[Translation]

政府總部
運輸及房屋局
運輸科
香港添馬添美道2號
政府總部東翼

Transport and
Housing Bureau
Government Secretariat
Transport Branch
East Wing, Central Government Offices,
2 Tim Mei Avenue,
Tamar, Hong Kong

本局檔號 Our Ref. THB(T)CR2/16/951/91
來函檔號 Your Ref. CB4/PL/EDEV

電話 Tel : (852) 3509 8195
傳真 Fax: (852) 2524 9397

Ms Shirley CHAN
Clerk to Panel on Economic Development
Legislative Council Complex
1 Legislative Council Road
Central,
Hong Kong

19 September 2018

Dear Ms CHAN,

Panel on Economic Development
Letter from Hon Holden CHOW Ho-ding dated 15 August 2018

Thank you for your letter ref CB4/PL/EDEV dated 20 August 2018 requesting the Transport and Housing Bureau to provide details of the occurrence in the Air Traffic Management System (ATMS) on 13 August 2018. I am authorised to reply as follows.

Details of the Occurrence

(I) Switchover to the Fallback System due to the momentary hitch in the two Flight Data Processors (FDPs) in the Main System

2. The FDPs of the Main System of the Civil Aviation Department (CAD)'s ATMS experienced a momentary hitch on 13 August 2018. Throughout the occurrence, full information (including essential information, namely flight position, altitude information, secondary surveillance radar code, and supplementary information such as call sign and aircraft type) of the vast majority of flights in the Hong Kong Flight Information Region (HKFIR) was continuously displayed on the radar screens, except for three flights for which only the three pieces of essential information, i.e. flight position, altitude information and secondary surveillance radar code, could be shown. After the technical staff on-site switched the ATMS to the Fallback System (an identical and operating system) in accordance with the established procedures, the processing and display of the flight data returned to normal. The occurrence lasted for six minutes. As a precaution, the Air Traffic Control Officers (ATCOs) deferred giving clearance to departing flights momentarily for about six minutes. Arrivals and flights flying through the HKFIR were not affected. Aviation safety was not affected by the occurrence.

3. As a matter of fact, the ATMS consists of two identically designed but independent systems (i.e. Main System and Fallback System), each equipped with two FDPs. In the event that both FDPs in the Main System do not function properly, the Fallback System can immediately take up the role of the Main System for continuing the system operation. In the afternoon on 13 August, when the two FDPs of the Main System experienced a momentary hitch, the ATMS displayed an alert message to ATCOs and technical staff as per system design. After the technical staff on-site switched the ATMS to the Fallback System in accordance with the established procedures, the processing and display of the flight data returned to normal. The occurrence lasted six minutes, during which time the ATCOs were able to keep direct voice communication with the pilots and provide air traffic control (ATC) services at all times. They were also able to simultaneously obtain all flight information that should be shown through the displays using Automatic Dependent Surveillance-Broadcast (ADS-B) technology, including full information of the three flights for which only all three pieces of essential information, i.e. flight position, altitude information and secondary surveillance radar code, could be shown. Certain non-critical system functions were affected during the occurrence, such as the flight data exchange functions with the adjacent Flight Information Regions (FIRs) through automation. The ATCOs continued to maintain close liaison with the adjacent FIRs through voice communication in accordance with the established procedures to ensure safe transfer of flights between FIRs[1]. All professional ATCOs have received rigorous training and have the skills and experience required to deal with unexpected circumstances in accordance with the established procedures, so as to continue to provide ATC services and safeguard aviation safety.

(II) Restart of the concerned Main System to turn it into the Fallback System

4. The ATMS has built-in multiple fallback systems to tackle different scenarios. The two systems of the ATMS are independent but identical systems with the same design and functionality, which can immediately take up the role of other in the event of an outage for maintaining ATC services continuity. As the Fallback System is operating (i.e. its data remain synchronised with the Main System), it is not necessary to perform "data synchronisation" during the switchover to the Fallback System. After the Main System experiences momentary hitch, it will immediately terminate the "data synchronisation" with the other system as per system design to avoid the problematic data from affecting the other system that functions properly. Therefore, before restarting the concerned Main System to turn it into the Fallback System, "data synchronisation" will be required. On that day, having co-ordinated with the ATC supervisors on-site, the technical staff restarted the concerned Main System in accordance with the established procedures, and performed detailed inspection, followed by a four-minute "data synchronisation" to resume it as the Fallback System. The entire restart process lasted about one hour. In the meantime, the original Fallback System, which became the Main System after switchover, has been operating normally and remained unaffected. The operation of the concerned Main System returned to normal and it then served as a backup as per system design.

