Report on Air Traffic Management System Occurrences on 29 November & 12 December 2016

1. Introduction

1.1 On 29 November and 12 December 2016, the Civil Aviation Department (CAD) experienced two similar occurrences as detailed below.

29 November 2016 - During full operation of the Air Traffic Management System (ATMS) at 13:15 (HK time), the primary server of the Flight Data Processor (FDP#1) of the Main System experienced a file access anomaly induced by an interactive playback session initiated on FDP#1, triggering automatic switchover to its hot-standby server (i.e. the secondary server – FDP#2), while putting FDP#1 offline. As per the system design, the process was automatically initiated and completed. External links with interfacing systems were not affected during the switchover. At 13:20, per standing procedures, the offline FDP#1 server was manually restarted to restore full hot-standby dual operations of the FDP. During the restoration process, at 13:25, the screen refreshed with momentary flight plan dis-association affecting those targets that were already associated with flight plans at the time at all logged-on workstations. Display of information was affected for about 26 seconds. The root cause of flight plan dis-association was that the FDP#2 had to handle the flight information synchronisation to FDP#1 required for the restoration of FDP#1 in parallel with the on-going flight plan association process, with the former being set to take a higher priority, thus the occurrence of temporary flight plan dis-association.

12 December 2016 - At 11:47, retrieval and archiving of data from the FDP of the Main System was initiated. Shortly after the process was initiated, radar screens refreshed with flight plan dis-association for currently associated targets at all logged-on workstations momentarily. The flight information reappeared automatically after about 75 seconds - a similar observed phenomenon and the same root cause as that of the 29 November 2016 occurrence described above.

1.2 The Transport and Housing Bureau has requested NATS to assess the course of actions taken in response to these two occurrences, to advise the impact to the safety and readiness of new ATMS, and to make relevant recommendations based on NATS' experience in similar system transitions.

1.3 The framework applied for the NATS' review has been based on the key elements of existing NATS process, experiences of investigating and subsequently resolving similar occurrences. This report details the following aspects of the occurrences in turn to assess how the events and associated corrective actions were handled, and whether appropriate steps are in place to minimise the risk of recurrence. Accordingly, NATS' review is focused on three areas, as follows:

a) Incident Management and System Fallback / Recovery;

b) Incident Investigation / Tracking / Rectification / Testing; and
c) Impact on staff training and procedures.

1.4 To facilitate its review, CAD has provided relevant documents and supporting evidence including system logs and records, system health checks, operational and engineering instructions and contingency procedures, briefing materials, internal and external communication materials to support NATS' assessment and to address NATS' recommendations in ensuing paragraphs.

2. Incident Management and System Fallback / Recovery

Expectation of display occurrences within normal Air Traffic Control (ATC) operations

2.1 Teething problems are not unexpected particularly for a large and highly complex system such as an ATMS during the initial period following the full system commissioning. From NATS' experience, some outages such as a radar station loss have little impact on our service due to resilience of multi-radar tracking, providing a mosaic of overlapping coverage such that loss of any single radar rarely leads to a service impact. Noting the high potential impact to operations of inadvertent system outage NATS further minimises risks of service outage by undertaking 'higher potential impact' activities overnight when traffic levels are relatively low to allow more time to manage / overcome any transition issues and to make decisions.

NATS Observation 1 – While safety is of utmost priority, it is not practical to achieve zero risks or have a system with no issues reported. According to the ICAO requirements, risks need to be assessed and mitigated to an acceptably low extent. In NATS' experience, it is not unusual for new systems or new functionality introduced that were stable during trial to cause issues when transitioned into service. The occurrences on 29 November and 12 December are not unusual given these facts and factors.

Safety assurance and handling of event during and following the occurrences

2.2 Both occurrences (on 29 November and 12 December) resulted in the temporary flight plan dis-association (for 26 and 75 seconds respectively). During these periods controllers were still able to see from their radar displays the essential flight information including the aircraft position and altitude, and identification of the aircraft from their assigned Secondary Surveillance Radar Code (SSR Code), which is a 4-digit identifier code uniquely assigned to each individual flight prior to departure. Additionally, for the case on 12 December, air traffic control officers could elect to obtain references to additional flight information through the then recently-implemented ASM (ADS-B Surveillance Monitor) at the Executive positions. Direct controller-pilot radio communications were

maintained and fully functional at all times. In both occurrences there was no report of safety related occurrences by ATC.

