Incident Report on Air Traffic Management System (ATMS)
Occurrence 27th October 2016

1. Introduction

1.1. Arising from a recent occurrence of the ATMS when some workstations entered into a "Display Degraded[1]" mode on the 27th October 2016[2] during a Phased Functional Implementation (PFI) session at East Air Traffic Control Centre (E-ATCC), THB have requested NATS to assess the course of actions undertaken in response to the occurrence, to advise on the safety and readiness of new ATMS, and to make relevant recommendations based on NATS' experience of similar system transitions. This report details the following aspects and consideration factors of the occurrence in turn:

a) The sequence of the event.
b) In the context of the specific event, did the associated operational and engineering reversion procedures adequately deal with the issue to maintain a safe air traffic service and minimise the operational impact?
c) In the context of the specific event, have CAD identified the root cause of the event and put in place appropriate revisions to the systems and training to ensure that this event will not re-occur?
d) In the wider context, should this event have occurred after Full Transition, would the system have been sufficiently robust to continue to provide a safe service with managed impact on service provision?
e) In the light of this event, are there recommendations that NATS would make to support CAD's full commissioning of the new ATMS?

2. Sequence of the Event

2.1 During the Full E-ATCC PFI session on 27 October 2016, a full team of frontline operational and engineering staff were manning respective positions of the new ATMS (Autotrac 3 or AT3) at E-ATCC handling all 3 ATCC functional streams, viz. approach/departure (APP/DEP), terminal (TMC) and area (AREA) with AT3's North Tower (N-TWR) in parallel operation mode. Concurrently, South Tower (S-TWR) and West Air Traffic Control Centre (W-ATCC), served by the existing ATMS, were respectively providing operational aerodrome control and parallel ATC operations to support the PFI session with capability of instant reversion to W-ATCC according to the pre-defined PFI reversion process and criteria for all planned and unplanned completion of PFI[3] to ensure seamless ATC operations.

[1] Workstation "Display Degraded" indicates a data mismatch has been detected and contained by disabling the associated software processing thread in the workstation only. Other threads running simultaneously in the workstation remain unaffected. "Display Degraded" mode is not a system crash, but is an automated system strategy in AT3 as per system design to contain potential system issues at affected workstation whilst preserving data integrity and continuing a safe ATC service.

[2] All times in Hong Kong local time.

[3] A previous unplanned reversion was called during the PFI on 27 September 2016 when an inbound flight declared emergency due to engine failure. Reversion to W-ATCC operation was initiated per pre-defined PFI reversion process and criteria and completed without impact on safety or ATC operations.

2.2 Noting that the bi-annual China International Aviation and Aerospace Exhibition would be held in Zhuhai, a Flight Data Operator (FDO) concerned attempted to input some "non-routine" command / scenario data into the new ATMS primarily for information of frontline colleagues.

2.3 At 10:23, a flight plan (FPL) for an airshow practice flight (not entering HK Flight Information Region - HKFIR) in association with the Zhuhai Airshow was received and rejected by AT3 and as per system design, channelled into its Problem Message Queue (PMQ)[4]. The PFI commenced at 10:33. At 11:29, the FDO retrieved a rejected FPL from the PMQ for review and noted that the FPL had departure aerodrome, route, destination aerodrome fields all indicating Zhuhai airport, which was unusual. In an attempt to recover the FPL, the FDO first deleted the route field entry but the change was rejected by AT3. In a second attempt, the FDO revised the FPL route to go directly to a navigation route fix called ROMEO ("direct to ROMEO"). It should be noted that ROMEO is not a route fix within HKFIR. The change was applied and the FPL was processed by the system.

2.4 This unusual FPL, though processed, did not indicate entry into HKFIR, and was followed subsequently by 3 controller positions[5] in Terminal Stream assigned to process the FPL for flight planning purpose entering into "Display Degraded" mode automatically. These positions were not involved in providing active control of aircraft. This is an automatic protection mechanism by system design to contain the data mismatch at these positions, whereby all executive control positions with radar display used for direct communication with flights were operating normally as usual at all times.

2.5 In recognition of multiple workstations entering into "Display Degraded" mode and in consideration of on-going parallel operation at W-ATCC with full operations/engineering team and instant reversion capability, the PFI managers (one each from operations and engineering), in accordance with pre-defined PFI reversion process and criteria[6], initiated the reversion procedure at 11:35 notwithstanding the availability of Fallback System as well as the Ultimate Fallback System (UFS) running in parallel in the background in addition to the normal operation of the Main System. The reversion was completed safely and successfully at 11:41. While AT3 was under shadowing operations, spare positions in the AT3 were logged on, per standing instruction, in an attempt to recover from the degraded workstations and a similar issue was observed.

