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)CR 2/16/951/91
來函檔號 Your Ref.: CB4/PL/EDEV

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

香港中區
立法會道一號
立法會綜合大樓
經濟發展事務委員會秘書
陳向紅女士

陳女士：

新航空交通管理系統(航管系統)

閣下二〇一八年八月二十日就周浩鼎議員要求本局交待關於新航管系統在二〇一八年八月十三日出現短暫故障的詳情，我獲授權回覆如下。

事發當日的情況

(一)主系統的兩個航班數據處理器出現故障因而轉用備用系統

民航處航管系統主系統的航班數據處理器八月十三日曾出現短暫故障。故障期間，雷達顯示屏幕一直顯示香港飛行情報區內絕大部分航班的全部資料（包括必要資料:航班位置、高度、二次監察雷達編碼以及輔助資料:如航班呼號、飛機型號等），只有三班航班僅能顯示全部三種必要資料（即航班位置、高度和二次監察雷達編碼）。工程人員按既定程序轉用設計相同並在運作中的備用系統後，航班數據的處理和顯示回復正常運作，整個過程歷時六分鐘。為審慎起見，航空交通管制主任（空管人員）按程序曾短暫延遲放行離境航班約六分鐘，抵港及飛越香港飛行情報區的航班則不受影響。有關事件並沒有對航空安全構成影響。

事實上，航管系統有兩個設計相同但獨立的系統（即主系統和備用系統），各自配備兩個航班數據處理器，倘若主系統兩個航班數據處理器出現狀況時，可即時轉用備用系統。八月十三日下午，主系統的兩個航班數據處理器出現短暫故障，而系統按設計即時出現提示訊息，以提醒空管人員和工程人員出現狀況。當工程人員按預設程序轉用備用系統後，航班數據的處理和顯示回復正常運作，整個過程歷時六分鐘。該六分鐘其間，空管人員一直透過話音系統與所有航班保持聯絡及提供空管服務，亦可以透過衞星導航監察技術（ADS-B）顯示屏幕掌握全部航班（包括上述的三班航班）所有應顯示的資料。另外，有個別並非最關鍵的系統功能，例如用作與鄰近飛行情報區透過航班數據處理器交換航班資料的功能受到影響，空管人員根據既定程序以語音通話繼續與鄰近飛行情報區緊密溝通，確保安全交接飛機[1]。專業空管人員受過嚴格的訓練，有能力和經驗根據既定程序作出應變以處理這些突發情況，並繼續提供空管服務，保障航空安全。

(二)重啟發生故障的主系統令其成為後備系統

航管系統設有多重備用系統，以應付各種情況。兩個系統各為獨立的系統，但設計和功能完全相同，因而可以在其中一個系統出現故障時立即取而代之，無間斷地維持空管服務的正常運作。由於備用系統一直處於運作中的狀態（即與主系統一直進行「數據同步」），轉用備用系統期間無需再特別進行「數據同步」程序。在主系統發生故障後，按安全設計，該系統會即時停止與另一系統的「數據同步」，以防有問題的數據影響運作正常的另一系統。因此，在重啟發生故障的主系統後並讓其成為後備系統之前，需要進行「數據同步」。當日工程人員與在場的空管主管協商後，按程序重啟發生故障的系統，進行各項詳細檢查及歷時約四分鐘的「數據同步」，讓其成為後備系統，整個重啟過程約一小時。其間，已轉為主系統的備用系統一直正常運作，並沒有受到影響。其後，出現狀況的主系統在重啟後已回復正常運作，並按設計用作後備之用。

航管系統除了主系統和備用系統外，還有最終備用系統。當日，整個過程中無需啟動最終備用系統。

---

1 目前國際間不少空中航行服務提供者亦未配備與鄰近飛行情報區透過航班數據處理器交換航班資料的功能，仍然按照國際民用航空組織的標準透過語音通話。

民航處在事發後的跟進工作

民航處非常重視今次事件，並已在事發後即時責成承辦商雷神公司徹底調查事件和盡快提交長遠的解決方案。根據承辦商提交的報告（**見附件**），事件成因是主系統一個軟件程式在處理一項航班飛行路線元素[2]資料更新時，出現了未能預計的數據損壞(data corruption)，導致飛行路線元素意外地包含無效數值，軟件程式因而無法進一步處理飛行路線元素的資料。按系統設有多重備用保障的設計，主系統的一號航班數據處理器停止運作以策安全，主系統隨即自動切換至二號航班數據處理器，但基於同樣的原因（即飛行路線的元素包含無效數值），二號航班數據處理器亦按系統設計停止運作。

