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' and SECMP0067 'Service Request Traffic Management'

November 2019 Ad-Hoc Working Group Meeting

19 November 2019, 12:00 – 15:00, Gemserv Offices.

Meeting summary

Modification Proposal Overviews

SECMP0062 Overview

SECMP0062 'Northbound Application Traffic Management - Alert Storm Protection' looks at providing the implementation of a traffic management solution to protect the DCC system and Service Users against Alert Storms originating from a single device. Currently, there is little protection in the DCC Systems to prevent against nuisance Alerts which unnecessarily uses up capacity in the systems.

At this point in the Modification Proposal's timeline, the Proposal was returned to Refinement from the Change Board due to points of clarification needed for the solution. The DCC were asked to provide updates to the Working Group to highlight where queries had arisen in the Modification Report Consultation and the previous Change Board meeting.

SECMP0067 Overview

SECMP0067 'Service Request Traffic Management' is looking at throttling Service Requests from individual Users in instances where the DCC Systems may suffer an outage due to abnormally heavy traffic. The proposed solution is to introduce capacity thresholds for the DCC Systems and for each individual User and in the case of a DCC Systems capacity being breached, it will throttle the User down to their allocated capacity or the remaining capacity in the system, whichever is greater. This means that only Users who overwhelm the DCC Systems with Service Request traffic will be subject to throttling, rather than the current system behaviour which would throttle all Users indiscriminately.

At this point in the Modification Proposal's timeline, the Proposal is still in Refinement. A request for the Impact Assessment at Change Board was rejected due to clarifications being required on the business case and solution. Additionally, it was recommended that SECMP0062 and SECMP0067 were both looked at together for a holistic approach on traffic management. DCC were asked to provide updates on the clarifications requested at Change Board and to give an update on the overall approach for Traffic Management in SEC Change.

Working Group discussions

Wider Traffic Management Strategy

The DCC delivered a presentation on Traffic Management. In this presentation, the DCC confirmed that the original forecast daily Alerts traffic was estimated at 2 million Alerts between SMETS1 and SMETS2 devices. This contrasts with the current reality which has daily Alert volumes at approximately 34 million Alerts, with less than 10% of Smart Meters installed. The DCC have also stated that the Technical Operations Centre (TOC) is also being utilised to help remedy other issues outside of the SEC Change process. The TOC's activity includes identifying devices sending high levels of messages (known as 'Top Talkers') and investigating the root causes of the nuisance Alerts.

A question was raised about the longevity of the solution of SECMP0062 as part of this wider strategy, asking whether this was short term but urgent. DCC stated that if a CSP traffic management solution were to be implemented, the SECMP0062 DSP solution wouldn't be the first layer of protection but would be used in the case of the CSP failing. The DCC added the point that without a CSP solution being implemented and funded, the DSP solution would be the only form of DCC System protection against Alerts. The DCC stated that a CSP solution where the throttling or management of Alerts that could be delivered on the HAN is aspirational, and at least 2 years away. This is due to existing firmware releases scheduled that need to be delivered for the current generation of Communications Hubs. This confirmed the view that SECMP0062 and SECMP0067 would be needed whilst a CSP solution is being developed so that a level of protection could be provided to the DCC Systems.

It was agreed that SECMP0062 and SECMP0067 should be progressed independently of one another. This way, one Modification Proposal would not be held up by the other. Additional actions were noted that DCC would need to take in the next steps before SECMP0062 is taken to Panel or SECMP0067 is issued for Refinement Consultation and subsequently Impact Assessment.

SECMP0062 Working Group Discussions

The DCC presented the "User Story" of SECMP0062 which explained the origins of the Modification Proposal. Currently, the DCC systems identify anomalous behaviours including counting Alerts from Devices, they do not perform any actions to resolve them and no longer raise Incidents for Users to take action (this was switched off owing to the overwhelming number of Incidents being raised).

When a threshold is reached the DSP would begin counting Alerts per Device per Alert Code. Initially, all Alerts are delivered, but if another threshold is met within a time period, the DSP will forward to the User a proportion (1 in n) of the Alerts from a Device per Alert Code. For clarity, if a Device starts to produce different Alerts it will not be automatically filtered because a different Alert is being filtered. Similarly, if a different Device starts to produce the same Alert it will not be filtered unless it meets the thresholds.

A list of Alerts that will not be filtered will exist and all parameters are configurable – these will be global (e.g. for "1 in n", "n" will apply for all Alert Codes). The configurable parameters will be managed by the Operations Group, with input from other Sub-Committees, as appropriate.

A 'deadband' period is used to avoid creation of Incidents when Devices repeatedly flip above and below thresholds in short periods of time. A Working Group member commented that setting this period of time to 24 hours may hinder a Supplier's ability to determine whether actions to resolve anomalous Alert generation has been successful.

When asked about making the parameters configurable by Alert Code, the DCC responded that this had been considered but recommended making it the subject of a future enhancement.

One Working Group member asked if the DUIS changes for Device Alerts would include the metadata in the header. DCC confirmed this, that the DSP adds data (such as Alert 1 of N) to the Alert's original content, but only if Alerts of a specific Alert Code from a specific Device is subject to throttling. This way, an Alert that hasn't been subject to throttling will not include the metadata in the header. The DCC stated that this functionality will only be available for Users who have the version of DUIS the solution is included into, but will maintain backwards compatibility and will not cause failures for Users retaining previous versions of DUIS. A view of the Device and Alert Code combination is available as part of the solution on the Self Service Interface (SSI) dashboard. Between this and the TOC's analytics, the DCC say that a full view of the traffic management provided by the Alert Storm protection is available. DCC confirmed that the settings for the Alert Storm Protection are "global settings" and cannot be set at an individual Alert Code level. The decisions on who sets the parameters for the Alert Storm Protection settings will be overseen by the Operation Group. Additionally, the Security Sub-Committee (SSC) and Technical Architecture and Business Architecture Sub-Committee (TABASC) can offer their input by sending representatives to the Operations Group.

