Reliability and Safety Analysis

Year: \_2019\_ Semester: \_Spring\_ Team: \_\_17\_\_ Project : \_Face Tracking Drone\_\_\_\_\_\_

Creation Date: \_\_\_\_\_Mar 26, 2019\_\_\_\_\_\_\_\_\_\_ Last Modified: March 3, 2015

Author: Yi Qiao\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Email: qiao22@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:

1. Reliability Analysis

There are three main components that are most likely to fail. They are chosen for reliability analysis because of their dominative complexity or the role of power provider. STM32F407VG [1] has high complexity which is used to control the entire system. OKI-78SR [2] is used to provide power to the digital circuits. FTDI232 [3] also has similarly high complexity as microcontroller. According to MIL-HDBK-217F [4], the failure per 10^6 hours (𝝀P) and mean time to failure (MTTF) are calculated. The model of digital CMOS IC microprocessor model and CMOS Switch-Mode Regulator are used. The formula, 𝝀P = (C1 · πT + C2· πe) · πl · πq is used for all of following components. The result shows MTTF and 𝝀𝑷 are in the expected range. Any failure of these components would not directly cause harm to the users.

STM32F407VG

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter name | Description | Value | *Comments* |
| C1 | Die complexity | 0.56 | Based on the MIL-Hdbk217f for 32 bit microcontrollers |
| πT | Temperature coeff. | 1.8 | Assuming a worst case junction temperature of 105C based on worst operating temp of microcontroller |
| C2 | Pin/Package Constant | 0.053 | SMT with 100 Pins |
| πe | Environmental Constant | 4.0 | AIC, lower performance smaller aircraft |
| πl | Learning Factor | 1.0 | The IC is more than two years in production |
| πq | Quality Factor | 10 | Commercial part |
| Entire design: |  |  |  |
| 𝝀P | | 12.2 | |
| MTTF | | 0.0820 | |

Figure 1. Microcontroller analysis

OKI-78SR

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter name | Description | Value | *Comments* |
| C1 | Die complexity | *0.01* | *1 to 100 bipolar transistors is used* |
| πT | Temperature coeff. | *0.1* | CMOS, 𝑻𝒋= 25 C |
| C2 | Pin/Package Constant | *0.00022* | 3 pin Flatpacks |
| πe | Environmental Constant | 4.0 | AIC, lower performance smaller aircraft |
| πl | Learning Factor | 1.0 | The IC is more than two years in production |
| πq | Quality Factor | 10 | Commercial part |
| Entire design: |  |  |  |
| 𝜆𝑃 | | *0.0188* | |
| MTTF | | *53.19* | |

Table 2. Voltage convertor analysis

FTDI232

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter name | Description | Value | *Comments* |
| C1 | Die complexity | 0.14 | Based on the MIL-Hdbk217f [2] for 8 bit microcontrollers |
| πT | Temperature coeff. | 0.98 | Assuming a worst case junction temperature of 85C based on worst operating temp of microcontroller |
| C2 | Pin/Package Constant | 0.01 | SMT with 28 Pins |
| πe | Environmental Constant | 4.0 | AIC, lower performance smaller aircraft |
| πl | Learning Factor | 1.0 | The IC is more than two years in production. |
| πq | Quality Factor | 10 | Commercial part |
| Entire design: |  |  |  |
| 𝝀P | | 1.772 | |
| MTTF | | 0.5643 | |

Table3. UART analysis

**Reliability Summary**

The microcontroller has a minimum MTTF among the three component. Even so, it is expected to last for an average of 0.082\*106 hrs, which is around ten years. The failure rate is on the scale of 10-5 per hour. While the system is supposed to last for around 10-15 minutes per charge, the actual failure rate will be far lower causing by the infrequent use, thus acceptable. Moreover, while the system will mostly operate in the air, the actual working temperature will be far lower than the assumption maximum temperature, reducing the temperature coeff, making the system more reliable in real life situation.