2.6 With the presence of a full operations/engineering team, as part of the testing, shadowing operations commenced at E-ATCC at 12:08 using ATMS Fallback System and "Display Degraded" at the workstations concerned was observed as expected. At 12:30, the UFS was used to continue with shadowing operations and to further confirm all of the workstations were functioning normally without workstation "Display Degraded" as expected. The shadowing operations completed at 13:00.

[4] "Problem Message Queue" (PMQ) is AT3's repository of problematic FPLs detected with syntactic or semantic errors for manual processing.

[5] Currently, there are about 50 controller working positions in E-ATCC and N-TWR.

[6] The PFI reversion process with entry/exit criteria was reviewed by NATS in its Phase 2 study.

NATS Observation 1 – NATS noted a good engineering practice of new ATMS architecture design and contingency provision in its Main System, Fallback System and UFS. There is no provision of UFS in the existing ATMS. NATS also noted that provisions are available for the Main System itself to handle multiple scenarios of failure, which are not available in the existing ATMS.

Moreover, the Main System and Fallback System are exactly the same in terms of hardware and software design. Thus, the Fallback System, by offering contingency provisions, can cater for multiple hardware problems, e.g. overheating and failure of circuit boards and the design was such that it responded in the same manner as the Main System to the "non-routine" command/scenario data, as expected.

On the other hand, the UFS is different from the Main System and Fallback System in terms of software and hardware design and therefore did not encounter the same problem. The testing conducted in E-ATCC, after reversion of operations to W-ATCC, is a good demonstration and confirmation to ascertain the response of the new ATMS Fallback System and the UFS with expected results tallied with the design of the system in ensuring the continued provision of ATC service.

Moreover, the Main System, Fallback System and UFS were stable. No system crash was observed at all times.

2.7 In parallel, CAD and the on-site engineer of the new ATMS Contractor (the Contractor) investigated the issue by collecting data logs while leaving the system in its then present state to facilitate testing/investigation. The concerned FPL causing the issue was positively identified (see Section 4).

2.8 At 14:15, a de-briefing session was held to inform CAD staff who had participated in the PFI in that morning about what had happened, cause of the occurrence, decision for reversion to existing ATMS, system designed protection mechanism available, immediate workaround, follow-up fix, and a Question & Answer (Q&A) session to provide as much information to the CAD staff as available on hand.

NATS Observation 2 – CAD had undertaken significant and stringent system testing. However the specific scenario that occurred during the PFI had not been identified as part of testing and procedure design. NATS has experienced similar issues with flight planning data causing system inconsistencies during both system transitions and normal operations in UK. Even with all reasonable efforts and endeavours, there could still be possibilities to have set-backs of this type during introduction of a new system. This underlines the importance of contingency, transition and fallback provisions, procedures, and associated training that were duly covered in Phase 2 Study. Moreover, new ATMS design to have “Display Degraded” mode to contain a data mismatch at the workstation level, without causing system or workstations crash, is obviously an improvement over the existing ATMS to preserve data integrity and ensure a safe ATC service.

3. Effectiveness of System Reversion from PFI

3.1 As detailed within the NATS' PFI Stage 2 and Full Transition Assessment (Phase 2 Study – see Reference 1), in preparation for PFI and Full Transition, CAD has established a framework of evidence that the people, procedures, equipment, and safety management processes for each stage of the PFI and Full Transition are operationally ready. This scope includes the following specific PFI criteria that are related to the occurrence:

a) Operational entry and exit criteria were established for both planned and unplanned occurrences (CAE Ref 1.1)
b) Both engineering and operational ATC Staff are adequately briefed (CAE Ref 1.3, 2.1, 2.2, 2.3)
c) ATC Procedures are in place for staff participating in live and parallel operations (including temporary instructions) (CAE Ref 3.1)
d) Engineering Procedures (including temporary instructions) are in place to cover steady state and fallbacks (CAE Ref 3.2 & 3.3))
e) System entry and exit criteria (planned and unplanned) are in place (CAE Ref 4.1)
f) System Test Evidence for ATMS build is in place (CAE Ref 4.3)
g) There is evidence of the PFI configuration to enable parallel operations, entry and exit from the session is understood, including any limitations/shortcomings (CAE Ref 4.4)

3.2 Phase 2 Study details the evidence provided against these areas by CAD in its overall finding, NATS confirms that CAD has achieved a robust evidence based approach and is satisfied that "CAD is ready to proceed with Full Transition as planned, well supported by clear entry and success criteria, robust fallback contingency measures if needed, and with demonstrated operational readiness in the areas of planning, people, procedures, equipment and safety management processes, that together evidence safe implementation of the new ATMS."

