

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.



MP102

‘Power Outage Alerts triggered by an OTA firmware upgrade’

Modification Report

Version 0.2

Corporate member of
Plain English Campaign
Committed to clearer
communication

592



Managed by



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.....	4
3. Assessment of the proposal	6
Appendix 1: Progression timetable	8
Appendix 2: Glossary	9

Contact

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

Bradley Baker

020 7770 6597

bradley.baker@gemserv.com

1. Summary

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

Power Outage Alerts (POA) are used by DNOs to improve customer service by becoming aware of power outages sooner than relying on the customer to phone in enabling them to restore supply to affected customer more efficiently and more quickly.

Over the Air (OTA) firmware updates on some Electricity Smart Metering Equipment (ESMEs) generate a POA. The DNO is unable to tell whether there is a real issue with the power to the premises or whether it was just a firmware upgrade to the ESME.

OTA firmware upgrades have been required to stop this happening – 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, that will continue to initiate a POA when an OTA firmware update is implemented and this cannot be rectified.

2. Issue

What are the current arrangements?

Power Outage Alerts (POA) are intended to identify when the incoming power supply from a Distribution Network Operator (DNO) to a customer's premises fails for a period greater than three minutes. Such POAs are used by DNOs 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, a DNO needs to be confident that the POAs it receives are genuine and actually relate to supply interruptions to customers' premises.

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 DNO, 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 DNOs need to respond to each POA, a POA initiated by an OTA firmware update will cause a DNO to put in place systems to check every POA to understand 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, that will continue to initiate a POA when an OTA firmware update is implemented. This issue cannot be resolved retrospectively for the ESMEs already installed – these devices will continue to generate a POA on OTA firmware updates for the duration of their life. Ultimately these ESMEs would need to be replaced to resolve the problem. During this time, there is currently no solution that can stop POAs from being forwarded to the relevant DNO unnecessarily.

In summary there are two issues:

1. There is no obligation in the Smart Energy Code (SEC) to require an OTA firmware update not to generate a POA.
2. There is no means of identifying or suppressing 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 suppress 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 upgrade 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:

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

Both these options will result in the DNO incurring additional costs.

3. Assessment of the proposal

Observations on the issue

The proposal was presented to the Change Sub-Committee (CSC) for decision on 2 January 2020. The CSC discussed the issue and a DNO representative stated that the issue only relates to SMETS2 Devices and is limited to two manufacturers. The CSC agreed that the issue is clearly defined and recommended that the Draft Proposal should be converted into a Modification Proposal.

Once in the Refinement Process, discussions commenced between the Proposer, SECAS and the DCC regarding the number of meters affected by this issue. SECAS have advised that the DCC should undertake research for transparency of the issue. This research will allow the DCC to identify which meter models will cause the CH to reboot for a duration in excess of three minutes. The DCC have confirmed that this will have to be investigated under the request of the Preliminary Assessment.

SECAS have engaged with meter manufacturers in order to understand the magnitude of the issue. The meter manufacturer Landis and Gyr have stated that approximately 1,400,000 of their meters are affected by this issue.

Landis and Gyr also informed SECAS that they are undertaking a project to list all Global Unique Identifiers (GUIDs) of affected meters. Checking this list against their meter list, the industry will be able to establish where an OTA firmware upgrade will generate false AD1 Alerts.

Views of a SEC Party

During the Refinement Process, SECAS sought the views of a Networks Party in order to deliver fully refined business requirements. The Networks Party offered their full opinion of the issue identified.

Electricity Distributors have an obligation under Statutory Instrument 2002 No. 2665 'The Electricity Safety, Quality and Continuity Regulations 2002 (as amended)' to have and use distribution equipment in such a way so as to prevent interruption of supply to Customers' premises, so far as is reasonably practicable. Hence there is a legal obligation to maintain supplies to Customers.

Electricity Distributors have an obligation under Statutory Instrument 20015 No. 699 'The Electricity (Standards of Performance) Regulations' to pay Customers a prescribed sum of money where the supply to a Customer's premise is interrupted as a result of a fault on their network which is not restored in a prescribed period of time. There is therefore a need for the Electricity Distributors to know when a Consumer's supply is interrupted so that they can respond appropriately. Failure to respond and restore supplies within the prescribed time will have an adverse impact on Customer service and create an obligation to pay customers compensation.

Depending on the location of the faulty equipment, Electricity Distributors have a number of means of detecting the interruption of supplies to a customer's premise, the AD1 Alert being one of them. At the moment under the RIIO-ED1 regulatory instructions and guidance (RIGs) Annex F 'Interruptions', published by Ofgem and which forms part of the Electricity Distributors licence obligations, the Electricity Distributor need not respond on receipt of a single AD1 Alert, but there is a clear expectation that when the AD1 Alerts become more reliable the RIGs will be changed accordingly. It is therefore essential that the AD1 Alerts are as reliable as possible; when the RIGs are changed, Electricity Distributors will need to respond to an AD1 Alert. False or spurious AD1 Alerts are likely to initiate an unnecessary Customer contact either by phone or a site visit, which will increase costs, ultimately borne by Customers, and have an adverse impact on Customer service.

Support for Change

Working Group

The modification was taken to the SEC Working Group to discuss the scale of the issue and to further develop the business requirements that will be used as a framework for a DCC Preliminary Assessment. A Working Group member commented that the initial estimate of 500,000 affected ESMEs was a substantial under-estimate. SECAS informed the Working Group of discussions held with meter manufacturer Landis & Gyr, who are currently running their own project to understand the scale of the issue. They claim that so far they have identified 1.4 million ESMEs affected by the issue.

The Working Group and Proposer felt that the business requirements would need further development before proceeding to the DCC Preliminary Assessment. The Working Group agreed that the business requirements were too open at the moment and offered an unnecessary level of ambiguity. SECAS, the Proposer and Networks Parties will collaborate to refine the business requirements. A paramount requirement was discussed that all AD1 Alerts should be legitimate.

Details of a DCC investigation outlined by SECAS were discussed, however a Working Group member confirmed that the work they had been completing with the DCC should provide the results required. The DCC confirmed that they would share their findings for the benefit of the modification.

It was agreed by the Working Group that the modification would be split into two separate modifications to reduce the potential lead time. One to address the technical specifications so going forwards, meters are manufactured to not reboot for more than three minutes, and another to address existing meters already installed.

Appendix 1: Progression timetable

During the Refinement Process SECAS will work with the Proposer to draft the business requirements for this modification. The business requirements will then be discussed with the SEC Working Group for further refinement. SECAS will then request a Preliminary Assessment from the DCC.

Timetable	
Event/Action	Date
Draft Proposal raised	18 Dec 2019
resented to CSC for comment and recommendations	2 Jan 2020
Panel converts Draft Proposal to Modification Proposal	17 Jan 2020
Business requirements developed with Proposer and DCC	Mar 2020
Business requirements discussed with Working Group	1 Apr 2020
Preliminary Assessment requested	6 Apr 2020

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
CH	Communications Hub
CSC	Change Sub-Committee
DCC	Data Communications Company
DNO	Distribution Network Operator
ESME	Electricity Smart Metering Equipment
GBCS	Great Britain Companion Specification
GUID	Global Unique Identifier
OTA	Over The Air
POA	Power Outage Alert
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SMETS	Smart Metering Technical Specifications