2.3 On 29 November, as a usual precaution, departure flights were temporarily held on ground for 15 minutes while an on-site review meeting was immediately held at the East Air Traffic Control Centre (E-ATCC) between Management staff, Supervisors and Subject Matter Experts (SMEs) from both engineering and operational divisions. Given the momentary loss of flight association and quick and automatic resumption of normal system operation, the meeting concluded to resume normal ATC service given the availability of other contingency measures (including the Fallback System and Ultimate Fallback System (UFS)) at all times. Accordingly the temporary stoppage of departure flights, which lasted for 15 minutes, was lifted.

2.4 On 12 December, as a usual precautionary measure, departure flights were temporarily held on ground for 4 minutes while an on-site review by engineering and operational staff was conducted. Given the momentary loss of flight plan association and automatic recovery, the continued availability of the Fallback System and UFS, it was decided to resume normal ATC service. There was minimal impact on departure flights resulting from the temporary suspension of departure flights.

NATS Observation 2 – Whilst the temporary loss of certain flight information could affect the normal working practices of ATC, the alternate identification methods available that had been covered in the basic training for every controller still enabled the controllers to provide a safe ATC service. It was a prudent and safety measure for ATC to temporarily withhold outbound aircraft under the circumstance allowing the situation to be assessed by multidisciplinary professionals prior to resuming normal service. This is on par with that adopted by NATS and international best practice. The two levels of fallback provisions (i.e. Fallback System and UFS) were unaffected and available at all times during the occurrences.

Curtailed service delivery during the 29 November occurrence

2.5 On 29 November a total of nine departure flights were held on the ground during the temporary departure suspension. Neither flight cancellations nor knock on delays were reported as a result of the occurrence. On 12 December no flights were significantly delayed as a result of the temporary suspension of service to departing aircraft.

NATS Observation 3 - It is an international norm that implementation of safety measure should always outweigh delay. Whilst the slight impact in terms of delays and punctuality was unfortunate and to be avoided as far as possible, given the speed of response to the scenario and the need to assess the stability of the system following the resumption of normal performance of the ATMS, the temporary suspension of departure flights is considered proportionate to the scale and impact of the occurrence.

3. Incident Investigation / Tracking and Rectification

Fault diagnosis

3.1 **Occurrence on 29 November** - CAD requested the Contractor to promptly investigate into the occurrence with system logs and relevant data immediately provided to the Contractor. Following prompt investigation and analysis of the occurrence, the Contractor provided an investigation report (Reference 1, Appendix 1) with root cause and workarounds identified within 48 hours of the occurrence.

3.2 **Occurrence on 12 December** – upon investigation, the Contractor had promptly confirmed that the occurrence of December bearing the same root cause with a common fix for both occurrences.

3.3 On both occurrences, the temporary loss of flight plan information from the ATC display was caused by the Flight Data Processor having to respond to a manually triggered maintenance processes. For both occurrences there was no loss or corruption of flight plan data. The Surveillance Data Processor (SDP), which tracks and displays essential positional data and flight identification of aircraft (SSR code), and all other functions were also functioning normally. Moreover, the Fallback System and the UFS were operating normally and available for selection at all times.

NATS Observation 4 – The Contractor has promptly analysed the system log and diagnosed the issues with explanation consistent with the occurrences and confirmed no loss or corruption of flight plan data. The two levels of fallback provisions were unaffected and available at all times during the occurrence.

Strategies to minimise risk of recurrence until a permanent fix of the root cause is established

3.4 Given the quick identification of the cause of flight plan dis-association and the causal circumstances, the proposed mechanism for a fix should be available shortly and the interim workarounds should avoid the causal factor associated with engineering procedures i.e.

- Interactive Playback sessions should only be carried out in the Fallback System at all times without inducing any risk on the operational system or impacting Main System operation; and
- CAD should manage synchronisation of flight information by scheduling to bring up the offline FDP during periods of low traffic, while not retrieving or archiving data from the Main system under normal circumstances.

3.5 NATS is satisfied that these measures are both effective and readily available. Beyond the two instances included in the report, there have been no further instances up to the time of publication of this report (5 March).

> **NATS Observation 5** – CAD has clearly identified both ATC and engineering operating instructions to adopt workarounds above to minimise the risk of recurrence through revised procedures which have been promulgated to staff concerned, while a permanent software change is being developed and tested.

Testing the Change

3.6 The change was planned to be available in December 2016, with CAD reporting that their review with the Contractor on 6 December 2016 had confirmed availability was on course. CAD has requested the Contractor to conduct thorough testing at factory before delivering the change to Hong Kong for subsequent on-site testing / regression testing / system reliability performance / safety assessment prior to launch. CAD's established Safety Management System (SMS) procedures, in compliance with the International Civil Aviation Organisation (ICAO) Doc 9859 requirements, would mean that the timing of the launch of the change is currently estimated to be within the first quarter of 2017. The detailed on-site test and launching plan is being developed jointly with the Contractor.

