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.

SECMP0062

'Northbound Application Traffic Management – Alert Storm Protection'

Modification Report

Version 32.10

About this document

This document is the Modification Report for SECMP0062 'Northbound Application Traffic Management – Alert Storm Protection'. It provides detailed information on the background, issue, solution, costs, impacts and implementation approach. It also summarises the discussions that have been held and the conclusions reached with respect to this Modification Proposal.

Contents

This document has ~~six~~seven annexes:

- **Annex A** contains the business requirements for the proposed solution.
- **Annex B** will contain the redlined changes to the Smart Energy Code (SEC) required to deliver the proposed solution. This document is currently being updated.
- **Annex C** contains the 'Traffic Management Mechanism Document' which will be introduced as part of this modification.
- **Annex D** contains the full Data Communications Company (DCC) Impact Assessment response.

- **Annex E** contains the Working Group Consultation responses.
- **Annex F** contains the first Modification Report Consultation responses.
- **Annex G** contains the second Modification Report Consultation responses.

1. Summary

Alert Storms occur when Devices repeatedly send Alerts to DCC Systems and Service Users. Although these Devices have gone through rigorous test assurance processes, it is inevitable that not every possible combination and scenario will have been accounted for. This means that many Devices pose a risk of entering a state whereby they repeatedly and rapidly ~~generates~~generate the same Device Alert, adding unnecessary traffic to the Communication Service Provider (CSP) or Smart Metering Equipment Technical Specification (SMETS) 1 Service Provider (S1SP) Gateway between the DCC Systems and Service Users. Currently there is little protection against Alert Storms, meaning that multiple Alerts are being counted and entering the gateway, rather than being filtered out, even after recognising they are originating from the same single Device.

In December 2019 the DCC stated that the original system had been designed and built to a contracted capacity of one Alert per Device per month, which was what was estimated when the system was designed. However, actual figures showed 43 million Alerts had originated from 4 million meters on 31 December 2019 alone, with 1.3 billion Alerts across the month of December 2019.

The proposed solution is to provide Alert Storm protection through a DCC designed mechanism which will count the number of Alerts originating from a specific, individual Device within a defined time window. If the Device sends the same Alert above a pre-determined threshold value, the mechanism will consolidate excess Alerts from the Device and only forward one copy of that Alert in a designated period agreed by the DCC on to the intended Users. Consolidated Alerts will be counted for Anomaly Detection purposes and Service Users will be notified ahead of time for the exact actions being taken. This solution will be implemented over two stages.

This modification will impact Supplier Parties, Network Parties, Other SEC Parties and the DCC. The ~~central~~total cost of implementation for this modification ~~is approximately~~will be £1~~ million~~,088,392. The proposed implementation date for this modification is the June 2020 SEC Release for the core solution and the November 2020 SEC Release for the ~~enduring reporting arrangements~~DCC User Interface Specification (DUIS) changes.

2. Background

Context to DCC Systems Communications

The DCC and Service Users communicate using the DCC Systems to send service requests and Alerts for different registered Devices. Due to the DCC System having a finite capacity for how many requests and Alerts it can handle, if this system becomes overloaded, it will affect the stability and performance of the whole system. This system could also be subject to Alert Storms, a state where individual Devices may frequently generate the same Alert and send it through the DCC Systems. This adds needless traffic to the DCC Systems and, as a result, slows down the response time for other Alerts and service requests. Alert Storms therefore need to be avoided as much as possible, or alternatively, traffic management needs to be in place to prevent repeated Alerts from a faulty Device entering multiple Alerts into the system.

What is the issue?

Alert Storms are one of the biggest issues faced by the DCC with its systems for handling service requests and Alerts from Service Users. Currently, the DCC uses a detection solution for northbound traffic (traffic passing from Devices to Users) which follows a pattern where Alerts are counted over a specified time window. If the total number of Alerts exceeds a pre-determined threshold (which is defined by either amber or red levels) the event is recorded in the security log and an incident file is saved.

However, this solution does not prevent the Alerts from being forwarded to the relevant Service Users, so therefore does not protect the DCC Systems against overload or traffic generated by Alert Storms. In December 2019 the DCC stated that the original system had been designed and built to a contracted capacity of one Alert per Device per month, which was what was estimated when the system was designed. However, actual figures showed 43 million Alerts had originated from 4 million meters on 31 December 2019 alone, and a total of 1.3 billion Alerts for the month of December 2019. The DCC reported that Alert traffic was currently doubling every three months, and this would increase as the rollout continued to unmanageable levels.

Whilst the DCC's aim is to manage Alerts at the Communications Hub in future, this is not currently possible and will need development time of an estimated 24-36 months. In the meantime, a solution is needed to manage the Alerts traffic. The DCC thereby needs to take direct action to protect its systems to ensure availability of the service for ~~their~~its Service Users and incorporate a new means of traffic management to prevent, where possible, excess Alerts from entering its system.

