Toolbox Plane Design Document

Paul Nykiel

February 4, 2023

Contents

1 Introduction

This is the requirements and design document for Toolbox Plane, an automated model plane. It is designed to fly autonomously for up to 100km with an automated launch and landing.

This document is structured into three chapters: the first chapter captures the requirements and refines them to be used as a basis for implementation and verification. The second chapter assesses the safety risk posed by failures of the different components and describes mitigations to limit the risk. The last chapter describes the exact interfaces and protocols used between the different components.

2 Requirements

This chapter shall capture all requirements posed to the system by this task and refine them to use as a basis for both implementation and verification.

The refinement consists of multiple levels:

- The operational requirements (OP) capture all requirements directly necessary for airplane operation. The verification of the OP requirements is done during mission execution.
- The plane high-level (P-HL) requirements decompose the operational requirements into testable requirements and extend them by design-decision relevant to the implementation of the complete plane. The verification of the P-HL requirements is done using flight tests.
- The plane low-level (P-LL) requirements further decompose the plane high-level requirements and allocate them to specific systems. The verification of the P-LL requirements is done via the verification of the system specific HL requirements.
- The system-specific high-level requirements consist of the plane low-level requirements allocated to this system and system-specific design decisions. The verification of the system-specific high-level requirements is done via integration tests of the system.
- The system-specific low-level requirements refine the system-specific high-level requirements for implementation. The verification of the implementation requirements is done using unit tests.

An exemplary overview of the structure is given in Figure 2.1.

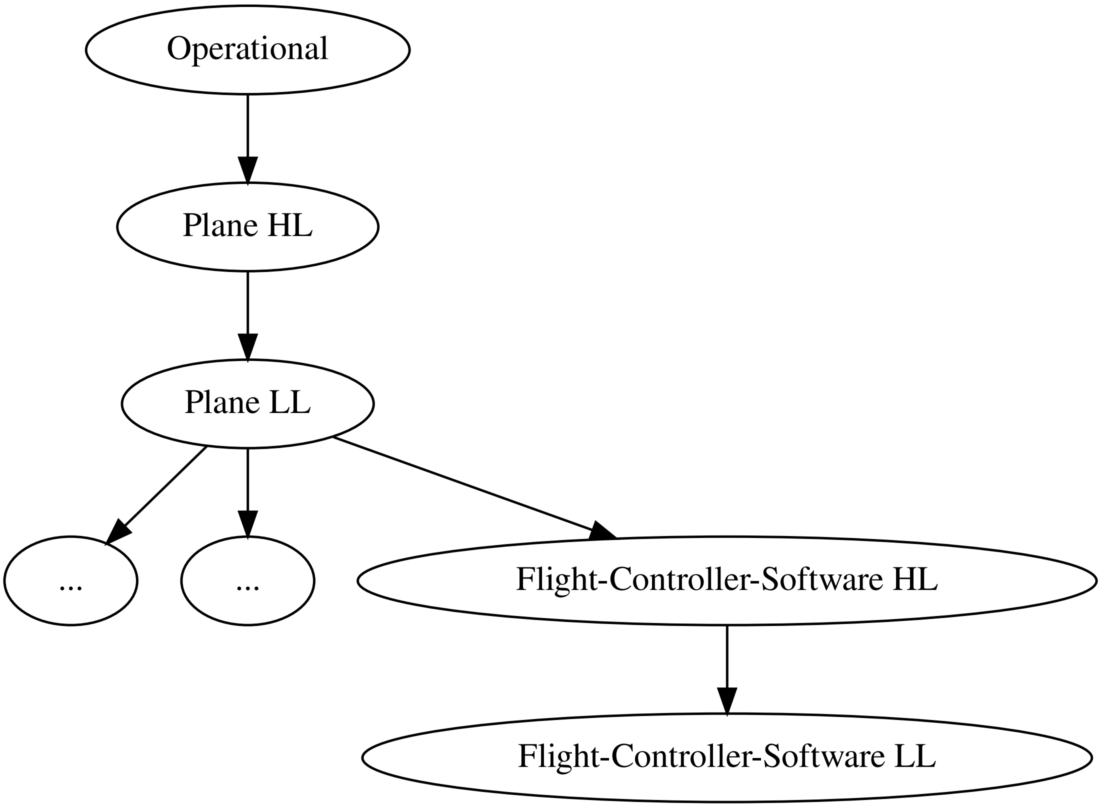

Figure 2.1: Structure of the requirements.

Requirements are formulated using the wording defined in [1], with keywords in all UPPERCASE.

2.1 Operational

OP-REQ-1: Take-Off

Description: The airplane MUST be able to be launched by a single person by throwing the plane.

Parent Requirements:

Implemented by:

- Launch detection
- Velocity estimation
- Velocity control
- Orientation estimation
- Orientation control

OP-REQ-2: Climbing

Description: The airplane MUST climb to a altitude of 50(5) m above ground after launch and circle the launch site at this altitude with a radius of 30(10) m.

