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.

SECMP0067

'Service Request Traffic Management'

Modification Report

Version 1.2

20 July 2020

Corporate member of Plain English Campaign
Committed to clearer communication
592

About this document

This document is a Modification Report. It currently sets out the background, issue, solution, impacts, costs, implementation approach and progression timetable for this modification, along with any relevant discussions, views and conclusions. This document will be updated as this modification progresses.

Contents

1. Summary 3
2. Issue 3
3. Solution 4
4. Impacts 8
5. Costs 9
6. Implementation approach 10
7. Assessment of the proposal 10

Appendix 1: Progression timetable 21

Appendix 2: Glossary 21

This document also has eight annexes:

- **Annex A** contains the Service Request Traffic Management Mechanism Document.
- **Annex B** contains the business requirements for the proposed solution.
- **Annex C** contains the Reporting Wireframes.
- **Annex D** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the proposed solution.
- **Annex E** contains the full Data Communications Company (DCC) Impact Assessment response.
- **Annex F** contains the full Refinement Consultation responses.
- **Annex G** contains a worked example of how the solution will work.
- **Annex H** contains the Business Case.

Contact

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

Harry Jones, 020 7081 3345; Harry.jones@gemserv.com

1. Summary

This proposal has been raised by Graeme Liggett on behalf of the DCC.

The DCC Systems are limited by a finite capacity. As numbers of Smart Meters and Devices increase in the Smart Metering Implementation Programme (SMIP), this will increase the traffic of Service Requests in the DCC Systems. In exceptional instances this traffic, if left unchecked, could result in an overload of the DCC Systems and cause an outage, resulting in no Service Requests being sent from the Data Service Provider (DSP). The DCC has recommended management of the System, in order to prevent an outage without the expense of expanding the DCC infrastructure.

The Proposed Solution is to introduce a mechanism to regulate the volume of Service Requests when the DCC System is experiencing heavy traffic. **This mechanism would be activated if the DSP system capacity threshold is breached and only take place in exceptional circumstances**. Service Users will be allocated their own capacity thresholds, proportional to their portfolio; they can exceed this allocation where there is spare System capacity but will be forced to operate within that allocation if the System is near capacity and the mechanism is active.

The DCC will provide reporting on the frequency of how often the mechanism is used and its duration, as well as individual Users' allocation and monthly traffic. **It is noted that only Users who exceed their capacity threshold will have their Service Requests regulated if the solution's mechanism is in effect**. Any User who keeps within their capacity will not be regulated. Users can independently prioritise their Service Request traffic as part of their business processes.

This modification was submitted to Ofgem for Authority Decision in April 2020 but was sent back to industry for further work in May 2020. The Working Group was reconvened, and the business case was discussed again and the impacts of moving to a June 2021 implementation were assessed.

All SEC Parties are expected to be impacted by this Modification Proposal. The central costs of the solution will be approximately £1.6m. The proposed implementation date of this Modification Proposal if approved is the June 2021 SEC Release.

2. Issue

What happens currently in DCC Systems?

The DCC System has a finite capacity. Even when configured to meet forecasted demand and making the most efficient use of the System's current capacity, it may be unable to cover accidental or unanticipated large bursts of Service Requests sent by Users. In the current DCC System configuration, F5 Load Balancers provide the only protection for the DSP against overloading from the network. Once the system is overloaded the F5 Load Balancers will respond with 'Http 503 Service Unavailable' error messages to all the Users and will essentially stop the input so that no Users can send anything. There is no processing or prioritisation of any Service Requests, all Users are impacted, and the DSP would not be able to be able to respond to any further Service Requests sent by any User. This would include any high priority Service Requests such as prepayment top-ups.

What is the issue?

The DCC System has a finite capacity and is unable to meet accidental or unexpected large bursts of Service Requests. The causes of these bursts might include User System's sending excessive numbers of Service Requests or Denial of Service (DoS) attacks.

The current system penalises Service Users equally rather than those responsible for the overload.

What is the impact this is having?

This means that if the System is overloaded, all Service Requests will be rejected, and Users must request retries. Additionally, this results in Service Users who have operated responsibly not being able to use the DCC System at its expected performance whilst it deals with this traffic.

This proposal is designed to provide reliable and predictable System behaviour under extreme conditions.

It will enable the System to control the Service Requests of only those Service Users whose use of the service exceeds their fair share.

3. Solution

Proposed Solution

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

The details of the solution's mechanism and the Capacity Allocation Formula can be found in the Service Request Traffic Management Mechanism Document in Annex A. Please note that the Service Request Traffic Management Mechanism Document introduced in this Modification Proposal is independent of the Traffic Management Mechanism Document that is created in SECMP0062 'Northbound Application Traffic Management - Alert Storm Protection'.

Capacity allocation formula

Service Users will be notified of the DSP System Capacity by the DCC. Under it, each Service User will be allocated a proportion of the available capacity based on an agreed formula. This formula can be found in the Service Request Traffic Management Mechanism Document and can only be amended by Panel (or a Sub Committee of their choosing, which the Smart Energy Code Administrator and Secretariat (SECAS) recommends should be the Operations Group).

The proposed capacity allocation formula will operate at a SEC Party ID level and is built on the weighted proportionality principle; that is, each allocation is scaled using one or more weighting factor(s). To ensure fairness, capacity will be allocated on a basis that is clear and does not disadvantage any one User. Two considerations will be applied here:

- Allocation will be based on installed Devices to which that User has an allocated role; and
- Allocation will be based on the financial contribution of that User to the DCC System, as measured by the User's charging group weight factor.