Breakdown of SMETS1 and SMETS2 Alerts impacting the DCC Systems

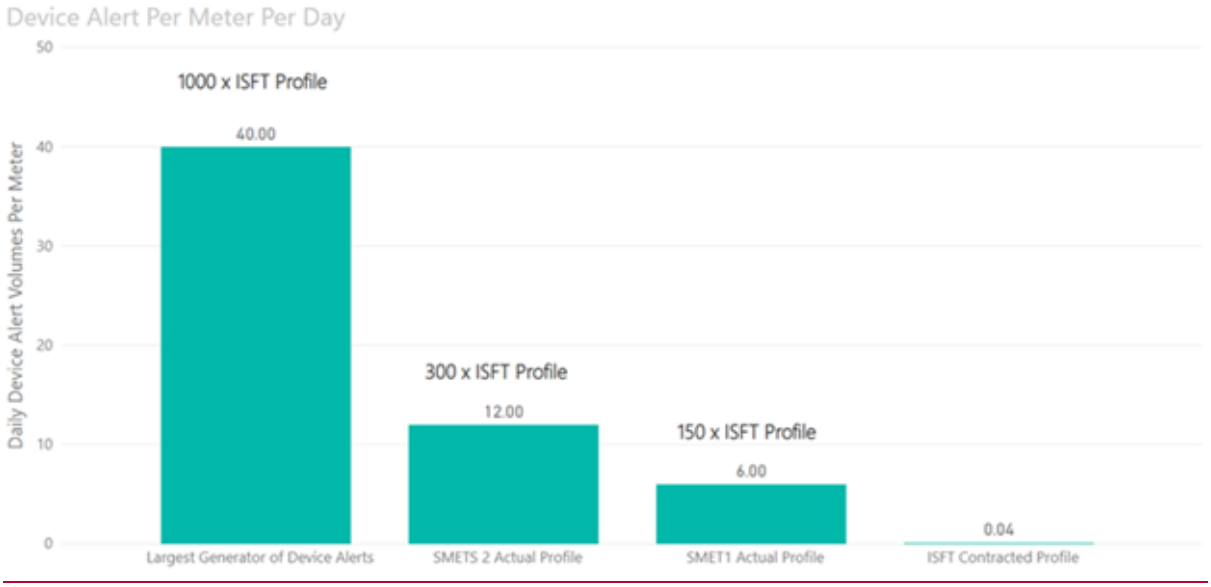
A question was raised around the level of SMETS1 Alerts and how they are affecting the DCC Systems currently, and whether the DCC System was designed to deal with the number of Alerts it is currently experiencing. The DCC responded that the number of SMETS1 Alerts are much lower than the number of SMETS2 Alerts. It stated that Alert volumes, as set out in the original 'Invitation to Submit Final Tender' (ISFT) contracts awarded by the Department of Energy and Climate Change (DECC), requires service users to scale to meet an average profile of 0.04 Device Alerts per meter per day. On 13 November 2019, SMETS1 meters generated on average six Device Alerts per meter per day (150 x the ISFT Profile); a volume significantly higher than the ISFT profile. On the same day

for SMETS2 an average of 12 Device Alerts were generated per meter per day (300 x the ISFT profile). These are summarised in the graph below.

The Device Alert volumes for SMETS2 not only exceed the contracted volumes as described above, but with a small number of Devices each responsible for thousands of device alerts per day, this geographically concentrates traffic on the CSP networks, compounding the problems caused by device alerts.

In summary:

- SMETS1 Alerts are more geographically distributed and dispersed across five SMETS1 Alert codes, whereas 80% of SMETS2 alerts are accounted for by a single Alert code (8F3E – unauthorised access) and the majority are generated by a small number of devices
- The number of Alerts varies by Service User. The Service User receiving the most device alerts, receives them at a rate 1,000 times greater than contracted rate per meter per day.



3. Solution

Proposed Solution

The proposed solution is to provide Alert Storm protection through a DCC designed mechanism which will count the number of Alerts originating from a specific Device within a designated timeframe. If the Device sends Alerts above a pre-determined threshold value, the mechanism will consolidate excess Alerts from the Device, and only forward one per a configurable number of Alerts (n) per designated period on to the intended Users. Consolidated Alerts will be counted for Anomaly Detection purposes and Service Users will be notified ahead of time for the exact actions being taken.

A visual summary of the impacts on the DCC Systems can be found in Appendix 1. The business requirements for this solution can be found in Annex A.

How will the mechanism operate?

The mechanism operates by periodically checking the total number of Alerts generated by a Device to see if it exceeds a "red" threshold ~~anomaly –~~. This is the point at which too many (a value defined by the DCC in the Traffic Management Mechanism Document in Annex C) Alerts ~~in~~ are being received from that specific ~~Alert Code will trigger~~Device, triggering the solution's mechanism. This will be known as "red" in terms of Alert thresholds. If a "red" threshold anomaly is detected at the Device level, the mechanism then counts each specified Alert Code. If the ~~counter for an~~count of a specific Alert Code exceeds ~~its limit in the designated timeframe,~~the 'Alert Code Specific Threshold' within the 'Alert Code Specific Rolling Window' then the code will be marked as "~~overloaded".~~HighAlertRate" and subject to consolidation. It is noted that if an Alert Code is ~~throttled~~consolidated at Device level, this only affects the Devices generating the Alerts that ~~break~~exceed the threshold. Any Devices that are not exceeding the threshold~~,~~ but still generating those Alerts will not be subject to having their Alerts counted and consolidated.

The DCC has confirmed that these Alert Code settings are "global~~"~~", meaning the threshold is the same for all Alert Codes and can't be tailored on an individual basis. This was justified because configuration in that area would add expense and time to the development of the solution.

The parameters to this mechanism will be fully configurable, for example the Alert Code threshold, the number of consolidated Alerts and a "rolling window" indicating how long an incident would last. These parameters will be recorded in the Traffic Management Mechanism Document. Any changes to these parameters will be managed by the Operations Group.

If an Alert Code isn't ~~"overloaded~~marked as "HighAlertRate" it is passed on to Request Management as normal. If an Alert Code is "~~overloaded"~~HighAlertRate" then it will ~~allow~~be subject to consolidation and only one in n Alerts ~~to be let through,~~will be forwarded to Request Management, together with the count of the ~~remaining~~consolidated Alerts ~~sent to Request Management~~. Once the number of Alerts falls below the "red" threshold, then that specific Alert Code counting will cease, and any ~~overloaded~~"HighAlertRate" Alert Codes will be cleared.

