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 1.0

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

1. Summary 3
2. Background 4
3. Solution 5
4. Impacts 6
5. Costs 8
6. Implementation approach 9
7. Discussions and development 10
8. Conclusions 12

Appendix 1: Glossary 14

This document also has five annexes:

- **Annex A** contains the business requirements for the proposed solution.
- **Annex B** (standalone document) contains the redlined changes to the Smart Energy Code (SEC) required to deliver the proposed solution.
- **Annex C** contains the 'Northbound 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 full Working Group 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 it repeatedly and rapidly generates 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.

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 defined time window. If the Device sends the same Alert above a pre-determined threshold value, the mechanism will discard 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. Discarded 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 cost of implementation for this modification is approximately £1 million. The proposed implementation date for this modification is the November 2019 SEC Release for the core solution and the November 2020 SEC Release for the enduring reporting arrangements.

2. Background

Context to DCC Systems Communications

The DCC and Service Users communicate through the use of DCC Systems for sending 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 their 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. The DCC thereby needs to take direct action to protect their systems to ensure availability of the service for their Service Users and incorporate a new means of traffic management to prevent, where possible, excess Alerts from entering their system.

SECMP0062 was raised by the DCC on 27 September 2018 to resolve this issue.

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 discard excess Alerts from the Device and only forward one, in a configurable number of Alerts (N) per designated period, on to the intended Users. Discarded Alerts will be counted for Anomaly Detection purposes and Service Users will be notified ahead of time for the exact actions being taken.

The mechanism operates by periodically checking the total number of Alerts generated to see if it exceeds a “red” threshold anomaly – the point at which too many Alerts in that specific Alert Code will trigger the solution’s mechanism. If a “red” threshold anomaly is detected at the Device level, the mechanism counts each specified Alert Code. If the counter for an Alert exceeds its limit in the designated timeframe, the code will be marked as “overloaded”.

If an Alert Code isn’t “overloaded” it is passed on to Request Management. If an Alert Code is “overloaded” it will allow only 1 in N Alerts to be let through, with the count of the remaining 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 Alert Codes will be cleared.

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 which is 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. During this stage, the Self Service Interface (SSI) will act as the means of reporting to inform Service Users whether any Alert Storm Protection is currently active for any of their Devices. The DCC will also be able to provide email notification to Users when a device/Alert Code combination is being controlled, it’s the User’s choice whether they are actively emailed in every incident occurrence or won’t receive an email in any instance.
- 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 business requirements for this solution can be found in Annex A.

Legal text

The changes to the SEC required to deliver the proposed solution can be found in Annex B. The ‘Northbound 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

Supplier Parties, Network Parties and Other SEC Parties will be subject to the effects of the throttling effects and discarding 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

DCC System

The DCC Systems will be impacted due to adding the mechanism which delivers the solution set out in this Modification Proposal.

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 will not be impacted.

5. Costs

DCC costs

The estimated 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. A breakdown of costs by part will be sought and an update provided to the Panel on this.

The DCC has informed the Panel that they would absorb the post-PIT costs of any modifications implemented as part of the November 2019 SEC Release, meaning there would be no post-PIT costs attributed to Part 1 as long as it is implemented as part of this release.

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, amounting to approximately £2,400. The activities needed to be undertaken for each Stage are:

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

SEC Party costs

Parties were consulted on to request any individual costs they would incur as part of the Working Group Consultation. The 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

Agreed implementation approach

The SEC Panel agreed a two-part implementation approach where:

- Part 1 will be implemented on **7 November 2019** (November 2019 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 21 August 2019.

This approach was put forward due to the DCC's Impact Assessment identifying a six-month lead time to deliver the modification's full solution, meaning it would not be possible to include Part 2 in the November 2019 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.

7. Discussions and development

Will the mechanism in the proposed solution have unintended consequences in its filtration 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 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 'Northbound 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 them) before they take effect.

What is the scope 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 analysis that suggests if the mechanism they have designed is implemented, it should eliminate approximately 90% 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 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 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 they 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 they 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 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 there be some form of active notification being given to Users when the Alerts are being controlled, 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 they could provide an email notification 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.

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 provided a worked example of Alert Storm values carried out over an eight-day window that had multiple repeated Alerts entering the DCC Systems. Under these conditions the example demonstrated a reduction of approximately 90% of the repeated Alerts generated under this scenario.

Drawbacks

- In Working Group discussions, a member raised the issue that the changes to the SEC may require compulsory changes to 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 was the timeline of the modification. The earliest time that the modification could be effective from is November 2019, 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, or otherwise it could fall back to 2020. 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.

Proposer's rationale against the General SEC Objectives

Objective (a)[1]

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.

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

Objective (e)[2]

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 that this modification better facilitates General SEC Objectives (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.

Sub-Committee views

The Security Sub-Committee (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.

Panel's conclusions

The Panel agreed that this modification is ready to proceed to a decision as a Self-Governance Modification.

[2] (e) Facilitate innovation in the design and operation of energy networks to contribute to the delivery of a secure and sustainable supply of energy

Appendix 1: 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
DSP	Data Service Provider
DUIS	DCC User Interface Specification
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
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

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'

Annex A

Business requirements – version 1.0

About this document

This document outlines the detailed business requirements for SECMP0062.

Summary

The DCC and Service Users communicate through the use of DCC Systems for sending 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 system. This system is also vulnerable to Alert Storms, a state where individual Devices will encounter a scenario where they 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 that have to use the same system as a means of communication. 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 the system.

This solution will protect against the scenario in which a specific Alert is generated repeatedly and rapidly by individual Devices. However, it is noted that it will not, and is not intended to, protect the DCC Systems against a large quantity of Devices that generate a small number of alerts which enter the DCC Systems (e.g. due to a power outage over a large area).

Business Requirements

Requirement 1: The DCC will implement a mechanism that will block Alerts from entering the DSP Central System and being routed on to the User where the number received exceeds a given threshold.

The DSP (Data Service Provider) System will monitor the number Alerts received from a Device. When the total number of Alerts received from an individual Device within a rolling time period T exceeds a threshold A, an incident is created for that Device.

While an incident is open, the DSP System will monitor the number of each specific Alert received from the Device. When the total number of copies of a specific Alert received from the Device within a rolling time period R exceeds a threshold B, the Device/Alert combination will be marked as overloaded and an additional incident is created for that specific Device/Alert.

As part of the Impact Assessment, DCC will specify the expected Service Level Agreements for DCC and DCC Users to respond to incidents.

When a Device/Alert combination is marked as overloaded, only 1 in N copies of the Alert will be passed to the User, with all other copies being blocked by the DSP System. The copies of the Alert that are allowed through will still be subject to the normal Target Response Times.

A Device/Alert combination will no longer be overloaded when the number of copies of that Alert received in a rolling time period R falls below threshold B. At this point, those Alerts will no longer be blocked. The number of blocked Alerts will still be counted in determining this threshold.

The values to be set upon implementation of SECMP0062 are:

- T = 30 minutes
- A = 50
- R = 5 minutes
- B = 10
- N = 10

The values of T, A, R, B and N will be configurable values in the DSP System that can be changed at any time. They will not be hard-wired into the System.

The parameters will be ‘global’ values that are applicable to all DCC Users. It will not be possible for different Users to set different values specific to them.

This process will be applied to all SMETS (Smart Metering Equipment Technical Specification) 2 Alerts. It will also be applied to any SMETS1 Alerts that have been mapped to an equivalent SMETS2 Alert.

As part of the Impact Assessment, DCC is asked to provide details of what will happen to blocked Alerts in terms of storage and discarding.

Requirement 2: The relevant User will be notified when Alerts have been subject to throttling.

Users will be notified that Alerts have been blocked through the non-mandatory metadata fields of those Alerts that are allowed through. Users will be required to update their systems if they wish to be able to receive this additional information.

It is expected that this requirement will be implemented through a new DCC User Interface Specification (DUIS) version.

The Working Group is considering the potential for a staggered implementation approach where Requirements 1, 3, 4, 5 and 6 are implemented as soon as possible while the DUIS changes for Requirement 2 are implemented in a later SEC Release. To inform the appropriate way forward, DCC is asked to provide an approach to be taken for alerting DCC Users in the interim period, to include the expected time period in which DCC Users will be notified of when the throttling of Alerts begin if the mechanism is in operation, as part of its Impact Assessment response.

Additionally, as part of the Impact Assessment response, DCC is asked to provide a full analysis of a solution with email notification during the first stage during this staggered approach, and one without.

Requirement 3: There will be a configurable list of exempted Alerts that will not be subject to throttling or subject to a different level of throttling.

The DSP System will contain a configurable list of Alerts that will not be subject to this mechanism or will be subject to this mechanism but with different values for the parameters R, B and/or N. The number of copies of these Alerts received will still be used to determine a breach of the threshold A. This list should be capable of being updated at any time and will not be hard-wired into the System.

Any variations set using this Requirement 3 will be 'global' variations that are applicable to all DCC Users. It will not be possible for different Users to set different values specific to them.

Requirement 4: DCC will not amend the list of exempted Alerts without approval from the Panel or a delegated Panel Committee.

DCC will not amend the list of exempted Alerts without obtaining approval from the Panel (the Panel may delegate this responsibility to a Panel Committee determined by the Panel).

Requirement 5: DCC will not change the values of the parameters without approval from the Panel or a delegated Panel Committee, except in well-defined exceptional circumstances.

DCC may change parameter values without consent in clearly defined circumstances which will be agreed as part of the solution definition in response to an urgent need to amend one or more parameters. It will then retrospectively report any changes of these to the Panel.

Otherwise, DCC will not change the values of parameters without obtaining approval from the Panel (the Panel may delegate this responsibility to a Panel Committee determined by the Panel).

As part of the Impact Assessment, the DCC is asked to provide examples of where it would need to urgently respond to events that warrant a rapid change of the parameter values. The Working Group will use this to determine if any such circumstances should be defined.

Requirement 6: DCC will provide reporting on the use of throttling of Alerts.