Parent Requirements:

Implemented by:

- Velocity estimation
- Velocity control
- Orientation estimation
- Orientation control
- Position estimation
- Position control
- Altitude estimation
- Altitude control

OP-REQ-3: Mission

Description: The airplane MUST follow a predefined set of waypoints, consisting of latitude, longitude and altitude. Each waypoint MUST be traversed with a tolerance of ±5 m both horizontally and vertically at a predefined velocity (tolerance ±25%).

Parent Requirements:

Implemented by:

- Velocity estimation
- Velocity control
- Orientation estimation
- Orientation control
- Position estimation
- Position control
- Altitude estimation
- Altitude control
- Mission Execution

OP-REQ-4: Landing

Description: The airplane MUST be able to land at a predefined landing zone with a length of at least 50 m and a width of at least 4 m.

Parent Requirements:

Implemented by:

- Velocity estimation
- Velocity control
- Orientation estimation
- Orientation control

- Position estimation
- Position control
- Altitude estimation
- Altitude control
- Mission Execution

OP-REQ-5: Range

Description: The minimum range of the aircraft MUST be 100km.

Parent Requirements:

Implemented by:

- Energy Storage

OP-REQ-6: Error Handling

Description: The airplane MUST provide flight information when on the ground and during loitering.

Parent Requirements:

Implemented by:

- Debug Channel
- Debug Display

2.2 Plane High-Level

P-HL-REQ-1: Launch detection

Description: The plane MUST signal a launch if the acceleration is larger than $6\,\mathrm{m/s^2}$.

Parent Requirements:

- Take-Off

Implemented by:

- IMU
- IMU Measurements
- State Estimation
- Launch Detection
- FCS data transmission
- FCS data reception

P-HL-REQ-2: Velocity estimation

Description: The plane MUST estimate the current velocity with a relative error of less than 10%.

Parent Requirements:

- Take-Off
- Climbing
- Mission
- Landing

Implemented by:

- Pitot-Sensor
- Airspeed Measurements

- State Estimation
- NAVS data transmission
- NAVS data reception

P-HL-REQ-3: Velocity control

Description: The plane MUST control the velocity such that the relative error between estimated velocity and desired velociy is less than 10% after 10 s.

Parent Requirements:

- Take-Off
- Climbing
- Mission
- Landing

Implemented by:

- Thrust
- Motor Command Execution
- Velocity Controller
- Motor Setpoint Receive
- Motor Command
- Motor Setpoint Transmission

P-HL-REQ-4: Orientation estimation

Description: The plane MUST estimate the current orientation with an error of less than 5° on each axis.

Parent Requirements:

- Take-Off
- Climbing

- Mission
- Landing

Implemented by:

- IMU
- IMU Measurements
- State Estimation
- FCS data transmission
- FCS data reception

P-HL-REQ-5: Orientation control

Description: The plane MUST control the orientation such that the error between estimated orientation and desired orientation is less than 10° after 10 s.

Parent Requirements:

- Take-Off
- Climbing
- Mission
- Landing

Implemented by:

- Elevon Actuator Performance
- Control Surfaces
- Lift
- Orientation Controller
- Servo Command Transmission

P-HL-REQ-6: Position estimation

Description: The plane MUST estimate the current position with an accuracy of ±1 m.

Parent Requirements:

- Climbing
- Mission
- Landing

Implemented by:

- GPS Sensor
- GPS Measurement
- State Estimation

P-HL-REQ-7: Position control

Description: The plane MUST be able to fly a path to a position such that the distance between the estimated position and the desired position becomes less than 1 m TODO TIME.

Parent Requirements:

- Climbing
- Mission
- Landing

Implemented by:

- Elevon Actuator Performance
- Control Surfaces
- Lift
- Orientation Controller
- Position Controller

- Orientation Setpoint Transmission
- Orientation Setpoint Reception
- Servo Command Transmission

P-HL-REQ-13: Altitude estimation

Description: The MUST estimate the current altitude over ground with an error of less than 0.2 m while lower than 20 m and less than 2 m while higher thant 20 m above ground.

Parent Requirements:

- Climbing
- Mission
- Landing

Implemented by:

- Barometer
- LIDAR
- Barometer measurement
- Lidar measurements
- State Estimation
- NAVS data transmission
- NAVS data reception

P-HL-REQ-14: Altitude control

Description: The plane MUST control the altitude over ground such the error between estimated and desired altitude is less than 0.5 m TODO TIME.

Parent Requirements:

- Climbing

- Mission
- Landing

Implemented by:

- Control Surfaces
- Lift
- Altitude Controller

P-HL-REQ-8: Mission Execution

Description: The airplane MUST fly a mission consisting of the following states:

1. Pre-Takeoff
2. Launch
3. Loiter
4. Waypoint following
5. Approach
6. Landing
7. Mission completion

A waypoint consist of latitude, longitude and altitude information and optional heading.