How will the solution be implemented?

This solution will be implemented in two stages:

- The first stage (Part 1) will have a single default value for Alert Code thresholds, which will be configured using a basic configuration file similar to that currently used for more generic Alert

Anomaly Detection Thresholds. It will also have an exclusion list of Alert Codes which will be exempted from this mechanism. This list of Alert Codes will be managed by the Panel; the ~~Panel~~Working Group agreed with the Smart Energy Code Administrator and Secretariat (SECAS) recommendation ~~to delegate~~that this responsibility should be delegated to the Operations Group. This results in an Alert either being subject to a configurable but global traffic management setting or exempted from this traffic management.

During this stage, a new dashboard in the Self-Service Interface (SSI) will ~~act as the means of reporting to inform~~show Service Users whether any Alert Storm Protection is currently active for any of their Devices~~. This solution~~; this will ~~also incorporate the~~ be defined and designed via the SSI update process following approval of SECMP0062. The DCC's Technical Operations Centre (TOC) will be utilised to provide reporting based on additional ~~elements to~~data feeds from the ~~reporting~~proposed solution. The TOC can provide data approximately 15 minutes behind real time, allowing it to indicate trends for DCC System traffic~~. The DCC will also be able~~ – this data will be used by DCC to help identify root causes of Alert Storms where possible.

Alert consolidation can be used to create Incidents within the DCC Service Management System (DSMS); this will be a system configuration parameter. The DSMS enables Users to ~~provide~~ elect to receive email ~~notification to Users~~ notifications when ~~a Device/Alert Code combination is being controlled; it's the User's choice whether they~~incidents are ~~actively emailed in every incident occurrence or won't receive an email in any instance. The DCC has advised this feature can be switched off in the short term and turned on once the DCC System traffic has lessened. This is so that Users would not be burdened with large quantities of emails causing administrative issues.~~created.

- The second stage (Part 2) of the solution will introduce ~~configuration parameters for specific Alert Code values and associated Self-Service Management Interfaces (SSMI) management changes and incorporate DCC User Interface Specification (~~DUIS~~)~~ Schema changes (these changes are defined more explicitly as part of the DCC Impact Assessment in Annex D). The Alerts will have metadata in their headers to distinguish between an Alert that has or hasn't been subject to Alert Storm Protection. The DUIS changes will only be included in the new version of DUIS created in the relevant SEC Release, and will not apply to previous versions.

How will Incidents be managed under Part 1 of the solution?

The solution includes a system configuration parameter to allow the creation of a DSMS Incident whenever consolidation is first initiated for a specific Device/Alert Code combination. This incident would be allocated to the Known Remote Party for that Device/Alert Code as defined in the GBCS.

Any Alert Code in the exclusion list will never be subject to Alert Storm Protection. A full list has been discussed and agreed with Service Users (see Annex C), and any future changes would be managed by the Panel.

No new incident would be created for the same Device/Alert Code combination until it has remained below the threshold for longer than the 'Alert Storm Protection Incident Deadband Period'.

The configuration parameter 'Alert Storm Protection Incident Creation' operates system-wide and so is a single setting that will affect all Users.

Due to the current Alert volumes, this will be configured 'OFF' when Part 1 goes live, until such time as (a) Alert volumes have returned to more reasonable levels, and (b) Users are in agreement that

they wish this to be enabled. As the ON/OFF settings will be recorded in the Traffic Management Mechanism Document, changes to this must be agreed with the Panel (or a Sub-Committee nominated by it) before they take effect.

How will email notification be managed under Part 1 of the solution?

Email notifications of incidents are an existing feature of the DSMS. Users can elect to enable or disable this feature, but it does operate across all Incidents allocated to that User, not just those originating from the Alert Storm Protection solution.

As stated above, incident creation will be turned off initially, to avoid Users receiving large numbers of emails once SECMP0062 is implemented.

~~The business requirements for this solution can be found in Annex A.~~

Legal text

The changes to the SEC required to deliver the proposed solution will be found in Annex B. The 'Traffic Management Mechanism Document' cited in the legal text can be found in Annex C.

4. Impacts

This section summarises the impacts that would arise from the implementation of this modification.

SEC Parties

SEC Party Categories impacted			
✓	Large Suppliers	✓	Small Suppliers
✓	Electricity Network Operators	✓	Gas Network Operators
✓	Other SEC Parties	✓	DCC

All SEC Parties will be subject to the effects of the throttling effects and ~~discarding~~consolidation of Alerts, and will therefore need to manage any resulting reporting of this accordingly. Following the Working Group Consultation sent out to SEC Parties, one respondent cited they would incur additional costs in developing their internal systems and processes to accept the changes proposed under this modification and that they would require a minimum of six months lead time to uplift their systems and add functionality changes.

Following the Modification Report Consultation, Electricity Network Parties expressed concerns as to how the reporting would be managed and that they would suffer administrative issues through Part 1 of the solution. Clarifications were made to the reporting following this and SECAS agreed with the DCC that the email notification of alerts and incidents could be turned off initially so that email notifications would not cause administrative issues for Users.

DCC System

The DCC Systems will be impacted due to adding the mechanism which delivers the solution set out in this Modification Proposal. However, if this modification is not implemented the stability and performance of the DCC Systems will be at risk and the response times for other Alerts and service requests will slow down.

The full impacts on the DCC Systems and DCC's proposed testing approach can be found in the DCC Impact Assessment response in Annex D.