NATS Observation 3 – CAD's exit criteria, fallback procedures and transition out of PFI to normal operations, as reviewed and agreed by NATS in the Phase 2 study, worked as intended and allowed CAD to smoothly and safely transition out of PFI and assume continuous operations without any safety or operational impacts. The de-briefing session with the staff involved is a good practice as part of overall communications and staff engagement.

4. Fault Identification and Resolution

4.1 Following the occurrence, CAD immediately forwarded relevant system records and system logs plus relevant observation documents to the Contractor for urgent investigation and rectification. The following are findings and proposed remedial actions by the Contractor:

a) The immediate cause – that it was the route data deemed invalid by the system in the unusual FPL as determined by CAD was confirmed.

b) The root cause –the occurrence was confirmed to be in the FPL posting logic for flight planning function. An explanation of the mechanism leading to the occurrence is given in Appendix 1.

4.2 With the root cause positively identified, the Contractor has already worked out a software fix and successfully tested at their factory confirming that the same issue will not recur. The fix has also been verified in Hong Kong for all such unusual FPL scenarios with satisfactory results.

4.3 The implementation of the fix is to handle the data mismatch for HKFIR entry time before applying the posting logic. In case of no HKFIR entry time, posting logic based on HKFIR entry time would not be applied. The FPL concerned will be displayed at the auxiliary screen of the ATMS (which is next to the radar screen) for reference by the air traffic controller(s) and flight planner(s) concerned, i.e. the FPL data checking has been improved to handle such situations.

NATS Observation 4 – CAD together with the Contractor have been able to quickly identify the root cause and recreate the occurrence. NATS is satisfied that enhancement measures including the software fix and procedural changes have been implemented and verified to both solve and avoid the recurrence.

5. Potential Impact if the Issue of "Display Degraded" Had Occurred After Full Transition

5.1 If the same FPL issue causing display degrade had occurred after Full Transition without the new fix, based on established procedures, the concerned FDO would immediately retrieve the problematic FPL, of which the route field content had been modified and applied just before the workstation had entered into "Display Degraded" mode. The FDO could quickly remove the problematic FPL using his own workstation. After the FPL is deleted, affected workstation(s) with "Display Degraded" would be rebooted to resume normal operations.

5.2 NATS' assessment is that the impact of the issue should it occur after Full Transition would be minor with no safety concern because:

a) There was neither system "outage" nor system "crash". The Main System, Fallback System and UFS[7] of the new ATMS kept operating normally.
b) Only 3 out of some 50 controller positions showed "Display Degraded" and these positions are used for flight planning rather than controlling flights. All other positions in E-ATCC and N-TWR remained fully operational without affecting safety.
c) Each of the concerned positions could resume normal operation after deletion of the concerned FPL and the workstations were re-booted afterwards. The recovery process can be completed within 15 minutes with minimal operational

[7] There are multiple backup hardware and software modules with the Main System, and the same for Fallback System. The UFS would be used for operation only when the hardware and software of both Main System and Fallback System fail simultaneously. It is noted that the backup ATMS system for existing ATMS system has not been used for operation since its commissioning.

impacts and without the need to switch to Fallback System or UFS. This has been verified by a drill based on established procedures on 30 October 2016.

6. *Review Framework*

6.1 The framework applied for the NATS review of this occurrence has been based on key elements of existing NATS processes, in accordance with safety management system, and experiences of investigating similar incidents (including those for Flight Data Processing systems). These include:

a) System Fallback and Recovery;
b) Incident Management;
c) Problem Tracking / Investigation; and
d) Problem Fix delivery and testing.