DCC will report on how often the mechanism introduced under SECMP0062 is used. This will cover the number of incidents raised and the number of Device/Alert combinations that are classed as overloaded within a given reporting period. As part of this report, DCC will provide a full updated list of Alert parameter values and any exempted Alerts or Alerts with different parameters, so DCC Users know which restrictions are placed against each types of Alert.

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'

Annex C

Northbound Traffic Management Mechanism Document

Purpose of this Document

This document has been prepared in accordance with SEC Section H3.30 where the Alert Management Mechanism implemented by the DCC has its mechanism parameters and exempted Alert Codes clearly defined.

Parameter Values

Parameter	Summary	Value
A	Device Alerts Threshold	50
T	Device Alerts Time Window	30 minutes
B	Individual Alert Threshold	10
R	Individual Alert Time Window	5 minutes
N	Number of dropped alerts between forwarded alerts	10

The parameters above are global settings and will apply equally to all devices and alerts, unless that alert code is on the Exempted Alert Code list below.

When a Device/Alert Code is marked as overloaded and the protection mechanism is active, the Alerts to be dropped will be logged and counted but then discarded from the system.

Exempted Alert Codes

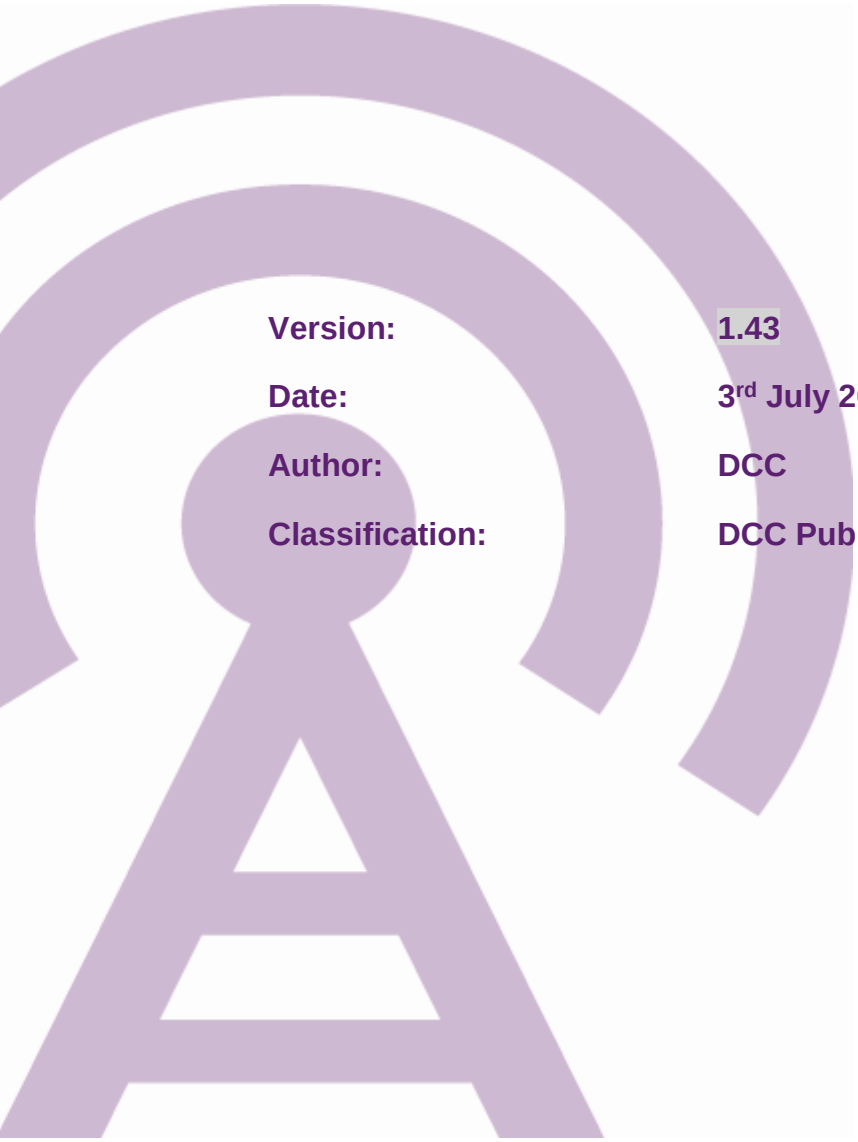
The following Alert Codes are to be exempt from the global settings applied to all Alerts by the Northbound Traffic Management Mechanism. This list will be subject to change through the sub-committee designated by the Panel.

Exempted Alert Codes
0x8F78 Unauthorised Physical Access - Other
0x8F77 Unauthorised Physical Access - Second Terminal Cover Removed
0x8F76 Unauthorised Physical Access - Terminal Cover Removed
0x8F75 Unauthorised Physical Access – Strong Magnetic field
0x8F74 Unauthorised Physical Access - Meter Cover Removed
0x8F73 Unauthorised Physical Access - Battery Cover Removed
0x8F3F Unauthorised Physical Access - Tamper Detect
0x8F1F Low Battery Capacity
0x8F1D GSME Power Supply Loss
0x81C0 Supply Disconnect Failure
AD1 Power Outage
0x8F36 Power Restore
0x8F35 Power Restore

SEC Modification Proposal, SECMP0062

Alert Storm Protection

DCC Full Impact Assessment



Version:	**1.43**
Date:	**3rd July 2019**
Author:	**DCC**
Classification:	**DCC Public**

Contents

1 Introduction 3
2 Impact on DCC's Systems, Processes and People 5
3 Impact on the SEC....17
4 Testing Considerations....18
5 Implementation Timescales and Releases....19
6 DCC Costs and Charges....20
7 RAID....22
8 Related Documents....23

1 Introduction

1.1 Document Purpose

The purpose of this DCC Full Impact Assessment (FIA) is to provide the relevant Working Group with the information requested in accordance with SEC Section D6.9 and D6.10.

1.2 Previous information provided by DCC

The DCC Preliminary Assessment was provided on 31/01/2019.

1.3 DCC Contact Details

Please raise any queries regarding this DCC Impact Assessment using the contact details provided below.

Name	DCC - SEC Modification queries
Contact email	mods@smartdcc.co.uk

1.4 Modification Description

This modification is to enable the implementation of a traffic management solution to protect the DCC (Data Communications Company) system and Service Users against alert storms originating from a single device.

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 generate the same device alert, adding unnecessary traffic to the Communication Service Provider (CSP) Gateway, which in turn results in increased traffic between the DCC Systems and Service Users. Currently there is little protection against alert storms, meaning that multiple alerts are entering the gateway, rather than being filtered out, even after recognising they originate from the same single device.

1.5 Requirements

The requirements for this modification have been developed by the Working Group during the Refinement phase and are documented in the Business Requirements v1.0 document [Ref 1] and summarised below. The impact on DCC has been assessed against these Business Requirements.

BR #	Summary	Relevant Sections of this document
1	*The DCC will implement a mechanism that blocks Alerts from entering the DSP System where the number received exceeds a given threshold.*	Section 2
2	*The relevant User will be notified when Alerts have been subject to throttling.*	Section 2.1 Section 2.1.3 Section 2.1.4 Section 2.1.9
3	*There will be a list of exempted Alerts that will not be subject to throttling or subject to a different level of throttling.*	Section 2.1.2
4	*DCC will not amend the list of exempted Alerts without approval from the Panel or a delegated Panel Committee.*	Section 2.1.11
5	*DCC will not change the values of parameters without approval from the Panel or a delegated Panel Committee, except in well defined exceptional circumstances.*	Section 2.1.11
6	*DCC will provide reporting on the use of throttling of Alerts*	Section 2.1.12

2 Impact on DCC's Systems, Processes and People

This section describes the impact of SECMP0062 on DCC's Services and Interfaces that impact Users and/or Parties.

2.1 Description of Solution

In the Preliminary Impact Assessment [Ref 2], a two stage implementation approach was proposed to enable early implementation of the core functionality with the DUIS Alert specification changes following later.

Stage 1 of the solution will incorporate:

A Core Alert Storm Protection mechanism, that will provide a means of counting and discarding excess alerts. Generate anomaly events and initiate incidents. Create event and discarded alert records for reporting and monitoring.

To provide visibility of system activity, a dashboard will be provided in the SSI (Self Service Interface) and SSMI (Self Service Management Interface). When the protection mechanism is activated for a specific device/alert code combination an anomaly event will be recorded and will result in the creation of a DSMS (DCC Service Management System) Incident.

Specific alert codes may be configured to be excluded from the protection mechanism. This will be a global configuration.

Protection mechanism events and discarded alerts will be recorded, and used to form the basis of defined reports.

No changes to User systems will be required for this stage.

Stage 2 of the solution will incorporate:

Changes to the Alert Structure specification within the DUIS (DCC User Interface Specification). These changes will provide real time notification of alert throttling and enable Users to leverage this if required. To achieve this Users would need to implement the update to DUIS.

The details of the Stage 2 functionality are in section 2.1.9.

2.1.1 Core Alert Storm Protection Processing

The DSP system already includes an anomaly detection solution for northbound alerts from a single device. This follows a pattern where alerts are counted over a configured time period (for example 30 minutes). If the total number in that rolling time period exceeds a configured threshold (defined by amber and red levels) then an anomaly is reported via the security log and a DSMS (DCC Service Management System) incident is created.

However the existing anomaly process does not protect the service by either quarantining or limiting alert volumes.

In order to protect the system from high volumes of northbound alerts, the existing anomaly detection service will be extended as follows.

1. When the number of Alerts from a given device within time window [T] exceeds the threshold value [A] the system will begin to count the number of Alerts from that device on a per Alert Code basis.

2. If any individual Alert Code count within time window [R] exceeds the configured threshold value [B] then that Originating Device/Alert Code[1] combination will be marked as being 'overloaded'.

3. If an Alert Code is marked as 'overloaded' for a device, then only one in every [N] such Alerts will be processed. All other Alerts with that same Alert Code from the same device will be discarded.

