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.

DP102 'Power Outage Alerts triggered by an OTA firmware upgrade'

Problem statement – version 0.1

About this document

This document provides a summary of this Draft Proposal, including the issue or problem identified, the impacts this is having, and the context of this issue within the Smart Energy Code (SEC).

Proposer

This Draft Proposal has been raised by Matthew Alexander from Scottish and Southern Electricity Networks (SSEN).

What is the issue or problem identified?

What are Power Outage Alerts used for?

Power Outage Alerts (POA) are intended to identify when the incoming power supply from an Electricity Network Party to a customer's premise fails for a period greater than three minutes. Such POAs are used by Electricity Network Parties to improve customer service by becoming aware of power outages sooner than relying on the customer to phone in, and to develop a faster more complete view of the premises affected and hence enable them to restore supply to affected customer more efficiently and more quickly.

In order to achieve this, an Electricity Network Party needs to be confident that the POAs it receives are genuine and actually relate to supply interruptions to customers' premise.

What is the issue?

Experience has shown that implementing an Over The Air (OTA) firmware updates on some Electricity Smart Metering Equipment (ESMEs) generates a POA. This is because when some ESMEs activate a new firmware version it results in an interruption of the power supply to the Communications Hub (CH) (power to the CH is supplied by the ESME). If the power supply for the CH is interrupted for more than three minutes then the CH must send a POA (the AD1 Alert).

The Data Communications Company (DCC) then sends the AD1 Alert to the relevant Electricity Network Parties (ENP), who can't tell whether there is a real issue with the power to the premises or whether it was just a firmware upgrade to the ESME. As ENPs need to respond to each POA, a POA initiated by an OTA firmware update will cause an Electricity Network Party to put in place systems to check every POA to establish if it relates to a genuine power outage.

This issue was previously highlighted in industry forums and resolved by current ESME manufacturers agreeing that all future OTA firmware updates would be designed so as not to initiate a POA event (the ESME must not cut the CH power supply for three or more minutes during a firmware upgrade to prevent the CH from sending the AD1).

OTA firmware upgrades have been required to implement this change – however this agreement should be seen as being an interim solution until an enduring obligation is implemented through this modification. A new ESME manufacturer may be unaware or not comply with such an agreement.

Alongside this, there are still a set of ESMEs, approximately 500,000, that will continue to initiate a POA when a OTA firmware update is implemented. This issue cannot be resolved retrospectively for those 500,000 ESMEs already installed – these devices will continue to generate a POA on OTA firmware updates for the duration of their life. Ultimately these 500,000 ESMEs would need to be replaced to resolve the problem. During this time, there is not a solution that can stop POAs from being forwarded to the relevant Electricity Network Party unnecessarily.

In summary there are two issues:

1. There is no obligation in the SEC to require an OTA firmware update not to generate a POA.
2. There is no means of identifying or supressing erroneous POAs associated with an OTA firmware update from the 500,000 ESMEs in service where this issue can't be addressed.

How does this issue relate to the SEC?

The Proposer has stated that there will need to be amendments to the Smart Metering Equipment Technical Specifications (SMETS) (SEC Schedule 9) and the GB Companion Specification (GBCS), (SEC Schedule 8). At the moment there is no specific text in the device specifications (SMETS or GBCS) prohibiting a POA from being issued during an OTA firmware upgrade. Nor is there a mechanism to supress POAs from being generated incorrectly when an OTA firmware update is processed by a device that cannot be modified to inhibit their creation.

What is the impact this is having?

As DNOs need to respond to each POA, the issue of a POA initiated by an OTA will require a DNO to put in place systems to check every POA to establish if it relates to a genuine power outage. This could require the DNO to develop and implement systems that would automatically check the energisation status of each meter from which POA is received to confirm that the POA is genuine, or in the worst case, send a member of staff to site to investigate the reported POA.

What is the impact of doing nothing?

There are two significant impacts if this issue is not addressed:

- Electricity Network Parties will either need to check the energisation status of each meter from which POA is received, or
- Electricity Network Parties will need to send a member of staff to site to investigate.

Both these options will result in the Electricity Network Party incurring additional costs.