Reliability and Safety Analysis

Year: 2021 Semester: Fall Team: 6 Project:RevEx

Creation Date: 10/28/2021 Last Modified: Oct 31, 2021

Author: Matthew Rumple Email: rumple0@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 several components that are being analyzed for reliability in our design. Most of these components include more complicated chips and high-use parts that are critical to the design. These components will be analyzed and the mean time to failure will be calculated. After the analysis, the component in question will be reviewed, and at the end of this section a summary will provide an overview of the reliability analysis conclusions.

* 1. Microcontroller: **STM32L081KZTx**
     1. Reasoning

Easily the most complex chip on the board, with the most I/O pins as well as transistors.

* + 1. Failure Model [2]

Failures / Hours

Table 1: Microcontroller Analysis

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter name | Description | Value | Comments |
|  | Die complexity Failure Rate | .56 | Due to the 32-bit nature of the uC [3] |
|  | Temperature Coeff. | 1.5 | Assumed based on average operating temp |
|  | Package Failure Rate | .018 | Based on 32-pin SMD QFP |
|  | Environmental Factor | .5 | Based on rating for |
|  | Quality Factor | 10.0 | Commercial Screening |
|  | Learning Factor | 1.0 | Chip production started in 2016 |
|  | Failure per Hours | 8.49 |  |
|  | Mean Time to Failure | .118 |  |

* + 1. Analysis Result

According to the failure model calculation shown in Table 1, the mean time to failure for this microcontroller is approximately 118,000 hours. This equates to almost a year and a half of continuous runtime. A failure of this microcontroller would only cause the product to not operate correctly without causing any harm to the user.

* 1. IMU: **ICM-20948**
     1. Reasoning

An EMI sensitive component due to the magnetometer, with 24 pins.

* + 1. Failure Model [2]

Failures / Hours

Table 2: IMU Analysis

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter name | Description | Value | Comments |
|  | Die complexity Failure Rate | .28 | Due to the 16-bit nature of the chip [1] |
|  | Temperature Coeff. | 1.5 | Assumed based on average operating temp |
|  | Package Failure Rate | .011 | Based on 24-pin LGA |
|  | Environmental Factor | .5 | Based on rating for |
|  | Quality Factor | 10.0 | Commercial Screening |
|  | Learning Factor | 1.0 | Chip production started in 2017 |
|  | Failure per Hours | 4.26 |  |
|  | Mean Time to Failure | .235 |  |

* + 1. Analysis Result

According to the failure model calculation shown in Table 2, the IMU has an average predicted failure of 4.26 in 1 million hours. This comes out to a MTTF of 235,000 hours. The MTTF is within an acceptable range for our product. Additionally, if this component were to fail, it would only cause the device information to be transmitted incorrectly, causing no harm to the user.

* 1. Optoelectronic Relay: **CPC1020N**
     1. Reasoning

One of the most worked chips in the system, probably not built for the current use case of very rapid turn on/off.

* + 1. Failure Model [2]

Failures / Hours

Table 3: Optoelectronic Relay Analysis

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter name | Description | Value | Comments |
|  | Base Failure Rate | .013 | Chip uses a phototransistor |
|  | Temperature Coeff. | 1.5 | Assumed based on average operating temp |
|  | Environmental Factor | .5 | Based on rating for |
|  | Quality Factor | 10.0 | Commercial Screening |
|  | Failure per Hours | .0975 |  |
|  | Mean Time to Failure | 10.256 |  |

* + 1. Analysis Result

According to the calculations in Table 3 above, the Mean Time to Failure for the CPC1020N is approximately 10 million hours. This is just an approximation, but it helps that we are well within safety margins after considering the use case where we may be pushing the relay’s abilities by switching it so quickly. This is well within safety margins of our product, and if the part fails there would only be loss of passive haptic feedback on the device, causing no harm to the user.

* 1. N-Channel MOSFET: **RQ6E050AJ**
     1. Reasoning

Very sensitive to static electricity and internal failure. Also oscillating at a PWM frequency.

* + 1. Failure Model [2]

Failures / Hours

Table 4: N-Channel MOSFET Analysis

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter name | Description | Value | Comments |
|  | Base Failure Rate | .012 | Chip is a MOSFET |
|  | Temperature Coeff. | 1.5 | Assumed based on average operating temp |
|  | Application Factor | .70 | Used for only small signal switching |
|  | Quality Factor | 8.0 | Commercial Screening, plastic part |
|  | Environmental Factor | 1.0 | Based on rating for |
|  | Failure per Hours | .1008 |  |
|  | Mean Time to Failure | 9.921 |  |

* + 1. Analysis Result

Based on the calculations found in Table 4, our choice of a N-Channel MOSFET should be more than reliable enough for our product. With a mean time to fail of approximately 10 million hours, it should stay operational for the lifetime of the product. As long as the user follows the user guide and doesn’t introduce static electricity to the MOSFET on the board, it should remain operational. Should the MOSFET fail, the only loss would be haptic feedback, no harm would come to the user.

**Summary**

Overall, the calculations have shown that some of the more failure prone parts of our design are reliable enough for our use case. The design and component selection seem high quality and should work great for our design long term. If there were a design change to improve the reliability of our design, it would be picking a 16-bit microcontroller to make it less likely to fail.

