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.

MP102B

‘Power Outage Alerts triggered by an OTA firmware upgrade – enduring solution’

Modification Report

Version 0.8

20 September 2021

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 10

Appendix 2: Glossary 10

This document also has one annex:

- **Annex A** contains the business requirements for the solution.

Contact

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

Bradley Baker

020 7770 6597

bradley.baker@gemserv.com

1. Summary

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

Power Outage Alerts (POAs) are used by Distribution Network Operators (DNOs) to improve customer service by becoming aware of power outages sooner than relying on their customers to contact them. POAs enable the DNO to restore supply to affected customers more efficiently and more quickly.

Over the Air (OTA) firmware updates can cause Electricity Smart Metering Equipment (ESME) to generate a POA. The DNO is unable to tell whether there is a real issue with the power to the premises or whether it the POA was generated as a result of a firmware upgrade to the ESME.

OTA firmware upgrades have been required to stop this happening. However, this agreement is 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.

Furthermore, there is still a set of ESME, that will continue to initiate a POA when an OTA firmware update is implemented, and this cannot be rectified.

Investigations during the Refinement Process found the scale of the issue affecting existing meters much greater than initially envisaged. Due to an anticipated lengthy lead time for implementation where meter Manufacturers could potentially still produce Devices that cause erroneous POAs, it was agreed that there should be two separate solutions to address the issue:

- MP102A: a Technical Specifications document change for meter Manufacturers to abide by for ESME produced after implementation (implemented as part of the November 2020 SEC Release); and
- MP102B: an enduring solution for meters that are currently installed.

2. Issue

What are the current arrangements?

It is the intended purpose of POAs to notify DNOs when the power supply to a customer's premises fails for a period greater than three minutes. POAs are used by DNOs to improve customer service by becoming aware of power outages sooner than relying on the customer to contact the DNO, and to develop a faster, more complete view of the premises affected and hence enable them to restore supply to affected customers 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 activating an OTA firmware update on particular ESME generates a POA. This is because when some ESME 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 to 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 forwards the AD1 Alert to the relevant DNO, who cannot verify whether there is a real issue with the power to the premises or whether the outage occurred due to a firmware upgrade to the ESME. As DNOs need to respond to each POA as per their business processes, a POA initiated by an OTA firmware update will require a DNO to respond in the same manner as if it were 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). 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.

Furthermore, there is still a set of ESME that will power down for three minutes or more, and thus continue to initiate a POA when an OTA firmware update is implemented. SECAS have been advised that this issue cannot be resolved retrospectively for the ESME already installed. These Devices will continue to generate a POA upon OTA firmware update activations for the duration of their life. 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 supressing erroneous POAs associated with an OTA firmware update from the high number of ESME in service where this issue can't be addressed.

How does this issue relate to the SEC?

Currently there is no specific text in SEC Schedule 8 'GB Companion Specification' (GBCS) and SEC schedule 9 'Smart Metering Equipment Technical Specifications' (SMETS), prohibiting a POA from being generated upon an OTA firmware upgrade activation. 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 upgrade will require a DNO to put in place systems to check every POA to establish whether or not 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 extreme cases, 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 a 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.

Scale of the issue

During the Development Stage, SECAS was made aware of two Device Manufacturers that had built Devices that caused POAs to be generated when an OTA firmware upgrade takes place. Landis + Gyr advised that they had built approximately 1.4m ESME that can potentially take longer than three minutes to resume normal operation following the firmware activation. This is due to the ESME design containing a bootloader specification (part of the Device's software) that impacts the reboot duration of the Device.

The second Device Manufacturer, Aclara, have approximately 1,400 ESME currently installed that can cause the issue. SECAS liaised with the manufacturer to better understand the impact of the issue moving forwards. Aclara stated that this was an issue that affected the first generation of their hardware (Certified Products List (CPL) model code 00000000). They commented that later revisions of SMETS require an upgrade to the Zigbee stack within the ESME. This is not possible on this particular model. As such, Aclara confirmed there cannot be no further upgrades issued for this hardware and therefore these meters are not considered to be within the scope of the modification.

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 advised that the DCC should undertake research for transparency of the issue. This research would allow the DCC to identify which meter models will cause a reboot for a duration in excess of three minutes. The DCC stated that this would have to be investigated under the request of the Preliminary Assessment.

SECAS engaged with meter Manufacturers in order to understand the magnitude of the issue. The meter Manufacturer Landis + Gyr have stated that approximately 1.4m of their meters are affected by this issue. Landis + 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 will enable them to establish where an OTA firmware upgrade will generate spurious AD1 Alerts.