4. Once the rate of Alerts for the device falls below threshold [A] then the specific Alert Code counting will stop and any overloaded Alert Codes will be cleared. Alert processing will then return to normal.

The initial proposed configuration parameters are:

Parameter	Summary	Value
A	Device Alerts Threshold	50
T	Device Alerts Time Window	30 minutes
B	Individual Alert Threshold	10
R	Individual Alert Time Window	5 minutes
N	Number of dropped alerts between forwarded alerts	10

The parameters above are global settings and will apply equally to all devices and alerts., unless that alert code is on the excluded list.

When a Device/Alert Code is marked as overloaded and the protection mechanism is active, the Alerts to be dropped will be logged and counted but then discarded from the system.

[1] Uniqueness of counts will be by Originating Device AND Alert Code

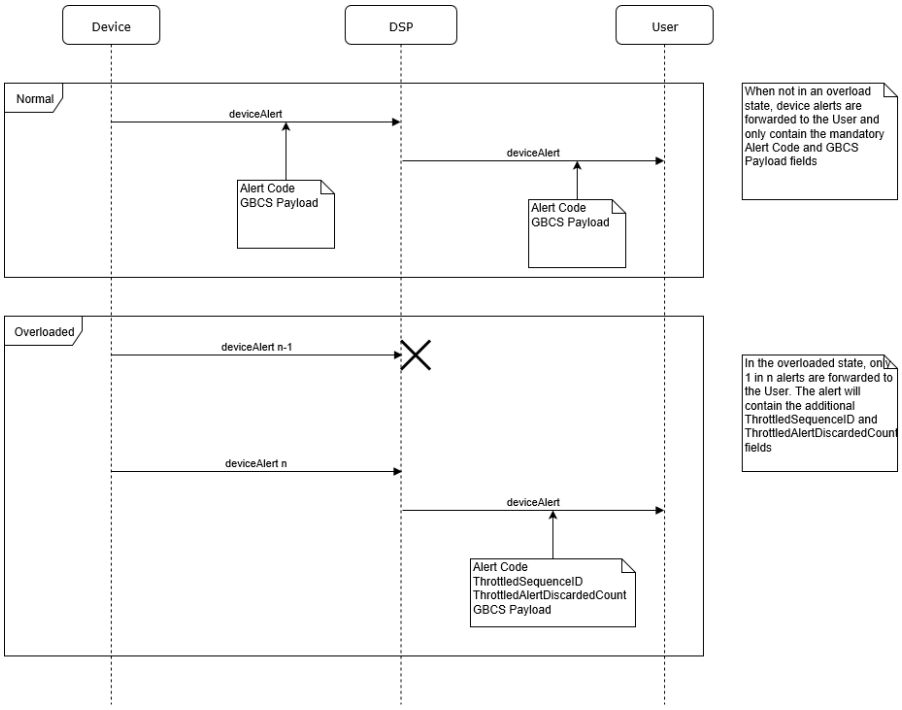


Table 1 Normal and Overloaded message flows

The diagram below shows the existing sub-components impacted due to this change and the new sub-components that are required to be built along with the key steps involved.

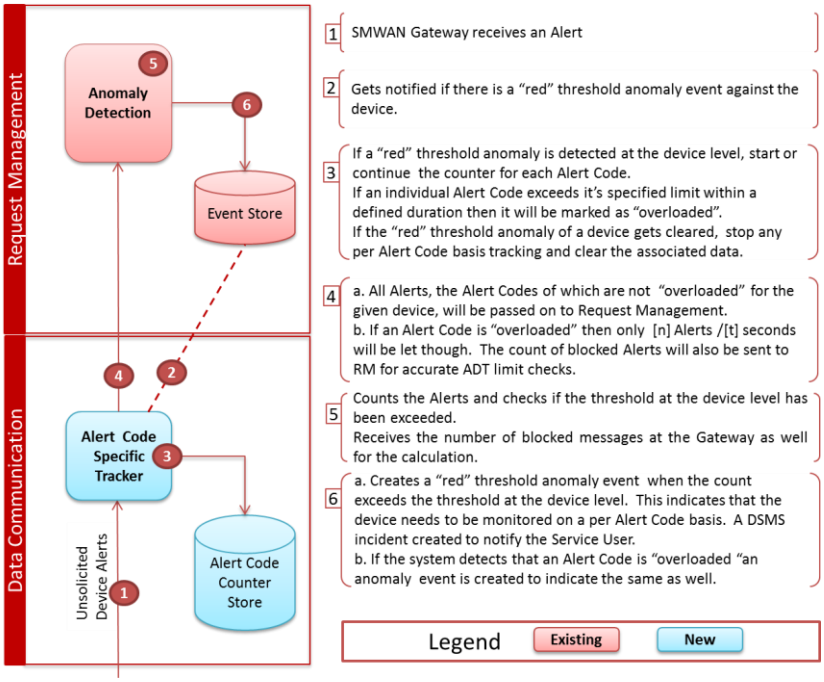


Figure 1: Northbound Alert Protection - Steps involved

2.1.2 Configuration Settings

The Alert Code Threshold settings will be managed using application configuration parameters, similar to the way the generic northbound ADT settings are managed currently. These configuration parameters will be global, i.e. apply to all Users, Devices, and Alert Codes (with the exception of exempted Alert Codes).

The list of Alert Codes, which shall be exempted from the Alert Storm Protection processing, will also be managed using application configuration parameters. DCC assumes that an agreed list of exempt Alert Codes will be provided by the SEC Panel or a delegated committee such as TABASC.

2.1.3 Status Dashboard

A new Self Service Interface (SSI) dashboard for Service Users will be built using the existing dashboard design principles. This dashboard will provide the Alert Storm Protection data to the Service Users, which will include the following details.

- Devices that exceed the threshold;
- Alert Codes that are subjected to Alert Storm Protection processing for each Device;
- Number of Alerts received for each Alert Code per device;
- Number of Alerts discarded for each Alert Code per device.

These would be ‘live’ views, and with an ability to view and download historic data. Users will only be able to see details of devices for which they have a defined Role.

2.1.4 DSMS Incident Management Strategy

Incidents may be created by the Device Level threshold and the Alert Code threshold being breached. A notification of an incident may also be sent be email to a User. However Alert Storm Protection may initiate rapidly and potentially frequently if a device is generating alerts close to threshold values.

To avoid large number of incidents being created a revision to the anomaly events handling mechanism will limit the number by introducing a deadband duration between the events as shown in the diagram below.

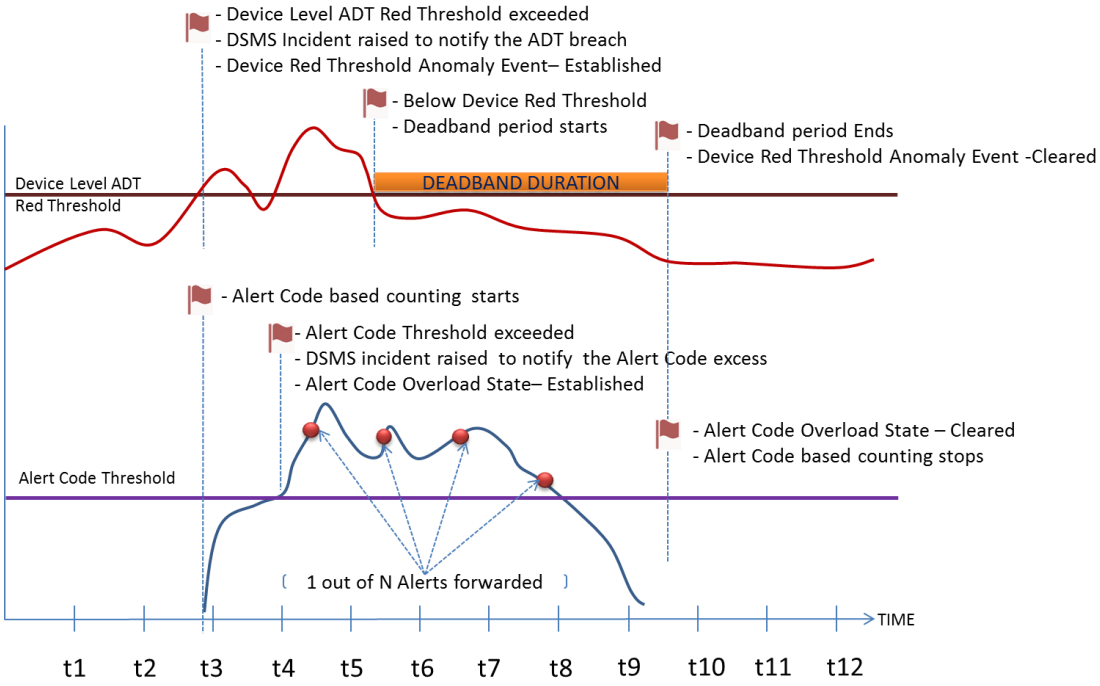


Figure 2 Incident Management and Deadband duration

The device threshold anomaly event will be cleared only when the number of alerts falls below the threshold and stays below that threshold for a configurable deadband period.

If the rate drops below the threshold and then rises above the threshold again within the deadband period then a new anomaly event will not be created, instead the rise will be linked to the existing anomaly event. The previous deadband period will be cancelled and will be restarted once the rate falls below the threshold again. This mechanism allows longer time windows between events, resulting in a reduced number of DSMS incidents being created.

Additionally, creation of the following Traffic Management incidents will be configurable:

- DSMS incident created to notify the generic ADT threshold breach;
- DSMS incident created to notify the Alert Code specific threshold breach.

When an incident is created it will be assigned to the Target recipient of the Alert. If the alert is from a PPMID then the DSP will assign the incident to the Lead Supplier.

Email notification of incident creation can be enable/disabled on a per Service User basis – this will be a global setting for that User and applies to all incidents not just those for Alert Storms.

