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

DP237

'Management of Emergency Firmware Updates'

Modification Report

Version 0.1

14 March 2023

Corporate member of Plain English Campaign
Committed to clearer communication
592

About this document

This document is a draft Modification Report. It currently sets out the background, issue, and progression timetable for this modification, along with any relevant discussions, views and conclusions. This document will be updated as this modification progresses.

Contents

1. Summary 3
2. Issue 3
3. Assessment of the proposal 5

Appendix 1: Progression timetable 6

Appendix 2: Glossary 6

Contact

If you have any questions on this modification, please contact:

Kev Duddy

020 3574 8863

kev.duddy@gemserv.com

1. Summary

This proposal has been raised by David Rollason from the Data Communications Company (DCC).

Over-the-air (OTA) firmware upgrades are applied to deliver improvements or fix bugs within Devices. There may be instances where a very large number of Devices are impacted and could require an emergency fix. The DCC would be responsible for deploying firmware updates to Communications Hubs, and Suppliers would be responsible for deploying firmware updates to other Devices, using the DCC system.

Whilst there are emergency processes to follow in the event of security incidents, there are none for operational incidents. There is currently no reference within the Smart Energy Code (SEC) to allow the DCC to manage User traffic to shorten the timeframe required to deploy a firmware upgrade to all affected Devices.

2. Issue

What are the current arrangements?

Firmware upgrades

OTA firmware upgrades are applied when manufacturers make improvements to functionality or features within the Device software. A new firmware version may also be introduced to fix any defects that have previously been identified on a Device. Whilst it is the Device manufacturer that develops the new firmware upgrade, they are not responsible for the rollout of that firmware to their Devices. The DCC is responsible for the rollout of new firmware upgrades to Smart Metering Equipment Technical Specification (SMETS) 2 Communications Hubs. Suppliers are responsible for the rollout of new firmware upgrades to all other SMETS1 and SMETS2 Devices.

The DCC System is used for delivering and activating firmware upgrades. In the case of Electricity Smart Metering Equipment (ESME), Gas Smart Metering Equipment (GSME), Standalone Auxiliary Proportional Controller (SAPC) and Home Area Network (HAN) Connected Auxiliary Load Control Switches (HCALCS), the Supplier will send Service Request (SR) 11.1 ‘Update Firmware’ followed by SRV 11.3 ‘Activate Firmware’. Suppliers can send a single SR 11.1 to up to 50,000 Devices, but each Device must receive an individual SR 11.3 to activate the firmware on the Device. Prepayment Meter Interface Devices (PPMIDs) can be upgraded using a single SR 11.4 ‘Update PPMID Firmware’ for each affected Device.

Communications Hubs firmware is managed, delivered and activated by the DCC without the need for Service Requests or Supplier involvement. The processes for this is set out in the DCC Comms Hub Firmware Management Overview.

Security incidents

There is a possibility where a security defect may be identified on a particular Device that could require an immediate response. This could affect a great number of Devices and require an emergency mass deployment of firmware upgrades to ensure security and stability of supply or DCC Services.

The Joint Industry Cyber Security Incident Management Plan (JICSIMP) contains the broad cross-industry processes that should be followed when identifying and managing a security incident. In the event of a security incident, the Security Sub-Committee (SSC) will convene the Smart Metering Incident Response Team (SMIRT) through which a coordinated industry response or communication strategy can be agreed and implemented to address security incidents or vulnerabilities.

The need for a large-scale rollout of firmware to mitigate against passive or active security vulnerabilities in a Device model(s) is a planned-for scenario outlined in the JICSIMP, which is regularly reviewed and tested by the SSC.

What is the issue?

While there is a process for emergency firmware upgrades, this event could be on an extremely large scale and impact a high percentage of Smart Meter installations. In these scenarios the average network traffic could disrupt or slow down a firmware upgrade rollout. This would mean a longer time might be required before security or stability issues are resolved. Additionally, a high volume of firmware deployment could impact other network traffic.

There could also be scenarios on a very large scale whereby Smart Meter installations are affected by a defect that is not security related but might affect an operational service impacting many consumers.

To urgently deploy such firmware upgrades on a mass scale may require suspension or restriction of the business-as-usual services (e.g. Service Requests) in all or part to facilitate such a rollout in a much shorter time period than usual.

