compared to the original system design. **Note these and the following estimates have been reviewed and further estimates are expected.**

Increasing the number of FWDL channels per TK from the current 3 to the system maximum of 6 will provide a 100% increase in FWDL capacity providing the maximum FWDL capacity at each TK.

Once 6 FWDL channels are available at each TK, they will be available to all FWDL Jobs irrespective of device type and therefore the system will be more resilient to large peaks in FWDL Job numbers issued by Service Users across all device types.

4.1.3.4. NMS functionality

The Communications Hub contains a default channel table, which details the frequencies of all channels being used in the current channel plan including all FWDL and GBCS Messaging channels, plus the three uplink control channels L2Ack, RTS and CH Alert.

When 3 additional FWDL channels are introduced into the system at each TK, Communications Hubs will need to be informed of the frequencies of these new FWDL channels in order to be able to operate on them as part of the FWDL OTA process. This will be done by means of a new automated process within the NMS, which will send messages to the Communications Hubs informing them of the new FWDL channels. This updating of the CH channel table can currently be done manually but a new automated process will be required in the NMS to update Communications Hubs on a larger scale.

Transceiver Kit (TK) transmit channels

Transceivers at each base station are required to transmit on multiple channels and currently are set up to be able to transmit on up to 16 different channels. Within the current channel plan, TKs may transmit on:

- Admin channel
- 1-4 Primary messaging channels
- 3 FWDL channels
- Time Sync messages on up 11 secondary channels

When these additional FWDL channels are introduced into the system, an expansion in functionality will be required to enable the TKs to transmit on an increased number of channels.

This new functionality requires a change request to Sensus on several aspects of the TK functionality.