2.1.5 Feature Switches

This CR will be built behind multiple Feature Switches:

- A Feature Switch to manage the introduction of Alert Storm Protection;
- A Feature Switch to control whether the Device alerts are actually discarded;
- A Feature Switch to control whether the Discarded Alert Log is delivered to DCC.
- A Feature Switch to enable the DUIS Alert Format change.

Feature switches provide flexibility by allowing new features and functionality to included in a release, tested, and then disabled until required. This potentially allows environment usage to be optimised.

2.1.6 Affected Components

Data Communication

The Data Communication component will need to introduce the following new functions:

- A mechanism to determine when to start/stop tracking the number of alerts on a per Alert Code basis at a device level and the associated housekeeping functions;
- Any message that is allowed to be passed on to Request Management (and subsequently to Anomaly Detection) while an alert is “overloaded” will include the number of alerts that are discarded at the CSP Gateway;
- The discarded alerts will be recorded in a “Discarded Alert” log at the CSP Gateway. This log will be transferred to the DCC via the Enterprise Systems Interface every 15 minutes in a similar fashion to the Service Audit Trail. (Noting that if no data exists for a 15 minute period then no log file will exist and no data will be transferred).

Anomaly Detection

Anomaly Detection will introduce a mechanism used by Data Communication to notify the number of alerts that are blocked at the CSP Gateway. This is required to perform a correct calculation of the breach of ADT levels.

Data Management / Data Model

Data Management will require changes to support the new anomaly detection level configuration for tracking on a per Alert Code basis.

Data Model changes are required to support the new alert tracking mechanism.

Request Management

Request Management will need to introduce new alarm identifiers to differentiate the Traffic Management incidents that are raised because of overloaded alerts. The creation of these incidents will be made configurable.

Request Management will receive additional information about the discarded alerts from Data Communication when a Device Alert is passed through to Request Management for onward delivery to the User. Request Management will record this additional information in a Traffic Management log. This log will contain the details that will be displayed in the SSI dashboard. In situations where the alerts are targeted at the ACB (for example alerts from PPMIDs) then the corresponding Service User Id shall be included in the logs. The Traffic Management log will be transferred to the Reporting Database component.

Reporting Database

The Reporting Database will process the Traffic Management log and create a set of aggregated data at 15-minute intervals, which will be used by SSI/SSMI.

SSI/SSMI

The SSI (Self Service Interface) will need a new dashboard to present the details of blocked Alerts and the associated Device to the Service Users. This data comes from the aggregated Traffic Management Log data held in the Reporting Database.

The same dashboard will be made available via SSMI for use by DCC and DSP.

Incident Client

The existing interface for creating incidents will not require any changes.

DCC Service Management System

A change will be needed to support a new incident type(s) to notify the overloaded alerts. This requires a new Remedy Incident Template(s) and configuration for the new DSP alarm identifier(s).

In addition, the assumption is that the DCC requires all alert monitoring incidents to be automatically assigned to the related Service User. This will be achieved by new auto-triage workflow.

Once the rate of alerts for the device falls below the red threshold level then the specific alert code counting will stop and any overloaded alert codes will be cleared. However, any related open incidents will need to be resolved by the Service User or DCC in accordance with the DCC incident handling procedures.

The following activities will be required for DSMS:

- Update of the DCC SMS Design documents to include a new incident type;
- Co-ordinating the production of the Remedy Incident Template with DSP and DCC Operations;
- Configuration of the data load template and linkage to DSP alarm identifier on all Remedy environments;
- PIT Testing;
- Support for post-PIT Testing for all environments.

There are a number of BAU support activities required:

- Production deployment of data load template configuration and linkage to DSP alarm identifier;
- Receive knowledge transfer for the solution changes;
- Release management.

Operational Monitoring

The changes made under this CR will need to be integrated with the DSP's operational monitoring facilities.

Events created for alert code specific anomaly thresholds being breached or cleared will be tracked and reported in the DSP operational monitoring tools.

Events or alarms created by the DSP operational monitoring tools will be available for distribution to the DCC. It is expected that any operational integration to DCC systems will be a separate improvement item to be elaborated and implemented under a separate Change Request.

2.1.7 Non Functional Impacts

Impact on Performance

DCC does not expect that there will be a material impact on system performance as a result of this modification. This will be validated by the use of some specific regression tests during the implementation phase.

Impact on Resilience

There is no impact on the underlying resilience of the DSP solution.

Impact on Disaster Recovery

There is no change to the Disaster Recovery solution or BCDR procedures.

Impact on Security

This change includes the implementation of a traffic management solution in the northbound highway. There is no impact on the Protective Monitoring because there is no new infrastructure.

Once the traffic management solution is designed there may be a need to include it within scope of a future penetration test to ensure it is configured correctly.

Security Assurance will be provided to:

- Support to the PIT Team during implementation
- Review of design document where there is a potential security consideration
- Review of changes to the security audit trail logging
- Review of test artefacts and outcomes where there is a potential security consideration
- Attendance at meetings where required by the PIT Team

2.1.8 Impact on processing, storage and/or transmission of the DCC Data

No material impact has been identified on the processing, storage and transmission of DCC Data from the proposals within this Change.

However DCC is already seeing volumes of alerts in excess of forecast values. If this Change were not to be implemented then there would be an impact on the DCC systems.

2.1.9 Impact on Interfaces

For Stage 2 changes will be made to the Device Alert Structure and the DCC Alert Structure as defined in DUIS.

DeviceAlertMessage Format

The DeviceAlertMessage format is applicable to SMETS2 or later Device Alerts. This message combines the GBCS Payload received from the Device with the Alert Code extracted from the GBCS Payload. If an Alert Code is subject to throttling, two new optional data elements are included for the sequence number of the passed through alert and the count of discarded alerts:

- ThrottledAlertSequenceID
- ThrottledAlertDiscardedCount

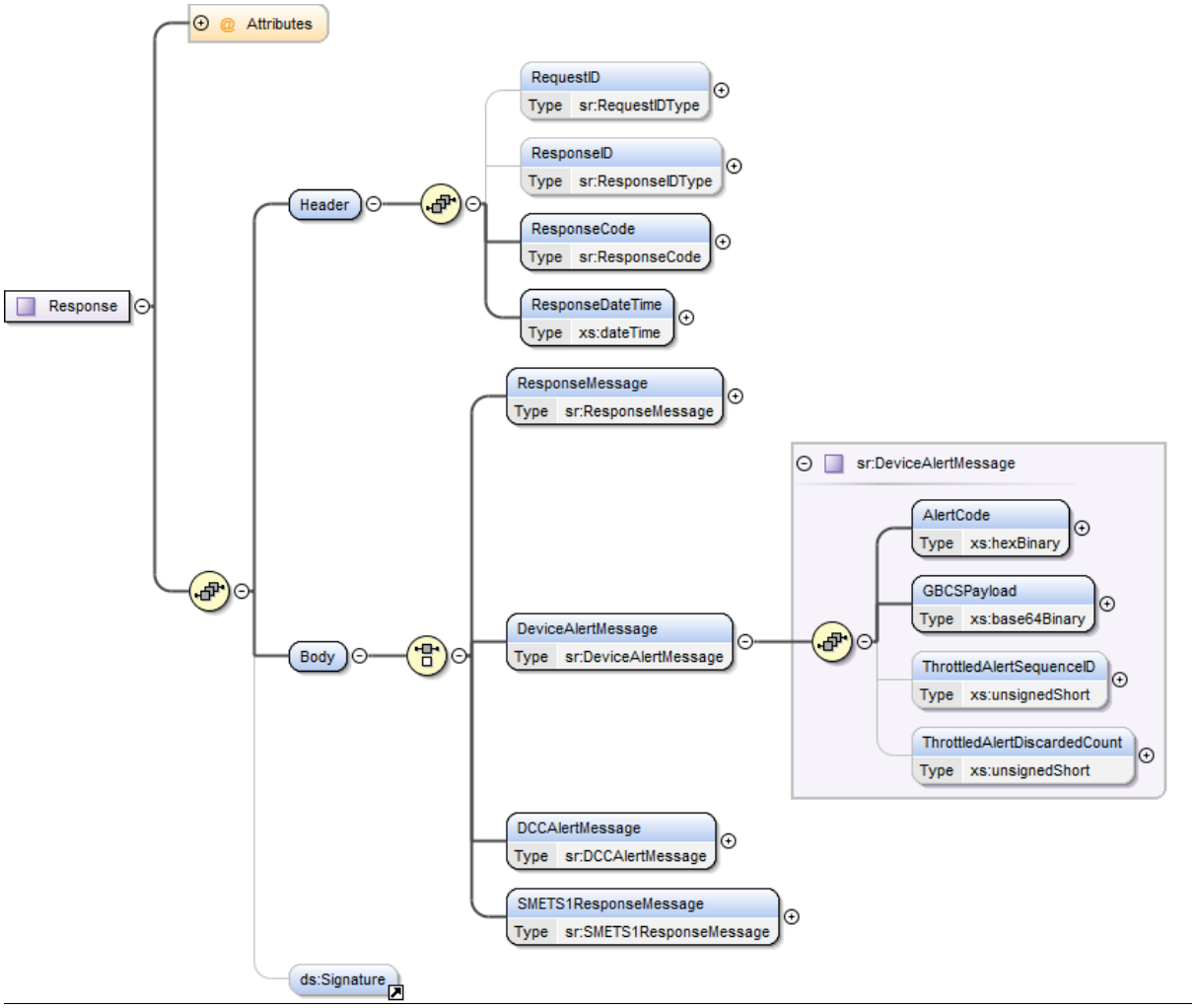


Figure 3 - DeviceAlertMessage Structure

Data Item	Description / Valid Set	Type	Mandatory	Default	Units	Sensitivity
AlertCode	Code indicating the alert or reason for the alert to be generated GBCS includes '0x' at the start of such codes. This definition uses a hexBinary representation for valid values. Valid set: See GBCS for base list and apply hexBinary representation of these GBCS defined values	xs:hexBinary	Yes	None	N/A	Non-Sensitive
ThrottledAlertSequenceID	An optional data item that identifies that this Alert Code is currently subject to throttling by the DCC Data Systems. If this attribute is included in the Alert then it indicates the sequence number for this Alert message since Alert throttling began.	xs:unsignedShort	No	None	N/A	Non-Sensitive
ThrottledAlertDiscardedCount	An optional data item used to indicate the number of Alerts that have been discarded by DCC Data Systems since the last Alert was forwarded to the Service User.	xs:unsignedShort	No	None	N/A	Non-Sensitive
GBCSPayload	See GB Companion Specification for Details for message construction. For Critical Device Alerts: Grouping Header || Alert Payload || 0x40 || SMD Signature For Non-Critical Device Alerts: MAC Header || Grouping Header || Alert Payload || 0x00 || SMD-KRP MAC	xs:base64Binary	Yes	None	N/A	N/A

Figure 4 - DeviceAlertMessage Format

DCCAlertMessage Format

The DCCAlertMessage format is applicable to DCC Alerts generated by the DCC Data Systems.