> **NATS Observation 6** – The availability of a fix notwithstanding, CAD's request for thorough factory and off-site testing /evaluation in accordance with ICAO standards prior to launch of the change is prudent, a view which is bolstered by workarounds already put in practice.

4. The Impact on Staff Training and Procedures

Effectiveness of standing ATC and Engineering procedures

4.1 CAD has assessed that no ATC additional training will be involved since colleagues have been trained on the use of the Main System, Fallback System and the UFS (i.e. the two levels of fallback) and the standing contingency procedures.

4.2 From the engineering perspective, the manual resumption of offline FDP server to online state would initiate necessary flight information synchronisation from the operational FDP server. The recommended practice in the Contractor's report to avoid such a restoration process at a time of high traffic was a sensible recommendation to prevent data synchronisation from potentially pre-empting the flight plan association process. Likewise, the recommendation to conduct interactive playback on the Fallback System rather than the operational system was a logical recommendation, which could have avoided the causal circumstances that led to flight plan dis-association in the first place. Since both procedures are standing procedures and the recommended

workarounds involved the timing or the system onto which such procedures were to be carried out, there was no impact on staff training, ATC or engineering procedures.

Internal and external communication

4.3 NATS places importance on open and accurate reporting, and for this reason asks all external communication to be directed through official channels. NATS notes CAD has taken a consistent manner, similar to the occurrence on 27 October 2016, communicating with their staff through various means to convey clear and accurate factual information on the occurrence in a timely manner.

4.4 Various briefing sessions have been conducted to frontline staff explaining the cause leading to the occurrence on 29 November 2016, precautionary measures taken, fallback options available, immediate workaround measures and upcoming changes. A press briefing and a press release (with subsequent updates) were provided on the day of occurrence to explain the preliminary findings to provide accurate information to the public (Reference 2 and Reference 3).

4.5 For the 12 December 2016 occurrence CAD has provided briefing for engineering staff. CAD also released a press statement to the public via CAD's website on the same day of the 12 December 2016 occurrence.

NATS Observation 7 – NATS is satisfied with the effective and speedy communication by CAD to apprise its staff and media/public of details pertinent to the occurrences and expects CAD to maintain its good practice of maintaining clear communications through official channels only.

5. NATS Summary and Recommendations

5.1 NATS has reviewed the two specific occurrences. Overall NATS confirms that the occurrences are not unusual, and are examples of the kind of issues foreseen in previous analysis and experience from NATS. CAD's engineering and ATC responses were effective and proportionate, maintaining safety and initiating both short term measures and system changes to resolve the issue.

5.2 In the course of the assessment work, NATS has reviewed the evidence and the information provided by CAD and identified seven observations as shown in the previous sections. Given the complexity of an ATMS, even with all reasonable efforts and endeavours, there could still be possibilities for further issues, as NATS' own experience could attest. NATS has observed good practice by CAD in incident management and system fallback / recovery provisions, prompt incident investigation / tracking / rectification, availability of immediate and effective measures, leading to minimal changes to training arrangements associated with procedures and equipment. On the basis of the

evidence provided to NATS, CAD's handling on the occurrence is considered effective resulting in no impact to safety and minimal interruption to ATC operations.

5.3 NATS' observations are summarised as:

- The expectation of zero issues for such a large and highly complex ATMS is impractical;
- There was no safety impact caused by both occurrences. The impact on ATC operation was minimal and brief. Essential flight information was available at all times at the radar screens, the Fallback System and UFS were unaffected and available at all times;
- The decision to temporarily suspend outbound traffic, as a usual precautionary measure, was prudent before the situation was assessed and prior to the decision taken to resume normal ATC service. The resulting delays were proportionate. The contingency handling by CAD was on par with international best practice;
- The investigation and analysis by the contractor had resulted in prompt identification of the cause of the problem and assurance that both issues represented momentary flight plan data display issues rather than loss of flight data. There was further assurance from the investigation that the Fallback System and UFS were available and operating normally;
- Given the identification of the cause of the issue, effective workarounds were readily available. CAD had promptly implemented the workarounds with adequate communication including briefing materials to the staff. NATS is satisfied that these measures are effective and readily available, and that beyond the two instances included in the report, there have been no further instances up to the time of publication of this report (5 March);
- CAD is following its SMS process and test / evaluation procedures to ensure the fix is well tested at factory and at site prior to its launch; and
- Noting the importance of accurate information reaching staff, stakeholders and the media / public, NATS is satisfied with the effective and speedy communication by CAD to apprise its staff and media/public of details pertinent to the occurrences and expects CAD to maintain its good practice of maintaining clear communications through official channels only.