These two factors will be multiplied together. Thus, if either of the factors is zero the weight itself becomes zero. Consideration will also be given to the expected additional volume of Service Requests required to manage prepayment customers relative to non-prepayment customers. The proposed formula will also guarantee a minimum allocation for Other Users.

Users who pay most and those with the most customers and the most meters to serve will therefore receive larger allocations than smaller Service Users. These two principles, minimum allocations and weighted proportionality, form the base for a fair and equitable capacity allocation formula.

Notification of capacity allocations

The DCC will notify the DSP of the agreed DSP System Capacity and Service User Capacity settings via the upload of a configuration file in a similar fashion to that used for DCC System Wide Anomaly Detection Thresholds (ADT).

Service User Capacity settings will be expressed as a percentage of the total capacity, thus allowing the overall DSP System Capacity to be increased without the need for new Service User Capacity settings to be uploaded.

Capacity management process

The DCC will set amber and red threshold percentages for each of the DSP System Capacity and Service User Capacity setting, which will form the basis of the invocation of the traffic management mechanism.

The DSP will record two new sets of values as Service Requests are received or actioned:

- a count of all Service Requests processed in the last [1] seconds; and
- a count of all Service Requests processed for each Service User in the last [1] seconds.

It should be noted that this includes DSP Scheduled Service Requests, but these will be subject to existing DSP load management features to ensure they are processed at a controlled rate. This rate will be set to ensure that there is always DSP System Capacity available for On Demand requests.

The time period for counting Service Requests will be a configurable rolling interval managed in a similar fashion to the intervals used in anomaly detection, albeit that the interval used for traffic management is expected to be much shorter.

The count of Service Requests over the period shall determine a ‘requests per second usage’ value for the DSP System as a whole and for each Service User. These values will be compared against the DSP System Capacity and the Service User Capacity as follows:

- If the DSP System usage exceeds the amber threshold for DSP System Capacity, then a System Usage Warning event will be recorded and notified to the DSP monitoring solution.
- If any Service User usage exceeds the amber threshold for Service User Capacity, then a Service User Usage Warning event will be recorded for each Service User and notified to the DSP monitoring solution.
- If any Service User usage exceeds the red threshold for Service User Capacity but the DSP System usage remains below the red threshold for DSP System Capacity then a Service User Excess Usage event will be recorded for each Service User and notified to the DSP monitoring solution.

- If the DSP System usage exceeds the red threshold for DSP System Capacity, then a System Overload event will be recorded and notified to the DSP monitoring solution. This event may also be configured to create an Incident in the DCC Service Management System (DSMS) if required.
- The system will disable Schedule Activation, DSP Future Dated execution, Low Priority Execution and Certificate Replacement requests while there is a System Overload event in place.
- If the DSP System usage exceeds the red threshold for DSP System Capacity and any Service User usage exceeds the red threshold for Service User Capacity, then a Service User Overload event will be recorded for each Service User and notified to the DSP monitoring solution. Any Service User who has exceeded capacity will be marked as subject to Traffic Overload.

Once a Traffic Overload event occurs, the processing for each Service User will operate as illustrated below.