---

[1] Currently many air navigation service providers (ANSPs) around the world are not equipped with the ability to exchange flight data with adjacent FIRs through automation, and these ANSPs still use voice communication in accordance with the standards set by the International Civil Aviation Organization.

5. Apart from the Main System and the Fallback System, the ATMS is also equipped with an Ultimate Fallback System. On the day of the occurrence, it was not necessary to activate the Ultimate Fallback System throughout the process.

Follow-up Actions by the CAD

6. The CAD attaches great importance to the occurrence. The contractor, Raytheon Company, was tasked right after the occurrence to conduct a thorough investigation and come up with a solution as soon as possible. According to the report submitted by the contractor (copy attached at the **Annex**), the cause of the occurrence was that when the system software was updating the flight route elements[2], an unexpected data corruption had occurred, resulting in an undefined situation where an array of elements of a flight route unexpectedly contained an invalid value. As a result, the software could not continue its processing. This triggered for safety assurance the shutdown of the primary FDP of the Main System as per multi-layer redundancy in system design. The shutdown of the primary FDP was then followed by an automatic switchover of operation to the secondary FDP. The shutdown of the secondary FDP was triggered by the same reason (i.e. the flight route element contained an invalid value).

7. Upon the CAD's request, the contractor conducted an in-depth review on the program algorithm and coding involving the flight route element comparison, and confirmed that the program algorithm and coding were in order. To prevent the operation of the FDPs from being affected by corrupted data in future, the contractor has provided in mid September the software fix to the CAD.

8. In the current system design, when the ATMS first accepts the flight route elements, the system will verify the data to ensure the validity. For subsequent updates, the ATMS will check the relevant updates to ensure that only valid data will be accepted, followed by the execution of flight route element comparison. The software fix to be implemented will validate the flight route elements (including the updates) once again (i.e. one additional validation as compared to the past) prior to the execution of flight route element comparison. The following three new features will be introduced in the ATMS through this software fix:

(i) When a flight route contains an invalid value, the system will not proceed to the flight route element comparison for that flight;

(ii) The software will stop processing the flight route in question when it encounters the scenario mentioned in paragraph (i). It will then confine the flight route in question and will continue to process information of other flight routes to prevent the FDPs from shutting down and other flight data from being affected; and

(iii) At the same time, the software will display an alert message to ATCOs and technical staff together with the relevant flight information for subsequent and separate handling of the flight route in question.

[2] A flight route comprises an array of elements, such as standard instrument departure procedures, standard instrument arrival procedures, waypoints, airways, etc.

9. CAD is carrying out the on-site testing of the software fix that has been provided by the contractor and it is in progress. Upon completion of the test and relevant safety assessments by the CAD, the software fix is expected to be implemented in the ATMS in late October. The CAD will brief the relevant ATCOs and technical staff regarding the cause and follow-up actions of the occurrence, and is in the process of exploring the need for further refining the procedures involving the switchover from the Main System to the Fallback System in order to ensure aviation safety.

Hon Holden CHOW has mentioned about "a system fault"

10. We noticed that Hon Holden CHOW has mentioned in his letter about "a system fault" in November 2016, which should refer to the occurrence on FDPs on 29 November 2016. In that occurrence, when the two FDPs started to synchronise flight information, the synchronisation process took priority and the flight plan association process was expected to take place shortly afterwards, resulting in the momentary flight plan dis-association in matching corresponding radar data[3]. The nature of that occurrence was different from that of 13 August 2018. That occurrence was completely solved by deployment of a software fix.