Parent Requirements:

- Mission
- Landing

Implemented by:

- Control Surfaces
- Lift
- Reading Mission Configuration
- Mission State

- Launch Detection
- Waypoint Handling

P-HL-REQ-9: Energy Storage

Description: The airplane MUST have sufficient energy to complete a distance of 100km.

Parent Requirements:

- Range

Implemented by:

- Energy Storage

P-HL-REQ-11: Debug Channel

Description: The airplane MUST transmit data if closer than 200 m to the launch site.

Parent Requirements:

- Error Handling

Implemented by:

- Cellular Module
- Debug Data Collection
- Debug Data Transmission

P-HL-REQ-12: Debug Display

Description: Debug information transmitted by the plane MUST be displayed to the user.

Parent Requirements:

- Error Handling

Implemented by:

- Voltage and Current Sensor
- Voltage and Current Monitoring
- Debug Display Visualization
- PDBS data transmission
- PDBS data reception
- Debug Display Data Reception

P-HL-DD-1: Partitioning

Description: The plane is partitioned into the following components:

- Mechanical:
  - Airframe (AF)
  - Actuators (AC)
- Electronical:
  - Flightcontroller (FC)
  - Flightcomputer (FCP)
  - Power Distribution Board (PDB)
  - Navigation Board (NAV)
- Software:
  - Flightcontroller-Software (FCS)
  - Flightcomputer-Software (FCPS)
  - Power Distribution Board Software (PDBS)
  - Navigation Board Software (NAVS)
  - Debug Display Software (DDS)
- External Components:

  - RC-Receiver (RX)
  - RC-Transmitter (TX)

An overview of the data flow between the partitions is given in Figure 2.2.

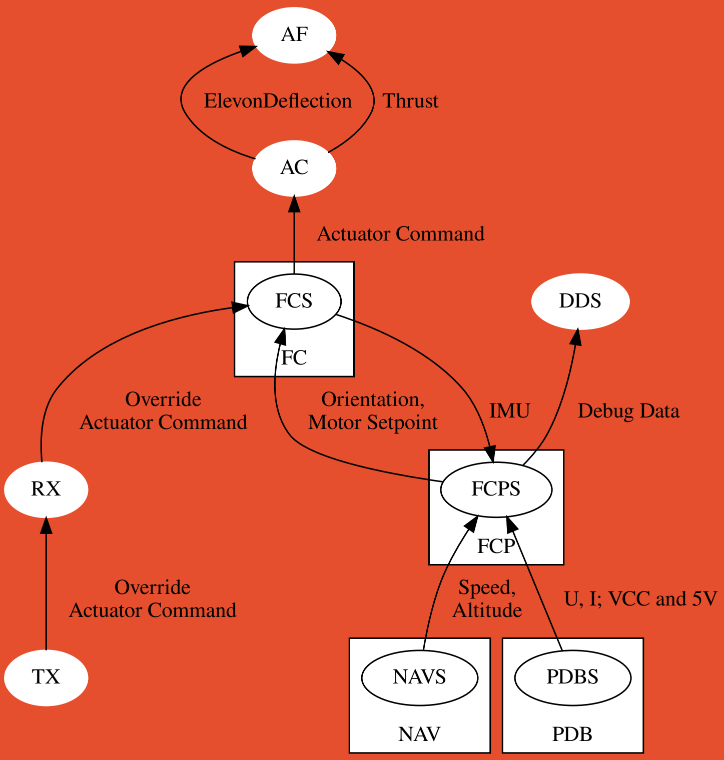

Figure 2.2: System Partitioning and Data Flow

Reasoning: This partitioning allows to implement the components individually from each other and thus allows to limit the complexity of the mission-critical components.

Implemented by:

- Voltage and Current Sensor
- Voltage and Current Monitoring
- Debug Display Visualization
- PDBS data transmission

- PDBS data reception
- Debug Display Data Reception

P-HL-DD-3: Frequency of FCPS control loop

Description: The FCPS runs all control loops with at least 10 Hz.

Reasoning: This guarantees sufficient time for all calculations but also guarantees a sufficient controller performance as 100 ms is much smaller than all time-constants of the orientation-controlled system.

Implemented by:

- Voltage and Current Sensor
- Voltage and Current Monitoring
- Debug Display Visualization
- PDBS data transmission
- PDBS data reception
- Debug Display Data Reception

P-HL-DD-4: Frequency of FCS control loop

Description: The FCS runs all control loops with at least 50 Hz.

Reasoning: The motor and servo commands can only be sent at this frequency, thus a faster control loop would not bring any advantages.

Implemented by:

- Voltage and Current Sensor
- Voltage and Current Monitoring
- Debug Display Visualization
- PDBS data transmission
- PDBS data reception

- Debug Display Data Reception

P-HL-DD-2: Manual override

Description: The plane shall be able to be controlled manually while closer than 200m to the pilot.

Reasoning: This allows handling errors during launch without risk of crashing.