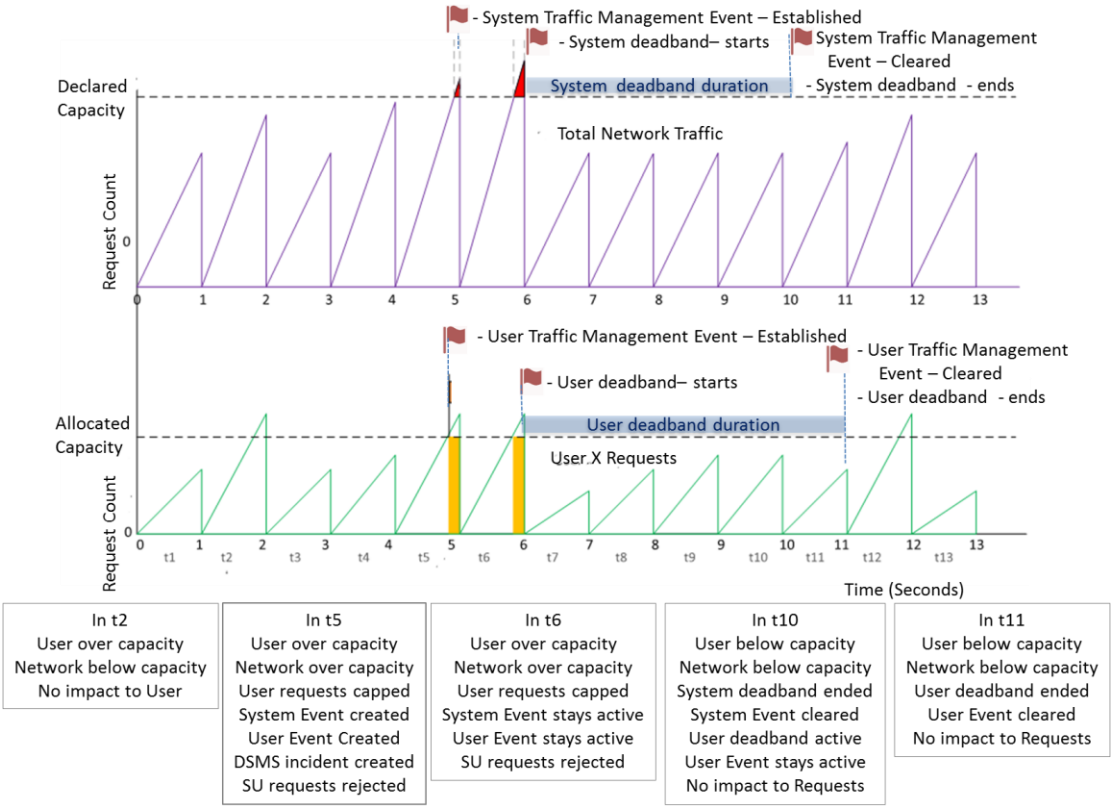

Figure 1 Southbound Traffic Management Processing

Within each [1] second window, the DSP will accept Service Requests up until the Service User reaches its Service User Capacity. At this point, the Service User will be marked as subject to Traffic Overload for the remainder of that window.

The processing at the DSP boundary within the Message Gateway will check whether a Service User is marked as subject to Traffic Overload and if so then the following action will be taken:

- Any Service Request with a Service Request Variant (SRV) which is identified as being subject to Traffic Management will be rejected using a configurable Http Status code.

- Any Service Request with an SRV that is identified as NOT being subject to Traffic Management will be processed as normal.

The list of which SRVs are subject to Traffic Management will be configurable and held within the DSP solution. Updates to this list will be managed by the SEC Panel (who may choose to delegate this responsibility to a Sub-Committee).

The processing under Traffic Management mode will continue until the DSP System usage returns below the red threshold for DSP System Capacity and stays there for a period greater than the system deadband duration. During the system deadband period, if the DSP System goes over capacity there will not be a new event created; instead this will be linked to the existing system traffic management event. Once the rate of messages falls within the system capacity then the deadband window will be restarted. This mechanism will help reduce the number of incidents. The deadband durations for both System and User will be configurable.

(Note: The deadband durations in Figure 1 are kept shorter for illustration purposes; these can be configured for longer durations).

If a Service User who is subject to Traffic Overload returns below the red threshold for Service User Capacity before the DSP System usage returns below the red threshold then that Service User will be cleared of being subject to Traffic Overload.

Otherwise, when the DSP System usage returns below the red threshold for DSP System Capacity then any Service User who is above the red threshold will be cleared of being subject to Traffic Overload.

Reporting

Events generated by the Traffic Management system and any Service Requests that are rejected will be recorded and made available to the reporting and monitoring systems.

The reporting in this solution will be undertaken by logging events in the DCC's Technical Operations Centre. This will form the basis for monthly reporting which will include details considering System Configuration, System Capacity, Users and any Trends. The DCC confirmed its support for the Panel to delegate responsibility to the Operations Group to oversee management of the reporting as well as the management of the Priority Service Request list and the wider solution mechanism's configurable parameters. The Working Group agreed with this but wanted the Security Sub-Committee (SSC) and the Technical Architecture and Business Architecture Sub-Committee (TABASC) to provide input to the Operations Group meetings where this is discussed.

An example of the reporting that will be provided by the DCC can be found in Annex C.

Legal text

The changes to the SEC required to deliver the proposed solution can be found in Annex D and the Service Request Traffic Management Mechanism Document can be found in Annex A.

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 and Network Operators will be affected by this modification due to having to work to their capacity allocation in times of heavy Service Request traffic.

Other SEC Parties will be affected by this modification for the same reasons but will be guaranteed some capacity during heavy traffic to ensure that they can still send requests during this time.

Some Users' systems may need to be amended to be able to interpret the new Http error code being introduced and to prioritise Service Requests when the mechanism is active.

DCC System

The DCC has developed a mechanism responsible for throttling Service Requests once the total capacity threshold is breached. The DCC has defined the formula for allocating capacity for Service Users and deliver reporting on a monthly basis. These will be implemented within the DCC Systems.

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

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Section H 'DCC Services'
- Appendix AB 'Service Request Processing Document'
- Appendix AD 'DCC User Interface Specification'

The redlined changes to these documents can be found in Annex D

The Service Request Traffic Management Mechanism Document will also be created to account for traffic management changes being introduced. This can be found in Annex A.

Consumers

Consumers are less likely to suffer an outage of service (such as not being able to top-up prepayment meters) as the actions of one User will not impact other Service Users.

Other industry Codes

There is no impact on any other industry Codes.

Greenhouse gas emissions

There are no impacts on greenhouse gas emissions.

5. Costs

DCC costs

The estimated DCC implementation cost to implement this modification is £1,629,167. The breakdown of these costs are as follows:

Breakdown of DCC implementation costs	
Activity	**Cost**
Design	£65,095
Build and Pre-Integration Testing (PIT)	£1,406,345
Systems Integration Testing (SIT)	£36,768
User Integration Testing (UIT)	£55,738
Implement to Live	£0
Application Support	£65,221

More information can be found in the DCC Impact Assessment response in Annex E.

SECAS costs

The estimated SECAS implementation costs to implement this modification is two days of effort, amounting to approximately £1,200. The activities needed to be undertaken for this are:

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

SEC Party costs

As part of the first Refinement Consultation, respondents were asked about the costs that they face individually as SEC Parties outside of the central costs above. All Parties said there would be implementation costs, but no monetary values were given nor any idea of the magnitude of these costs.