Views of the ATMS Expert Panel on the Performance of ATMS

11. The CAD set up the ATMS Expert Panel shortly after the commissioning of the ATMS comprising local and overseas experts and academia in the fields of air traffic management, engineering and aviation safety management to offer independent advice to the CAD on the teething issues identified since the full commissioning of the ATMS. The Expert Panel published its final report[4] in November 2017 which stated that the performance of the ATMS had been exceeding the important safety criteria adopted by most European aviation authorities, i.e. the availability of surveillance information of 99.999% for three pieces of essential information (i.e. flight position, altitude information and secondary surveillance radar code) since the system commissioning. Although two FDPs of the Main System experienced momentary hitch on 13 August 2018, all three pieces of essential information were shown as per system design. The Expert Panel also stated in its report that as the ATMS was a large-scale, complex and comprehensive computer system, minor occurrences would occur intermittently for different reasons (including human factors) especially during the initial stage of its operations. The Expert Panel stressed the importance of a pragmatic approach on resilience and multi-layers of fallback in system design, well-trained professionals with standing procedures for contingency handling and an effective Safety Management System to anticipate and manage risks. The Expert Panel acknowledged in its report that the above mentioned arrangement were all in place in the CAD.

---

[3] More details at http://www.info.gov.hk/gia/general/201612/01/P2016120101041.htm

[4] The executive summary in Chinese and the final report (English only) are available on CAD's website:Executive Summary:
http://gia.info.gov.hk/general/201711/21/P2017112100575_272401_1_1511262331248.pdf
Final Report:
https://www.cad.gov.hk/reports/Final%20Report%20by%20the%20Air%20Traffic%20Management%20System%20Expert%20Panel%20dated%20November%202017.pdf

12. The CAD will continue to closely monitor the performance of the ATMS, and optimise the ATMS as well as overall ATC services in a sustained manner, and remain committed to ensuring that aviation safety is our top priority.

Yours sincerely,

(Joyce N. S. CHAN)
for Transport and Housing Bureau

Encl. Investigation Report on Shutdown of Dual Flight Data Processor on 13 August 2018

c.c.
Director-General of Civil Aviation
(Attn: Mr LI Tin-chui, Simon)
Hon Jeffery LAM Kin-fung, GBS, JP
(Chairman of the Panel on Economic Development)

Investigation Report on Shutdown of Dual Flight Data Processor on 13 August 2018

1. Observation

1.1 The Air Traffic Management System (ATMS), namely AutoTrac III (AT3), has been operating since full commissioning in November 2016. CAD reported that the Fallback System of the ATMS had to be activated on 13 August 2018 since both of the Flight Data Processors (FDPs) of the Main System had encountered problem (the Occurrence). The Fallback System and the Ultimate Fallback System (UFS) of ATMS were operating normally during the Occurrence, though activation of the UFS was never necessitated during the Occurrence. Details are given in the ensuing paragraphs.

At CAD's request, Raytheon promptly analysed relevant system logs and recorded data and conducted an investigation into the Occurrence.

1.2 Description of the Occurrence is set out below.

1.2.1 On 13 August 2018 at 16:20 (Local Time, ditto), the ATMS was running with the Main System. When the primary FDP in the Main System was processing flight information, it detected an undefined situation where an array of elements of a flight route[1] contained an invalid value. This triggered the shutdown of primary FDP as per system design.

1.2.2 The shutdown of the primary FDP was then followed by an automatic switchover of operation to the duplicated FDP, the secondary FDP. When the secondary FDP was processing flight information, the shutdown of the secondary FDP was triggered by the same reason (i.e. the detection of an invalid value). As a result, the Main System shut down both FDPs and displayed a system alert banner of "Emergency State" as per system design. During the "Emergency State", the ATMS remained capable of providing a continuous display of aircraft target updates at air traffic controllers' workstations[2] for situational awareness (please see 1.2.4) and air traffic controllers could keep direct voice communication with aircraft under their respective purview to issue clearance to pilots.

---

[1] A flight route comprises an array of elements of a particular flight, such as standard instrument departure (SID) procedures, standard instrument arrival (STAR) procedures, waypoints, airways, etc.. Each element is of a certain pre-defined type (e.g. for waypoint, only valid waypoint names, say "SIERA", "ELATO" are recognizable by the system).