承辦商應民航處要求，詳細審查了航管系統的軟件程式邏輯和涉及比較飛行路線元素的軟件編碼，並確認程式邏輯和軟件編碼均符合設計原意。承辦商已於九月中旬向民航處提交新的軟件程式，以防止日後如再出現受損壞的資料會影響航班數據處理器的運作。

在現行設計中，當航管系統首次接收飛行路線元素時，系統會進行驗證，確保資料的有效性。其後如再有新的輸入，系統會核對有關輸入，確保只有有效的資料才能成功輸入，並由系統執行比較飛行路線元素的程式。擬透過新軟件加入的程式旨在執行比較飛行路線元素程式之前，再次對元素的內容進行驗證，包括新輸入的內容，即較過往再進行多一重的驗證程式。安裝新程式後，系統並會有以下三個新功能：

(一) 若發現飛行路線包含無效數值，系統將不會執行比較程式；

(二) 遇上（一）的情況出現，軟件程式會停止處理有問題的飛行路線，並將其隔離，以便繼續如常處理其他飛行路線，避免令整個航班數據處理器停止運作或影響其他航班的資料；及

(三) 與此同時，軟件程式會向空管人員和工程人員發出提示訊息，並提供相關航班的資料，令相關人員可以立刻獨立處理該飛行路線和採取適當跟進。

---

[2] 飛行路線包括一系列元素，例如標準儀表離場程序、標準儀表進場程序、航點、航路等。

民航處正就承辦商提供的新軟件程式進行現場測試。待相關測試完成及經安全評估後，預計可於十月下旬安裝到航管系統使用。民航處會就事件的成因和跟進行動向有關空管人員及工程人員進行簡報。民航處並正檢視如有需要由主系統轉用備用系統時的相關程序，在保障航空安全的大前提下，探討進一步優化該程序的空間。

周議員提及的「一次系統失誤」

我們留意到周議員在信中提及二○一六年十一月曾發生的「一次系統失誤」，應該是指航班數據處理器在二○一六年十一月二十九日出現的情況。該次事件涉及兩組航班數據處理器進行航班資訊同步時，首先處理資訊同步並預期在短時間內再處理航班數據，導致航班數據短暫未能夠及時與雷達資料配對[3]。該次事件與二○一八年八月十三日的事件性質不同，而且已透過軟件更新而全面解決。

航空交通管理系統專家小組對系統表現的意見

民航處在航管系統啟用初期成立了航空交通管理系統專家小組，邀請本地及海外在航空交通管理、工程及航空安全管理方面的專家和學者參與，就航管系統全面啟用後出現不順暢的情況，向民航處提供獨立意見。專家小組於二○一七年十一月發表的最後報告[4]指出自航管系統啟用以來，其表現一直優於大部份歐洲航空當局採納的重要安全指標，必要資料（即航班位置、高度和二次監察雷達編碼）的可用度高於99.999%的目標。二○一八年八月十三日，雖然主系統的兩個航班數據處理器均出現故障，但期間系統依然按設計顯示全部三種必要資料。專家小組在報告中指出，鑑於航管系統乃大型、複雜而全面的電腦系統，尤其是在運作初期，間或會因為不同因素（包括人為因素）而出現一些輕微狀況。專家小組強調，要有效預測和管理風險，必須要以務實的態度應變、具有多重備用系統的設計、久經訓練的專業人員按既定程序處理事故，及一套有效的安全管理系統。專家小組在報告中肯定民航處具備上述各項條件。

---

3 詳情見：http://www.info.gov.hk/gia/general/201612/01/P2016120100838.htm

4 最後報告的行政摘要(中文)及報告全文(只有英文)載於民航處網頁:
行政摘要 -
http://gia.info.gov.hk/general/201711/21/P2017112100575_272401_1_1511262331248.pdf
報告全文-
https://www.cad.gov.hk/reports/Final%20Report%20by%20the%20Air%20Traffic%20Management%20System%20Expert%20Panel%20dated%20November%202017.pdf

民航處會繼續密切監察航管系統的表現，為持續不斷優化航管系統、以至整體航管服務而努力。民航處亦會繼續致力以保障航空安全為首任。

運輸及房屋局局長

(陳雅思女士　代行)

附件：承辦商提交的報告（只有英文）

副本送：　民航處處長
　　經濟發展事務委員會林健鋒主席

二〇一八年九月十九日

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

* * * * *