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

There are four criticality levels for this project, level 1, level 2, level 3 and level 4. The severity increases as the number increases. Level 4 covers any situation that involves user injuries. Such as system defections which make the device out of control and cause further injuries and situations like burn and chemical liquid leakage caused by battery defection. Level 3 covers any situation that involves severe devices damage along with infrastructure damage, such as damaging public infrastructure and vehicles. Level 2 covers things like devices damage with physical collisions and important components got damaged or shorted, such as crashing on the wall and soaked by rain. Level 1 will be some minor failure that can be recovered with little costs such as system shut down. The acceptable failure rate for Level 4 is 10-10, 10-6 for Level 3, 10-3 for Level 2 and 10-2 for Level 1. We hope users could use this device with cautions and do prepare before operating this device. Also, we hope users will not use this product in improper situations which could cause injuries and property lost.

3.0 Sources Cited:

[1] St.com. (2019). [online] Available at: https://www.st.com/resource/en/datasheet/dm00037051.pdf [Accessed 29 Mar. 2019].

[2] Power.murata.com. (2019). [online] Available at: https://power.murata.com/pub/data/power/oki-78sr.pdf [Accessed 29 Mar. 2019].

[3] Ftdichip.com. (2019). FT232R. [online] Available at: https://www.ftdichip.com/Products/ICs/FT232R.htm [Accessed 29 Mar. 2019].

[4] Engineering.purdue.edu. (2019). [online] Available at: https://engineering.purdue.edu/ece477/Course/Assignments/Reference/Mil\_Hdbk\_217F.pdf [Accessed 29 Mar. 2019].