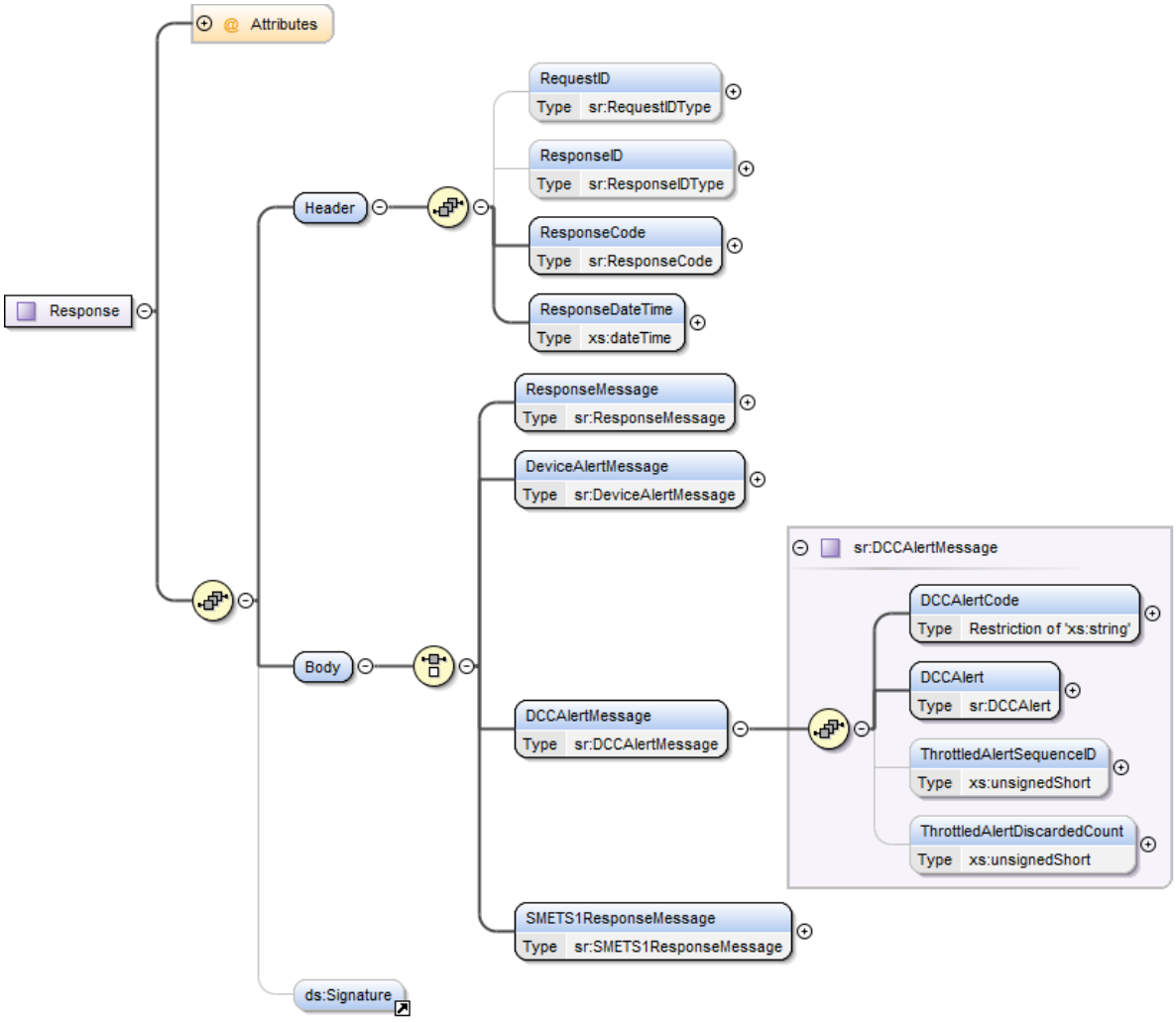


Figure 5 - DCCAlertMessage Structure

There are circumstances where the Device Alert may have to be delivered to the User as a DCC Alert (e.g. Alerts from a PPMID). Two new attributes will need to be added to the definition of the DCC Alert in a similar fashion to the DeviceAlertMessage structure.

Data Item	Description / Valid Set	Type	Mandatory	Default	Units	Sensitivity
DCCAlertCode	Code indicating the Alert or reason for the Alert to be generated by DCC Valid set: See Table 49	Restriction of xs:string (Enumeration)	Yes	None	N/A	Non-Sensitive

Data Item	Description / Valid Set	Type	Mandatory	Default	Units	Sensitivity
DCCAlert	This is body specific content dependent on the DCCAlertCode being sent. See section 13 and Annex 16 for body specific format.	Sr:DCCAlert See section 13 and Annex 16	Yes	None	N/A	N/A
ThrottledAlert SequenceID	An optional data item that identifies that this Alert Code is currently subject to throttling by the DCC Data Systems. If this attribute is included in the Alert then it indicates the sequence number for this Alert message since Alert throttling began.	xs:unsignedShort	No	None	N/A	Non-Sensitive
ThrottledAlert DiscardedCount	An optional data item used to indicate the number of Alerts that have been discarded by DCC Data Systems since the last Alert was forwarded to the Service User.	xs:unsignedShort	No	None	N/A	Non-Sensitive

Figure 6 - DCC Alert Message Format

2.1.10 Impact on Infrastructure

No impact identified.

2.1.11 Impact on Business Processes

Amendments to the list of exempted Alerts

DCC will develop appropriate Business Processes in support of Business Requirement 4, to ensure that changes to the list of exempted Alerts includes explicit approvals from the delegated SEC Panel committee.

Amendments to the Alert Storm Protection configuration parameters

DCC will develop appropriate Business Process in support of Business Requirement 5, to ensure that changes to the Alert Storm Protection configuration parameters includes explicit approval from the delegated SEC Panel committee.

2.1.12 Impact on Reporting

To meet Business Requirement 6, DCC will report on how often the mechanism introduced under SECMP0062 is used. This will cover the number of incidents raised and the number of Device/Alert combinations that are classed as overloaded within a given reporting period.

In addition, the SSI dashboard will enable Service Users to view current Device and Alert code combinations that are currently being controlled and the associated numbers of forwarded and dropped alerts. It will also provide a means to download a historic report.

3 Impact on the SEC

No changes to the GBCS are required.

A change to DUIS is required – the details are included in Section 2.1.9.

Detailed changes to the SEC will be a deliverable at the Design Stage, and will be implemented by SECAS.

4 Testing Considerations

This section outlines the testing required to complete the Design, Build and Test phases for this SEC Modification.

4.1 Pre-integration Testing

During Pre-Integration Testing (PIT), each Service Provider tests its own solution to agreed standards in isolation of other Service Providers. Specifically, the development team will carry out unit testing and the build will be subject to continuous build and automated testing to identify build issues at the earliest opportunity.

PIT will operate as a single phase of activity with a single drop. It will consist of a defined subset of system tests being observed by DCC.

4.2 Systems Integration Testing

Systems Integration Testing (SIT) is the testing of the DCC Total System, which brings together the components, e.g., DSP and CSP Systems, to allow testing of the end-to-end solution by DCC. SIT is carried out for every DCC System release and incorporates the test and integration of multiple changes. The SEC Modification and associated system changes will need to be demonstrated and tested as part of the integration test phases.

4.3 User Integration Testing

User Integration Testing (UIT) is referred to as User Testing in the SEC. User Testing of Modification Proposals is provided using the Modification Implementation Testing Service. It enables Users to run specific tests to support their implementation of a change.

5 Implementation Timescales and Releases

5.1 Change Lead Times

From the date of approval, (in accordance with Section D9 of the SEC), in order to implement the changes proposed DCC requires a lead time of **6 months.**

For Stage 1 DCC propose the following implementation plan:

Table: November 2019 Release Timescales

Phase	Start	End
SECAS and DCC confirmation of required November 2019 scope	March 2019	
Design, Build, and PIT Test	April 2019	Mid-July 2019
SIT Phase	July 2019	September 2019
UIT Phase	October 2019	October 2019
Transition to Operations and Go Live	October 2019	November 2019

For Stage 2 DCC propose the following implementation plan:

Table: June 2020 Release Timescales

Phase	Start	End
SECAS and DCC confirmation of required June 2020 scope	July 2019	
Design, Build, and PIT Test	August 2019	September 2020
SIT Phase	January 2020	April 2020
UIT Phase	May 2020	May 2020
Transition to Operations and Go Live	May 2020	June 2020

6 DCC Costs and Charges

6.1 Cost Impact

6.1.1 Implementation Costs

The table below details the cost of delivering the changes and Services required to implement both Stage 1 and Stage 2 of this Modification Proposal.