SEC Section H10 'Business Continuity' provides for Emergency Suspension of Services where a User's actions put the DCC system at risk of compromise. However, where the User needs to undertake urgent action, such as mass deployment of firmware, it would not be appropriate for that User to see their Services Suspended. An agreement on how to manage these scenarios should be considered and a defined process is required to support this.

What is the impact this is having?

Whilst this situation has not occurred, if there was a need to process emergency firmware for a very large number of Devices the security of supply or stability of systems could be at risk. There is a risk that emergency firmware isn't deployed at the pace required, or DCC systems are put into a state of compromise.

Impact on consumers

If a security defect is discovered that requires a firmware upgrade on a mass scale, the risk from that defect exists until the firmware upgrade is completed. The longer it takes to deliver that upgrade, the bigger the risk of a consumer being adversely impacted.

Similarly, if an Operational defect occurs that requires a firmware upgrade on a mass scale to correct the consumer could be affected up to the point of resolution. The longer the timeframe, the bigger the risk of being impacted.

The specific impact to consumers depends on the nature of the issue identified that needs fixing.

3. Assessment of the proposal

Areas for assessment

What constitutes 'mass deployment'?

There would need to be a threshold number of Devices impacted to constitute a 'mass deployment' and enable any counter measures to be deployed. This will need to be drawn out during the Refinement Process.

Do existing processes cover these requirements?

The existing processes developed for security incidents could be amended or re-used to develop appropriate processes to also cover Operational scenarios. However, this is currently enacted by the SSC. Any solution will need to consider if it should also be responsible for the same process where an incident is not security related.

There is currently no detail within the SEC that provides clarity to Parties on what the DCC can or cannot do to maintain the integrity of the system within an Operational based scenario.

Could there be a situation that constitutes an emergency mass deployment of firmware upgrades to SMETS2 Devices, other than Communications Hubs?

Each Smart installation at a premises will have a Communications Hub, however there are many different Device Manufacturers with many different products and firmware versions on those products. Analysis will be needed to understand whether any single Device Model has sufficient numbers that if a defect developed it would be classified as requiring emergency mass deployment.

Sub-Committee input

The Smart Energy Code Administrator and Secretariat (SECAS) will engage with the Chairs from the Operations Group (OPSG), the Technical Architecture and Business Architecture Sub-Committee (TABASC), the SSC and the Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA) to confirm what input is required from these forums. SECAS believes the following Sub-Committees will need to provide the following input to this modification:

Sub-Committee input	
Sub-Committee	**Input sought**
OPSG	Input on the issue and solution
SMKI PMA	Input on the issue and solution
SSC	Input on the issue and solution
TABASC	If the modification requires a solution that impacts the DCC Systems then TABASC input will be required.

Appendix 1: Progression timetable

This modification was raised 14 March 2023. SECAS will present the proposal to the Change Sub-Committee (CSC) for initial comment on 21 March 2023

Timetable	
Event/Action	**Date**
Draft Proposal raised	14 Mar 2023
Presented to CSC for initial comment	21 Mar 2023
Modification discussed with Sub-Committees	*Apr 2023*
Analysis on volumes per Device Model	*Apr 2023*
CSC converts Draft Proposal to Modification Proposal	*16 May 2023*

Italics denote planned events that could be subject to change

Appendix 2: Glossary

This table lists all the acronyms used in this document and the full term they are an abbreviation for.

Glossary	
Acronym	**Full term**
CSC	Change Sub-Committee
DCC	Data Communications Company
ESME	Electricity Smart Metering Equipment
GSME	Gas Smart Metering Equipment
HAN	Home Area Network
HCALCS	HAN Connected Auxiliary Load Control Switches
JICSIMP	Joint Industry Cyber Security Incident Management Plan
OPSG	Operations Group
OTA	Over-the-air
PPMID	Prepayment Meter Interface Devices
SAPC	Standalone Auxiliary Proportional Controller
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SMETS	Smart Metering Equipment Technical Specification
SMIRT	Smart Metering Incident Response Team
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SR	Service Request
SSC	Security Sub-Committee
TABASC	Technical Architecture and Business Architecture Sub-Committee