The first Refinement Consultation Responses can be found in Annex F.

6. Implementation approach

Recommended implementation approach

SECAS is recommending an implementation date of:

- **24 June 2021** (June 2021 SEC Release) if a decision to approve is received on or before 30 September 2020; or
- **4 November 2021** (November 2021 SEC Release) if a decision to approve is received after 30 September 2020 but on or before 4 November 2020.

The Proposer wants to deliver this Modification Proposal as soon as possible, if approved.

From the first Refinement Consultation responses, two SEC Parties stated they would take longer than six months from the point of approval to prepare themselves for the planned changes. They stated their lead time required would be closer to 12 months. Other SEC Parties stated that they could either meet this within six months, couldn't gauge it or didn't comment in the consultation. The full first Refinement Consultation responses can be found in Annex F.

When the Modification Proposal was taken to the Change Board on 22 April 2020, several members stated that they would require between six and 12 months to change their internal processes and systems to accommodate these changes. The Authority subsequently sent the Modification Report back to the Panel to assess the impact of moving the implementation date from the November 2020 SEC Release to the June 2021 SEC Release.

SECAS is recommending this modification be included in the June 2021 SEC Release if a decision to approve is received by 30 September 2020. This allows Users the time requested to implement any changes ahead of the June 2021 SEC Release while also not unduly delaying implementation if approved. If this cut-off date is missed, the modification would fall back to the November 2021 SEC Release.

Moving the implementation date to June 2021 will allow Users more time to prepare for these changes; however, it also leaves the DCC Systems at risk for another 12 months, or longer if the implementation date is delayed further. The impact will affect the Service Users if SECMP0067 is not implemented as early as possible.

7. Assessment of the proposal

How does the mechanism work?

Service Users will be given a capacity allocation based on their portfolio of operational Devices and weighted DCC Service Request usage (i.e. Suppliers need to send more Service Requests than Network Parties). Other SEC Parties will also be given a capacity allocation to ensure they are able to send Service Requests. If the DCC System is running under total capacity and a User breaches their capacity allocation they will not be regulated. If the DSP System usage exceeds the red threshold for DSP System Capacity and any Service User usage exceeds the red threshold for Service User Capacity, then a Service User Overload event will be recorded for each Service User and notified to the DSP monitoring solution. Any Service User who has exceeded capacity will be marked as subject to Traffic Overload. The processing at the DSP boundary within the Message Gateway will check

whether a Service User is marked as subject to Traffic Overload and if so then the following action will be taken:

- Any Service Request with an SRV which is identified as being subject to Traffic Management will be rejected using a configurable Http Status code
- Any Service Request with an SRV that is identified as NOT being subject to Traffic Management will be processed as normal.

The list of which SRVs are subject to Traffic Management will be configurable and held within the DSP solution. Updates to this list will be under the governance of the Panel (or a Sub-Committee nominated by it).

The processing under Traffic Management mode will continue until the DSP System usage returns below the red threshold for DSP System Capacity and stays there for a period greater than the system deadband duration. During the System deadband period if the DSP System goes over capacity there will not be a new event created, instead this will be linked to the existing system traffic management event. Once the rate of messages falls within the System Capacity then the deadband window will be restarted. This mechanism will help reduce the number of incidents. The deadband durations for both System and User will be configurable.

This means Service Requests sent over and above a User's capacity allocation will get a Http 429 Response. In the initial stages of the modification the DCC suggested an Http 503 response would be used, but the Working Group questioned this. The Working Group thought that receiving an Http 503 would not differentiate anything regulated through the modification's mechanism as opposed to any business-as-usual reasons. Following the Impact Assessment, the DCC changed this to a Http 429 'too many requests'.

Within the header of the Http 429 will be a retry time delay. This is a minimum time that the User should delay sending a retry. The Working Group spent time debating whether the System Deadband period and User Deadband period should be different, but in the end concluded that keeping them the same was the simplest answer.

The Retry After attribute was also debated, and specifically whether this should be less than or greater than the System Deadband period. The Working Group concluded that this should be less than the System Deadband period, otherwise there would be a danger of constantly ending the System level Traffic Management event only to trip back over it a few seconds later when the User sends in another burst of requests from the retry processing. By keeping the 'Retry After' less than the Deadband there will be just one Traffic Management event that continues until the overload situation has ended.

A retry strategy was discussed at the Working Group as well. This retry strategy has a 'short retry' and 'long retry', with the short sequence being retrying 45 seconds after an initial failed attempt, then a third attempt after waiting 60 seconds and ending with a fourth retry after 75 seconds. If this 'short retry' fails to submit the User's Service Request, the 'long retry' sequence should be used where the User waits an hour before retrying the 'short retry' sequence again. If that doesn't work, the User should wait two hours before retrying the 'short retry again', then wait four hours if unsuccessful and so on. The DCC recommended that the rate of Service Requests that are retried do not exceed the User's allocation so that this doesn't risk triggering the Modification Proposal's solution. Further details of the retry strategy can be found in the Impact Assessment in Annex E.

This was presented at the Working Group on 16 March 2020. The Working Group was keen to see an example of how this would work for an individual User. A worked example was provided by the DCC and can be found in Annex G.

