Full Report on CSL Service Interruption on 13 May 2013

1. Introduction

On 13 May 2013, CSL 2G & 3G services covering Shatin/Tai Wai/Ma On Shan/Tai Po areas were interrupted for about 1.8hrs, affecting both voice and data services. 4G LTE coverage plus its associated data services were not affected. This preliminary report summarized the event of this incident and the steps taken to recover our services.

2. Incident Description

The service interruption was found to be caused by a software problem, which corrupted a 3G Radio Network Controller (RNC) configuration file, causing failure of both voice and data service under the aforesaid areas. When the 3G handsets attempting on 2G layer, the enormous traffic volume had overloaded a 2G Base Station Controller (BSC) covering the same areas resulting into intermittent or failure to access voice and data services.

3. Incident Event Log

Date and time of the outage incident:	13 May 2013, 10:10pm to 14 May, 12:00am
Affected areas:	Shatin/Tai Wai/Ma On Shan/Tai Po
Estimated number of customers affected:	20,000 active customers

Time	Event
10:10pm	CSL's Service Operations Centre observed alarms in the RNC and BSC serving Shatin/Tai Wai/Ma On Shan/Tai Po areas. Customers also reported difficulty in accessing 2G and 3G voice and data services in the affected areas. The problem was immediately escalated to support engineers and vendor for investigation.
10:15pm	Support engineers tried to recover the respective RNC and BSC by hardware and software reset but could not restore their traffic handling ability. Vendor was investigating the problem in parallel.
10:40pm	Vendor support engineers identified part of a RNC system configuration file was corrupted and a BSC was being flooded with customers who were falling back from the 3G network.
10:50pm	Vendor tried restoring the RNC system configuration file from the latest backup but the RNC could not be started up properly. Suspected the corruption had extended to the latest backup version.
11:06pm	CSL's Service Operations Centre contacted OFCA duty officers to report the incident to proactively provide information and minimize confusion.
11:30pm	Vendor attempted to restore the RNC from the next older version of backup file. After completion of the restoration of the file, the problematic RNC became operable.
12:00am	All affected cell sites resumed operation. Verified with traffic data and

	customers that 3G service was restored and the congestion in the BSC was also relieved.
12:03am	CSL's Service Operations Centre provided update to OFCA duty officer that the service resumed normal. Agreed with OFCA to provide another update before 1:00am.
12:56am	CSL's Service Operations Centre provided update to OFCA to confirm again resumption of service after observing network statistics and customer feedback.

4. Remedial Actions Taken

It is the network design of CSL to allow 2G network picking up traffic from 3G network when the latter encounters problem. This mechanism worked as planned at that time but the performance of 2G network was observed with degradation due to repeated access attempts by the affected customers during the incident.

Our support engineers and vendor took immediate actions to investigate the problem. Our vendor had identified that the problem with the RNC was due to corruption of part of the RNC configuration file. We then reloaded the RNC with the latest backup file but failed. Our vendor suspected it might be related to corruption of the backup file. We decided to reload the problematic RNC with the next older version of backup file and successfully restored the RNC. The congestion on 2G BSC was also relieved.

5. Root Cause Analysis

According to the findings and analysis, there were two key points to address:

a) RNC configuration data corrupted

The affected RNC was a new model with higher processing power. A software upgrade was planned at 2am on 14 May and was the first of its kind to be upgraded. As part of our quality assurance, both software features and upgrade procedures had gone through verification in our offline lab environment and no deficiency was found.

At 6pm on 13 May, our vendor started the pre-upgrade check followed by upgrading an RNC command interface according to the approved upgrade procedure run-down. This part of the upgrade procedure was a proven and non-service affecting activity so we agreed with our vendor to carry out at 6pm as part of the preparation work before the actual RNC software upgrade at 2am in the next morning. At 10pm on 13 May, a planned daily routine for radio capacity adjustment via an execution of auto-script command was automatically activated in this RNC. The routine sent commands to the new interface and the new configuration data file was subsequently downloaded to the RNC that was still with the old software version. Due to

the version incompatibility, the command was incorrectly interpreted by the RNC and therefore caused corruption to both the RNC online configuration files and backup software.

According to our vendor's investigation, the data corruption was due to the fact that their software did not screen for incompatible commands across different software versions. Also, their upgrade procedure did not inhibit auto script command execution in between upgrade steps.

b) Underlay BSC was unable to take up all traffic from 3G

According to the network design, our 3G users would automatically select 2G network when 3G network was unavailable. As a result, we observed the respective underlying BSC was being overwhelmed by our customers' repeated attempt to get voice and data services at the same time. Such action created a snowball effect causing an overloading of the BSC. Consequently, the affected customers could hardly use the 2G service and some of them might suffer from "no service".

6. Number of Affected Customers

The estimated number of customers affected is less than 20,000 active customers, who might have attempted to make outgoing or incoming call voice or data calls.

7. Communication with Customers and the Media

All staff of customer service hotline were briefed before and after service recovery to handle call enquiries of the incident.

Once the service was back to normal, a SMS message was sent at 00:45am on 14 May to the affected customers who had called in for enquiring the incident to inform them the service resumed normal and to apologise for the inconvenience caused.

A detailed statement was prepared to provide information of the incident including root cause, affected area, time of service interruption and recovery at 10:00 am on 14 May for frontline staff to answer enquiries and for media to understand the incident in more details. The statement also mentioned that the incident had only affected the 2G and 3G voice and data services for around 1.8 hours in the late evening while 4G mobile data service remained normal.

CSL communicated with customers, the media and the general public via the following channels:

<u>Customer hotline</u>

- CSL pulled together all frontline staff at the call centres to handle customer enquiries before and after service recovery.

<u>SMS</u>

- Once the service resumed normal, a SMS message was sent at 00.45am on 14 May to the affected customers who had called in for enquiries on the incident.

Retail shops

- All frontlines were briefed about the incident and the statement for handling potential customer enquiries before the retail shops opened for business on 14 May.

Media

- The statement was issued to the media at 10:00 am on 14 May to inform the details of the incident. CSL had been following up with the media during and after the incident.

Facebook and websites

- The statement was posted on 1O1O and one2free official Facebook at 10:00am and 1O1O and one2free websites at 11:00 am on 14 May.

8. Measures to prevent similar incidents

In order to prevent the occurrence of similar incidents in future, we together with our vendor have implemented the following measures:

- Our vendor had enhanced the upgrade procedure by adding steps to inhibit auto script command activation from all sources except the upgrade console. By suppressing this function, we would eliminate any unexpected modification of the system configuration data in the course of upgrade.

- Our vendor had enhanced their software with screening function for incompatible commands across different software version. With this enhancement, we would eliminate any unexpected conflict between two software versions that may cause any adverse impact to the live network.

- These new procedures had already been re-run in our lab environment and live network, including simulations of accidental activation of daily routine script. The result was positive with no software data corruption being found.

- Our analysis showed that data service request contributed significantly to the overload situation on the night of 13 May. In response, we had developed procedures to control traffic overflow mechanism to 2G service during emergency situation in order to provide a stable service to customers who are being affected.