SEC and subsidiary documents

The following parts of the SEC will be impacted by Part 1:

- ~~Section A 'Definitions and Interpretations'~~
- Section H 'DCC Services'
- Appendix AB 'Service Request Processing Document'
- Appendix AH 'Self Service Interface Design Specification'

The following part of the SEC will be impacted by Part 2:

- Appendix AD 'DCC User Interface Specification'

Other industry Codes

No other Energy Codes will be impacted by this modification.

Greenhouse gas emissions

Greenhouse ~~Gas Emissions~~gas emissions will not be impacted.

5. Costs

DCC costs

The ~~estimated~~confirmed DCC implementation costs to deliver this modification is £1,088,392. The breakdown of these costs are as follows:

Breakdown of DCC implementation costs	
Activity	**Total**
Design	£964,346
Build	
Pre-Integration Testing (PIT)	
Systems Integration Testing (SIT)	£96,995
User Integration Testing (UIT)	£9,359
Implementation to Live	£17,692

The DCC costs have been provided for both parts combined. More information can be found in the DCC Impact Assessment response in Annex D.

SECAS costs

The ~~estimated~~ SECAS implementation costs to implement this modification is two days of effort for each ~~Stage~~part of the solution, amounting to approximately £~~2,400~~1,200. The activities needed to be undertaken for each ~~Stage~~part are:

- Updating the SEC and releasing the new version to the industry.

SEC Party costs

Working Group Consultation respondents said that they would all incur costs to a degree, either through changes to their business processes or technical implementation costs. Some respondents noted they required additional information before being able to provide an accurate picture of how large these costs would be. One respondent noted that the costs incurred to them would be low and another estimated the overall cost to them would outweigh the benefits this modification would deliver. The full responses can be found in Annex E.

6. Implementation approach

Implementation approach

The Panel agreed a two-part implementation approach where:

- Part 1 will be implemented on **25 June 2020** (June 2020 SEC Release); and
- Part 2 will be implemented on **5 November 2020** (November 2020 SEC Release)

if a decision to approve is received on or before ~~22 January~~7 February 2020.

The DCC's Impact Assessment identifies a six-month lead time to deliver the modification's full solution, meaning it would not be possible to include Part 2 in the June 2020 SEC Release. The DCC has confirmed it can deliver the changes for Part 1 of the solution in the June 2020 SEC Release. The November 2020 SEC Release is currently the next SEC Release where DUIS changes are anticipated, and so for efficiency it was agreed that Part 2 should be included alongside these. If other DUIS changes are approved for implementation at an earlier date, the Panel can request the Authority revise the date for Part 2 accordingly.

Part 1 of the Modification Proposal's solution will look to be implemented in the June 2020 SEC Release. This way, Part 1 of the solution with the solution's ~~filtration~~consolidation mechanism and reporting will be active, without requiring DUIS changes. After discussing the first Modification Report Consultation responses with Electricity Network Parties, so long as the email notifications being generated from SECMP0062 could be turned off whilst there are numerous incidents and that clear reporting is taking place through the SSI and the TOC, Part 1 got agreement from the Working Group to be implemented in the June 2020 SEC Release.

7. Discussions and development

Will the mechanism in the proposed solution have unintended consequences in its ~~filtration~~consolidation process?

The Working Group considered unintended consequences that could arise. One potential impact noted was that the solution's mechanism could potentially filter out Alerts that Users want to keep a record of. It was noted that, under the initially proposed configurable parameters, a User would receive in excess of 50 copies of a particular Alert before throttling would occur and would still receive one in 10 of subsequent copies. However, members still felt there would be some Alerts for which they would want to receive all copies, regardless of the situation. The Working Group therefore created a list of Alerts they deemed it would be beneficial to be exempted from the mechanism. The content of this list of Alerts affected was determined as part of this modification's refinement and a question was asked in the Working Group Consultation asking for Alert Codes that respondents feel should not be subject to throttling.

The Working Group agreed that a new document, called the 'Traffic Management Mechanism Document', would be created, which would document the list of exempted Alert Codes plus the parameters used by the DCC. This document would sit outside the SEC, meaning it would not require a Modification Proposal to amend its contents. However, all changes to this must be agreed with the Panel (or a Sub-Committee nominated by it) before they take effect.

~~What~~How big is the ~~scope~~impact of the proposed solution?

The Working Group considered the scope of the proposed solution. It was noted that the solution that was being designed only counters Alerts that are generated by Alert Storms from a single Device rather than multiple Devices sending out the same Alert. The DCC confirmed this was the case as each Device would be registered as an individual incident for the purposes of recording Alerts breaching the threshold to trigger the throttling mechanism.

The DCC provided the following analysis to model outcomes where its mechanism is in effect against the four Alert Codes with the greatest volume. The DCC modelled this by taking an actual count of each Alert type on a per Device level that was queried from the service audit trail for the 31 December 2019. This query returned a list of 380,861 devices generating a total of 43.3 million device alerts for that day. This day was chosen as it was one of the days with the highest number of Device Alerts. This may not be correct in all instances, especially where a large quantity of Devices are generating a small number of Alerts as this may not breach the Red Threshold for Alert Anomaly Detection.

The approach for each calculation is summarised below:

1 in 10

Where a Device generated more than 10 Device Alerts on the 31 December 2019 and generated more than 10 Device Alert of a specific alert type (e.g. 8F3E), then only 1 in 10 of that Device Alert is passed on.

1 in 500

Where a Device generated more than 10 Device Alerts on the 31 December 2019 and generated more than 10 Device Alert of a specific alert type (e.g. 8F3E), then only 1 in 500 of that Device Alert is passed on.