Which circumstances will trigger the solution's management mechanism?

The Working Group questioned the DCC on how often it would expect this management mechanism to be activated and whether this was specifically for situations outside the normal business processes or for everyday use. Working Group members felt the obligations of the DCC to provide an efficient system meant this solution should only be used in exceptional circumstances where events only lasted a few seconds. The rationale was that if this was an everyday occurrence, then it should not be industry members that fund this change.

The DCC stated that this solution was designed for exceptional circumstances, not for standard business operations. In a business case (see Annex H) that the DCC presented, it stated that DoS attacks and accidental (human error or technical error) or malicious surges of Service Requests were the situations this mechanism was designed to deal with. It stated that a scenario has occurred before in standard business operations where several Users had submitted large quantities of Service Requests around the same time of day causing a strain on the System. Severe weather events were also mentioned as causing large bursts of Service Request traffic; however, Network Parties pointed out that they need to send large numbers of SRs to check customers are on supply. Network Parties will be able to manage their SRs within their capacity allocation however they see fit, determining the prioritisation themselves.

The Working Group queried the business case and asked whether the DCC could provide any estimated quantities and frequencies of events this mechanism could mitigate. The DCC took note of this and provided information about historic outages to strengthen this area of the overall business case. One Working Group member also asked whether this business case had gone through review by the Security Sub-Committee (SSC), particularly concerning the potential DoS attack. SECAS subsequently presented the modification business case and solution to the SSC. The SSC was supportive although pointed out this the mechanism would protect the System from DoS attacks but would not prevent them.

How will this be affected by Half Hourly Settlement changes?

One Working Group member asked how the System and mechanism would be affected by the new Half Hourly Settlement arrangements. The DCC has confirmed that as Service Users usage increases due to Half Hourly Settlement or business as usual rollout, they will receive a higher Capacity Allocation and the DCC Systems will be scaled to deal with the increased traffic.

Were other solutions considered during the Refinement Process?

Consideration of other options

Three other solution options were considered during the Refinement Process. A summary of these options and the costs are presented below.

A Buffering system

A potential Alternative Solution was considered by the Working Group. This differed from the Proposed Solution by introducing a buffering system to the mechanism that has been detailed in the Proposed Solution as a sixth business requirement. Instead of returning a Http 503 response

requesting the User try again and re-sending the Request, it would instead queue the Request until the next applicable time window opens where the Request could be accepted. A notification response would be sent to the User through a variant of the Http 503 to inform them that their Request has been queued rather than rejected and needing a retry attempt. Otherwise, the Alternative Solution was identical to the Proposed Solution.

Following Preliminary Assessment by the DCC the Alternative Solution was presented to the Working Group. One Working Group member stated they would prefer the notification to attempt a retry rather than having a Service Request queued. This was because with a retry a response would be given back in a timely manner, whereas they feared through queuing the response would be slower to return. The additional business requirement for the Alternative Solution was estimated to cost between £350,000-£750,000. That would take the cost of solution up to PIT to between approximately £2,000,000-£2,400,000. Other Working Group members felt this was too expensive to justify its inclusion into the solution, especially where it wasn't delivering a significant improvement. Both the Working Group and the Proposer expressed a clear preference for the Proposed Solution over the Alternative Solution, and so the Alternative Solution was not progressed further.

Following the Preliminary Assessment, the Working Group expressed concern about the cost of the modification. They questioned why this was the best solution and asked the DCC to consider if:

- additional infrastructure would be a better solution at an equal (or lower) cost; and
- if these events are rare perhaps 'taking the hit' of a DCC System outage and subsequent Disaster Recovery (DR) plans would be cheaper over a period of time.

The DCC investigated both proposals and responded with the following comments:

Additional Infrastructure ('Motorway Lane')

One alternative option is to increase the capacity of the existing DCC System by building additional 'Motorway' lanes that could accommodate surges in Service Request volumes.

Each additional Motorway is equivalent to the processing of 450 transactions per second. The total set up costs for one Motorway lane is £280,000, with annual operational charges of £50,000 per lane. These are estimated DSP costs only. There will be further Communications Service Provider (CSP) costs that will be associated with the set-up and operation of additional Motorways, though these have not been included. The table below shows the total costs for implementing up to five Motorway lanes:

Breakdown of DCC costs for new Motorways				
Number of additional Motorway lanes	**Cost (£280k per lane)**	**Operational costs (£50k per lane)**	**Total cost**	**Additional transactions per second**
1	£280,000	£50,000	£330,000	450
2	£560,000	£100,000	£660,000	900
3	£840,000	£150,000	£990,000	1,350
4	£1,120,000	£200,000	£1,320,000	1,800
5	£1,400,000	£250,000	£1,650,000	2,250

To increase the DSP Motorway to Profile 2[1], equivalent to 2,250 transactions per second, would require five more Motorway lanes at a cost of £1.4m with £250,000 of operational charges (although there could be some economies of scale here). However, other DSP infrastructure is likely to be needed to accommodate the accelerated rate of transactions such as change of Supplier (CoS), data management, databases etc, which will drive costs up further. This capability would then have to be replicated in the CSP costs, but if they're required to cope with surge volumes rather than actual usage, then they may need to scale to three or four times actual traffic volumes; this cost has not been included and would be additional to the costs set out above.

