CS132: Software Engineering
HW2: Risk Management

On Mar 10 2019, Ethiopian Airline ET302 from Addis Ababa to Nairobi crashed 6 minutes after takeoff, killing all 157 people on board. This accident and the previous Lion Air accident result in full investigation of the Boeing 737 Max model, and all aircraft with the same model are therefore grounded. In the lecture we analyzed how the tragedy happened. In this exercise, assume you work for Boeing, please do Fault Tree Analysis (FTA) on the incident, and analyze potential solutions to the problem. Note that there are 100 pt for this homework, but on blackboard the score will be divided by 10.

Fault Tree Analysis on the faulty design

We now know that the accidents happened because the planes were sent into nosedive by MCAS at low altitude, and the MCAS was mistakenly activated due to a faulty AOA sensor. Construct a fault tree and calculate the probability for "MCAS mis-activation when the actual AOA is normal".

Note: In this faulty design, there are two AOA sensors on each 737 Max aircraft, and MCAS is activated if one of the AOA sensors reports high AOA.

Note: For all the calculations in this homework, assume the probability for one AOA sensor to report high AOA when the actual AOA is not high is 1%, the probability for one AOA sensor to report low or normal AOA when the AOA is high is 1%, and the probability for an AOA sensor to report correct AOA is 98%.

A More Aggressive Design

Someone proposed that instead of activating MCAS after one of the sensors reports high AOA, requiring both sensors to report high AOA for MCAS activation may reduce the chance for MCAS mis-activation. Draw the fault tree for this new design and analyze whether the probability for MCAS mis-activation has been reduced.

Balancing False-Positives and False-Negatives

There is another risk that we must consider, that is "the MCAS fails to activate when needed". This may happen when AOA sensor reports low AOA when the AOA is high. Draw the fault tree for the hazardous situation "MCAS fails to activate when needed" for 1) the faulty design and 2) the new aggressive design and compare their probabilities.

Adding Another AOA Sensor

Someone also proposed to use 3 AOA sensors instead of 2 to increase redundancy. The MCAS now requires 2 AOA sensors to report high AOA in order to be activated. For this new design, draw FTA for both "MCAS mis-activation when the actual AOA is normal" and "MCAS fails to activate when needed", and discuss whether this is an overall better design.

Submission

Construct the 6 fault trees mentioned above, and fill in the probabilities in the form below. The deadline of this homework is Apr. 3rd at 23:59. Please submit a .pdf file with name "CS132_HW2_YourName.pdf" electronically on BlackBoard.

	Faulty	Aggressive	2/3
MCAS mis-activation			
MCAS fails to activate when needed			