Implemented by:

- Voltage and Current Sensor
- Voltage and Current Monitoring
- Debug Display Visualization
- PDBS data transmission
- PDBS data reception
- Debug Display Data Reception

2.3 Plane Low-Level

P-LL-REQ-1: IMU

Description: The FC MUST be equipped a sensor for measuring the orientation.

Parent Requirements:

- Launch detection
- Orientation estimation
- Partitioning

Partition: FC

P-LL-REQ-7: Pitot-Sensor

Description: The NAV MUST be equipped with a sensor for measuring airspeed.

Parent Requirements:

- Velocity estimation
- Partitioning

Partition: NAV

P-LL-REQ-20: GPS Sensor

Description: The FCP MUST be equipped with a sensor for measuring positions.

Parent Requirements:

- Position estimation
- Partitioning

Partition: FCP

P-LL-REQ-31: Barometer

Description: The NAV MUST be equipped with a sensor for measuring absolute altitude.

Parent Requirements:

- Altitude estimation
- Partitioning

Partition: NAV

P-LL-REQ-35: LIDAR

Description: The NAV MUST be equipped with a sensor for measuring relative altitude above ground.

Parent Requirements:

- Altitude estimation
- Partitioning

Partition: NAV

P-LL-REQ-54: Voltage and Current Sensor

Description: The PDB MUST be equipped with a sensor for the following quantitites:

- Battery Voltage
- Battery Current
- 5V-Rail Voltage
- 5V-Rail Current

Parent Requirements:

- Debug Display
- Partitioning

Partition: PDB

P-LL-REQ-37: Cellular Module

Description: The FCP MUST be equipped with a transmitter for transmitting debug data.

Parent Requirements:

- Debug Channel
- Partitioning

Partition: FCP

P-LL-REQ-29: Energy Storage

Description: The AC MUST provide sufficient energy for 2 h at $15\,\mathrm{m\,s^{-1}}$.

Parent Requirements:

- Energy Storage
- Partitioning

Partition: AC

P-LL-REQ-16: Thrust

Description: The AC MUST provide sufficient thrust to achieve a velocity of 15 m/second during flight.

Parent Requirements:

- Velocity control
- Partitioning

Partition: AC

P-LL-REQ-19: Elevon Actuator Performance

Description: The AC MUST set the position of the control surfaces every 20 ms.

Parent Requirements:

- Orientation control
- Position control
- Partitioning

Partition: AC

P-LL-REQ-58: Control Surfaces

Description: The AF MUST be equipped with two elevons which allow for control of both the roll and pitch axis.

Parent Requirements:

- Orientation control
- Position control
- Altitude control
- Mission Execution
- Partitioning

Partition: AF

P-LL-REQ-59: Lift

Description: The AF MUST provide lift to carry a total system weight of 2.5 kg at 15 m s^{-1}

Parent Requirements:

- Orientation control
- Position control
- Altitude control
- Mission Execution
- Partitioning

Partition: AF

P-LL-REQ-60: Mounting

Description: The AF MUST provide mounting places for the following components:

- SA
- PW
- FC
- FCP
- PDB
- NAV

Parent Requirements:

- Partitioning

Partition: AF

P-LL-REQ-2: IMU Measurements

Description: The FCS MUST read the following data around all three axis

- Orientation angle
- Rotation-rate
- Acceleration

every 20 ms.

Parent Requirements:

- Launch detection
- Orientation estimation
- Partitioning
- Frequency of FCS control loop

Partition: FCS

Implemented by:

- IMU Measurements

P-LL-REQ-8: Airspeed Measurements

Description: The airspeed MUST be measured by the NAVS every 100 ms.

Parent Requirements:

- Velocity estimation
- Partitioning
- Frequency of FCPS control loop

Partition: NAVS

P-LL-REQ-21: GPS Measurement

Description: The FCPS MUST query the GPS sensor for new data every 100 ms.

Parent Requirements:

- Position estimation
- Partitioning
- Frequency of FCPS control loop

Partition: FCPS

P-LL-REQ-32: Barometer measurement

Description: The NAVS MUST read the altimeter every 100 ms.

Parent Requirements:

- Altitude estimation
- Partitioning
- Frequency of FCPS control loop

Partition: NAVS

P-LL-REQ-36: Lidar measurements

Description: The NAVS MUST read the LIDAR every 100 ms.

Parent Requirements:

- Altitude estimation
- Partitioning
- Frequency of FCPS control loop

Partition: NAVS

P-LL-REQ-55: Voltage and Current Monitoring

Description: The PDBS MUST measure the following physical quantities

- Battery Voltage
- Battery Current
- 5V-Rail Voltage
- 5V-Rail Current

every 100 ms

Parent Requirements:

- Debug Display
- Partitioning
- Frequency of FCPS control loop

Partition: PDBS

P-LL-REQ-15: Motor Command Execution

Description: The AC MUST react on every motor command in at most 20 ms.

