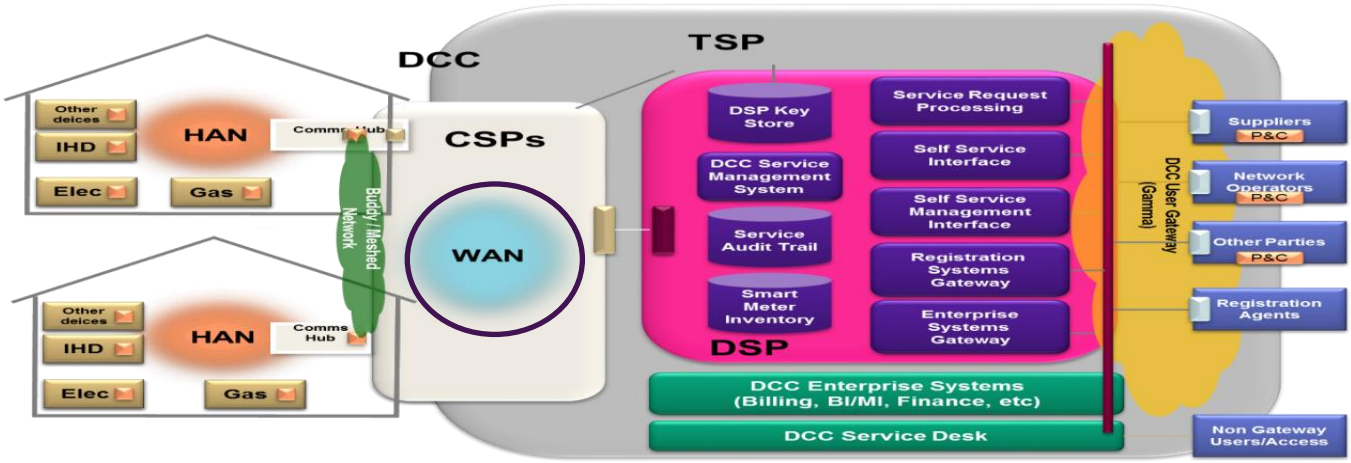
DCC Major Incident Review Report

(Produced in accordance with Section H9 of the SEC)

Date of Incident(s)	30/11/2020
DCC Incident Reference Number	INC000000661032
DCC Problem Reference Number	PBI000000121832
Service Impacted	CSP North Region
Date/ Time Incident reported	30/11/2020 09:02 (Actual outage start time)
Parties involved	CSP North
Date &time incident resolved	30/11/2020 09:25 (Outage restoration time)
Time taken to restore Service(s) (Hours)	23 Minutes
Resolution within SLA (Y/N) *[SEC 9.14(b)]*	Y
Potential SEC Modifications [SEC H9.14(g)]	N
Major Incident summary report *[SEC 9.14(a)]* attached: Y / N	**Y - SEE APPENDIX 1**

Infrastructure Topology View



Summary of Impact [SEC H9.14(c)]

At 09:33 30/11/2020, A Service User raised incident INC000000661032 confirming they were experiencing issues with Install and Commission Activity. The Incident was escalated to DCC Major Incident Management (DCCMIM) at 09:58 where an initial call was placed into the CSP North helpdesk. CSP North confirmed they had experienced an outage between 09:02 and 09:25 and full service was now restored.

DCCMIM declared a retrospective Category 1 Incident due to the total network outage for 23 minutes.

A Major Incident Management bridge was hosted by DCC Incident Management, where it was identified that full service had been restored and the CSP North systems were processing transactions as normal following the earlier outage. DCC TOC also confirmed that traffic volumes had returned to normal levels.

Full-service restoration was observed at 09:25 by CSP North Network Management Centre (NMC) engineers following the failover of traffic.

This impacted all Service Requests across the CSP North Region between 09:02 and 09:25. Approximately 68 Installs were affected, and 224 Service Requests required retries.

Incident Mitigation [SEC H9.14(c)]

As an immediate mitigation CSP North have added a further 2 rectifiers into their infrastructure to ensure there are no Single Points of Failure. Further checks are being carried out across their ecosystem to ensure there is resilience within each critical area of the CSP North SMETS2 solution.

A High priority case has been raised with their Vendor to investigate the network routing bug which caused the delay in failing over traffic.

Following the Problem Management investigation, it was found that the routing issue had no impact on this Major Incident.

CSP North have introduced additional advanced monitoring capability (U2000) across their estate, which will improve response to service interruption and help ensure quicker service restoration.

Preventative Measures [SEC H9.14(d)]

CSP North introduced a further 2 rectifiers on 30th November in an active/active state to support power resilience at the Data Centre.

Active/Active state would mean a seamless failover with no downtime.

CSP North have introduced enhanced monitoring to assist with multiple failures to determine/assess impact at time of MI declaration.