Implementation costs							
Phase:	**Design**	**Build**	**Pre-Integration Testing**	**System Integration Testing**	**User Testing**	**Implementation to Live**	**Total**
SECMP0062	*£964,346*			*£96,995*	*£9,359*	*£17,692*	**£1,088,392**

Implementation costs – supplementary information	
Implementation cost assumptions	*A. Costs are exclusive of VAT and any applicable finance charges* *B. Majority of the costs above represent labour costs.* *C. Costs provided for Design, Build and Pre-Integration Testing are quotes provided by the Service Providers and assuming there is no scope change can be considered the final costs. DCC have reviewed and challenged the costs from the Service Providers to ensure this reflects best price to date.* *D. Costs will be refined during future assessments.*
Explanation of Implementation Phases	*DCC's implementation costs are provided by implementation phases. The following describes the purpose of each phase:* • *Design: The production of detailed System and Service design to deliver all new requirements.* • *Build: The development of the designed Systems and Services to create a solution (e.g. code, systems, or products) that can be tested and implemented.* • *Pre-integration Testing: Each Service Provider tests its own solution to agreed standards in isolation of other Service Providers. This is assured by DCC.* • *System Integration Testing: All Service Providers' PIT-complete solutions are brought together and tested as an integrated solution, ensuring all Service Provider solutions align and operate as an end to end solution.* • *User Integration Testing: Users are provided with an opportunity to run a range of pre-specified tests in relation to the relevant change.*

	• *Implementation to Live Costs: The solution is implemented into production environments and ready for use by Users as part of a live service. This service is subject to implementation costs.*

6.2 Impact on Charges

This section describes the potential impact on Charges levied by DCC in accordance with the SEC.

DCC notes that SECMP0062 does not propose any changes to the charging arrangements set out in SEC Section K. DCC has made the assumption that, in the absence of an agreed alternative arrangement by the Working Group, the costs associated with the implementation of SECMP0062 will be allocated to DCC's fixed cost based and passed through to Parties via Fixed Charges.

Subject to the commercial arrangements put in place to support the relevant Release, DCC expects the increase in Charges associated with the implementation of SECMP0062 to commence in the month following the modification's implementation.

7 RAID

7.1 Risks

Ref.	Risk Description	Risk Impact
R-001	None identified at this stage	n/a

7.2 Assumptions

Ref.	Description	Impact
A-001	Reports to be published for Business Requirement 6 will be made available via DCC Sharepoint	Low
A-002	The solution presented here includes the raising of DSMS Incidents. It is assumed that there is no requirement for the automatic closing of incidents after the related device falls below the device threshold.	Low
A-003	For northbound responses, the DSP system already includes a simple anomaly detection service that rejects/discards any Response for which the DSP does not have an outstanding corresponding Request. Assuming that a southbound traffic management solution will be put in place for Requests, there is no need for any extra northbound traffic management for Responses since any overload of valid Responses will be prevented by the traffic management on Requests and any overload of invalid Responses will be prevented by the anomaly detection service.	Low

7.3 Dependencies

Ref.	Description	Impact
D-001	SEC Panel or delegated Sub Committee to provide an agreed list of exempt Alert Codes (Section 2.1.2)	Medium

8 Related Documents

Ref:	Title
1	SECMP0062 Northbound Application Traffic Management – Alert Storm Protection Business Requirements – version 1.0
2	SECMP0062 – DCC Preliminary Impact Assessment v1.1
3	SECMP0062 Working Group Consultation Responses

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'

Annex E

Working Group Consultation responses

About this document

This document contains the full non confidential collated responses received to the SECMP0062 Working Group Consultation.

Question 1: Do you agree with the solution put forward?

Question 1			
Respondent	**Category**	**Response**	**Rationale**
Bryt Energy	Small Supplier	Yes	While we agree in principle that the solution will meet the objectives of preventing alert storm capacity issues within the DCC and SEC User Systems, we are concerned two key steps need to be taken in parallel to support interim: • The change in alert management architecture and alert storms was discussed in detail in initial DCC design workshops and discounted on the basis that DCC and DSP should not be responsible for alert management and pass all traffic to the SEC User. In this instance several actions need to be agreed before this MOD is passed: ○ TABASC agreement that the solution architecture and principles for DCC are changed under alert management; ○ Root cause analysis on the current devices causing anomalous alert volumes, identifying alert type, identifying if the alert type is a valid GBCS alert device type, device firmware, SEC User; (Additional data should be time date postal code should be used to enrich the analysis) ○ Identification of alert storms on the proposed alerts not to be subject to "Throttling", in which would circumvent the proposed solution; ○ SSC should be notified of the volume of anomalous alerts & types; i.e. at present we do not know if they are security related and pose a genuine security risk to a device or firmware • DCC and SEC Users under the SEC have an obligation to investigate into anomalous alert & alert volumes as per their internal ISMS Policies;

Question 1			
Respondent	**Category**	**Response**	**Rationale**
			○ If this issue is related to a manufacture, device, particular firmware or particular alert, these parties along with SEC User should be tasked with resolving the issue at their cost; • DCC should undertake this root cause analysis and present into SEC Operations Working Group and task SEC Users to identify if the devices they currently supply and are responsible which are producing alerts that are anomalous a root cause based on: ○ Genuine root cause reason; i.e. Large DNO outage in a geographical postal code; ○ Anomalous root cause in device; i.e. Firmware Defects, Incorrect Device Configuration, Device Defects, Security Defects/Incidents ○ Identify SEC Users not actively managing anomalous alerts; ○ Core defect within GBCS or associated technical specifications; ○ SEC Users to report back with analysis and next course of actions; ○ Framework for interim analysis, reporting and monitoring agreed to be conducted on a regular basis until the DCC solution is fully implemented; Proactive root cause analysis needs to be undertaken urgently for the following reasons: • If the current anomalous alert volume increases exponentially in line with current installations this could cause outages to the DCC and severely impact SEC Users • SEC Users could through CoS Gain be in receipt of unanticipated volumes of anomalous alerts that their architecture and solutions may not be able to cope with;

Question 1			
Respondent	**Category**	**Response**	**Rationale**
			With this said, we would still recommend the throttling solution to minimise any future incidents, however recommend that anomalous alert management be tabled as an item in the Operation Working Group on a monthly basis to identify trends.
EDF Energy	Large Supplier	Yes	We agree that the proposed solution appears to be reasonable, and would reduce the number of alerts that are unnecessarily processed through the DCC systems and consume processing resources unnecessarily. A clear definition of what constitutes a duplicate or excess alert will need to be clarified in order to develop the technical solution. It may be necessary to differentiate between alerts that are sent repeatedly as a result of an ongoing issue/situation/state in regards to the device sending the alert, as compared to repeat alerts that are occurring because the same situation/issue is being created repeatedly. In the latter case filtering the alerts may serve to hide the true nature of the problem.
Western Power Distribution	Networks Party	No	We believe that the solution will help protect the DSP and User systems against only some Alert Storms and unnecessary volumes of traffic.
SSEN	Networks Party	No	This should assist in providing a throttle on the amount of device alerts we are currently receiving and alleviate pressure on our adapter based on current volumes. However, this will not solve the issue for all alerts that should be supressed or assist in a sustainable throttle notification mechanism.
E.ON	Large Supplier	Yes	E.ON understands Alert Storms are one of the biggest issues faced by the DCC and recognises the DCC needs to take direct action to protect their systems and ensure availability of service. E.ON is supportive, in principle, for the need to implement changes.
Npower	Large Supplier	Yes	Will prevent DCC from falling over due to alert storms

Question 1			
Respondent	**Category**	**Response**	**Rationale**
Smartest Energy	Small Supplier	Yes	As a small supplier resource is/can be limited meaning there will inevitably be scenarios where Alerts are missed. Some alerts may be deemed more important than others (depending on the organisation) potentially resulting in a poor service from their Service Provider. Utilising software that is already used in one way or another (Alert Anomaly Detection Thresholds) would make it easier to manage Alerts as they come in, along with helping with any triage completed to prevent further alerts in the future.
Electricity North West	Networks Party	No	No we do not agree. Whilst we wholeheartedly agree with the need for traffic management to be implemented in order to protect both Users and the DCC system from device alert storms we view the proposed solution as too complicated and lacking the overall market intelligence to identify and remediate problematic smart meter models in an efficient manner. It is our view that alert storms in the vast majority of cases are not generated by 'individual' faulty devices but by problems affecting specific manufacturer/model/firmware versions, as such if one variant of meter is affected it is highly likely that large volumes of the same variant meters will also be impacted. This is already evidenced by a known SMETS2 meter model variant which is currently generating millions of incorrect 8014/8015 alerts. Having a system which throttles (discards) a proportion of the alerts at an individual device level goes some way to alleviating the problem but the DCC's focus should be on identifying and resolving root cause by examining device behaviour at the aggregate not the individual device level.

Question 1			
Respondent	**Category**	**Response**	**Rationale**
			We do not see the rationale of opening an incident for each individual device which has been subject to throttling, this simply creates a large burden of work both for the DCC and for end Users and given current issues with SSI performance and usability could possibly render the SSI system unusable. This is highly likely to lead to additional remediation work being required in the SSI and even more cost. Nor do we see any rationale for adding metadata to the % of alerts which have not been throttled in order to inform the User that other alerts have been throttled. Again using the example of the 8014/8015 alerts there are simply too many affected devices for Users to deal with this in this manner. It is another unnecessary cost which offers little value to the end User. We strongly suggest that a simpler approach is adopted by DCC: 1) The solution should throttle (discard) alerts as currently proposed. We note that DCC already have the mechanism to identify these alerts and therefore the only changes needed are those to discard the unwanted alerts. 2) Individual incidents are NOT raised for affected devices 3) NO changes to alert metadata or DUIS 4) DCC provide a 'day after' report to all parties detailing alert volumes by meter variant (possibly indicating meter variants to which alert throttling has been applied). Parties will use the report to look at alert volumes to identify discrepancies from the expected norm. Having a single report across all parties will help provide a 'total view' and avoid unnecessary duplication of effort

Question 1			
Respondent	**Category**	**Response**	**Rationale**
			. e.g.: Alert volumes received by DCC Manufacturer / Model / Firmware: a/b/c; b1/c1; c2; ../..; x/y/z; z1 Installed Devices: 2,000,000; 10,000; 50,000; 20,000; 50,000; 50,000 Alert codes 8nnn: 200,000; 1,200; 4,500; 1,800; 6,000; 6,000 Alert codes 8014: 8,000,000; 40,000; 2,400; 6,000; 6,000 Alert codes 8015: 8,000,000; 40,000; 2,400; 6,000; 6,000 Alert codes 8F36: 500,000; 2,500; 12; 5,000; 12,500; 12,500 An aggregated report should also be produced on a weekly and monthly basis. 5) The DCC should act as the primary owner of any issues identified and raise problem records to track accordingly – noting that DCC will not be responsible for actual resolution of defects if they are proved to be caused by faulty or non-compliant meters. Such an analytics based approach will enable problematic meter variants to be identified promptly and for corrective action to be taken at an early stage. In addition to identifying meter variants which are generating excess alerts it will also help identify meter variants which are NOT generating expected alerts. Such as known issues where Power Restore (8F36) alerts are not being received when power is restored to devices following a Power Outage (AD1).