Current Gamma connections, which Users use to connect to the DCC Systems via the DSP, are capable of transmitting the equivalent of 30,000 Service Requests per second. Profile 5 caters for up to 6,000 transactions per second for the DSP. This will require 15 more motorway lanes. There would also be significant DSP Infrastructure increases when traffic levels reach 5,000 transactions per second which have not been included in the table above.

To provide the same protection as the Proposed Solution, this alternative option should be scaled for a worst-case instance to accommodate all 30,000 transactions per second. This is equivalent to an additional 67 Motorway lanes and would require a total investment in the region of £19m with an on-going maintenance cost of £3.4m. Again, this is the DSP cost only and does not provide protection to the CSP. The cost to the CSP is likely to be more than to the DSP.

Allowing DCC outages and using Disaster Recovery

It takes up to a maximum of four hours to switch over to the DR infrastructure, and if the same number of requests are then directed at the DR system, then it will also fall over when traffic reaches the level, as the DR system is sized the same.

The DCC Business Case found in Annex G estimates that for every hour the DCC System is down approximately £1m of costs would be incurred by the industry. Since it is not possible to estimate how frequently these events will occur and for how long, this leaves the DCC and the industry extremely exposed if they were to rely on DR only.

The costs are summaries in the Table below:

Indicative costs of all options considered		
Option	**Description**	**Potential cost**
1	Proposed Solution	£1,600,000
2	Input buffer to absorb peak demand	£2,350,000
3	Increased Capacity	£19,140,000[2]
4	Disaster Recovery	£4,000,000[3]

A Working Group member also suggested ADTs could be used instead as a solution. The DCC stated that ADTs were not granular enough to protect against a systematic error or DoS attack. They added

[1] Profiles are a stepped series of infrastructure allocations and configurations which will support increasing levels of traffic.
[2] This cost assumes the worst-case scenario of providing enough Motorway lanes to meet the maximum possible demand and thus provide the same level of protection as the Proposed Solution
[3] This cost assumes one use of the DR system lasting four hours

that Service Requests subject to ADTs are still received by the DSP. Because of this, the ADT mechanism would not prevent a DSP outage and therefore would not provide protection against the Service Request traffic leading to a DCC System failure. Finally, even if ADT thresholds were breached, it results in the messages being placed in quarantine rather than being rejected, which means they have to be fully processed by the DSP in order to place them in quarantine.

Conclusions and Summary of the Business Case

The Proposer believes the best option is the implementation of the traffic management mechanism. The Proposed Solution costs the least of all the solutions investigated. Furthermore, it provides enduring protection for the DSP System in the event of a spike in traffic.

The addition of five Motorway lanes will cost £1.4m with an additional estimated £250k of operational costs plus the ongoing costs of maintaining these. This would be large enough to cope with an additional 2,250 Service Requests per second. Each DCC User currently has the ability to submit 30,000 transactions per second.

Regardless of how many additional 'Motorways' could be added, a spike in Service Requests could still result in DSP failure or Service Users being 'crowded out' if the spike was large enough. Implementing the proposed traffic management mechanism at a cost of £1.6m would prevent this regardless of total capacity.

The Disaster Recovery choice was also discounted by the Proposer as in the event that the DSP fails there could be an outage of up to four hours (at an estimated cost to industry of £1m per hour, as detailed in Annex H). Furthermore, if the source of the influx of Service Requests had not been removed or restricted, the Disaster Recovery system would then also fail.

Which Service Requests need to be placed onto the Prioritised Service Request List?

The Working Group initially proposed an exemption list for priority Service Requests which would not be regulated even when the mechanism was in operation. The Working Group considered which Service Requests must have priority in the event of the DCC System approaching an overload. Early on, Working Group members wanted to include Service Requests relating to prepayment, as it was one driving factor for why the Modification Proposal had been raised. Calls were also made by Network Party members to include Service Request 7.4 'Read Supply Status' to give information on outages.

When the first draft of the Priority Service Request List was created, the Working Group agreed to remove the requests related to installing, commissioning and de-commissioning. The rationale was that these choices were not time-critical and advised that only Service Requests with target response times with 30 seconds should be considered.

The business requirements and subsequent Priority Service Request List were taken to the Technical Architecture and Business Architecture Sub-Committee (TABASC). The TABASC requested that it be the Sub-Committee that the Panel elects to manage and amend the list if the Modification Proposal is approved. However, the Working Group felt that all decisions relating to the traffic management under both SECMP0062 'Northbound Application Traffic Management Alert Storm Protection' and SECMP0067 should be delegated to the Operations Group. Some members felt the list included too many requests for a priority list; they agreed to it on the condition that it could be amended in future as stated in the business requirements.

As part of the Modification Proposal's Refinement Consultation, industry members were asked for any additional Service Requests they wanted to see on the list with accompanying rationale. Subsequent discussions with the Working Group highlighted that even if the mechanism was active the DSP would still be vulnerable to large bursts of these priority Service Requests. The DCC therefore agreed to take the advice of the TABASC and not to have a priority Service Request list. Service Users will know by receiving the http 429 that they have reached their capacity allocation and are being regulated and can then use their own business processes to prioritise their Service Requests as they see fit. This means that the Modification Proposal will move away from the objective of SECMP0028 'Prioritising Service Requests' which proposed introducing a DCC controlled prioritisation system for Service Requests. Instead, it will allow individual Users to submit their Service Requests in their preferred order within their Capacity Allocation, rather than it being a design of the DCC System to allocate a priority.