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

Due to the low power nature of our product, there are several mitigated risks that would otherwise be a cause for concern. Electrically speaking, the battery is really the only dangerous part of our system, as LiPo batteries are subject to certain issues. If the user takes care of the product and does not damage it internally, the battery should be safe. The next most dangerous part of our project that could potentially cause harm to the user is the stepper motor mounted on the elbow joint. If dropped, the stepper motor could damage the user, although it would be minor. There are three main criticality levels defined for use below. High criciality would mean harm could be caused to the user. Medium criticality would mean that the product would stop functioning completely. Lastly, low criticality would mean there would be no immediately observable impact on the product, and it would be noticed over time. We make assumptions that our product will not be exposed to any extreme conditions, as the reliability basis was based off of the Ground Benign environment, where it would not be exposed to outside elements and would not be thrown about. For a high-level failure, the acceptable failure rate would be , while the acceptable failure rate for medium and low criticality would be . Although the medium and low failure rate may seem high, there would be no immediate danger to the user and the product would only need to be repaired. The different subsections can be seen in Appendix A while the full failure analysis can be found in Appendix B. Due to the extremely low power and small component nature of our product, the ability of our product to hurt the user by means of electrical component failure theoretically does not exist. The most damage that could be caused to a user is a possible pinch point on the dropping of the device on a user’s foot. Both can easily be avoided by using the device with care and reading the user manual.

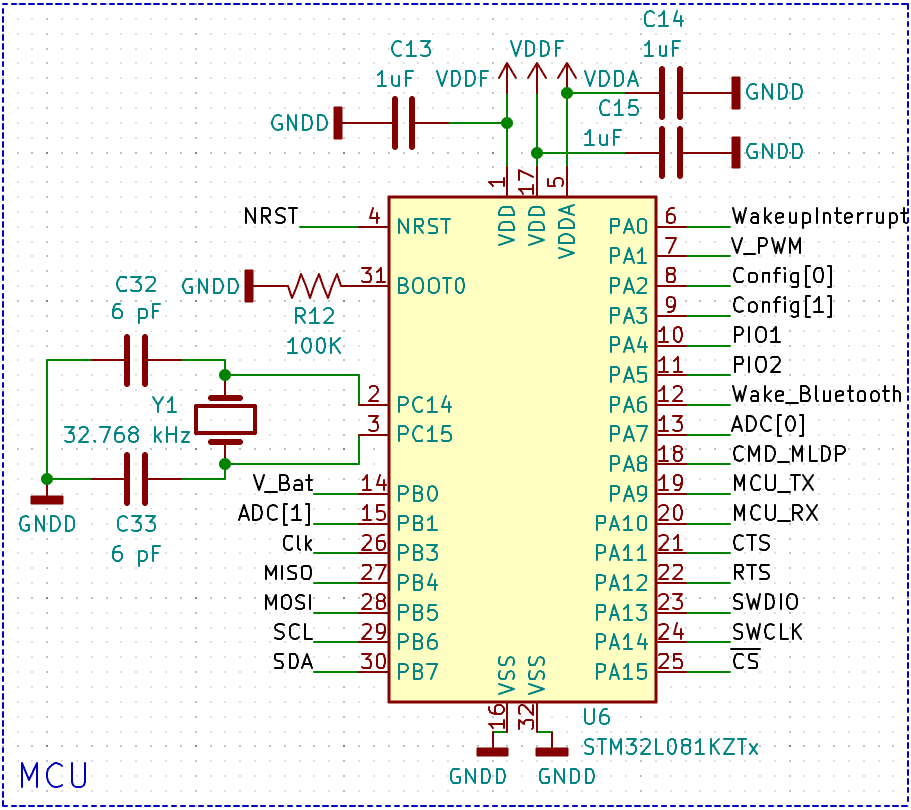
3.0 Sources Cited:

[1] InvenSense, “World’s Lowest Power 9-Axis MEMS MotionTracking Device,” ICM-20948 datasheet, Jun 2017. [[Datasheet Link](https://datasheet.octopart.com/ICM-20948-InvenSense-datasheet-115290367.pdf)]

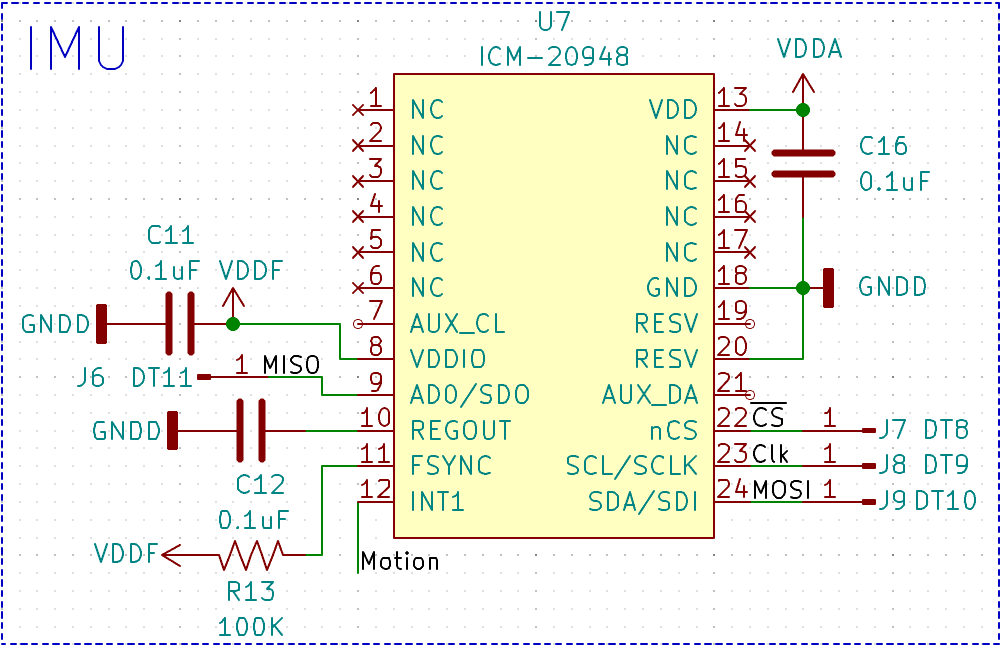
[2] “Military Handbook Reliability Prediction of Electronic Equipment” Department of Defense. Washington DC. MIL-HDBK-217F, Dec. 2, 1991.