Total Alerts under different scenarios			
Alert	**No consolidation**	**N=10**	**N=500**
8F3E	37,176,005	3,767,340	133,752
8014	602,857	114,232	70,404
8015	604,485	114,190	70,236
8F12	2,525,257	277,464	32,452
Sum	**40,908,604**	**4,273,226**	**306,844**
Reduction	**-**	**89.5%**	**99.3%**

This analysis suggests if the mechanism ~~they have~~ designed is implemented, it should eliminate approximately ~~90~~99.3% of individual Devices providing repeated Alerts through Alert Storms. It would mean, in this particular instance, the solution would reduce repeated Alert traffic in the DCC Systems considerably ~~but noted~~. However, where the problem is not limited to a single Device this will have a reduced effect.

Given the cost attached to the modification's solution to its limited scope, this focused the business case towards how much more capacity this can provide the DCC Systems compared to if the modification is not accepted and subsequently allowing the ~~System~~system to fail. Given this allowed greater efficiency of the current infrastructure rather than a more expensive expansion of the current DCC System capacity, the benefits for this modification were seen as worth the industry cost of the modification.

Would the traffic management solution be better placed as firmware for Devices, rather than specifically to the DSP?

Members of the Working Group raised the question as to whether it would be more effective if the solution was implemented through firmware to Devices to prevent excessive numbers of Alerts being generated through Alert Storms, rather than as part of the Data Service Provider (DSP) system. The motivation behind this was that by addressing the problem at an individual Device level rather than through the DCC Systems, it could be used to properly address the source of the problem rather than its symptoms.

The DCC considered this in the first Working Group meeting and understood the concerns raised. In turn it provided the Working Group with data and information relating to the CSP that showed why it would be more desirable to implement the solution through the DSP rather than through firmware. Ideas were therefore discussed surrounding the viability of an alternative solution with the same filtering mechanism being utilised at a CSP level.

The DCC informed the Working Group ~~it~~the Modification Proposal is intended for the consolidation of Alerts received by the DSP. It had taken this into account for an alternative solution but claimed this would create a significant issue. This alternative solution would mean adjusting the parameters of every affected Device rather than changing the settings of the central systems, which would take significantly longer to administer the changes. The DCC noted this could leave a number of Devices during this time without communicating capabilities through DCC Systems.

The DCC is working with the CSPs to identify both Communications Hub and Device based solutions; however due to the nature of the changes needed, they are likely to take an extended time to be implemented and would likely also be dependent upon SECMP0062 having been implemented. The

DCC has expressed that due to the impacts of Alert Storms currently being experienced, the DSP solution should be used whilst a CSP solution is being explored. Information gained from this solution will also be used as part of any root cause analysis to better identify future changes addressing the root cause of the issue.

The Working Group stated that the proposed solution was the ideal solution choice to be progressed under this modification. Any alternative solutions for consideration that look at providing Alert filtration should be raised in a separate modification and that way would provide another layer of security alongside SECMP0062.

Will there be a means of notification for Users when Alerts are being controlled in the first stage of the implementation approach?

As part of the solution's development, it was proposed that, in order to progress the modification faster and make sure the lead time was sufficient for delivering the solution, a two-stage implementation approach could be taken. The first stage would deliver all of the business requirements in Annex A with the exception of Requirement 2 around implementing a mechanism to notify Users when an Alert has been throttled. This would be delivered in the second stage with the relevant changes to DUIS being implemented at that point in time.

As part of this, the Working Group requested, during this first stage of the process, that a form of active notification be investigated given to Users as otherwise the only means of Users being able to identify Device/Alert Code combinations being controlled would be to manually check the SSI dashboard. The DCC informed the Working Group that it could provide an email notification when Incidents were created when a Device/Alert Code combination was being controlled. This received a mixed response form the Working Group, with some being in favour as this gave the desired notification, but others expressing concern that if this was an email for every Alert that this could cause administrative issues and create a backlog which would waste resources on the part of Users whose Devices generate large numbers of Alerts.

The Working Group elected to seek views from Parties as part of the Working Group Consultation to confirm which approach should be taken for notification. The Working Group Consultation returned an even split of respondents who saw benefit of being actively alerted in the case of incidents triggering the solution's mechanism and respondents who believed that this notification would cause administrative issues to them and negatively impact their business processes. The DCC, as the Proposer of the modification, took note of the consultation responses and altered the solution so that the User can choose whether to be notified by an email in the case of an incident triggering the mechanism or to not be notified by email, instead using the SSI dashboard to see when the mechanism is active.

~~Send back to the Refinement Process and further amendments~~

~~The Modification Proposal was approved to go to Change Board by the Panel on 19 July 2019. It was then sent out for a Modification Report Consultation, which received multiple comments back from Electricity Network Parties. Although receiving support from the other respondents initially, when presented to Change Board on 21 August 2019, the decision was to send the Modification Report back to the Working Group. The reasons cited by Network Parties were:~~

One respondent to the subsequent Modification Report Consultation had a concern that a significant number of incidents could be registered per Device in the DCC Incident Management System. In turn,

they believed this would increase both the DCC and User resource costs. The DCC believes that this concern will be covered by its "dead-banding" in the incident creation process. Under Alert Storm Protection only 1 in n (currently set to 500) Alerts will be delivered to the User. If the n limit is not reached within the configurable time period (currently set to 1440 minutes) then one Alert will be delivered to the User at this point. A new Incident will not be created unless the Alert count has been below the threshold for a continuous 1440 minute period.

The same respondent had concerns over the email system, asking whether building email functionality was the best choice of notification, considering that a large volume of email traffic would negatively impact both the DCC and Users. The DCC has stated that the email functionality would not be built from scratch, instead re-using the existing functionality in the DSMS, making it cost-effective. It further believes the Impact Assessment covered the effects that would be had on the DCC Systems, the DSMS and email systems.

