

Question 3 (a). Critical system specification

The safety critical system is designed for airplane control to take in 2 user input parameters, distance and speed, to calculate whether the destination airport is reachable or not. The system has the following variables:

Max_Speed_Possible

Min_Speed_Possible

Gas_Capacity

Max_Distance_Possible

Min_Distance_Possible

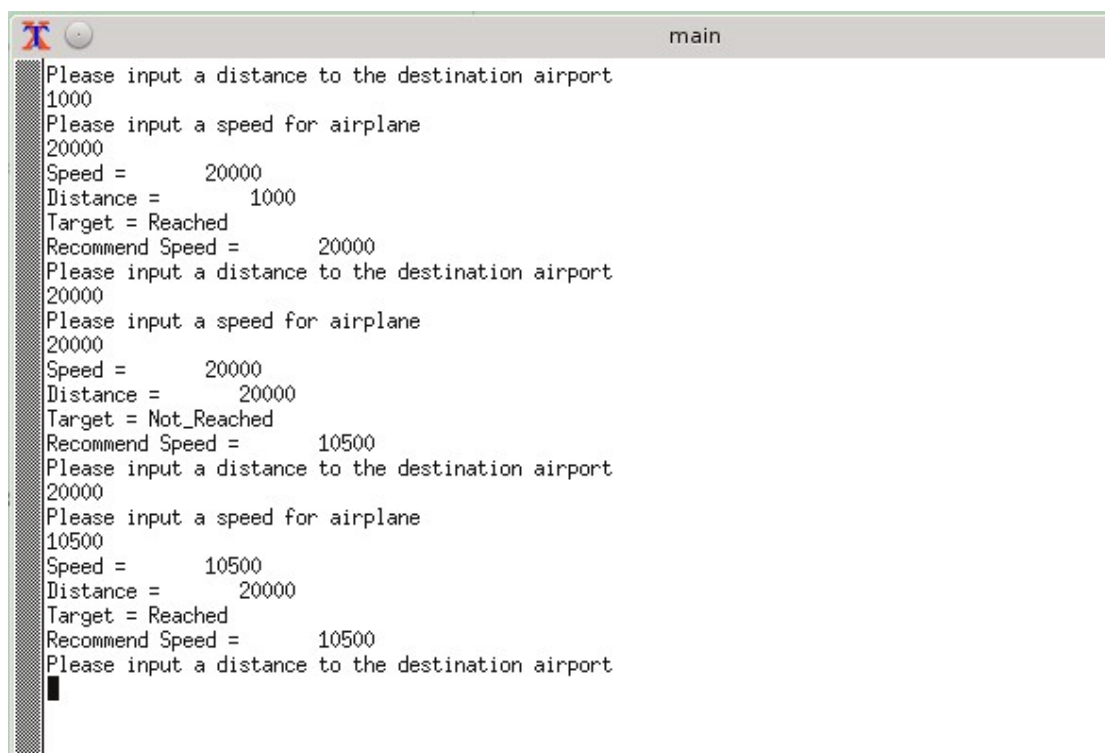
An airplane has a fixed Gas_Capacity of 1,000, speed ranges from 1,000 to 20,000 and a dynamic distance range that is dependent on speed. Higher speed means lower gas efficiency rate and thus shorter distance it can travel. Max_Distance_Possible is calculated using formula:

$$\text{Gas_Capacity}/500 * (\text{Max_Speed_Possible} - \text{Min_Speed_Possible}) + \text{Gas_Capacity}.$$

By using this formula, the distance ranges from 1,000 to 39,000.

The system will prompt for user input of distance and speed, then the system will calculate whether the distance is reachable or not given the input speed using function `Is_Reachable`. In both case, the system will work out the optimal speed based on the distance input in `Cal_Recommend_Speed` function.

If we slightly modify the system to take in another variable, `Gas_Remaining`, the system can be implemented on airplanes to monitor real time gas stock and adjust speed to ensure that the destination airport is reachable



```
main
Please input a distance to the destination airport
1000
Please input a speed for airplane
20000
Speed =      20000
Distance =    1000
Target = Reached
Recommend Speed =      20000
Please input a distance to the destination airport
20000
Please input a speed for airplane
20000
Speed =      20000
Distance =    20000
Target = Not_Reached
Recommend Speed =      10500
Please input a distance to the destination airport
20000
Please input a speed for airplane
10500
Speed =      10500
Distance =    20000
Target = Reached
Recommend Speed =      10500
Please input a distance to the destination airport
█
```

Figure 1 Results of different user input values

Figure 1 shows the results of different user input values.

- First attempt

- Distance: 1,000

- Speed: 20,000

In this attempt, the target is reachable and since the distance is really close, fuel will sustain the full speed for the entire flight.

- Second attempt

- Distance: 20,000

- Speed: 20,000

In this attempt, the target is not reachable because the distance is too far, fuel will sustain the full speed for the entire flight.

Therefore, the system recommends a speed of 10,500 in order to reach the destination.

- Third attempt

- Distance: 20,000

- Speed: 10,500

In this attempt, the target is reachable based on the recommended speed from the second attempt.

Question 3 (b). Hazard analysis

The attached Fault Tree Analysis.png allows zoom-in for a clearer view.