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

[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

controllers could keep direct voice communication with aircraft under their respective purview to issue clearance to pilots. 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)

Display showing other information (e.g. meteorological information, Hong Kong Aeronautical Information Publication, Automatic Dependent Surveillance-Broadcast (ADS-B) information).

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

* * * * *