What percentage of total traffic did the proposed Priority Service Request list account for?

The Working Group questioned how much of the current Service Request traffic is made up of the SRs proposed to be on the priority Service Request list. The DCC has confirmed that the overall, the proportion of total SRVs fluctuates from 0.5% to 5% depending on User activity and the day of the week. However, it should be noted that the DCC is recommending no SRs be on the priority Service Request list. This view was supported by the TABASC.

Why is User Integration Testing not six weeks?

The Working Group was concerned that only four weeks had been allocated for User Integration Testing (UIT). The DCC provided the following response:

> *In terms of this Modification alone, plans for UIT are for two short testing windows to be scheduled in the UIT-B environment. All Service Users will be notified well in advance of when these testing windows will be in operation. The functionality will be enabled through a reconfiguration of parameters. The participating Service User(s) will be invited to send Service Requests and, being subject to traffic overload, will receive a 'system busy' response from the DSP.*
>
> *The two testing windows will be spaced sufficiently apart to allow any remedial actions to be undertaken by the Service User between the first and second test window.*
>
> *Proposals for UIT testing of the whole November 2020 SEC Release will be gathered and published as part of the DCC Testing Advisory Document, which is shared with, and approved by, the Testing Advisory Group.*
>
> *For the November 2019 SEC Release there were 15 days of UIT testing, consisting of five days pre-UIT and 10 days UIT for Test Participants.*

The DCC explained that the UIT figures previously presented were only a part of that testing. The testing would be considered as part of the wider November 2020 SEC Release. The Working Group members agreed that this made sense. The Working Group were concerned that if the Final Operating Capability (FOC) release slipped there would be a conflict with the November 2020 SEC Release Testing. It agreed that this was outside the scope of this modification but asked that the potential conflict should be highlighted as a risk.

Following the send back by Ofgem in May 2020 the implementation date has been moved to June 2021. The DCC have allocated six weeks of UIT to ensure Users get the requested amount of time for testing.

What reporting will there be?

The Working Group wanted to know what reporting would be provided and where it would be sourced from. It requested to see a mock report. The DCC has provided Wireframes of the proposed reports and this can be found in Annex C.

Additionally, the Working Group questioned how this would be reviewed and how the DCC would deal with Users who were 'persistent offenders' regarding capacity allocation breaches.

The DCC responded that Service Users in breach of their threshold will receive a report each month documenting when and how they breached their threshold and the impact on their SRVs and others. The SEC Panel (or a Sub-Committee nominated by it) will receive a report stating who had breached their threshold and the impact on the overall service. It will then be responsible for holding Service Users to account.

The DCC presented its wireframe reporting documents and asked for comments. One Working Group member questioned if the DSP scheduled activity would always be reduced in a traffic management event. The DCC replied that the DSP would be aware of the scheduled activity and if a traffic management event were to take place, it would be able to manage the activity to ensure it was processed. One Working Group member suggested that it would be useful to have reporting on the DSP scheduled activity included in the reports presented. They further requested that this should include if the DSP scheduled activity was then carried out and received within or outside the SLA. Another Working Group member suggested that since most of the SLAs for scheduled activity were 24 hours it was highly unlikely they would be delivered outside the SLA, but the Working Group agreed that it would be good to have this information anyway.

The DCC said it would discuss this with its Service Provider to confirm if it was possible to get these figures. If it was, it would include them in the reporting.

Views against the General SEC Objectives

Proposer's views

Objective (a)[4]

The Proposer believes that SECMP0067 will better facilitate General SEC Objective (a) by improving the efficiency and protecting the DCC System in times of high demand therefore by reducing the likelihood of a DCC System outage leading to delays in installation and commissioning and prepayment meter top ups.

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

Objective (e)[5]

The Proposer believes that SECMP0067 will better facilitate General SEC Objective (e) by improving the design of the existing DCC Systems. The improvement and innovation are being able to provide protection to the DCC Systems from heavy Service Request traffic, rather than just identifying it. Preventing potential outages should also provide a securer supply of energy to consumers.

Working Group members' views

Working Group members agreed that the Modification Proposal better facilitates General SEC Objectives (a) and (e). They agreed with the Proposer's rationale for both on protecting the business as usual process, offering innovation in managing the System and providing a securer energy supply.

Refinement Consultation respondents' views

The responses from the first Refinement Consultation were mixed towards whether the Modification Proposal should be approved. At the time of the consultation, one of the most common reasons for not supporting the Modification Proposal was the question as to whether this was the best solution for the available funding and that this business case should be explored in more detail. All respondents acknowledged that they would be impacted and that they would incur some cost outside the SEC process in rearranging their business process to accommodate the solution, although not giving definitive figures to these. Only one respondent believed that the Modification Proposal should be accepted, the other respondents citing that further analysis was needed post-consultation before the Modification Proposal should be accepted.

The first Refinement Consultation respondents differed as to whether the SEC objectives were better facilitated, with Objective (a) being agreed with by those who said the objectives were better facilitated, but all respondents believing Objective (e) is left unaffected.

The full set of the first Refinement Consultation responses can be found in Annex F.