6.2 With the objective of satisfactory resolution of the issue, minimisation of risks and the viability of Full Transition, the following areas and the relevant procedures / documents / records have been the focus of NATS' review:

a) Technical details (Equipment) – the problem system data, mechanism leading to the issue and system behaviour;
b) The circumstances leading to the issue (Environment);
c) Operation details (People and Procedure) – the sequence of events, the decision and execution of reversion, potential operational impacts, contingency and fallback readiness;
d) The relevant processes and adequacy followed up by CAD in the investigation of the incident (Procedure);
e) Effectiveness of the fix, workarounds and further enhancement to prevent recurrence of same or similar issues from a system, operational and procedural perspective (Equipment, People and Procedure); and
f) Management and handling of the incident and its potential impact on the continuation of PFI and Full Transition.

NATS Observation 5 – The actions and activities undertaken by CAD, both during and subsequent to the occurrence to manage and resolve the situation are considered satisfactory, effective and on par with those of NATS.

7. Communication

7.1 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 undertaken substantial efforts in communicating with staff at all levels with an aim to conveying clear and accurate factual information on the occurrence in a timely and effective manner. With the cause leading to the issue positively identified and demonstrated to operational colleagues (the FDOs in particular), CAD had immediately provided a briefing on details of what had happened and cause of the occurrence on 27 October 2016, reversion decision, built-in system protection mechanism, and upcoming fix to colleagues who had participated in the PFI on 27 October 2016.

7.2 A separate briefing session was provided to engineering and system maintenance staff on 28 October 2016. An e-mail was also sent to all operational staff on 29 October 2016. Besides, operational staff participating in subsequent live traffic handling was also briefed on the related details.

7.3 CAD has issued a Press Release on 28 October 2016 to promulgate a correct and accurate message on the course of action, cause of the occurrence, and forthcoming actions. NATS is satisfied with the effective communication by CAD to appraise its staff and media/public on details pertinent to the occurrence.

8. NATS Summary and Recommendations

8.1 In the course of the assessment work, NATS has reviewed the evidence and the information provided by CAD and come up with five 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 an issue as experienced by CAD on 27 October 2016, as NATS' own experience could attest. NATS has observed good practice by CAD in system fallback provisions, incident management, containment of data mismatch, and recovery arrangements in the areas of people, procedures, and equipment. The five observations by NATS were summarised as follows:

a) NATS noted a good engineering practice of new ATMS architecture design and contingency provisions in its Main System, Fallback System and UFS to cater for multiple failure scenarios, which are more advanced than the existing ATMS. The Main System, Fallback System and UFS were stable. No system crash was observed throughout the occurrence;
b) NATS underlined the importance of contingency, transition and fallback provisions, procedures, and associated training by CAD that were previously assessed by NATS as effective and satisfactory. NATS noted the enhancement feature for new ATMS to contain the data mismatch which preserves data integrity and ensures a safe ATC service;
c) NATS noted that the occurrence was well-managed by CAD professionals in accordance with pre-defined PFI reversion procedures ensuring safe, smooth and effective ATC service;
d) NATS considered the investigation on the root cause and implementation of enhancement measures, including effective software fix and procedural changes

by CAD and the Contractor were efficient and effective. NATS is satisfied that the occurrence reported was satisfactorily resolved; and

e) NATS is satisfied with and impressed by CAD's overall management of the occurrence, including in particular the dissemination of information to internal and external parties, which is on par with NATS.

8.2 NATS has had direct experience of flight planning issues impacting both NATS' system transitions and live operations, arising from issues related to FPL format / data as well as issues within the core processing. On the occasions these have occurred during live operations, NATS has experienced high levels of traffic delay. To avoid disclosing piecemeal or isolated information to external parties that may cause unnecessary confusion, NATS has experience in treating information collected from occurrence of similar nature and in preserving its confidentiality until completion of investigation.

8.3 Noting the adverse impact of inaccurate information reaching the media/public through unofficial channels, despite all endeavours by CAD including issuing of circulars / reminder emails, it is suggested that CAD might consider to further reduce that risk by reiterating staff responsibility with regards to external communications, including information provided to social media, as appropriate.

8.4 On the basis of the evidence provided to NATS, CAD's handling on the occurrence was considered effective and the reversion procedure was conducted and completed as designed (as reviewed and agreed by NATS in its Phase 2 Study) resulting in no impact to safety and ATC operations. This is largely due to the clarity of the entry and exit criteria for PFI, and the level of staff training to support an instant reversion.