Parent Requirements:

- Velocity control
- Partitioning
- Frequency of FCS control loop

Partition: AC

P-LL-REQ-5: State Estimation

Description: The FCPS MUST filter the IMU and pitot data to guarantee

- an acceleration with $2\sigma_a \leq 0.6\,\mathrm{m/s^2}$

- the orientation with $2\sigma_{\text{orientation}} \leq 5^\circ$
- the velocity with $2\sigma_v \leq \hat{v} \cdot 10\%$
- the position with $2\sigma_{x,y} \leq 1\,\text{m}$.
- the altitude over the ground with $2\sigma_h \leq h_{\text{tol}}$, with $h_{\text{tol}} = 2\,\text{m}$ for $h \geq 20\,\text{m}$ and $h_{\text{tol}} = 0.2\,\text{m}$ otherwise.

Note: the accuracy requirements are reformulated as requirements regarding the standard deviation, using a confidence bound of $95\% \equiv 2\sigma$.

Parent Requirements:

- Launch detection
- Velocity estimation
- Orientation estimation
- Position estimation
- Altitude estimation
- Partitioning
- Frequency of FCPS control loop

Partition: FCPS

P-LL-REQ-27: Reading Mission Configuration

Description: The FCPS MUST read a list of waypoints and a target at startup. Both the waypoints and the target consists of the following information:

- Latitude
- Longitude
- Altitude above sea level
- Optional: Heading at which to pass the point

Parent Requirements:

- Mission Execution
- Partitioning

Partition: FCPS

P-LL-REQ-61: Mission State

Description: The FCPS MUST call the correct mission subprogram and switch mission state depending on the output of this subprogram.

Parent Requirements:

- Mission Execution

Partition: FCPS

P-LL-REQ-6: Launch Detection

Description: The FCPS MUST use the estimated state to signal a launch if the acceleration is larger than $6\,\mathrm{m\,s^{-1}}$.

Parent Requirements:

- Launch detection
- Mission Execution
- Partitioning

Partition: FCPS

P-LL-REQ-28: Waypoint Handling

Description: The FCPS MUST send the next waypoint as input to the position control and detect when a waypoint was hit and then forwards the next waypoint.

Parent Requirements:

- Mission Execution
- Partitioning

Partition: FCPS

P-LL-REQ-11: Velocity Controller

Description: The FCPS MUST be able to find a motor command such that the relative error between estimated velocity and desired velociy is less than 10% after 10 s.

Parent Requirements:

- Velocity control
- Partitioning

Partition: FCPS

P-LL-REQ-17: Orientation Controller

Description: The FCS MUST compute a actuator command every 20 ms, such that the error between estimated orientation and actual orientation is less than 10° after 10 s.

Parent Requirements:

- Orientation control
- Position control
- Partitioning
- Frequency of FCS control loop

Partition: FCS

Implemented by:

- Attitude Controller

P-LL-REQ-24: Position Controller

Description: The FCPS MUST find a dynamically feasible trajectory of orientation and velocities, such that the distance between the estimated position and the desired position becomes less than 1 m.

Parent Requirements:

- Position control
- Partitioning

Partition: FCPS

P-LL-REQ-61: Altitude Controller

Description: The FCPS MUST control the altitude such that the error between estimated and desired altitude is less than 0.5 m.

Parent Requirements:

- Altitude control
- Partitioning

Partition: FCPS

P-LL-REQ-30: Debug Data Collection

Description: The FCPS MUST collect the following data:

- All data from the FCS
- All data from the PDBS
- All data from the NAVS
- The estimated state
- The current flight state

Parent Requirements:

- Debug Channel
- Partitioning

Partition: FCPS

P-LL-REQ-40: Debug Display Visualization

Description: The DDS MUST be able to visualize all debug data.

Parent Requirements:

- Debug Display
- Partitioning

Partition: DDS

P-LL-REQ-45: Override Command

Description: The FCS MUST use the override information as command if the override switch is activated.

Parent Requirements:

- Manual override

Partition: FCS

Implemented by:

- Override Command

P-LL-REQ-46: Arm Command

Description: The FCS MUST always send the motor command 0 if the arm switch is not activated.

Parent Requirements:

- Manual override

Partition: FCS

Implemented by:

- Arm Command

P-LL-REQ-47: FC-FCP Interface

Description: The FC MUST be equipped with an interface to send and receive data to the FCP

Parent Requirements:

- Partitioning

Partition: FC

P-LL-REQ-48: FCP-FC Interface

Description: The FCP MUST be equipped with an interface to send and receive data to the FC

Parent Requirements:

- Partitioning

Partition: FCP

P-LL-REQ-49: NAV-FCP Interface

Description: The NAV MUST be equipped with an interface to send data to the FCP

Parent Requirements:

- Partitioning

Partition: NAV

P-LL-REQ-50: FCP-NAV Interface

Description: The FCP MUST be equipped with an interface to receive data from the NAV

Parent Requirements:

- Partitioning

Partition: FCP

P-LL-REQ-51: PDB-FCP Interface

Description: The PDB MUST be equipped with an interface to send data to the FCP

Parent Requirements:

- Partitioning

Partition: PDB

P-LL-REQ-52: FCP-PDB Interface

Description: The FCP MUST be equipped with an interface to receive data from the PDB

Parent Requirements:

- Partitioning

Partition: FCP

P-LL-REQ-53: Servo and Motor Interface

Description: The FC MUST be equipped with an interface to send commands to the CS and EP

Parent Requirements:

- Partitioning

Partition: FC

P-LL-REQ-43: FC-RX Interface

Description: The FC MUST be able to receive commands from the RX.