The DSP will record all Alerts being filtered and information will be available to Users. However, it is likely that Incidents will not be raised when the solution initial goes live (the volume of extraneous Alerts is likely to make this unhelpful). Once Incident creation is switched on for this solution, Users can then choose whether to receive email notification, but that functionality is either on or off for all Incidents, per User.

A point was made to clarify the reporting for the Proposed Solution in the modification report, so that Users know exactly what is being reviewed. The reporting will include the Exempted Alerts List and how often the Alert Storm Protection mechanism is used. The reporting will also include the values the configurable parameters are set to.

The implementation approach that was put forward is that Part 1 of the solution if the Modification Proposal is approved would be scheduled for June 2020 and Part 2 will be introduced in November 2020. These would be implemented alongside the appropriate SEC Releases. Design documentation for the solution, especially that necessary for Users to understand the impact on them, and legal text will be developed for each Part of the solution's implementation. SECAS took note of this and added it to their actions.

Finally, when a DNO member in the Working Group was asked whether this provided an improvement on their initial comments sent back in the Modification Report Consultation earlier on in the process, they agreed in part. Their condition was that the clarifications made in the Working Group had to be expressed in the Modification Report. This included making reference to the Alert Storm Protection being at an individual Device level, rather than across the board for an individual Alert Code.

SECMP0067 Working Group Discussions

The DCC presented the "User Story" of SECMP0067 which explained the origins of the Modification Proposal. The solution being proposed is to allocate service capacity to each User so that in the case of a capacity threshold being breached, a User will be throttled back to either their allocated capacity or the remaining capacity within the system, whichever is higher. The DCC confirmed this will only impact the Users who breach their allocated capacity, the Users who don't will remain unaffected. A list of priority Service Requests has been designed so that they aren't subject to throttling. This was due to certain time-critical Service Requests that Users will require every copy of, ahead of other Service Requests that could be throttled. It was noted that this list may have expanded owing to concerns that the throttling may take place for significant durations and that the effect of having a long priority list means less prioritisation. The window the Service Request throttling should take place in according to DCC would be a matter of seconds, not in minutes or hours.

There were confirmations that there would not be any DUIS changes in the modification. The DCC mentioned this was due to not using any metadata or making any new responses, instead using an existing “HTTP 503 System Busy” response. DCC also mentioned that the HTTP 503 could have a message asking to retry later but typically this is used when systems are taken down for a known period for maintenance.

It therefore made sense to keep any potential legal text to governance changes, rather than creating technical changes to the SEC documentation. SECAS confirmed that the parameters associated with the solution would be contained in a document outside the SEC, allowing for the Operations Group to manage it with greater ease. The Working Group agreed that the governance for managing the external document containing the parameters should be contained within the SEC. Additionally, the Working Group agreed that guidance should be used rather than technical obligations in the SEC. The suggestion was to use either the DUIS Guidance notes or DUGIDS to house these guidance changes. There was an action to review where the guidance would best be placed by taking advice from DCC and the TABASC. One Working Group member expressed a favour towards the DUIS Guidance notes over DUGIDS due to DUGIDS on occasion being out of line with DUIS and with the notes aligning with DUIS.

One Working Group member queried about the capacity allocation formula provided. Previously, a set of the guidelines for the formula and how it determines a User’s capacity was released in the Preliminary Assessment. However, these guidelines did not explain every variable associated with the formula or provide a simple breakdown. An action was therefore tasked to the DCC to improve on the explanation on the formula so that somebody with no prior knowledge would be able to understand the formula. SECAS confirmed that no approval would be sought before a layman’s terms version of the formula and its variables was made available for viewing.

The DCC confirmed that the DCC Systems’ designed capacity should always cater for known peaks in usage – regardless of whether the peak is daily, weekly, monthly, etc. The expected usage of this throttling mechanism is only to deal with situations where an individual User’s systems are behaving abnormally and that it will protect all other Users whose systems are causing normal traffic.

One key area of discussion in the Working Group meeting was the reporting that would be undertaken in SECMP0067. One of the key elements for the reporting that was agreed was the frequency of how often the solution’s mechanism is used and the reason for the mechanism being invoked. The Working Group agreed this as it would help identify any trends for why the DCC System capacity approaches full usage, particularly to confirm that it is protecting against abnormal events or being used in lieu of providing adequate capacity. Additionally, the members believed this would help to identify any peaks in the service capacity usage – thought to be when batches of Service Requests are sent by a User. The reporting will be taken to the Operations Group with accompanying rationale as to why the solution’s mechanism has been activated, whether by accident or if it was done deliberately.

Next Steps

DCC Actions

DCC will provide answers to questions asked in the Traffic Management overview. These are:

- How many SMETS1 Alerts were there?
- How have these SMETS1 Alerts been dealt with previously?
- How the DCC Systems were designed initially to deal with alerts, and how is this different to the current situation now? (In response to the original systems prediction being on 2 million daily alerts).

DCC will provide a layman's terms description of the service capacity allocation formula and explain every variable and constant associated with the formula.

SECAS Actions

SECAS will ensure all the questions raised are answered and take SECMP0062 Modification Report to December 2019 Panel and to January 2020 Change Board.

SECAS will request the SECMP0067 Impact Assessment sign off from the Change Board at the next available date. Following this, the business requirements will be restructured to include the details on reporting discussed in the Working Group. The new requirements will be used for an Impact Assessment and a Refinement Consultation will issued before going to TABASC and the Panel. In tandem with this, SECAS will consult on where the SECMP0067 guidance will be provided.