[3] STMicroelectronics, “STM32L081CB STM32L081CZ STM32L081KZ, STM32L081KZT Datasheet,” November 2019, [[Datasheet Link](https://www.mouser.com/datasheet/2/389/dm00162467-1798373.pdf)]

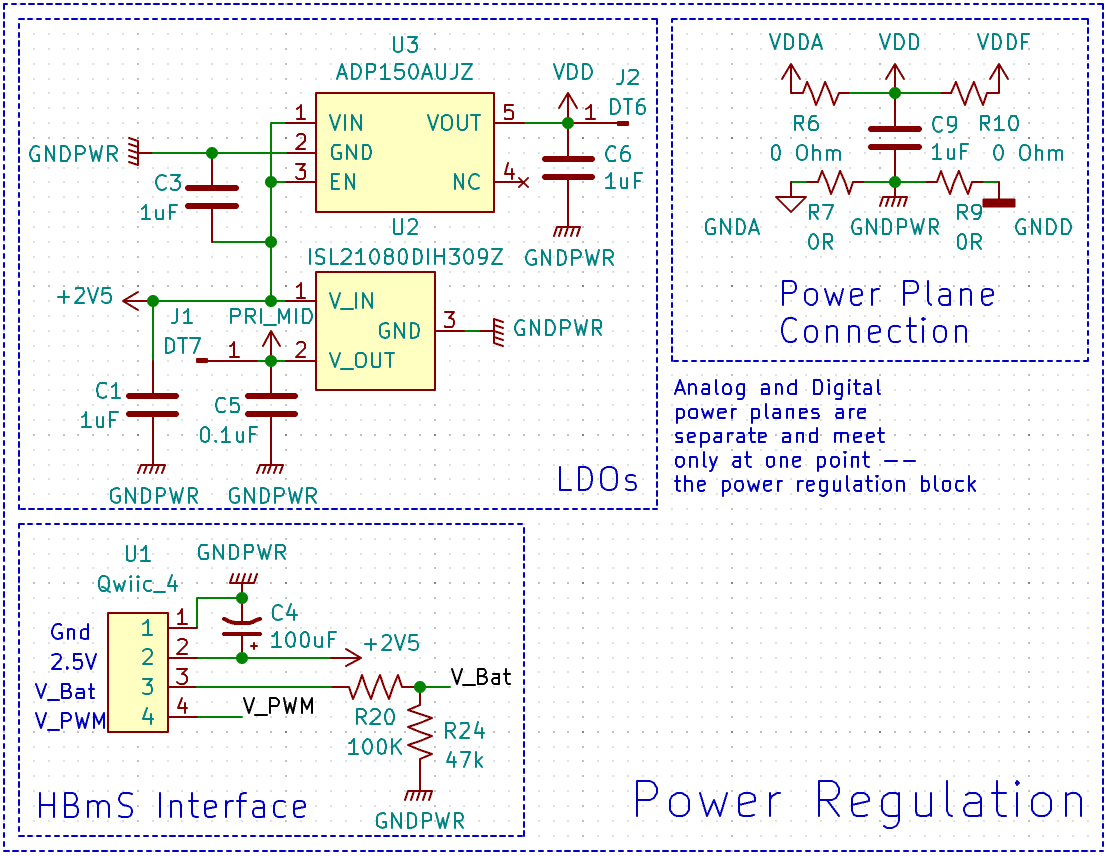
Appendix A.1.1: Schematic Functional Blocks -- MCU (DAqS)



