Walkthrough:

This document walks the reader through how the deliverables can be read to understand the solution to each objective of the case study.

“model” refers to fcs_archi.slx

“report” refers to “fcs_archi_report.pdf”

“plan” refers to “fcs_software_plan.pdf”

4. Problem Statement

- FCS Architecture : refer model
- RTOS architecture for determinism and deadline monitoring : refer RTOS architecture in report
- In case of loss of IMU+GPS, the UAV needs manual control to Return-To-Home or land safely (cannot be autonomous). RTH is treated as the highest priority override for Loss of Link (LoL) scenarios. However, it is explicitly superseded by Degraded/Manual modes in the event of total navigation failure (IMU + GPS loss), as autonomous RTH relies on valid state estimation.

5. Technical Tasks

5.1 FCS Architecture & Data Flow

- Architecture block diagram: refer model
- Data flow and separation of responsibilities: refer model and Inter-Process Communication in report

5.2 Real-Time Software Design

- Refer report RTOS architecture

5.3 Integration of Control Laws

- Input validation: refer Data_Acquisition_Task in model and Data Acquisition in report
- Output validation: refer Actuator_Command in model and Actuator Command in report
- Configuration: Refer Attitude_Control, Guidance, Autopilot_Mode_Manager and Measurement_Health in model and Sensor FDIR, Attitude Control, Autopilot Mode, Guidance (Position and Altitude Controller)

5.4 Mode Management & Transitions

- Refer Mission Management in report.

5.5 Fault Detection, Isolation and Recovery

Refer sensor FDIR stateflow in model

Scenario #1: IMU data frozen or intermittent

Detection

- IMU is flagged as D2
- FDIR mode is computed as No_IMU or No_IMU_GPS

Immediate Response

- Autopilot_Mode is switched to Degraded
- FDIR Notification sent to telemetry

Fallback Mode

- Kin_State_Propagator is notified of IMU loss by FDIR mode
- Kin_State_Propagator switches to internal UAV dynamics for high frequency prediction state
- If GPS is available, Measured_State_Propagator is able to correct lat/lon position every 20 ms
- Else, no correction step for position state (dead-reckoning)
- When IMU is not flagged as D2, Kin_State_Propagator switches back to IMU_Rate
- Autopilot_Mode is switched to Manual
- Pilot needs to engage Autonomous mode for normal operation

Scenario #2: Pitot tube icing

Detection

- Pitot is flagged as D2
- FDIR mode is computed to GPS_Spd

Immediate Response

- Autopilot_Mode is not changed (continues to be autonomous if previously it was)
- No impact on Attitude_Controller

Fallback Mode

- Measured_State_Propagator modifies the Measurement Matrix to not consider pitot measured speed and consider GPS measured speed.
- When Pitot is not flagged as D2, FDIR mode is computed back to Healthy

- Measured_State_Propagator modifies the Measurement Matrix to consider pitot measured speed

Scenario #3: Actuator saturation or runaway

Detection

- Actuator saturation flagged by Actuator_Command

Immediate Response

- FDIR_Mode is not changed
- Autopilot_Mode is changed to Stabilized if there are multiple failures (>= 2)

Fallback Mode

- Autopilot_Mode is fed to the Attitude_Controller and Guidance gain scheduler to move to safer gain margins
- When output is no longer saturating, Autopilot_Mode goes back to Autonomous mode

Scenario #4: Control Law Execution Overrun

Refer Threads and Priority in report.

Detection

- Deadline monitor timer elapses for Inner_Loop_Thread or Outer_Loop_Thread

Immediate Response

- Exit the thread and restart the thread

Fallback Mode

- Upon consecutive deadline monitor failure, stop the RMS and trigger a hardware failsafe that drives all actuators to a neutral state and cuts throttle.

5.6 Verification & Validation Strategy

Refer plan.

5.7 Safety & Engineering Discipline

Refer Configuration Management in plan.

6. Deliverables

1. FCS architecture description or diagram : model

2. RTOS task structure and scheduling explanation : report

3. Mode management and transition logic : model + report

4. Failure handling (FDIR) table or description : model + report

5. Assumptions and design trade-offs:

    - Manual mode is implemented **as a Rate Command / Attitude Hold (RCAH)** system. Releasing the control sticks commands a zero-degree rate of change, maintaining the UAV's current aerodynamic attitude rather than snapping back to level flight. This removes the sudden jump in target signals when Autopilot mode changes to Manual.
    - The functional design for most of the blocks are dummy implementations (only architectural design is focused).
    - The autogenerated C code should not be allowed to allocate new heap memory during execution.
    - Actuator failure control laws are part of the black box C code, FCS architecture is responsible to notify the control laws and accommodate the state estimation and gain scheduling.
    - Gain scheduling is performed using gains tuned on linearized models of the UAV at different trim points (takeoff, climb, cruise, descent, landing in nominal and failure modes)