Sub-Committee views on the modification

The TABASC reviewed the Modification Proposal's business requirements before a Preliminary Assessment was sought from the DCC. It queried the Priority Service Request List, in particular the inclusion of some requests it thought weren't time critical. The TABASC asked to be kept informed of any major changes to the Modification Proposal and expressed an interest in managing and amending the list, however the priority Service Request list has been removed from the solution.

The SSC was consulted in parallel with the Refinement Consultation. It agreed with the rationale that it could help prevent a DoS attack. However, it also noted that the Proposed Solution alone would only make it harder to inflict a DoS attack, not prevent one outright.

The Operations Group was supportive of the modification but was concerned about the priority Service Request list. As mentioned, the functionality for the priority Service Request list remains but currently no Service Requests are listed.

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

Panel's conclusions

The Panel raised concerns over the wider governance associated with including the Modification Proposal's solution into the Traffic Management Mechanism Document introduced in SECMP0062 'Northbound Application Traffic Management - Alert Storm Protection'. This was due to the Traffic Management Mechanism Document not being live at the time of the Modification Proposal going to Panel, and therefore making a change to that document was called into question. The Panel requested that the mechanism and accompanying details about the capacity allocation formula be moved to a new SEC referenced document. SECAS agreed to this.

One member of the Panel queried if this Modification Proposal could create unintended consequences if it goes live, given the number of other changes being introduced in the November 2020 SEC Release. The DCC stated it would share its testing strategy to ensure confidence that the Modification Proposal wouldn't create any adverse or unintended effects.

Following the Ofgem send back in May 2020 this modification is now targeted for June 2021. Fewer modifications are targeted for implementation in June 2021 and therefore the risk should be reduced.

Authority decision to send back

The Authority determined to send back the Modification Report on 14 May 2020. In its direction, the Authority requested the Modification Report include a clear succinct and complete assessment of the costs and benefits of the three options (the Proposed Solution, the additional 'motorways' and doing nothing). It also requested an assessment of the impacts of moving the modification from the November 2020 SEC Release to the June 2021 SEC Release.

Views on the modification after send back

Changing the implementation date

The DCC identified that one consequence of moving the implementation date to June 2021 was that the changes to DUIS to introduce the Http 429 would not be able to be implemented in June 2021 as there were no plans for a DUIS uplift. In order to ensure the mechanism could be implemented in June 2021 the DCC therefore suggested that the Http503 messages would be sent until the next DUIS uplift took place.

This was reviewed by the TABASC. They were concerned that the appropriate testing should take place and therefore expressed an opinion that the DUIS changes should take place in November 2021. They requested their opinions be shared with the Working Group.

The Working Group was reconvened and updated on the changes namely additional clarity to the business case and the change of implementation date to the June 2021 Release. The DCC's proposed approach which was supported by the TABASC was shared where the Http 429 response code would be linked to the DUIS version published in the November 2021 Release, where if a User uplifts to that version can use the response code. Prior to then, if implemented in June 2021, the solution will use Http 503 responses. The Working Group supported this approach but remained unconvinced by the Business Case and unconvinced that the Solution to the Modification Proposal will provide adequate traffic management.

A further question was raised in the Working Group about what happens if the CSP is down. A Working Group member was concerned that the DSP would still 'fill up' to capacity with messages that could not be passed onto the DSP. The DCC subsequently responded that in the situation where there is a CSP outage, the DSP will try to send messages to the CSP for a defined retry period. If the

CSP cannot accept them then the DSP will 'time out' fairly quickly and for any On Demand Service Request (with a 30 second Service Level Agreement (SLA)) will return a "Failed to send to CSP" message (Alert N12/error code E20) to the User. Only if the Service Request is Future Dated or DSP Scheduled (with a 24 hour SLA) will the DSP put the Service Request on a "long retry" queue and try again two hours later (for up to 24 hours). The DSP can manage the rate of handling retry messages to ensure it remains within capacity. In all cases, the number of requests sitting in retry queues (long or short) does not impact SECMP0067 or Traffic Management. The solution to this modification is all about managing the rate of receipt of new messages.

Appendix 1: Progression timetable

Following the send back by the Authority, this Modification Report will be presented to the Panel on 14 August 2020 with the recommendation it proceeds directly to the Change Board vote.

Timetable	
Event/Action	**Date**
Modification raised	30 Nov 2018
Initial Modification Report presented to Panel	14 Dec 2018
Modification discussed with Working Group	14 Apr 2020
Modification Report approved by Panel	17 Apr 2020
Modification Report Consultation	20 Apr – 24 Apr 2020
Change Board Vote	w/c 27 Apr 2020
Authority decision to send back	14 May 2020
Present to the TABASC	2 Jul 2020
Ad hoc Working Group meeting	9 Jul 2020
Issue Second Refinement Consultation	20 Jul 2020 – 3 Aug 2020
Present to the TABASC	6 Aug 2020
Present to Panel	14 Aug 2020
Change Board Vote	26 Aug 2020

Appendix 2: Glossary

This table lists all the acronyms used in this document and the full term they are an abbreviation for.

Glossary	
Acronym	**Full term**
ADT	Anomaly Detection Threshold
DCC	Data and Communications Company
DoS	Denial of Service
DSMS	DCC Service Management System
DSP	Data Service Provider
PIT	Pre-Integration Testing
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SMIP	Smart Meter Implementation Programme
SSC	Security Sub-Committee
TABASC	Technical Architecture and Business Architecture Sub-Committee
TOC	Technical Operations Centre
UIT	User Integration Testing