Reliability and Safety Analysis

Year: 2022 Semester: Fall Team: 08 Project: Hermes

Creation Date: ­11/5/2022 Last Modified: November 5, 2022

Author: Michael Langford Email: mjlangfo@purdue.edu

Assignment Evaluation:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **Score (0-5)** | **Weight** | **Points** | **Notes** |
| **Assignment-Specific Items** | | | | |
| **Reliability Analysis** |  | x2 |  |  |
| **MTTF Tables** |  | x3 |  |  |
| **FMECA Analysis** |  | x2 |  |  |
| **Schematic of Functional Blocks (Appendix A)** |  | x2 |  |  |
| **FMECA Worksheet (Appendix B)** |  | x3 |  |  |
| **Writing-Specific Items** | | | | |
| **Spelling and Grammar** |  | x2 |  |  |
| **Formatting and Citations** |  | x1 |  |  |
| **Figures and Graphs** |  | x2 |  |  |
| **Technical Writing Style** |  | x3 |  |  |
| **Total Score** |  | | |  |

5: Excellent 4: Good 3: Acceptable 2: Poor 1: Very Poor 0: Not attempted

Comments:

*Comments from the grader will be inserted here.*

1. Reliability Analysis

STM32F446

The STM32F4 Microcontroller is the heart of the flight controller for the drone, and critical to all flight systems. It has been selected for analysis both for its complexity and its criticality. Failure rate and mean time to failure are here calculated from section 5.1 of MIL-HDBK-217F.

Model chosen [Failures / 10^6 hours]:

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter name | Description | Value | Comments |
|  | Die complexity | *0.56* | MOS, 32 bits |
|  | Temperature coeff. | *1.5* | 5.8 |
|  | Package Constant | *.032* | 5.9 |
|  | Environmental Constant | *8* | 5.10, ARW |
|  | Quality Factor | *10* | Commercial components |
|  | Learning Factor | *1* | The IC is more than two  years in production. |
|  |  |  |  |
| Entire design: |  |  |  |
|  |  | 10.96 |  |
| MTTF |  | 0.0912 |  |

S13V15F5 5V Regulator

The S13V15F5 is the IC used in the Pololu step-up/down regulator module. This device regulates the ESC 10V supply efficiently down to 5V for use on the flight control board. It again has been chosen for its importance as well as complexity, for as yet it is the only power supply to the flight controller PCB and its daughterboards and is thus a critical component.

Failure rate and mean time to failure are here calculated from section 5.1 of MIL-HDBK-217F, modeling switched-mode CMOS supply.

Model chosen [Failures / 10^6 hours]:

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter name | Description | Value | Comments |
|  | Die complexity | *0.01* | MOS, 32 bits |
|  | Temperature coeff. | *1.5* | 5.8 |
|  | Package Constant | *.0072* | 16 pin SMT |
|  | Environmental Constant | *8* | 5.10, ARW |
|  | Quality Factor | *10* | Commercial components |
|  | Learning Factor | *1* | The IC is more than two  years in production. |
|  |  |  |  |
| Entire design: |  |  |  |
|  |  | 0.72 |  |
| MTTF |  | 1.377 |  |

LD1117AS33TR 3.3V Regulator

The LD1117AS33TR is used as the 3.3V regulator on the flight controller PCB. It is a low dropout linear regulator as opposed to a switched mode supply like the previous component. This device regulates the 5V switched regulator output supply down to 3.3V to power the microcontroller and IMUs. It again has been chosen for its importance as well as complexity, for as yet it is the only power supply to microcontroller and IMUs and is thus a critical component.

Failure rate and mean time to failure are here calculated from section 5.1 of MIL-HDBK-217F, modeling linear regulators.

Model chosen [Failures / 10^6 hours]:

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter name | Description | Value | Comments |
|  | Diode type/application | *0.002* | Voltage regulator |
|  | Temperature coeff. | *3.7* | 5.8 |
|  | Electrical Stress Factor | *1.0* |  |
|  | Environmental Constant | *24* | 5.10, ARW |
|  | Contact Construction Factor | *1* | Bonded |
|  | Quality Factor | *1* |  |
|  |  |  |  |
| Entire design: |  |  |  |
|  |  | 0.1776 |  |
| MTTF |  | 5.631 |  |

Summary

Judging by the results of this analysis, the system is very reliant on its power supplies and the single microcontroller performing flight control calculations. In particular, the switched mode regulator and microcontroller have high failure rates. This would be improved by adding redundant microcontrollers to assist in flight control, and redundant and independent power supplies.

1. Failure Mode, Effects, and Criticality Analysis (FMECA)

Due to the nature of most failures for this project, there are only low and high criticality levels. Low means that system performance is reduced, and minor functionality disabled. All other failures fall under high, defined as any failure that stops either results in a controlled crash, loss of control, or shutdown of the system, as all of these have direct potential for user injury.

Accepted failure rate for high criticality failure is , and for low criticality failure, . We assume all usage of the device at this stage of development will be indoors, and although much testing will be distant from users, this will not always be the case, hence the large factor used.

3.0 Sources Cited:

[1] STM32F446xC/E Data Sheet, ST Microelectronics, 2021.

[2] “Military Handbook Reliability Prediction of Electronic Equipment” Department of

Defense. Washington DC. MIL-HDBK-217F, Dec. 2, 1991.

[3] LD1117A, ST Microelectronics, 2013

Appendix A: Schematic Functional Blocks

Diagram, schematic

Description automatically generated

Figure . Power supply

Diagram, schematic

Description automatically generated

Figure . Microcontroller, reset, and programming

Diagram, schematic

Description automatically generated

Figure . Communication peripherals (USB, Radio, Pi UART)

Diagram, schematic

Description automatically generated

Figure . Backup motors and LIDAR

Diagram, schematic

Description automatically generated

Figure . IMUs

Appendix B: FMECA Worksheet

Table . Power supply FMECA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 1 | Voltage Drop | Supply capacitors | Radio receiver failure, Pi navigation computer brownout, flight controller and IMU brownout, loss of decoupling. | Loss of control, loss of navigation capability, crash | High |  |
| 2 | Voltage regulator fails short | 5V regulator, 3.3V regulator | Total loss of control, crash | Crash | High |  |

Table . Microcontroller section

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 1 | Unresponsive | Damaged power pins | Device does not start, unpredictable, can occur at any point in flight mode. | No start of device | High |  |
| 2 | Communication issues and failures | Oscillator failure, USART internal failure | Missed packets | Oscillator switched to HSI, reduction in controllability | Low |  |

Table . LIDAR

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 1 | Communication failure | Wiring disconnect | Loss of navigation capability | Crash | High |  |
| 2 | Blocked visibility | Dirt, grime accumulation | Loss of navigation capability | Crash | High |  |

Table . IMU

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 1 | Communication failure | Wiring disconnect, failure of internal SPI | Loss of control capability | Crash | High |  |
| 2 | Noise | Poor mounting, failed solder joint | Reduced control | Sluggish control | Low |  |