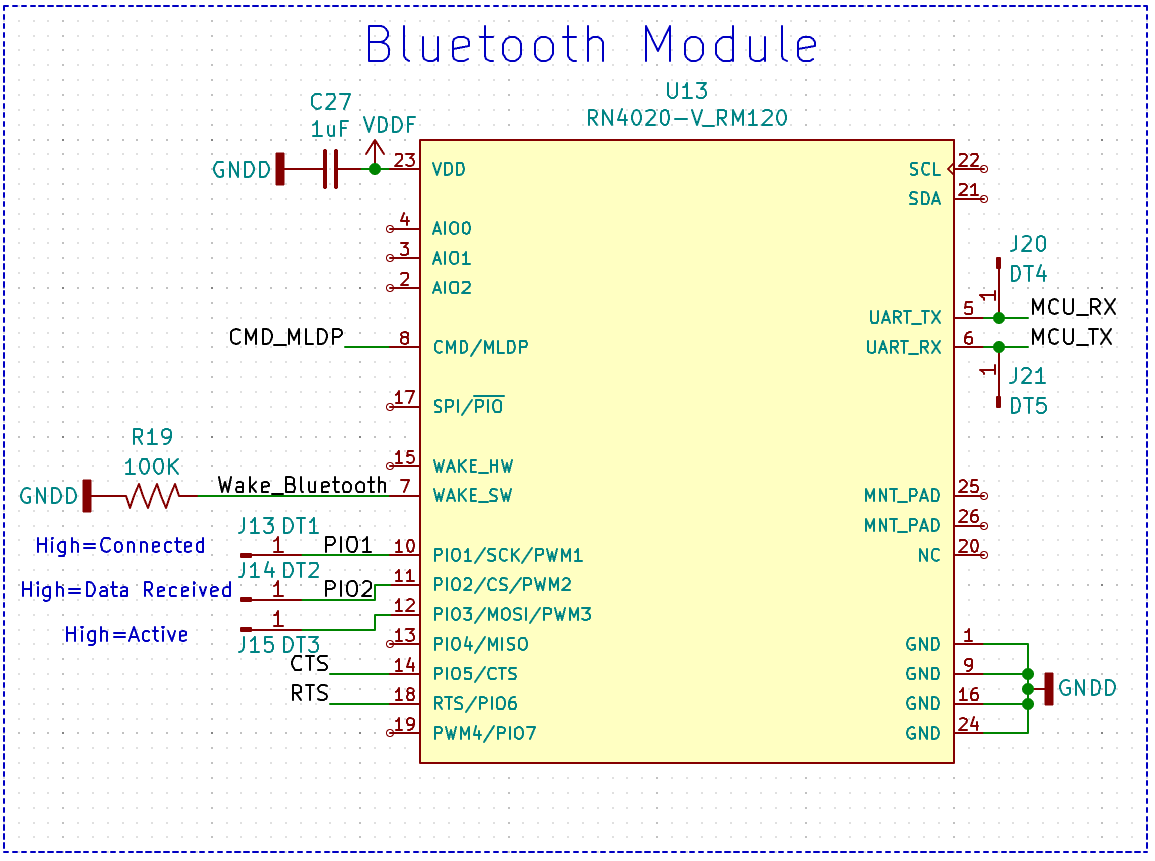
Appendix A.1.2: Schematic Functional Blocks -- IMU (DAqS)



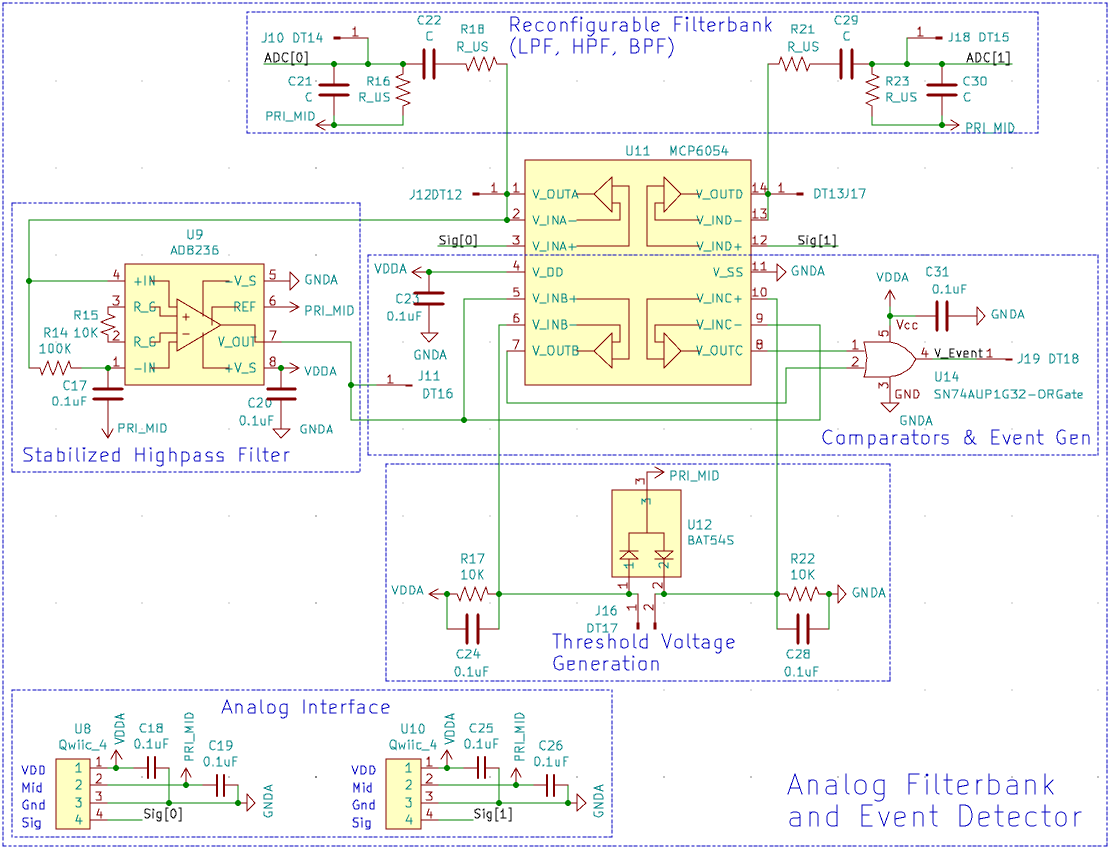
Appendix A.1.3: Schematic Functional Blocks -- Power Regulation (DAqS)