Views of the Proposer

During the Refinement Process, SECAS engaged with the Proposer to better understand the impact the issue is having. They offered their full opinion of the issue identified from the perspective of a Networks Party:

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 supply to a customer's premise, the AD1 Alert being one of them. The RIIO-ED1 regulatory instructions and guidance (RIGs) Annex F 'Interruptions' form part of the Electricity Distributors licence obligations. These state that the Electricity Distributor need not respond on receipt of a single AD1 Alert, but that 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

Scale of the issue

The modification was taken to the Working Group to discuss the scale of the issue and to further develop the business requirements to be used as a framework for a DCC Preliminary Assessment. At the April 2020 Working Group a Working Group member commented that the initial estimate of 500,000 affected ESME was a substantial under-estimate. SECAS informed the Working Group of discussions held with a meter Manufacturer who were running a project to understand the scale of the issue with the DCC. At the time of the meeting, they had identified 1.4m ESME affected by the issue. A Working Group member confirmed that other work they had been undertaking with the DCC should provide the results required. The DCC confirmed that they would share their findings for the benefit of the modification.

Further discussions were held in June 2020 regarding the scale of the issue to help establish a business case. The meter Manufacturer working on the project with the DCC confirmed that an approximate 1.4m meters had been produced that could result in an AD1 Alert being generated by the CH. However, the DCC testing had only identified an approximate 14,000 meters which were causing the issue. Several Network Party members questioned the accuracy of the DCC results. They stated that there had been instances where AD1 Alerts had been lost. A Working Group member stated that they had experienced three to five thousand cases where they had received a Power Restoration

Alert but not an AD1 Alert. For this reason the Working Group did not believe the DCC figure of 14,000 affected Device was accurate.

Splitting 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.

Business Case

SECAS presented the business requirements to the DCC IT Interaction Group (DIG) which questioned the testing that had taken place which identified only 14,000 meters as it felt that this reduced the business case of the modification. SECAS held a teleconference between the Proposer, Landis + Gyr, and Network Parties to allow the Network Parties to better understand the testing constraints of the meter Manufacturer and the DCC. The mismatch between the original list of 1.4m GUIDs and the reduced list of 14,000 Devices confirmed by the DCC to generate an AD1 as a result of an OTA firmware update were discussed.

Landis + Gyr stated that they had built 1.4m meters that may cause this issue. However, the DCC testing generated a list of just 14,000 meters where the DCC had seen an AD1 Alert generated soon after an OTA firmware update had taken place. Landis + Gyr stated that the 1.4m meters cannot be ruled out even though the vast majority were not identified during testing. This is due to the flash memory in meters deteriorating over time and the frequency of use. This has been proven in test laboratories where meters are subject to extensive use. It is known that as the meter ages, it takes longer to reboot. Comments were also received that the issue could worsen when a firmware update reaches the upper size limit of 750kb. Landis + Gyr further advised that for their meters to be upgraded to SMETS2 v4.2, there will be two firmware updates to upgrade the meters.

The Network Parties reiterated that they must respond to an AD1 Alert in the same manner as when a consumer reports a lack of supply, and with 1.4m Landis + Gyr meters that could cause the issue in the future, the meter Manufacturer agreed that the issue must be resolved.

Views of the TABASC

During the Refinement Process, SECAS presented the modification to the Technical Architecture and Business Architecture Sub-Committee (TABASC). TABASC members questioned the business case for the modification, asking SECAS whether a process of validation can be used before an engineer is sent to site to confirm whether the site does or does not have an energy supply. This could be done through sending Service Request (SR) 7.4 ‘Read Supply Status’. The Proposer felt that this would be unreasonable as this process of validation would have to be carried out for every POA that they receive (DNOs have no visibility of firmware upgrades).

SECAS have further investigated TABASC's suggestion and have identified that any Service Request could be sent to check power supply, not exclusively SR7.4. The Communications Hub will lose power and will not be able to process any SR and so a DCC error message should be sent back to the DNO. If a response is received from the Communications Hub, then the DNO knows the Communications Hub still has power. The implementation of the SEC Modification will eliminate

virtually all spurious AD1 Alerts following an OTA as they will be filtered by the Data Service Provider (DSP). If an AD1 is received by the DNO they will have to follow their own business process for handling what is perceived as a genuine outage.