[2] An air traffic controller's workstation at the ATC Centre has three displays, namely (i) AT3 Situation Display showing the surveillance information (i.e. aircraft targets); (ii) AT3 Auxiliary Display showing information as selected by individual air traffic controllers (e.g. arrival sequences, flight plans); and (iii) Operational Information Database System Display showing other information (e.g. meteorological information, Hong Kong Aeronautical Information Publication, Automatic Dependent Surveillance-Broadcast (ADS-B) information).

These permitted continued safe control of air traffic operations in the interim.

1.2.3 During that time, the Fallback System of ATMS, which is a fully identical system to the Main System, was operating normally and available at all times. CAD activated the Fallback System as the operational ATMS in a coordinated manner to resume operation as per established procedures. The Fallback System was activated and became the Main System at 16:26.

1.2.4 The Surveillance Data Processors (SDPs) of both the ATMS Main System and Fallback System, which operated independently of the FDPs, were running normally to continuously provide situational awareness. All flights were continuously displayed on the AT3 Situation Display throughout the Occurrence. All flights except three had their full information (i.e. essential information including flight position, altitude information, secondary surveillance radar code; and supplementary information such as call sign and aircraft type) shown on the AT3 Situation Display. For the three flights, all essential information, i.e. flight position, altitude information and secondary surveillance radar code, were displayed on the AT3 Situation Display but their supplementary information was not able to be obtained from the failed FDPs. During the entire Occurrence, the air traffic controllers were able to obtain all flight information (including full information of the three flights mentioned above) through the Operational Information Database System Display showing information from ADS-B technology.

2. Detailed Findings

2.1 Details of the findings after investigation are set out as follows.

2.1.1 There is a program in the system software to perform flight route element comparison. When air traffic controllers input into the ATMS a clearance issued to pilots, a new array of elements of the flight route concerned reflecting the clearance issued will be created. The program will analyse the array of elements of the flight route concerned in sequential order. For each element, the program will check its value, determine its type (e.g. standard instrument departure (SID) procedures, standard instrument arrival (STAR) procedures) by correlating it to a pre-defined type, and detect the changes. The changes will then be used to calculate and update the flight information.

2.1.2 During the Occurrence, the system software detected a very rare situation where an array of elements of a flight route contained an invalid value.

When the software encountered the invalid value during the flight route element comparison, the invalid value could not be correlated to any pre-defined type. As a result, in the absence of the type of an element, the software could not be executed further and the undefined situation could not be properly handled, which triggered exception handling in the primary FDP of the Main System and shut down of the FDP process as per system design. This was followed by the automatic switchover of operation to the secondary FDP of the Main System, which behaved in a similar fashion as the primary FDP.

2.1.3 The system alert banner showing "Emergency State" gave an alert to the air traffic controllers.

2.1.4 Raytheon has reviewed the program algorithm and coding involving the flight route element comparison, and confirms that the program algorithm and coding are in order and that the invalid value should not have existed. It is believed that an unexpected data corruption had occurred, resulting in an undefined situation where an array of elements of a flight route unexpectedly contained an invalid value.

2.1.5 Raytheon has confirmed that the cause is not related to (a) system performance, (b) software build in use since 26 September 2017, (c) prevailing air traffic volume, and adverse weather conditions during the time of the Occurrence.

3. Software Fix

3.1 Development of a software fix has been completed in Raytheon's factory to rectify the issue as follows:

(i) to validate the contents of the array of elements of a flight route prior to flight route element comparison. In the unlikely circumstance where an element of a flight route is invalid, the program will not proceed to the flight route element comparison for that flight and the situation will be handled under item (ii);

(ii) to enhance the software so as to handle and contain the exception situation. The software will stop processing the flight route in question, which will be handled under (iii), and will continue to process information of other flight routes; and

(iii) to display an alert message to air traffic controllers and system engineers with the relevant data for subsequent and separate handling of the flight route in question.

4. Availability of Fix

Raytheon has identified a solution for reviewing and testing in its factory, and delivered the software fix to Hong Kong in mid-September 2018 for further on-site testing and safety assessments.

Raytheon Company
September 2018

* * * * *