Appendix A: Schematic Functional Blocks

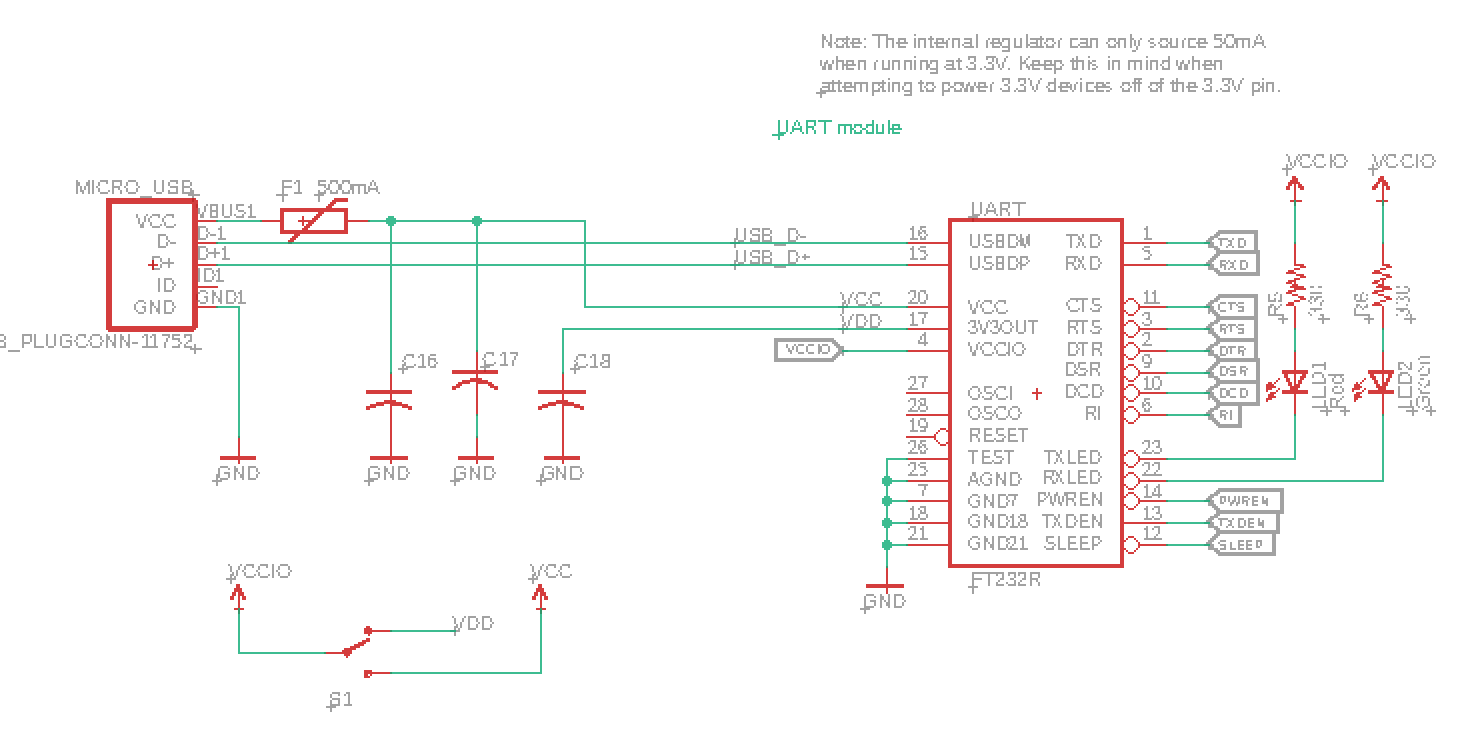


Figure 1. UART circuit

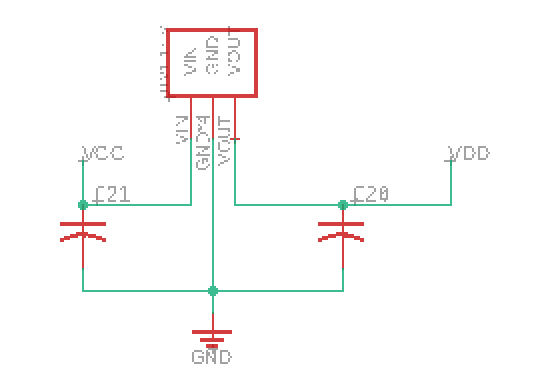


Figure 2. Voltage regulator circuit

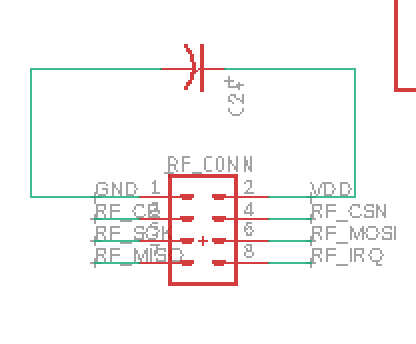


Figure 3. RF module circuit

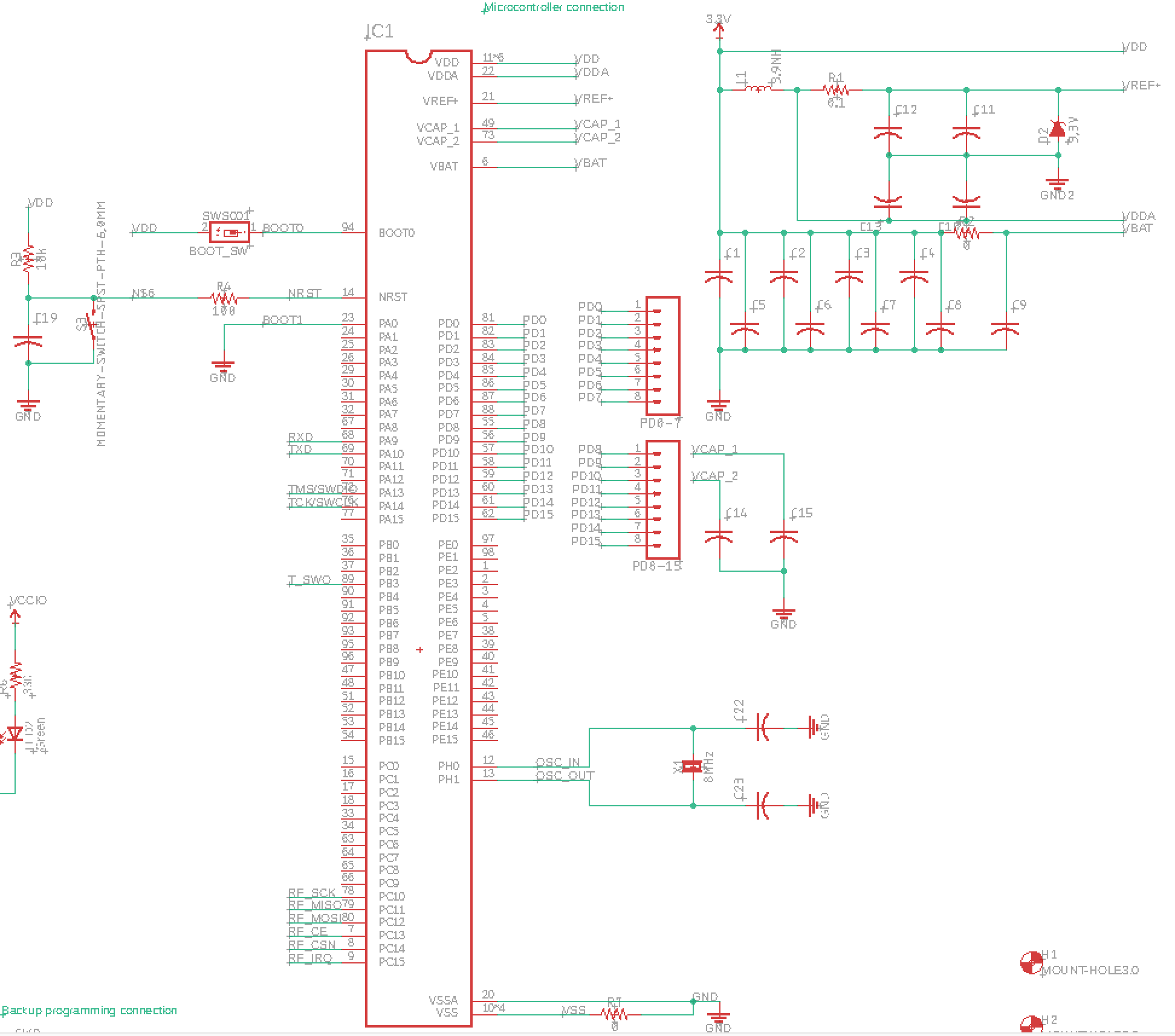
**

Figure 4. Microcontroller circuitAppendix B: FMECA Worksheet

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 1 | Outputting nonsense | clock does not align | Possibly lose control of the entire system | Through ground station software | Level 3 | The system will go to failsafe mode if such thing happens |
| 2 | Cannot program micro through UART | UART circuitry failure / Bootloader failure | Lose a user-friendly interface for firmware update | Through micro memory flash software | Level 1 | The firmware update can be pushed through backup SWDIO interface |

Table 4. UART circuit FMECA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 3 | High 3.3 voltage on the board | DC voltage converter failure | Micro freezes and becomes unresponsive | Observation | Level 4 |  |
| 4 | Low 3.3 voltage on the board | DC voltage converter failure | Micro is not powered | Observation | Level 1 |  |

Table 5. Voltage regulator circuit FMECA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 5 | RF module not responding | Distance between tx/rx too long | lose control of the entire system | Observation | Level 3 | The system will go into failsafe mode if such failure happens |

Table 6. RF module circuit FMECA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 6 | The micro is not be powered | Shorted bypass | there is no output signal from any pin of micro | Observation | Level 1 |  |
| 7 | The micro cannot be programmed | decoupling capacitor is open, passive resistors broke | Unpredictable | Observation | Level 1 | Based on the fact that the micro is powered normally |

Table 7. Microcontroller circuit FMECA