5.4 These are general recommendations from NATS, as good practice, to provide greater and wider assurance of a lower likelihood of occurrence of similar events in future. The recommendations together with CAD's responses are summarised in Appendix 2. All the recommendations have been adequately addressed and therefore closed.

6. Conclusion

6.1 While safety is of utmost priority, it is neither possible to eliminate all risks nor have a system with no issues reported, as reflected in the ICAO requirements, "risks need to be assessed and mitigated to an acceptably low extent". NATS believes that the occurrences demonstrate that CAD has a good safety ethos whereby both occurrences were managed

actively to ensure the safety of their services, and the impact on services was minimised, with normal ATC service being resumed within a short period of time.

6.2 In NATS' experience, it is not unusual for new systems or new functionality, such as the new ATMS, introduced on a previously stable system to cause issues when transitioned into service. NATS finds CAD's overall handling of and resolution to the occurrence thorough and proportionate. CAD's decision to temporarily withhold outbound aircraft, as a precautionary measure allowing the situation to be assessed prior to resuming normal service, is on par with that adopted by NATS and international best practice.

6.3 In addition to the existing actions undertaken by CAD, NATS has made some recommendations as good practice to further reduce the risk of future occurrences, including regular reviews of system and ATC performance to seek further improvements and to demonstrate that the system is effectively maintained in a 'stable state' over the system life-cycle.

6.4 On the basis of this occurrence and the associated evidence provided, NATS maintains its assessment that CAD's overall operational use of the ATMS is fit for purpose, with clear safety assurance to support full operations.

Appendix 1 - References

References	Description
1	Contractor's Investigation Report for the occurrence on 29 November 2016
2	CAD press release on 29 November 2016
3	CAD press release on 12 December 2016

Appendix 2 – NATS' Recommendations and CAD's Response

ID	Category	NATS Recommendation	CAD Response	Status
REC 1	Minimising likelihood of recurrence	CAD to review decoupling the "Replay" task from the Operational Main System to minimise risks to system performance.	CAD agreed with and has implemented NATS' recommendation with the task of "Replay" to be conducted on the Fallback System rather than the Operational Main System.	Closed
REC 2	Minimising the likelihood of recurrence	CAD to consider tracking the number and severity of similar ATC and engineering observations and issues to evidence that the system is bedding in, and identify any trends of similar system behaviour.	CAD has been tracking ATC and engineering observations and conducting regular reviews in accordance with standing practice under the established SMS process in CAD in compliance with the ICAO requirements.	Closed
REC 3	Monitoring of system performance	CAD to consider conducting system health analysis to watch out for any leading indicators following a transition of any system abnormal / concerning behaviours, e.g. increase in processor utilisation, increasing backlog of messages in queue through, for example, monitoring of computer processing utilisation (CPU), with suitable alert to engineering staff upon detection of abnormal trends for proactive actions.	Under a long established SMS regime, CAD has operational and engineering Subject Matter Experts (SMEs) to collect/analyse/categorise the observations, and conduct regular reviews. CAD has also been conducting proactive regular system health checks since system commissioning and has further enhanced system CPU monitoring mechanism for proactive actions.	Closed
REC 4	Effectiveness of change	CAD to review the system logic and heuristics that are initiated at start-up and changeover to ensure the integrity of the displayed data.	NATS' views have already been embedded in the software change to be implemented as per technical discussion with the Contractor. The Contractor has also confirmed that with the software change, the FDP will include specific logic to ensure the continuity of flight information display while responding to manually triggered maintenance processes. The effectiveness of the change will be verified through the	Closed

			CAD's stringent testing process in accordance with established SMS in compliance with the ICAO requirements.	
REC 5	Enhancement of response time, communication and fault handling	CAD to consider having a lead engineer in the Ops room at all times to discuss issues and options with ATC colleagues (the engineering team are normally located in a separate office and only enter the ops room when there is a fault). Working in this way has helped NATS resolve minor issues before they escalate.	Apart from a 24-x7 Watch Keeping Control Centre for the new ATC system next door to E-ATCC, CAD had established a 24x7 on-site Duty Engineer (DE) with its permanent position residing inside E-ATCC to directly liaise with the Operational Supervisors and to oversee the Operations and Maintenance (O&M) support of E-ATCC since its full commissioning. Moreover, a Resident Engineer / SME from the CAD's engineering team is also stationed next to the DE position at E-ATCC to enhance O&M support and effect prompt escalation, as appropriate.	Closed