Question 2: Will there be any impact on your organisation to implement SECMP0062?

Question 2			
Respondent	**Category**	**Response**	**Rationale**
Bryt Energy	Small Supplier	Yes	Any changes to DUIS and changes to alert management would require internal review. Any new management process and root cause analysis would required additional resources internally where required.
EDF Energy	Large Supplier	Yes	This change would reduce the amount of effort that is required for our systems to process and manage alerts. Ultimately the action we take is going to be the same as the underlying issue generating the alert is the same, but this change will help make it easier to understand and manage any issues or a more timely and cost-effective basis. We anticipate the most significant benefits to come from the DCC, and it would therefore be useful if they could quantify these. It is noted that the risk associated with not making this change is that excess volumes of alerts could cause the DCC systems to fail. The benefit to the DCC of making this change would then be the avoided cost of reinforcing their systems, and procuring additional capacity, in order to deal with the volumes of alerts and meets their SLAs. We would expect the benefits accrued by individual SEC Parties to be relatively small compared to the DCC's avoided costs. Were the DCC not to upgrade their systems to cope with the alert traffic and they were to fail as a result, this would have a significant material on us, especially if occurred at a time that meant that smart meters could not be successfully installed and commissioned.
Western Power Distribution	Networks Party	Yes	If this modification is approved it will result in both system and process changes within our organisation.

Question 2			
Respondent	**Category**	**Response**	**Rationale**
			Initially, in order to know if any alerts are being throttled, we will be required to monitor the SSI dashboard and this will mean a change to internal processes. We will then need to develop our systems so that they can receive and interpret the additional message data. Once the DUIS/XSD change has been implemented, we will need to update our back end systems and processes to handle the new information and respond accordingly.
SSEN	Networks Party	No	As these are handled before being delivered into our adapter, no changes are expected to be made.
E.ON	Large Supplier	Yes	E.ON anticipates changes will need to be implemented to our systems and procedures. However, before we can fully answer this question, we have the following points which we seek further clarification: 1. In Requirement 1 there is reference to an incident being raised where the generic alert threshold of >50 alerts of any type being received from a specific device within a 30 minute period. Which party will that alert be raised against? Is the intention that the alert is raised against the DSP to initiate the device/alert monitoring, or will it be raised against the responsible Supplier to notify them that this threshold has been breached? If raised against the responsible Supplier at this stage, what action are they expected to take? 2. In Requirement 1 there is reference to a second incident being raised when the device/specific alert threshold is breached. Who will this incident be raised against? Is the assumption correct that it would be raised against the KRP that would normally be in receipt of that alert? Please confirm.

Question 2			
Respondent	**Category**	**Response**	**Rationale**
			3. In the Business Requirements document, Requirement 2 – to notify users when alerts have been subject to throttling – may be delivered later than the remaining requirements. E.ON would like to understand an estimated delivery date. 4. If the alerts are throttled then we may lose visibility of patterns in SSI that are useful in diagnosing the source of a problem. The proposal would be much stronger if the monitoring and throttling of these alerts was investigated by the DSP to identify these patterns and root causes proactively, instead of raising an Incident against a Supplier. We will need DSP input to diagnose the issue anyway and any additional information that could be added to the incident ticket would be very helpful. 5. E.ON would like the DCC to provide more detail on how they would ensure the notifications land with the right Supplier contacts and in a way that highlights the relevant priority in a suitable way.
Npower	Large Supplier	Unknown	
Smartest Energy	Small Supplier	No	
Electricity North West	Networks Party	Yes	If the proposal is approved as it stands then each individual User will have to undertake their own analytics and problem identification even though the likely resolution is a change to the device/firmware variant. This is not an efficient use of resource and DCC are ideally placed to provide such analytics centrally, offering a 'whole system' view.

Question 3: Will your organisation incur any costs in implementing SECMP0062?

Question 3			
Respondent	**Category**	**Response**	**Rationale**
Bryt Energy	Small Supplier	Yes	Any changes to DUIS and changes to alert management would require internal review and cost. Any new management process and root cause analysis would require additional resources internally where required.
EDF Energy	Large Supplier	Yes	We will need to make changes to our working practices regarding the management of alerts and ensure that these are communicated and relevant training undertaken. We do not anticipate the implementation costs of making this change, especially in Stage 1, to be material as the actions that will be taken as a result of receiving filtered alerts should be the same as they would have been for filtered alerts, as the underlying issue causing the alerts to be sent will not have changed. In the event that a DUIS based solution is implemented the costs are likely to be higher – however we would usually incur a relatively fixed cost for upgrading to a new version of the DUIS, irrespective of the number of changes included in that new release. The technical implementation costs that would be associated with making an individual change such as this one is likely to be low.
Western Power Distribution	Networks Party	Yes	The main cost, beside the modification implementation costs, will be developing the systems to accept and handle the additional information within the alerts. It is difficult to determine exactly how much this modification will cost as it will depend what other changes form part of that particular DUIS/XSD release. There will be additional costs beyond the DUIS/XSD change to develop our back ends systems and processes to handle the additional information we are receiving.

Question 3			
Respondent	**Category**	**Response**	**Rationale**
			If we were to implement this change as a standalone change the cost to our organisation would be approximately £20,000. We will not benefit from any cost savings as a result of this modification.
SSEN	Networks Party	Yes	Due to the implementation plan for this, we are unsure of how you will communicate the volumes of supressed alerts. We will still have the desire to understand and report on the number of alerts received into our adapter Vs. the amount generated by a device. This will require extra time to gather and report on this information.
E.ON	Large Supplier	Yes	E.ON expects costs will be incurred but cannot evaluate these costs until more information is provided following testing of the proposed solution.
Npower	Large Supplier	Unknown	
Smartest Energy	Small Supplier	No	
Electricity North West	Networks Party	Yes	Changes to DUIS may be required although offering little or no practical benefit. Analytics will need to be developed to identify issues with particular device variants. Organisational changes to deal with significant volumes of incidents. Estimated £100k.

Question 4: Do you believe that SECMP0062 would better facilitate the General SEC Objectives?

Question 4			
Respondent	**Category**	**Response**	**Rationale**
Bryt Energy	Small Supplier	Yes	While we agree this better facilitates the General SEC Objectives, discussion is required on the SEC impacts this change brings. Obligations rest purely on a SEC User The current solution and SEC assume that the DCC is responsible for passing all alerts though to the SEC User who is responsible
EDF Energy	Large Supplier	Yes	We agree that this change would better facilitate SEC Objective (a) as reducing the volumes of alerts that need to be processed and managed will enable smart metering systems to be managed more efficiently. We do not agree that this change better facilitates SEC Objective (e) as it is not clear how this change would directly impact energy networks, and certainly not facilitate innovation in the design and operation of energy networks.
Western Power Distribution	Networks Party	Yes	We disagree with the proposer's rationale that this modification better facilitates Objective (a) as it does not impact the Smart Metering Systems at Energy Consumer's premises. This change impacts the DSP systems and northbound to the Users systems. We also disagree with the proposer's rationale that this modification better facilitates Objective (e) as it does not facilitate the innovation in the design and operation of the Energy Networks to deliver a secure and sustainable supply of electricity.

Question 4			
Respondent	**Category**	**Response**	**Rationale**
			We do believe that this modification better facilitates SEC Objective (b) as it will ensure that the DCC can fulfil their obligations by providing some additional protection to part of their system.
SSEN	Networks Party	Yes	We believe that this modification better facilitates general SEC Objectives (a) and (e) for the reasons documented in the SECMP0062 Modification Report
E.ON	Large Supplier	Yes	E.ON agrees with the rational proposed in pages 11 and 12 in the Modification Report.
Npower	Large Supplier	Yes	It will protect the DCC infrastructure from overload
Smartest Energy	Small Supplier	Yes	This modification would better facilitate SEC Objective (a) and (e) as this will help improve the operation of Smart Metering Systems with the use of additional precautions alongside the existing detection program in the DSP. This mod also demonstrates innovation in improving between Service Users and the DCC.
Electricity North West	Networks Party	Yes	We support the intent of the modification proposal however we challenge whether the proposed solution results in efficient operation.

Question 5: Noting the costs and benefits of this modification, do you believe SECMP0062 should be approved?

Question 5			
Respondent	**Category**	**Response**	**Rationale**
Bryt Energy	Small Supplier	Yes	Any DUIS changes would result in impacts and cost, however it is not possible to identify cost at this point until DUIS changes are finalised. Bryt Energy envisages no cost to any Alert Root cause analysis.
EDF Energy	Large Supplier	Yes	Subject to confirmation from the DCC that the benefits that they would accrue as a result of avoiding upgrades to their systems in order to meet their SLAs exceed the costs, we believe that this modification should be approved.
Western Power Distribution	Networks Party	No	We do not believe that this modification will provide an adequate solution to alert volumes and unnecessary traffic, based on what we are currently experiencing. Please see comments in Question 10.
SSEN	Networks Party	No	We feel the costs are acceptable due to the technical changes required to supress alerts. However, we believe the approach needs further work surrounding devices creating permanent alert storms and the email notification solution for impacted parties.
E.ON	Large Supplier	Yes	As per reasons noted above.
Npower	Large Supplier	Yes	
Smartest Energy	Small Supplier	Yes	As a small supplier resource is/can be limited. Where we have received alert storms in testing, it has proven to be time consuming going through the alerts to identify what the alerts are for. It also means where we may spend time trying to resolve an issue, we can potentially miss more important alerts that may have been received alongside other alerts deemed not as important.