Root Cause Summary [SEC H9.14(d)]

Following investigations carried out by CSP North and their support providers, root cause has been determined and they have concluded:

1. Rectifier Failure –The Root cause of the Incident is aligned with inadequate third-party proactive maintenance that exposed ineffective fault tolerance (causing a single point of failure).

   The cause of the fault was a power supply failure, as a result of a tripped circuit breaker for the IT racks in the data centre. This power failure triggered a failover of core back-haul circuits.

   The failed rectifier was successfully replaced. A further 2 rectifiers were installed to support power resilience at the datacentre on 30th November 2020.

2. A Software bug in the network routing protocol was delayed when failing over (23 minutes and should be instantaneous) – *Further investigation is ongoing under problem ticket PBI000000121832.*

Root Cause Actions

(Actions tracked under Problem investigation ticket - PBI000000121832)

Item	Description	Owner	Closed	Open	Enterprise wide Y/N
1.	Why did DCC Service Centre not send identified comms when the initial Incident came in advising 3 SEC parties were experiencing issues. – *This was an individual user error; and will be rectified with further training and updated WI's for Service Centre Operatives. MIM has met with senior Service Centre staff, Team Leader's and Ops Managers.*	DCC SC	✓		

2.	Why did CSP North not notify DCC of the issue with a high priority Incident. – *Multiple failures hindered notification process. CSP North have reviewed the process and moving forward Ops Manager will be reviewing and ensure it's notified to DCC within 15 minutes.*	CSP North	✓		
3.	Why did DCCTOC not identify this – *this incident was identified by TOC staff but due to a misjudgement the MI was not called. A training refresh with the engineers has taken place and they will engage MIM should monitoring identify any failures.*	DCC TOC	✓		
4.	CSP North raised Incident – INC000000660865 at 08:30 for 125 sites – *CSP North confirmed this was Related and was raised as a loss of resilience only which resulted in a CAT3. This was an early warning sign of the CAT1.*	CSP North	✓		
5.	Did CSP North Monitoring pick this up? – *Yes, but notification process to the DCC was delayed due to multiple failures within their infrastructure. New monitoring has been introduced by CSP North and changes to their triage process been carried out.*	CSP North	✓		
6.	Does/has CSP North monitoring need to be reviewed? – *Further monitoring tools (U2000) allowed NMC to look at dark circuits to compare when failure is occurring. System access arrangements are in flight for all engineers within their NMC.*	CSP North		✓	
7.	CSP North response to Major Incidents needs to be reviewed due to DCC finding out from Service Users after the issue was fixed – *Actions taken please refer to #Action 2.*	CSP North	✓		
8.	Root Cause – *Rectifier Single Point of Failure, Network Routing.* *Refer to root cause summary Item 1.*	CSP North	✓		
9.	Full architecture design review – *Ongoing, CSP North network refresh is planned for Q1 2021*.	CSP North		✓	
10.	When if/did CSP North Vendor notify them of this bug – *this is to be confirmed under problem ticket PBI000000121832.*	CSP North	✓		

Identified Risks:

(Actions tracked under Problem investigation ticket - PBI000000121832)

Item	Description	Owner	Closed	Open	Enterprise wide Y/N
1.	Vendor (Huawei) kit and future proofing against any new UK laws that come in that could cause issues on replacement kit. *CSP North to review internally.*	CSP North		✓	Y
2.	Network Routing bug causing delays with traffic re-convergence – Review to be completed under Problem ticket PBI000000121832. Monitoring to be put on hyper care (de-risked with extra rectifiers).	CSP North	✓		

Details of the review of the response to the Major Incident and its effectiveness [SEC H9.14(e)]

Identification	DCC were not proactively made aware of this failure until the outage was fixed and Service Users started to experience issues with Install and Commission.	
Classification/Prioritisation	Initial Incident came in as a Service User Category 5 and was escalated to a Category 3 by the Service Centre. Once MIM were engaged at 09:52 it was confirmed this was a total outage and this was escalated to a retrospective Category 1.	
Investigation/Diagnosis	Investigation had already been completed by CSP North and full service was restored.	
Resolution/Closure	Fix had already taken place before DCC MIM were made aware of the outage.	
Customer Communications	DCC MIM provided regular updates via the Incident Management team using SSI Broadcast but there was a significant delay from the DCC Service Centre when sending out Mass Comms.	

Any failures by Incident Parties to comply with their obligations under Energy Licences and/or this Code [SEC H9.14(f)]

None

The likelihood there will be a reduction in the DCC's External Costs arising as a consequence of the DCC Service Providers failing to achieve a restoration of any Services within the Target Resolution Time [SEC H9.14(g)]

None

Table of linked incidents

Incident	Linked incident	Nature of link
INC000000661032	INC000000660885	Duplicate
	INC000000660945	Related
	INC000000660865	Related
	INC000000660927	Related
	INC000000661168	Related
	INC000000661024	Related