Network Party concerns

Network Parties have cited a number of concerns with the proposed solution, including:

- They felt the solution in its current state would cause greater administrative burdens via email notification for every raised Incident than removing nuisance Alerts;
- The Alerts on the exemption list ~~did not include every Alert they wanted removed~~at the time; and
- The Modification Proposal deals more with the symptoms of the issue, rather than the root cause of why so many Alerts are being generated.

~~Once returned to the Working Group,~~ SECAS and the DCC arranged meetings to address the concerns raised by the Network Parties. After seeking additional feedback from the Electricity Network Parties who responded to the consultation, the DCC made amendments to the solution. These amendments included ~~changing~~extending the ~~frequency of reporting,~~deadband period so ~~instead of emailing in every incident, these~~that fewer incidents would be ~~added up and issued in a daily email.~~created (when enabled). This change was chosen due to the need for sufficient reporting while acknowledging the earlier concerns that emailing for every incident could cause administrative issues.

Who will manage the Exempted Alerts List and configurable parameters?

The DCC confirmed its support for the Panel to delegate responsibility to the Operations Group to oversee management of the reporting as well as the management of the Exempted Alert list and the wider solution mechanism's configurable parameters. The Working Group agreed with this but wanted the Security Sub-Committee (SSC) and the Technical Architecture and Business Architecture Sub-Committee (TABASC) to provide input to the Operations Group meetings where this is discussed.

~~**The addition of implementing the first stage of the solution in 'Monitor Mode' was also agreed with by the respondents. This would allow the industry sufficient time to prepare for when the Alert would be implemented whilst agreeing at the earliest opportunity confirmation of the solution's inclusion to a SEC Release. Finally, a clarification was made**~~**What is the longer-term plan for Traffic Management solutions?**

The DCC has stated that for other issues raised outside the scope of the Modification Proposal, future modifications would be the best route to pursue these. ~~The DCC proposed that future~~Future SEC modifications could be raised to address these particular issues:

- Creating a new configuration for different Alerts with different thresholds;
- Creating User- (or User Role-) specific configurations to account for Users who use differing configuration on Device; and
- Implementing changes to Device testing processes to further prevent generation of nuisance alerts, something raised by Network Parties to investigate the root causes of Alert Storms.

The DCC has stated that these will require DCC Assessments to assess in more detail.

~~Following this, an Ad-Hoc Working Group meeting was held on 19 November 2019 to clarify elements of the reporting and the solution. It was noted that there would be no material changes to the solution, ensuring that further DCC Assessment wouldn't be needed. It was stated that the email notifications would be turned off initially, and that it would be down to the individual User to reactivate them.~~

~~The DCC recommended, to avoid administrative issues via emailing in every incident case, that Users should wait until the number of Alert incidents fall to a manageable number before switching on email notification if they want. It stated the email notifications would be for all incidents, not just those relating to SECMP0062's solution. The DCC confirmed the reporting for the solution will be carried out by the SSI and the TOC to provide an update on which Alerts are being consolidated and to keep note of what Alert filtration is in effect. Additionally, the reporting will include the solution mechanism's parameter values and if any changes have been made.~~

~~The DCC confirmed its support for the Operations Group overseeing management of the reporting as well as the management of the Exempted Alert list and the wider solution mechanism parameters. The Working Group agreed with this but wanted the Security Sub-Committee (SSC) and the Technical Architecture and Business Architecture Sub-Committee (TABASC) to provide input to the Operations Group meetings where this is discussed.~~