Identifying the meters causing the issue

SECAS have worked with Landis + Gyr in order to identify the 1.4m ESME that can cause the issue. SECAS first explored using the CPL by filtering to specific Device models. This would be the most efficient way of addressing the issue, as any AD1 generated from a particular Device model could be suppressed by the DSP. Unfortunately, Landis + Gyr informed SECAS that the bootloader specification known to cause the issue was implemented across different Device models, which since installed will also be on varying firmware versions. Landis + Gyr advised that due to the varying hardware and firmware versions, this would not be a viable option.

SECAS also investigated the possible use of meter commission dates. However, Landis + Gyr commented that the introduction of the bootloader is extremely difficult to pinpoint, due to multiple manufacturing sites and the Manufacturer building Devices for multiple customers and their subsequent individual firmware versions. Furthermore, some Devices may have been warehoused following manufacture. Media Access Control (MAC) addresses were also explored under this option, however this was ruled out as they do not follow on sequentially.

Following these conversations, SECAS, the Proposer and Landis + Gyr agreed that the best way to confidently identify the Devices causing the issue is to use the original GUID list in Microsoft Excel format. The DSP will use this list to suppress AD1 Alerts from these Devices, following an OTA firmware update activation.

Business requirements workshop

SECAS stated that after much investigation, the most straightforward way of identifying the ESME that are or could potentially cause the issue is by referencing a GUID list provided by L+G that lists the 1.4m Devices. SECAS advised that other options such as using the CPL have been explored but to no avail.

The DCC queried whether this list would be subject to change or would remain static. Due to the implementation of MP102A, ESME will no longer follow reboot procedures exceeding three minutes, and L+G have previously identified and resolved the problem moving forwards. The DCC and DSP saw no negative impact of the list remaining in situ, despite the number of ESME expected to reduce (due to physical replacements over time).

SECAS advised that due to the anticipated additional processing for the DSP, it was the intention of the DNOs to have a solution investigated where POAs would be suppressed following an OTA firmware activation for all ESME. The SEC Operations team sought to clarify that this is in fact for all L+G ESME. It was agreed that the business requirements will be amended accordingly. The Proposer confirmed that they were comfortable with the possibility of suppressing genuine POAs during the 30-minute period.

An issue was raised whereby the validity of the solution could be jeopardised due to the ability to future date firmware activations. This adds extra complexity as the Target Response Time for future dated activations is 24 hours as opposed to 60 seconds for on demand activations. This makes the DSP's task of suppressing erroneous POAs more complex. It was advised that to resolve this issue, there may need to be changes at a CSP level.

Following the requirements workshop on 9 August 2021, the DCC took an action to analyse Technical Operations Centre (TOC)information to ascertain what percentage of firmware activations on Landis + Gyr are future dated. The data spanned from 2019 to present, and showed that approximately 13% of firmware activations on Landis + Gyr ESME are future dated. The data also shows a gradual increase in future dating by Suppliers from January 2021.

The modification subsequently returned to the requirements workshop for further refinement of the requirements. The key objective was to incorporate requirements that addressed the issue of future dated firmware activations. Members were happy with the progress made, and advised that a request for information (RFI) should be issued to better understand Supplier firmware activation processes.

Appendix 1: Progression timetable

SECAS will issue an RFI to better understand the business processes of Suppliers' OTA firmware activations. Following a review of the responses with the Proposer, SECAS will request the DCC Preliminary Assessment.

Timetable	
Event/Action	**Date**
Draft Proposal raised	18 Dec 2019
Modification discussed with the Working Group	1 Apr 2020
Modification discussed with the Working Group	3 Jun 2020
Business requirements developed with Proposer and DCC	Jun 2020 – Jul 2021
Proposed Solution developed with Proposer	Jun 2020 – Jul 2021
Business requirements workshop	9 Aug 2021
Request for information	21 Sep – 12 Oct 2021
Preliminary Assessment requested	1 Nov 2021
Preliminary Assessment returned	26 Nov 2021
Modification discussed with the Working Group	5 Jan 2022
Refinement Consultation	10 Jan – 28 Jan 2022

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
CPL	Certified Products List
CSC	Change Sub-Committee
DIG	DCC Interaction IT Group
DCC	Data Communications Company
DNO	Distribution Network Operator
DSP	Data Service Provider
ESME	Electricity Smart Metering Equipment
GBCS	Great Britain Companion Specification
GUID	Global Unique Identifier
MAC	Media Access Control
OTA	Over The Air
POA	Power Outage Alert

Glossary	
Acronym	**Full term**
RFI	Request for information
RIGs	RIIO-ED1 regulatory instructions and guidance
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SMETS	Smart Metering Technical Specifications
SR	Service Request
TABASC	Technical Architecture and Business Architecture Sub-Committee