Parent Requirements:

- Manual override

Partition: FC

P-LL-REQ-3: FCS data transmission

Description: The FCS MUST transmit IMU data every 100 ms to the FCPS.

Parent Requirements:

- Launch detection
- Orientation estimation
- Partitioning
- Frequency of FCPS control loop

Partition: FCS

Implemented by:

- FCS data transmission

P-LL-REQ-4: FCS data reception

Description: The FCPS MUST be able to receive FCS data every 100 ms.

Parent Requirements:

- Launch detection
- Orientation estimation
- Partitioning
- Frequency of FCPS control loop

Partition: FCPS

P-LL-REQ-33: NAVS data transmission

Description: The NAVS MUST transmit the following data

- Velocity
- Barometric altitude
- LIDAR

every 100 ms.

Parent Requirements:

- Velocity estimation
- Altitude estimation
- Partitioning
- Frequency of FCPS control loop

Partition: NAVS

P-LL-REQ-34: NAVS data reception

Description: The FCPS MUST receive the NAVS data every 100 ms.

Parent Requirements:

- Velocity estimation
- Altitude estimation
- Partitioning
- Frequency of FCPS control loop

Partition: FCPS

P-LL-REQ-56: PDBS data transmission

Description: The PDBS MUST transmit the measured data every 100 ms to the FCPS.

Parent Requirements:

- Debug Display
- Partitioning
- Frequency of FCPS control loop

Partition: PDBS

P-LL-REQ-57: PDBS data reception

Description: The FCPS MUST be able to receive PDB data every 100 ms from the PDBS.

Parent Requirements:

- Debug Display
- Partitioning

- Frequency of FCPS control loop

Partition: FCPS

P-LL-REQ-42: RX reception

Description: The RX MUST receive the information sent by the TX and forward it to the FCP.

Parent Requirements:

- Manual override

Partition: RX

P-LL-REQ-38: Debug Data Transmission

Description: The FCPS MUST transmit the collected debug data every 100 ms via the cellular connection.

Parent Requirements:

- Debug Channel
- Partitioning

Partition: FCPS

P-LL-REQ-39: Debug Display Data Reception

Description: The DDS MUST be able to receive the debug data every 100 ms via the cellular connection.

Parent Requirements:

- Debug Display
- Partitioning

Partition: DDS

P-LL-REQ-13: Motor Setpoint Receive

Description: The FCS MUST be able to receive a motor setpoint every 100 ms

Parent Requirements:

- Velocity control
- Partitioning
- Frequency of FCPS control loop

Partition: FCS

Implemented by:

- Motor Setpoint Receive

P-LL-REQ-14: Motor Command

Description: The FCS MUST transmit every motor setpoint as a command to the AC at most 20 ms after reception.

Parent Requirements:

- Velocity control
- Partitioning
- Frequency of FCS control loop

Partition: FCS

Implemented by:

- Motor Command

P-LL-REQ-25: Orientation Setpoint Transmission

Description: The FCPS MUST transmit every 100 ms the orientation and calculated by the position controller for the current timestep.

Parent Requirements:

- Position control
- Partitioning

Partition: FCPS

P-LL-REQ-26: Orientation Setpoint Reception

Description: The FCS MUST receive the orientation setpoint from the FCPS every 100 ms.

Parent Requirements:

- Position control
- Partitioning

Partition: FCS

Implemented by:

- Orientation Setpoint Reception

P-LL-REQ-12: Motor Setpoint Transmission

Description: The FCPS MUST transmit the calculated motor setpoint every 100 ms

Parent Requirements:

- Velocity control

- Partitioning
- Frequency of FCPS control loop

Partition: FCPS

P-LL-REQ-18: Servo Command Transmission

Description: The FCS MUST transmit the computed servo command every 20 ms.

Parent Requirements:

- Orientation control
- Position control
- Partitioning
- Frequency of FCS control loop

Partition: FCS

Implemented by:

- Servo Command Transmission

P-LL-REQ-41: TX command transmission

Description: The TX MUST transmit the following information:

- Motor arm switch position
- Manual override switch position
- Motor setpoint override
- Servo setpoint override

Parent Requirements:

- Manual override

Partition: TX

P-LL-REQ-44: Override reception

Description: The FCS MUST be able to receive the override information from the RX.

Parent Requirements:

- Manual override

Partition: FCS

Implemented by:

- Override reception

2.4 Flight-Controller-Software High-Level

FCS-HL-REQ-1: IMU Measurements

Description: The FCS shall read measurement the following data around all three axis

- Orientation angle
- Rotation-rate
- Acceleration

every 20 ms.