8.5 Considering that software fix and workarounds are already in place, the risk of recurrence of the same occurrence is assessed as low. Based on NATS experience, NATS would recommend CAD to take the following further steps before Full Transition:-

Minimising the likelihood of further FPL issues

a) Undertake testing to build confidence of the fix for this specific issue.

b) For non-conventional FPLs[8] that normally enter into the PMQ requiring manual processing, carry out testing to verify if manual amendment on those FPLs would cause no issues to AT3.

Minimising the impact of any future FPL issues

c) Enhance procedures and practice for FDOs to remove the problematic FPL once it is detected.

d) Review and refine the reversion and backup plan to cater for different scenarios/faults.

[8] Non-conventional flight plans involving:

- re-entrant flight – a flight that takes off and lands at same airport
- multiple-point flight – a flight passes through multiple navigation route fixes
- slow aircraft – a helicopter or small propeller-driven aircraft that flies by visual flying rules
- flights with duplicated identifiers – each flight with FPL under process by the system should have a unique identifier
- incomplete flight plan – a flight plan with missing information in its data field(s)

8.6 The CAD responses including actions to each of the recommendations are detailed at Appendix 2.

9. Conclusion

9.1 In conclusion, upon review of the occurrence, and CAD's responses to each of the NATS' recommendations, NATS is satisfied that CAD has implemented all actions arising from the recommendations, some of which bear the benefit of a wider and general coverage to other potential issues. NATS also find that CAD's actions are also supported by documentary evidence. Considering the nature of the occurrence, that corresponding effective mitigating measures have been in place and the event-tested reversion, NATS is confident that the issue as reported has been satisfactorily resolved, and NATS' assessment on CAD's readiness for Full Transition as previously concluded in Phase 2 Study remains unchanged.

References

1. Phased Transition Approach for Air Traffic Management System and Overall Transition Readiness for ATC Replacement System - PFI Stage 2 and Full Transition Assessment (Issue 1.5, October 2016)

Appendix I – Mechanism of flight strip posting logic leading to the occurrence

(a) A posting logic based on FIR entry time had been activated through system adaptation. Therefore, to determine when and where to post a FPL to controllers, AT3 required the FIR entry time to make the decision.

(b) The concerned FPL did not indicate any entry to HKFIR, which caused the FPL to be placed into the PMQ by the system. Subsequent manual amendment of the FPL also did not rectify the issue. Therefore, no FIR entry time could be determined by the system. The FPL posting logic at the workstation detected a data mismatch. As a result, when the concerned FPL was posted to the respective flight planning workstations, the protection mechanism was immediately triggered to protect the workstation from crashing with a "Display Degraded" shown onto the screen.

(c) All Executive Control positions, directly communicating with flights, were operating normally at all times, and with no safety and operational impacts due to the occurrence.

(d) As the amended FPL passed the format checking at the time and so no warning/error popup was displayed at the time of executing the FPL amendment. It is confirmed that the Main System, Fallback System, and UFS were working normally and stable as per system design with the issue occurred at flight planning workstation level only.

(e) As the concerned FPL was only required to be processed by the affected workstations, other positions not required to process the FPL were not affected by the occurrence.

Appendix 2 – NATS Recommendations & CAD Responses

ID	NATS Recommendation	CAD Comment/Response	Status
REC 1	• Undertake testing to build confidence of the fix for this specific issue.	• As an established practice, the fix developed by Contractor has undergone various tests including the factory testing at their factory at Marlborough, functional tests, on-site verification tests in Hong Kong and normal ATC operations (NATCO) so as to build confidence that the fix could successfully address the identified issue.	Closed
REC 2	• For non-conventional FPLs that normally enter into the PMQ requiring manual processing, carry out testing to verify if manual amendment on those FPLs would cause no issues to AT3.	• A thorough and structure review were conducted to trace the problematic FPLs from the PMQ of new ATMS. These problematic FPLs were fed into the AT3 for manual amendments at PMQ and it was confirmed that such actions did not cause any problem to AT3. The above-mentioned review was made during the subsequent PFI sessions with satisfactory results.	Closed
REC 3	• Enhance procedures and practice for FDOs to remove the problematic FPL once it is detected.	• Procedures have been enhanced and practice/briefing was conducted for FDOs to remove the problematic FPL once it is detected.	Closed
REC 4	• Review and refine the reversion and backup plan to cater for different scenarios/faults.	• The reversion and backup plan were reviewed and refined to cater for different scenarios/faults. Such review was conducted with documents updated.	Closed