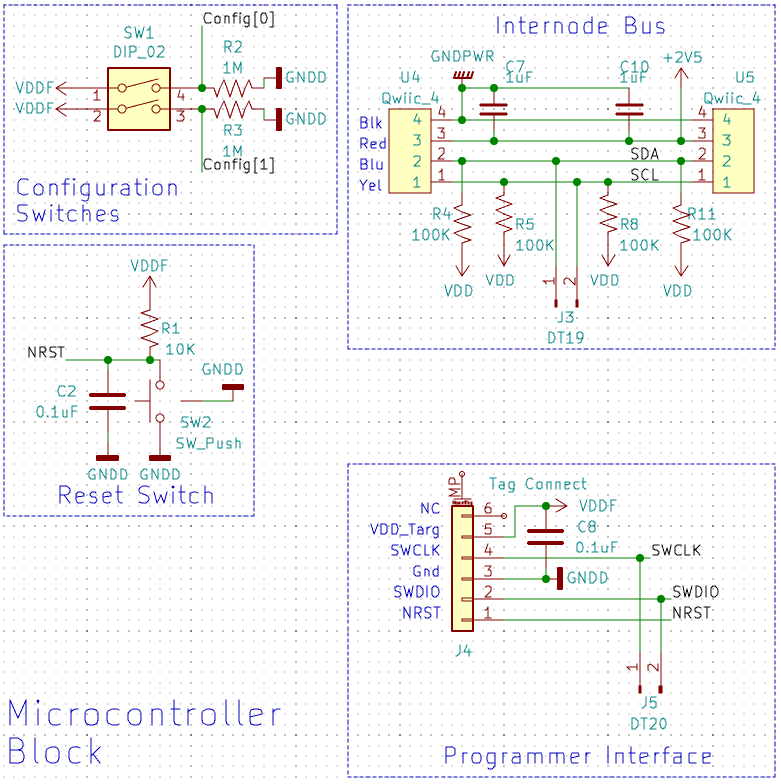
Appendix A.1.4: Schematic Functional Blocks -- Bluetooth Module (DAqS)



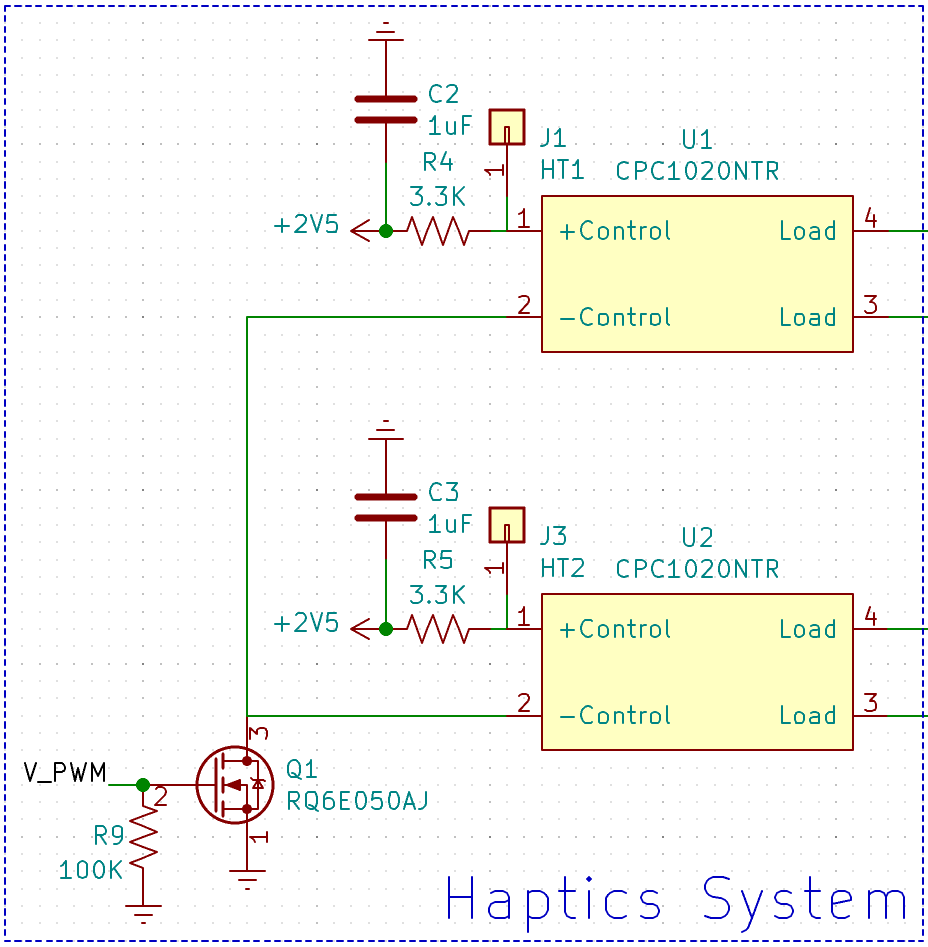
Appendix A.1.5: Schematic Functional Blocks -- Analog Components (DAqS)