Parent Requirements:

- IMU Measurements

Partition: FCS

FCS-HL-REQ-2: Attitude Controller

Description: The FCS shall compute a actuator command every 20 ms, such that the error between estimated attitude and actual attitude is less than 10° after 10 s.

Parent Requirements:

- Orientation Controller

Partition: FCS

FCS-HL-REQ-3: Override Command

Description: The FCS shall use the override information as command if the override switch is activated.

Parent Requirements:

- Override Command

Partition: FCS

FCS-HL-REQ-4: Arm Command

Description: The FCS shall always send the motor command 0 if the arm switch is not activated.

Parent Requirements:

- Arm Command

Partition: FCS

FCS-HL-REQ-5: FCS data transmission

Description: The FCS shall transmit IMU data every 100 ms to the FCPS.

Parent Requirements:

- FCS data transmission

Partition: FCS

FCS-HL-REQ-6: Motor Setpoint Receive

Description: The FCS shall be able to receive a motor setpoint every 100 ms

Parent Requirements:

- Motor Setpoint Receive

Partition: FCS

FCS-HL-REQ-7: Motor Command

Description: The FCS shall transmit every motor setpoint as a command to the AC at most 20 ms after reception.

Parent Requirements:

- Motor Command

Partition: FCS

FCS-HL-REQ-8: Orientation Setpoint Reception

Description: The FCS shall receive the orientation setpoint from the FCPS every 100 ms.

Parent Requirements:

- Orientation Setpoint Reception

Partition: FCS

FCS-HL-REQ-9: Servo Command Transmission

Description: The FCS shall transmit the computed servo command every 20 ms.

Parent Requirements:

- Servo Command Transmission

Partition: FCS

FCS-HL-REQ-10: Override reception

Description: The FCS shall be able to receive the override information from the RX.

Parent Requirements:

- Override reception

Partition: FCS

FCS-HL-DD-1: Architecture

Description: The FCS is structure into an architecture consisting of four layers with increasing abstraction and application-specificity. Each layer consists of independent modules, each module is responsible for exactly one system the FCS interfaces with.

The layers and modules are:

- Hardware-Abstraction-Layer (HAL):
  - UART: Handles the configuration of the uart interface for the connection to the IMU, RX and FCP
  - Pwm16Bit: Handles the configuration of the physical interface for generating Pulse-Width-Modulates Signals for the AC
  - Timer8Bit: Handles the configuration of the timer for all functionallity with timing requirements
- Drivers
  - Bno055-UART: Uses the UART Module to handle the read/write commands to the IMU
  - Bno055: Uses the Bno055-UART Module to provide functionallity to read sensor values and configure the sensor
  - SBus: Uses the UART Module to decode the packages sent by the RX
  - Protobuf: Uses the UART Module to decode and encode packages to the FCP
  - PPM: Uses the Pwm16Bit Module to generate Pulse-Position-Modulated Signals for the AC
- Components
  - IMU: Uses the Bno055 Module to configure the sensor for the application and read the required sensor data

  - Remote: Uses the SBus Module to decode the inputs and switches sent by the TX

  - Flightcomputer: Uses the Protobuf Module to send and receive data from the FCPS

  - Actuators: Uses the PPM Module to send commands to the AC

  - System: Uses the Timer8bit Module and configures the MCU for the application

- Application

  - Mode Handler: Collects data from the IMU, Remote and Flightcomputer Module and decides on the Flightmode depending on availability of the data

  - Controller: Uses the mode handler information to calculate an actuator signal

  - Application: Implements the application logic by controlling the other modules

  - Error-Handler: Provides mechanisms to signal warnings and error generated by the modules.

This architecture is depicted in Figure 2.4.