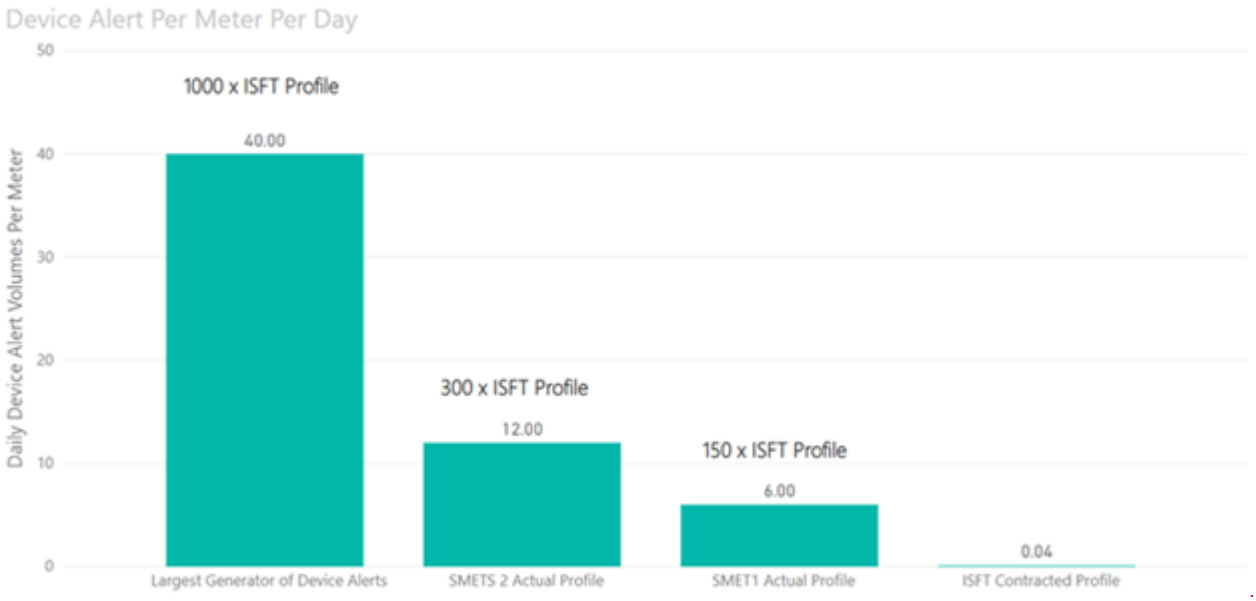
~~**Additional questions raised**~~

~~A question was raised around the level of SMETS1 Alerts and how they are affecting the DCC Systems currently, and whether the DCC System was designed to deal with the number of Alerts it is currently experiencing. The DCC responded that the number of SMETS1 Alerts are much lower than the number of SMETS2 Alerts. It stated that Alert volumes, as set out in the original 'Invitation to Submit Final Tender' (ISFT) contracts awarded by the Department of Energy and Climate Change (DECC), requires service users to scale to meet an average profile of 0.04 Device Alerts per meter per day. On 13 November 2019, SMETS1 meters generated on average six Device Alerts per meter per day (150 x the ISFT Profile); these volumes, although significantly higher than the ISFT profile, were suppressed by Device Alerts being switched off on a number of meters. On the same day for SMETS2 an average of 12 Device Alerts were generated per meter per day (300 x the ISFT profile). These are summarised in the graph below.~~

The Device Alert volumes for SMETS2 not only exceed the contracted volumes, but with a small number of Devices each responsible for thousands of device alerts per day, this geographically concentrates traffic on the CSP networks, compounding the problems caused by device alerts.

In summary:

- SMETS1 alerts are more geographically distributed and dispersed across five SMETS1 Alert codes, whereas 80% of SMETS2 alerts are accounted for by a single Alert code (8F3E – unauthorised access) and the majority are generated by a small number of devices
- The number of Alerts varies by Service User. The Service User receiving the most device alerts, receives them at a rate 1,000 times greater the contracted rate per meter per day.



8. Conclusions

Benefits and drawbacks

The Proposer and the Working Group have identified the following benefits and drawbacks in implementing this modification:

Benefits

- The main benefit of this modification is that it should prevent the overload of the DCC Systems as a result of an Alert Storm which would cause the DCC's DSP to fail and disrupt communications between Devices and Suppliers. If left unattended, the risk of Alert Storms causing this overload will continue to be an issue for the Service Users and the DCC where if the DSP does fail, this will incur both financial costs and time delays to the Service Users which could be avoided if this modification and its solution is enabled successfully. The DCC has quoted a rough order of magnitude cost from the DSP that stands at approximately £3 million to £3.5 million to cover the infrastructure demands that SECMP0062 could mitigate[1].

  The DCC provided a worked example of Alert Storm values carried out ~~over an eight-day window that had multiple repeated~~where 1 in 500 Alerts would be delivered to the User against the four Alert Codes entering the DCC Systems~~.~~ with the greatest volume. Under these conditions the example demonstrated a reduction of approximately ~~90~~99.3% of the repeated Alerts generated under this scenario~~.~~ reducing a total of 40,908,604 Alerts to 306,844. The DCC has confirmed this is only based on a single day's worth of Alert traffic, and that this may not be correct in all instances, especially where a large quantity of Devices are generating a small number of Alerts.

Drawbacks

- In Working Group discussions, a member raised the issue that the changes to the SEC may require compulsory changes to the DUIS, which could be unpopular with the wider industry if introduced quickly. This added a complication to the implementation approach which needed consideration given the Working Group wanted to have this Alert Storm protection as soon as possible. The two-stage implementation approach was proposed so that the DUIS changes could be implemented later.
- Another drawback that was raised in the Working Group was the timeline of the modification. The earliest time that the modification could be effective from is June 2020, due to the necessary length of the Refinement Process and implementation period needed for SEC Parties to carry out the changes that the modification proposes. This earliest time of implementation was criticised due to the desirability of the modification's solution and that it should be released ideally as soon as possible to gain the most utility from the protection it will provide against Alert Storms.

[1] See minutes for OPSG_27_0312

Proposer's rationale against the General SEC Objectives

Objective (a)[2]

The Proposer believes that SECMP0062 will better facilitate General SEC Objective (a) due to it allowing the DCC to better carry out their obligations as outlined in the SEC and improves the operation of Smart Metering Systems to a greater degree by providing additional protection to the DCC's DSP.

~~**Objective (e)[3]**~~

~~The Proposer believes that SECMP0062 will better facilitate General SEC Objective (e) due to it demonstrating innovation in improving communications between Service Users and the DCC by installing a mechanism which adds an element of Alert filtration alongside the existing detection programme in the DSP.~~

Working Group members' views

The Working Group ~~unanimously believe~~agreed that this modification better facilitates General SEC ~~Objectives~~Objective (a) ~~and (e)~~ for the reasons cited above.

Consultation respondents' views

The Working Group Consultation respondents returned a mixed set of responses. Five of the eight respondents were in favour of approving the modification and three were against it. The three respondents not in favour were Networks Parties whose reasons for rejecting the modification were due to not addressing the root cause of why such large quantities of Alerts are being generated. They suggested that the solution should be targeted at preventing the Devices generating such large quantities of Alerts, rather than filtering the Alerts after they've been sent.

In the first Modification Report Consultation, two Large Suppliers and the Security Sub-Committee were supportive. Four Electricity Network Parties were not supportive and expressed concerns as to how the reporting would be managed and that they would suffer administrative issues through Part 1 of the solution. Clarifications were made to the reporting following this and SECAS agreed with DCC that the email notification could be turned off so that email notifications would not cause administrative issues for Users.