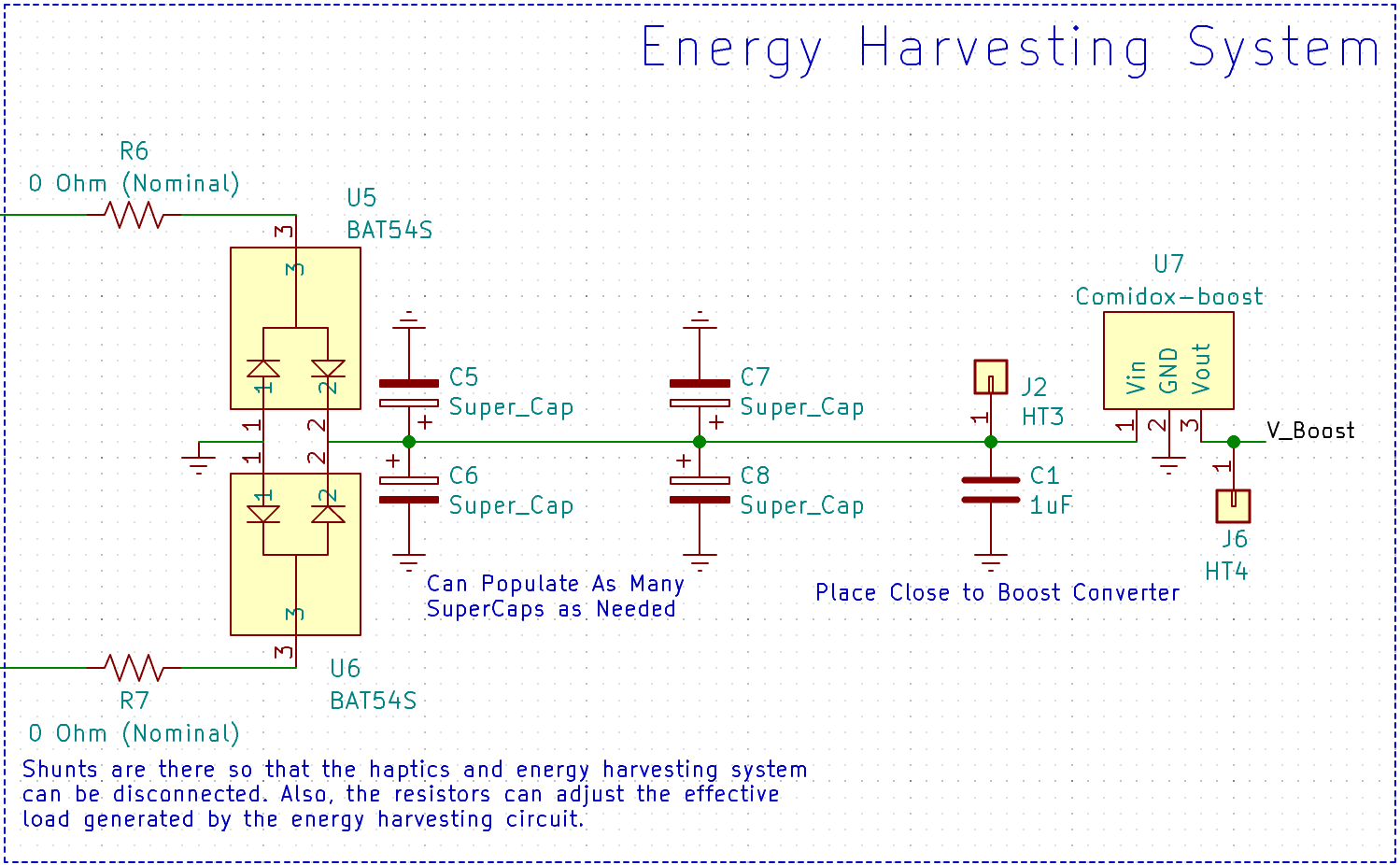


Appendix A.1.6: Schematic Functional Blocks -- Additional Microcontroller Circuits (DAqS)

