CS 7639 Project 3 Part 2 Report
Crazyflie design using AADL

Part 2: Safety Analysis

Note: I used the original model provided in the virtual machine.

Question 9:
The critical failures to Crazyflie are from Accelerometer, Gyroscope, Magnetometer, Sensor_Fusion, Controller, and Motor module components. Failures in any of these results invalid sensor readings, control command loss, or motor thrust failures, which leads to unstable system or crash. Added EMV2 properties to each of these abstract sensor modules for FHA. It includes the occurrence distribution, severity, likelihood, and hazard checks.

Question 10:
Generated the FHA report after instantiating impl, Accelero and Gyro provide inertial measurements that are necessary to detect movement and orientation. The Sensor_Fusion combines the data to estimate Crazyflie's state, which then the Controller uses to correct mechanical thrust commands. The Motors lastly carry out these commands to stabilize balance and position of the Crazyflie in the air. Failure in any of these modules results in difficulties that leads to crash in the flight system stabilization

Question 11:
It's in Operational state if all module components (Accelero, Gyro, Magneto, Sensor_Fusion, Controller, and Motor) are operational. If any one of them fails, it results to a Failed state. This is implemented using composite error behavior, which is under "system implementation Crazyflie_Functional_Chain.impl". After generating the FTA with state Failed selection, it showed that the computed failure probability was at 6.0e-09. Each of the module components had failure probability at 1.0e-09. The event gate type is XOR (failure in any component results in system failure.

Question 12:
Accelero, Gyro, Magneto has the error out propagations with error source flow to indicate the origin fault. Sensor_Fusion and Controller has in and out propagations with error path to process the data and forward it after. The Motor has an error sink for terminating the error propagation path.

Question 13:
In the Sensor_Fusion, it includes component error behavior for the hypothesis (any error as input will translate as an error as output). If there is any erroneous input from the sensor modules, it leads to a fault int he sensor fusion process. ("t1: Operational -[Accelero_In.ValueError or Gyro_In.ValueError or Magneto_In.ValueError]-> Failed;"). If there is a failure, it displays ValueError from Data_F_Out port ("Failed -[]-> Data_F_Out {ValueError};").

Question 14:
Instantiated the impl and generated the FTA report:
The computed failure probability was now 5.0e-09. This shows a decrease compared to previous value of 6.0e-09. It's expected because with the new updated changes, certain failure path are treated as normal event in the chain rather focusing on the individual events. The sensor fusion component fails conditionally based on accumulating sensor errors, which removes the redundancy.

Question 15:
Generated the FIA report using {ValueError} as the failure mode in Accelero, Gyro, and Magneto sensor module components, The report showed a fault propagation chain that matches EMV2 error path and component error behaviorsin the functional model.

If {ValueError} comes from Accelero, fault propagtes through Accelero_Out and then Fusion.Accelero_In. Sensor_Fusion fails and outputs as fault on Data_F_Out. Controller receives this message, and then fails, and passes the error to Motors, which then accepts this error as a sink. If {ValueError} comes from Gyro, then the fault propagates through Sensor_Fusion similar to Accelero and directly to Controller.Gyro_In

Each element of the FIA links to model elements (error propagations, error paths, and component error behaviors).

Question 16:
Updated both error behavior and propagation paths of the Motor and Controller components. Motor component has a failure condition triggered by receiving ValueError. Controller component propagates ValueError through both input ports Data_F_In and Gyro_In to its output port Motor_Out.

Checked FTA and FIA again:
FTA: Computer failure probability went down to 3.0e-09, which is more refined.
FTA: error sources from Accelero, Gyro, and Magneto now propagate across all intermediate components and terminate at the Motor component. It now shows accurate flow tracing throughout the functional chain.