In the second Modification Report Consultation respondents again returned a mixed set of responses. Three of the seven respondents were in favour of approving the modification and four were against it. The three respondents in favour were Large Suppliers, who believed that the Modification Proposal, whilst not directly dealing with root causes to Alert Storms, provides a solution to a considerable burden on the DCC Systems and should alleviate needless traffic. The four respondents who voted to reject were Network Parties who raised concerns that their previous comments weren't sufficiently addressed concerning the email notifications and that it still left the root causes of Alert Storms unchanged. The DCC responded to the concerns raised by Network Parties by explaining that a CSP based solution that would deal with the root causes would take approximately 2-3 years to develop. In the meantime, it stated that this provided a solution to a present and urgent issue.

[2] Facilitate the efficient provision, installation, operation and interoperability of smart metering systems at energy consumers' premises within Great Britain

[3] ~~Facilitate innovation in the design and operation of energy networks to contribute to the delivery of a secure and sustainable supply of energy~~

Sub-Committee views

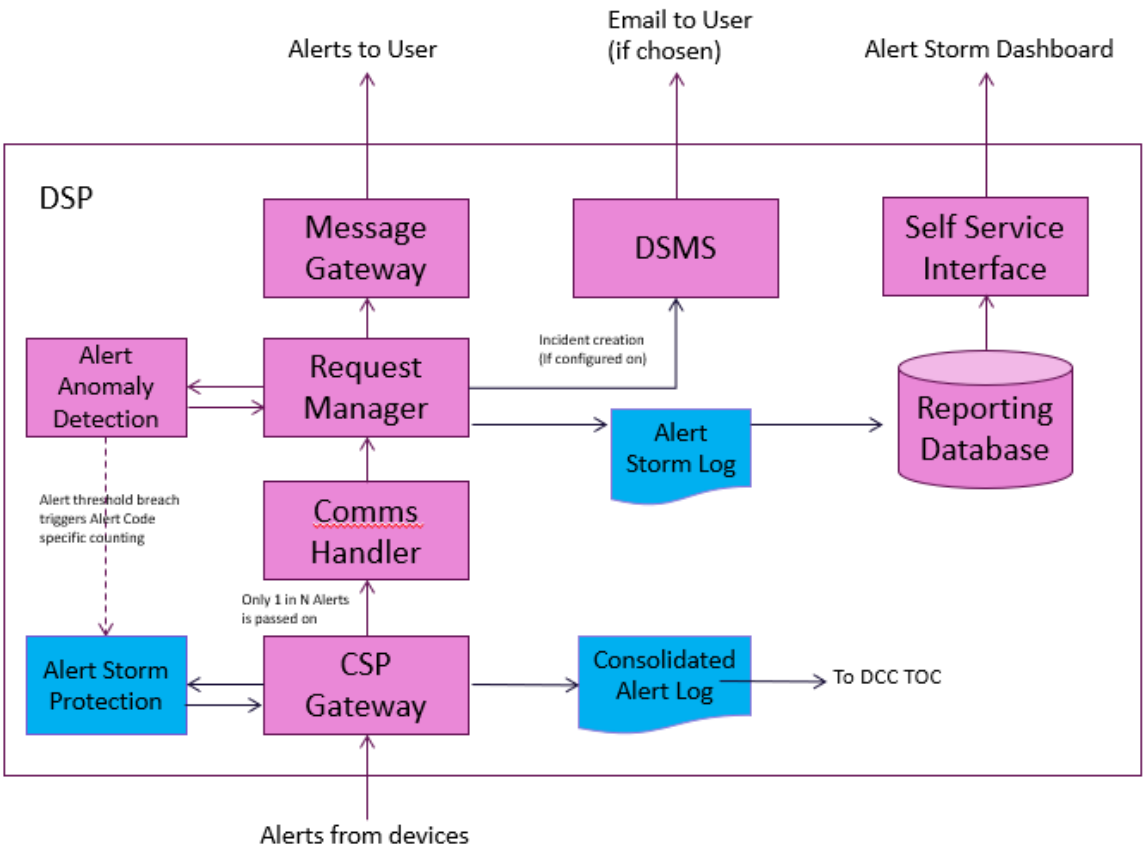
The SSC chairman was on the Working Group and attended one of the meetings when the business requirements were being formulated. The view provided on behalf of the SSC was that security Alerts should not be restricted. They stated a solution could be supported where a list of exempted security-related Alerts that will not be subject to throttling or subject to a different level of throttling can be approved by the SSC and for SSC to receive regular reports.

~~SEC~~The Operations Group agreed to have oversight of the reporting and manage any issues which might arise from the reporting. In addition, this group will have the responsibility to review and update the configuration parameters.

Panel's conclusions

The Panel agreed this Modification Proposal is ready to proceed to a decision under Self-Governance.

Appendix 1: DCC Systems changes



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**
CSP	Communication Service Provider
DCC	Data and Communications Company
DECC	Department of Energy and Climate Change
DSMS	DCC Service Management System
DSP	Data Service Provider
DUIS	DCC User Interface Specification
ISFT	Invitation to Submit Final Tender
PIT	Pre-Integration testing
S1SP	SMETS 1 Service Provider
SEC	Smart Energy Code
SIT	System Integration Testing
SMETS	Smart Metering Equipment Technical Specification
SSC	Security Sub-Committee
SSI	Self Service Interface
SSMI	Self Service Management Interface
TABASC	Technical Architecture and Business Architecture Sub Committee
TOC	Technical Operations Centre
UIT	User Integration Testing

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

Harry Jones

020 7081 3345

harry.jones@gemserv.com

Smart Energy Code Administrator and Secretariat (SECAS)

8 Fenchurch Place, London, EC3M 4AJ

020 7090 7755

sec.change@gemserv.com