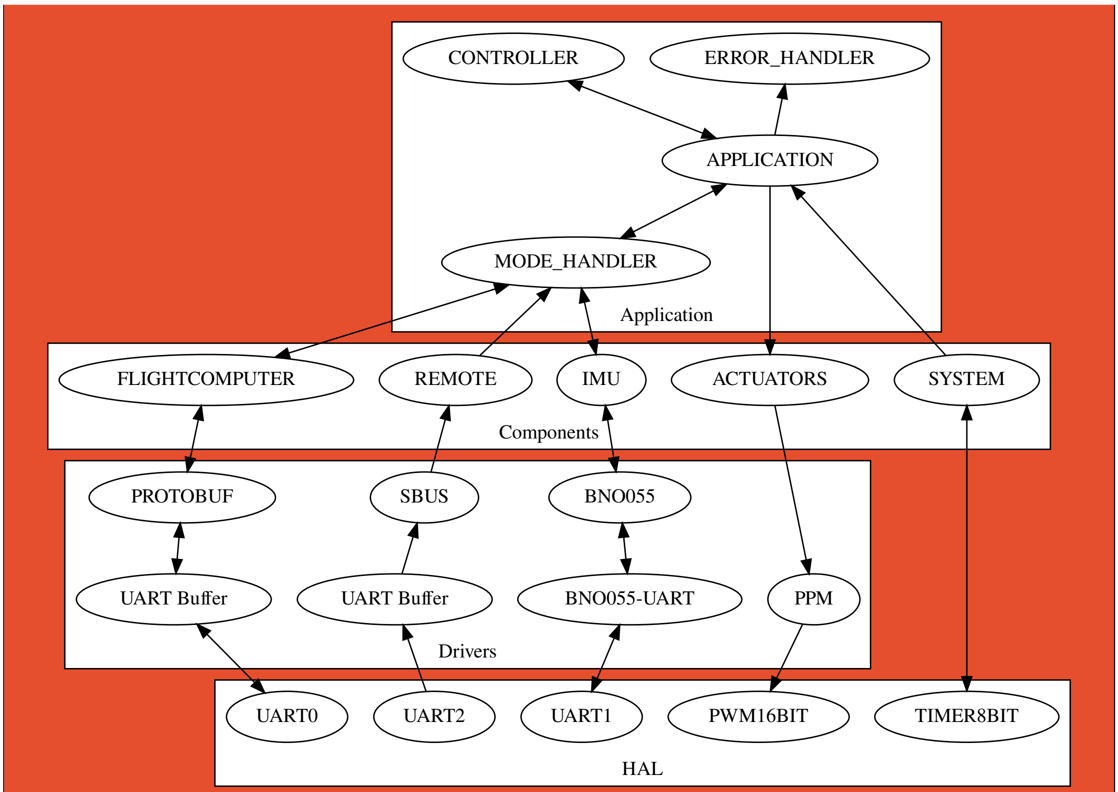

Figure 2.3: Architecture of the FCS

Reasoning: This layered architecture allows for simple, testable and reusable modules on all layers. In addition the application is independent of the physical interfaces and communication strategy, such that the application logic can be easily implemented and components can be easily replaced.

FCS-HL-DD-2: Fault Detection

Description: The following fault conditions shall be detected:

- Faults reported by the IMU (Self test at startup and status during operation)
- Faults reported by the MCU (Brownout)
- Violation of the timing constraints (Application Loop Runtime, Watchdog Timer reset)

- No data from the IMU for 100 ms
- No data from the flight-computer for 200 ms
- No data from the remote for 100 ms
- Overflow of the Remote or FCP Receive-Buffers due to invalid message size

and signalled to the error-handler component.

Reasoning: The detection of faults allows to adapt the mission as early as possible, avoiding that faults turn into failures of the airplane.

FCS-HL-DD-3: Fault Handling

Description: The following fault conditions shall be handled automatically:

- No data from the IMU for 100 ms: use remote as fallback
- No data from the flight-computer for 200 ms: use remote as fallback
- No data from the remote for 100 ms: do stabilised emergency runtime
- Overflow of the Remote or FCP Receive-Buffers: disable the respective receive interrupt

and signalled to the error-handler component.

Reasoning: Detectable failures which can be handled automatically should be handled automatically by the FCS.

2.5 Flight-Controller-Software Low Level

See the Flight-Controller-Software Documentation.

3 Safety Assesment

The following chapter lists the possible failure conditions and their severity. The severity of an issue is classified in five levels, depending on the influence of the performance of the complete system, Table 3.1 list these levels.

Level	Consequence of Failure
A	Failure will lead to loss of aircraft
B	Failure will lead to damage of aircraft
C	Failure will result in non-fulfillment of mission
D	Failure will lead to inconvenience during mission fulfillment
E	No consequence on aircraft

Table 3.1: Safety Levels

3.1 Failure Analysis

Table 3.2 lists all analyzed failures, the failures are determined by analyzing all external interactions of the systems under the aspects of availability and integrity of the interaction.

Failure	Severity	
Loss of control surface actuation	A	Without control surface actuation no stable flight can be guaranteed
Invalid control surface actuation	A	With incorrect control surface actuation no stable flight can be guaranteed
Loss of thrust	B	Without thrust an emergency landing must be performed
Invalid thurst control	C	
Loss of debug data	D	
Invalid debug data	C	

Table 3.2: Failure Conditions

3.2 Fault Analysis

For the failures listed above, all faults by components will result in the respective failure shall be analyzed and mitigations to avoid the fault shall be found. The extent and necessity of the mitigations are determined by the severity of the failure.

4 Interface Definition

4.1 Physical Configuration

USB

4.2 Electrical Configuration

4.2.1 UART Configuration

4.3 Encoding

Format Messages IDs

4.3.1 Flightcontroller Message

4.3.2 Nav Message

4.4 Remote Configuration

Bibliography

[1] Scott O. Bradner. *Key words for use in RFCs to Indicate Requirement Levels.* RFC 2119. Mar. 1997. DOI: `10.17487/RFC2119`. URL: `https://www.rfc-editor.org/info/rfc2119`.