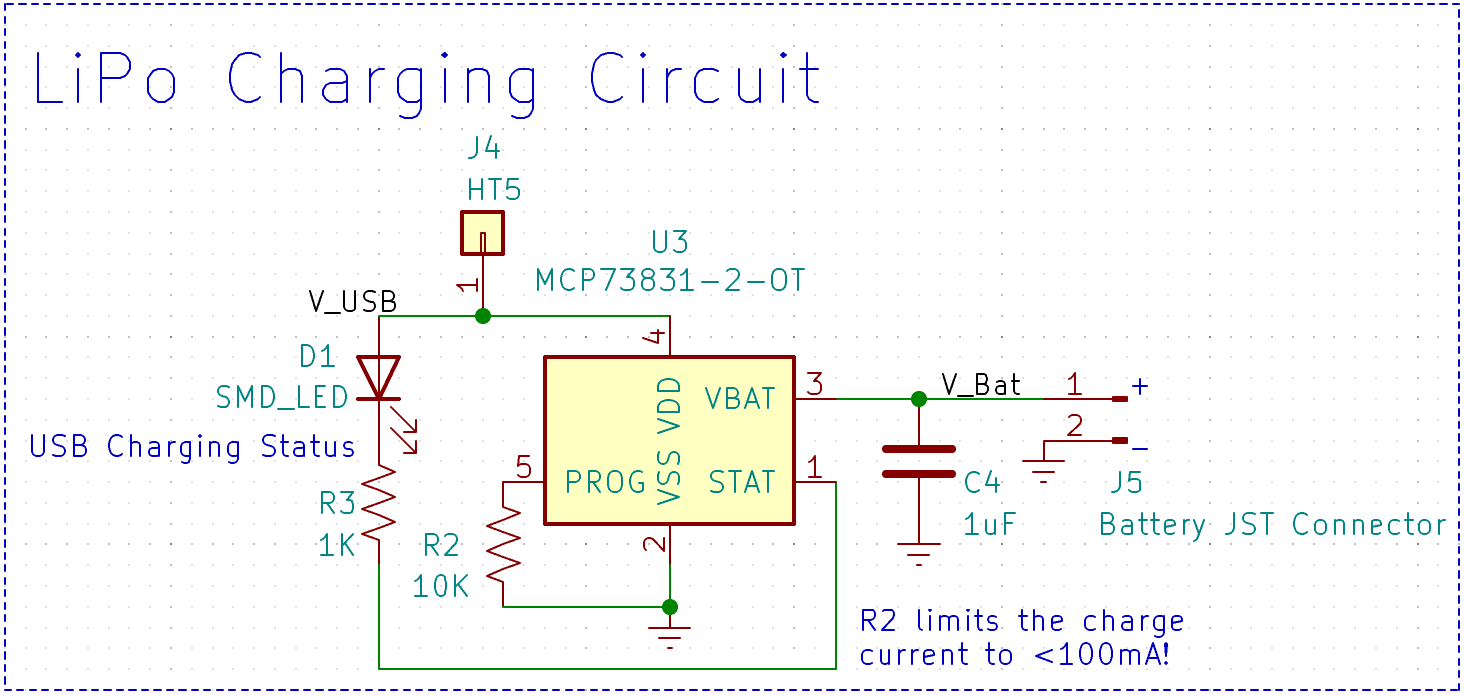


Appendix A.2.1: Schematic Functional Blocks -- Haptics System (HBmS)

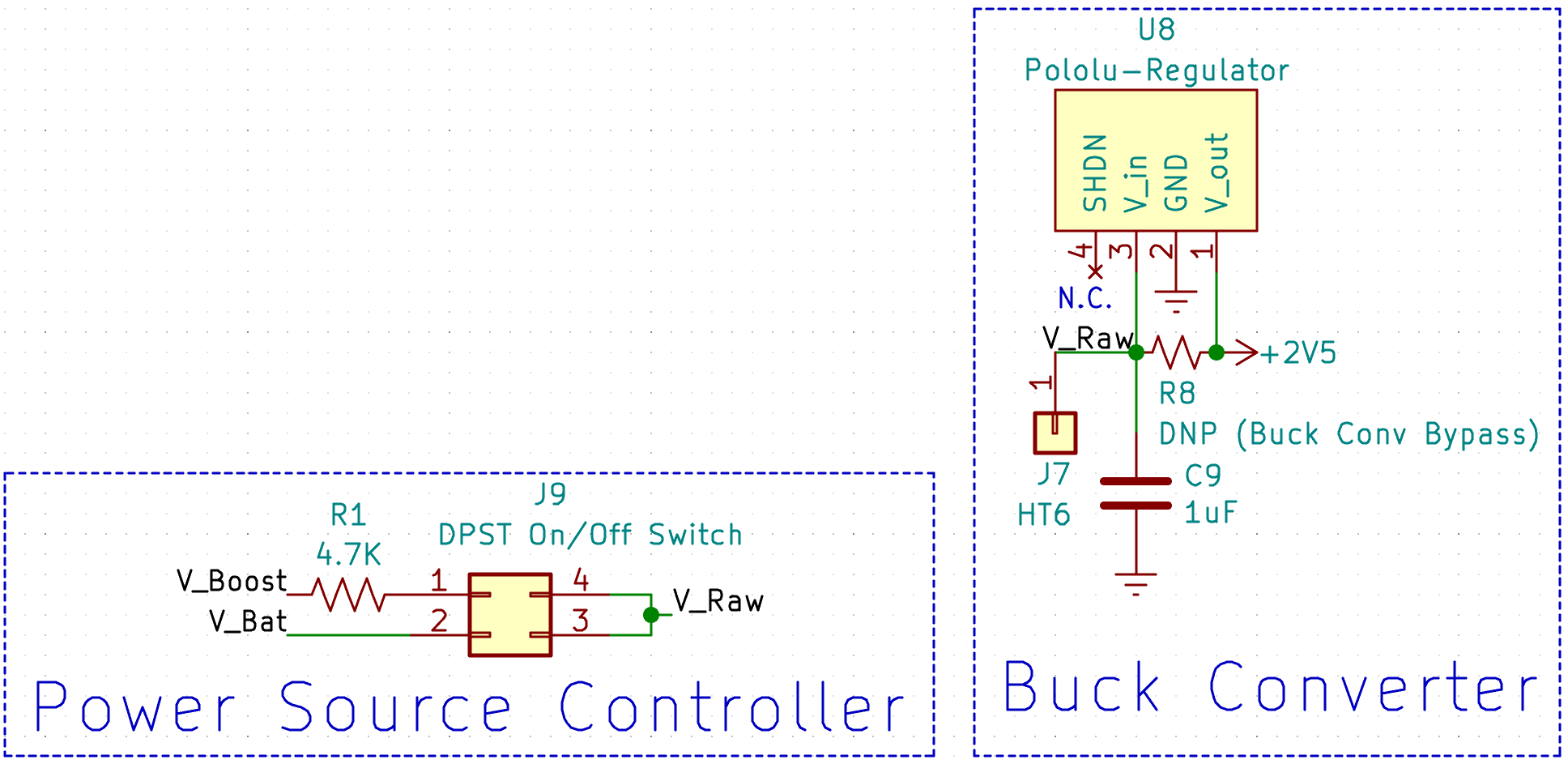
**Appendix A.2.2: Schematic Functional Blocks -- Energy Harvesting System (HBmS)



Appendix A.2.3: Schematic Functional Blocks -- LiPo Charging Circuit (HBmS)