Question 5			
Respondent	**Category**	**Response**	**Rationale**
Electricity North West	Networks Party	No	The current proposed solution is too complicated and lacking the overall market intelligence to identify and remediate problematic smart meter models in an efficient manner.

Question 6: If SECMP0062 is approved, should the solution include the email notification in Stage 1 of the implementation approach? DCC have stated this will occur in every incident event if this is included as part of the solution.

Question 6			
Respondent	**Category**	**Response**	**Rationale**
Bryt Energy	Small Supplier	Yes	SEC Users should have the option to receive email alerts along with SSI visibility. Email should be managed as per SEC Contacts.
EDF Energy	Large Supplier	No	The likely volume of e-mails is going to be high and just create another problem in managing that traffic. Making the relevant information available via the SSI should be sufficient in Stage 1.
Western Power Distribution	Networks Party	No	We do not feel that the receipt of an email will aid us and will cause additional burden to our resource, especially as there is a likelihood of large volumes.
SSEN	Networks Party	No	Due to the nature of some alert storms, we feel that this could cause administrative issues with the potential volume of emails received.
E.ON	Large Supplier	Yes	E.ON would like to receive email notification in Stage 1 of the implementation approach. Although the incidents will be raised in SSI by default, they may not be picked up immediately if in amongst a much larger volume of incidents already raised by, or against, E.ON. Specific email notification of this type of incident will support quicker review and resolution of the issue. As noted above, we would like the DCC to provide more detail on how they ensure the notifications land with the right Supplier contacts and in a way that highlights the relevant priority in a suitable way.
Npower	Large Supplier	Yes	Email is necessary to notify the user of the alert

Question 6			
Respondent	**Category**	**Response**	**Rationale**
Smartest Energy	Small Supplier	Yes	The solution should include email notification to keep all organisations informed with changes. It also gives the opportunity for the information to be shared/forwarded easily other colleagues at different levels of involvement within Smart Metering and takes away the manual aspect of checking the SSI Dashboard.
Electricity North West	Networks Party	No	Sending emails relating to individual devices is unnecessary and will only create extra complications and cost.

Question 7: How long from the point of approval would your organisation need to implement SECMP0062?

Question 7			
Respondent	**Category**	**Response**	**Rationale**
Bryt Energy	Small Supplier	We no issue with the proposed timelines for implementation for Bryt Energy	This is dependant on DUIS Changes being notified in advance and root cause analysis being undertaken.
EDF Energy	Large Supplier	1 month	We would need a month in order to be able to amend and train out revised working practices in regards to the management of alerts and use of the SSI.
Western Power Distribution	Networks Party	For the full solution including the DUIS change we would require a minimum of six months lead time.	This is due to the XSD change involved. This time scale allows time for planning the works to uplift the systems to the new DUIS version with appropriate regression testing, as well as additional system functionality to be built and full testing to be undertaken.
SSEN	Networks Party	N/A	As the modification will not result in any changes to our internal systems, we will not require a large lead time.

Question 7			
Respondent	**Category**	**Response**	**Rationale**
E.ON	Large Supplier	Clarification is required before an answer can be submitted.	E.ON anticipates changes will need to be implemented to our systems and procedures. However, before we can fully answer this question we require further information (see queries raised in our response to question 2).
Npower	Large Supplier	Unknown	
Smartest Energy	Small Supplier	N/A	N/A
Electricity North West	Networks Party	Dependent upon whether DUIS changes are mandatory then it would require a 6 month lead time.	Sufficient time is required in order to contract for changes with our own service providers in order to design, develop, test and implement.

Question 8: Do you agree with the proposed implementation approach?

Question 8			
Respondent	**Category**	**Response**	**Rationale**
Bryt Energy	Small Supplier	No	At present, we do not know the scope or range of alerts
EDF Energy	Large Supplier	Yes	We agree with the proposed implementation approach.
Western Power Distribution	Networks Party	Yes	We believe that it makes sense to implement a solution sooner rather than later to help protect the DSP systems, with a DUIS change following at an appropriate time.
SSEN	Networks Party	No	We are currently receiving in excess of 100,000 device alerts on a daily basis. With the timeline proposed, this will be implemented after a further increase of alert storm devices being enrolled and the migration of SMETS1 devices which could cause capacity issues with our adapter.
E.ON	Large Supplier	Yes	7 November seems a reasonable date to ensure a positive outcome.
Npower	Large Supplier	Yes	Caveat** the list of exempt needs to be fully agreed by all parties
Smartest Energy	Small Supplier	Yes	A two staged approach means that the solution can be provided with care and due diligence.
Electricity North West	Networks Party	No	Please refer to earlier responses

Question 9: Do you have any Alert Codes that you feel should not be subject to throttling as part of SECMP0062's solution?

Question 9			
Respondent	**Category**	**Response**	**Rationale**
Bryt Energy	Small Supplier	Yes	As per comment 1, until Identification of alert storms of alerts on the proposed alerts not to be subject to "Throttling", in which would circumvent the proposed solution is identified it is difficult to say if any alerts should be exempt. Proposals would be safety, theft, commissioning alerts etc. Root cause analysis needs to be undertaken first to understand what alerts are causing potential issues and if they are genuine or defective. For example, if there are only two types of alerts causing an issue, we would assume at implementation only these two would be throttled and the configuration of any other alerts not throttled. DCC would monitor and add or remove based on actual traffic as new devices and firmware enter the market. In terms of implementation we would also welcome a phased implementation approach to ensure robust of the DCC Solution in the Production environment. Initial implementation would be to throttle an anomalous non-critical alert and to measure the DCC solution is fit for purpose, before throttling an critical alert codes.
EDF Energy	Large Supplier	No	We have not identified any at this time. As noted in our response to question 1 a more detailed set of rules as to what constitutes an excess/duplicate alert will need to be defined to ensure that alerts are not unnecessarily filtered where they relate to multiple re-occurring issues rather than a single ongoing issue.
Western Power Distribution	Networks Party	No	

Question 9			
Respondent	**Category**	**Response**	**Rationale**
SSEN	Networks Party	No	We believe that all codes should be subject to throttling based on the time and volume parameters that are being implemented.
E.ON	Large Supplier	Yes	E.ON believes that there is more insight to be gained by having the raw data and alerts sent with appropriate time stamps. If the alerts are throttled then visibility of patterns that are useful in diagnosing the source of a problem is lost. The proposal would be much stronger if the monitoring and throttling of some alerts was done in partnership with the DSP to identify patterns and thus potential root causes. There is recognition that a pragmatic approach is required though our preferred method is that all data is passed. Any alerts relating to device / supply power loss, removal of covers or batteries (gas meters) should NOT be throttled. The following Alert Codes should not be subject to throttling as they highlight potential or actual Health and Safety events; 0x8F77 Unauthorised Physical Access - Second Terminal Cover Removed 0x8F76 Unauthorised Physical Access - Terminal Cover Removed 0x8F74 Unauthorised Physical Access - Meter Cover Removed 0x8F73 Unauthorised Physical Access - Battery Cover Removed 0x8F3F Unauthorised Physical Access - Tamper Detect 0x8F1F Low Battery Capacity 0x8F1D GSME Power Supply Loss 0x81C0 Supply Disconnect Failure

Question 9			
Respondent	**Category**	**Response**	**Rationale**
Npower	Large Supplier	Yes	These need to be in full agreement of all users
Smartest Energy	Small Supplier	No	All Alert codes should be subject to throttling to help identify common trends that trigger the alert storms. It will also help determine if intervention from specific parties is needed or need to be made aware of. This should help prevent the wrong actions being taken and potentially break systems/meters.
Electricity North West	Networks Party	Yes	Power Outage (AD1), Power restore (8F35 and 8F36) should not be throttled.

Question 10: Please provide any further comments you may have

Question 10		
Respondent	**Category**	**Comments**
Bryt Energy	Small Supplier	None
EDF Energy	Large Supplier	No
Western Power Distribution	Networks Party	Whilst we understand the idea behind this proposal, we are concerned that this solution will not prevent high volumes of unnecessary alerts and does not address the issue as to why devices are generating alerts in such high volumes. We have undertaken a review of 'nuisance' alerts that we are currently receiving, alongside this modification's proposed solution. Currently we are receiving extremely high volumes of two specific alerts, (doubling every month with over 9,000,000 expected for April), however, due to the number of devices generating these alerts, this solution would not actually prevent any of these alerts from coming through to us. We believe that there should be further discussions to fully understand the problem that the DCC are trying to resolve. We don't believe, based on what we are seeing on our systems, that the solution and parameters described in this modification will result in adequate protection.
SSEN	Networks Party	It is disappointing that this implementation approach was favoured above a firmware update approach as discussed in the first working group. Based on the volumes and time periods this will eradicate most alerts we receive, however based on the current level of Power Factor alerts we receive (around 200 every 5 minutes) we will still receive multiple alerts daily. This also prevents us for supporting the implementation of an email notification.

Question 10		
Respondent	**Category**	**Comments**
E.ON	Large Supplier	See above
Npower	Large Supplier	
Smartest Energy	Small Supplier	
Electricity North West	Networks Party	As describe above the modification should focus on identifying root cause issues by evaluating traffic as a whole across device variants. Raising individual device incidents and treating each as a separate issue is neither manageable nor in the best economic interests of customers. Focus should be on the aggregate impact across the DCC system and all Users as a whole.