Appendix A.2.4: Schematic Functional Blocks -- Power Delivery System (HBmS)



Appendix B: FMECA Worksheet

**Table B.1.1: MCU (DAqS) FEMCA**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 1 | Unstable input voltage to microcontroller | C13, C14, C15 Fail | Error in logic computations, possible resetting due to undervoltage | Product malfunctions / does not operate correctly | Low |  |
| 2 | RTC does not work correctly | C32, C33, Y1 Fail (If they are populated) | Some timing may be off, but nothing serious (We don’t rely on RTC) | Possible latency product (most likely not noticeable) | Low |  |
| 3 | Microcontroller fails to operate correctly | Internal failure of the microcontroller | Microcontroller will fail to run properly | Device appears to not respond and/or work correctly | Medium |  |

**Table B.1.2: IMU (DAqS) FEMCA**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 4 | Unstable input voltage to IMU | C11, C16 Fail | IMU may have errors in computation or may reset itself unexpectedly | Orientation in simulation appears to have errors sometimes | Low |  |
| 5 | IMU fails to operate correctly | Internal failure of the IMU | IMU will not respond to any register read requests | The orientation aspect of the simulation won’t work at all | Medium |  |

**Table B.1.3: Power Regulation (DAqS) FEMCA**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 6 | Unstable input voltage to the regulators or the board entirely | C6, C1, C5 Fail | Sensitive analog circuitry may malfunction, and supplies might be interrupted | Device fails to wake up upon movement, possible failure to connect to device | Low |  |
| 7 | Power rails fail | LDO stops working or HBmS interface connector fails | DAqS board would lose power supply rails, stopping all functionality | Device appears not to power on (doesn’t pair) | Medium |  |

**Table B1.4: Bluetooth Module (DAqS) FEMCA**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 8 | Unstable input voltage to the Bluetooth module | C27 Fail | Possible incorrect operation or errant resetting of the Bluetooth module | Device randomly drops connection and\or won’t reconnect | Low |  |
| 9 | Bluetooth module fails to operate correctly | Internal Bluetooth module failure | Bluetooth chip won’t start and will not communicate over UART | Bluetooth functionality of product is completely non-operational | Medium |  |

**Table B.1.5: Analog Components (DAqS) FEMCA**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 10 | Analog event detector does not work correctly | U9, U11, U14, U12 Fail | Would cause a failure in some subsystem of the analog event detector | Device will not wake properly from sleep state | Medium |  |
| 11 | Potentiometer fails to read correctly, or at all | U8 Connector Failure | Would cause the angle of the elbow to be read incorrectly | Offset or inoperation of elbow angle in the simulation | Medium |  |
| 12 | Unstable input voltage into analog IC’s | C31, C20, C23 Fail | Could cause errant unwanted signals, possibly during haptic feedback loop | Device may sleep at the wrong time | Medium |  |

**Table B.1.6: Additional Microcontroller Circuits (DAqS) FEMCA**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 13 | Programmer interface could not work correctly | Connector incompatibility or noise/bad connections to uC | Inability to program the Microcontroller | Microcontroller will not respond or reprogram | Medium |  |
| 14 | Inability to communicate to other nodes in the system | U4 or U5 fail | The connection between nodes in the system would not be stable | Inability to add nodes onto the system | Low |  |
| 15 | Inability to configure device mode on start-up | SW1 Fail | Inability to set the two configuration bits to high or low | Attempting to set the operating mode of the device will fail | Low |  |
| 16 | Inability to reset the DAqS system | SW2 Fail Open | The system and uC will not be able to be reset | Pressing the reset button on the product will do nothing | Low |  |
| 17 | DAqS system is stuck in a reset loop | SW Fail Closed or Shorted | The system will not be able to boot, as the reset pin will be stuck low | The device will appear not to boot up at all | Medium |  |

**Table B.2.1: Haptics System (HBmS) FEMCA**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 18 | Loss of haptic feedback | Q1, U1, U2 Fail | Haptic feedback will either not work, or the effect will be diminished | Lack of haptic feedback from device | Low |  |

**Table B.2.2: Energy Harvesting System (HBmS) FEMCA**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 19 | Failure to harvest energy | R6 and/or R7 Fail Open  U5, U6, U7 Fail  C5, C6, C7,C8 All Fail (if populated) | Inability to harvest energy during user movement | Device battery life will not last as long | Low |  |

**Table B.2.3: LiPo Charging Circuit (HBmS) FEMCA**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 20 | LiPo Charging Chip Fails | U3 Internal Failure | LiPo battery will no longer be rechargeable, the device will eventually become unusable | D1 does not illuminate while charging, device dies and won’t power back on | Medium |  |
| 21 | D1 Fails open | D1 Internal Failure or Burnout | D1 will not illuminate, may cause user to think device is not charging | D1 does not illuminate while charging device | Low |  |

**Table B.2.4: Power Delivery System (HBmS) FEMCA**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 22 | Switch J9 Fails Open | Internal or Mechanical Switch Failure | Device will not power on | Device will not pair or connect and user will be unable to use it | Medium |  |
| 23 | Switch J9 Fails Closed | Shorting of Switch or Switch is Stuck Mechanically | Device will not power off | Device will continue to drain battery until the LiPo has been discharged | Medium |  |
| 24 | Power Delivery to Board Fails | U8 Failure | Device will not be supplied the correct voltage needed to run | Device will appear to not power on, but will charge correctly | Medium |  |