Reliability and Safety Analysis

Year: 2020 Semester:Fall Team: 6 Project: Snow-WeAR Goggles
Creation Date: 11-02-202 Last Modified: 11-05-2020
Author: Mitchell Ciupak Email: ciupak@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.

*1.0 **Reliability Analysis***

The components in this design that are most likely to fail are the LT1129 Voltage Regulator [1], STM32L4 Microcontroller [2], RFM95W-868S2 LoRa Transceiver [3], and MTK3339 GPS [4]. The LT1129 Voltage Regulator was selected because it runs hot and must be able to supply a 3.3V output to the board. The STM32L4 Microcontroller was selected because it is the most complex IC on our board with the most I/O pins. The RFM95W-868S2 LoRa Transceiver was selected because it has untested communications in mountainous regions. The MTK3339 GPS was selected because it has a low ripple tolerance and while it has been allocated its own voltage regulator, we are unsure if we will use it until further testing is done.

Model and Assumptions

The model used to determine the failure rate was is from the Military Handbook (MIL-HDBK-217f) [5]:

$$\lambda_P = (C_1 \pi_T + C_2 \pi_E) \pi_Q \pi_L$$

The mean time to failure (MTTF) in years is from the same source:

$$MTTF = 10^6 / (24 * 365 * \lambda_P) \text{ years}$$

For this analysis, according to the handbook, all of our Environmental Factors (π_E) are rated at Ground, Mobile which rates a 4.0 value. Fortunately, all our components are also greater than 2 years old, giving a Learning Factor (π_L) of 1.0 across the board. The last consistent value seen across all devices analyzed here is the Quality Factor (π_Q) which is valued at 2.0 because these are all commercial products.

For the LT1129 Voltage Regulator [1], the microcircuit section in the handbook is the best fit section. From that I found the Temperature Factor (π_T) based on the MIL-Hdbk 217f [5] for devices with Aluminum Metallization, T_J of 150^c and V_S of 0.45s to hold a value of 0.02. After that I found the Complexity Failure Rate(C_1) based on the MIL-Hdbk 217f [5] for devices with 100 to 300 bipolar transistors to hold a value of 0.02. Lastly, I found the Package Failure Rate(C_2) based on page 43 of the MIL-Hdbk 217f [5] for Hermetic packages with 8 pins to hold a value of 0.0026. From that the mean time to failure was calculated to be 546.7205514 years.

For the STM32L4 Microcontroller [2], the microcircuit section in the handbook is the best fit section. From that I found the Temperature Factor (π_T) based on the MIL-Hdbk 217f [5] for microciruits with a temperature range of 85^C(STM32L's worst case) to hold a value of 0.98. After that I found the Complexity Failure Rate(C_1) based on the MIL-Hdbk 217f [5] for Bipolar 32-bit Microprocessors to hold a value of 0.24. While the STM32L4 has 100 pins, I found the Package Failure Rate(C_2) based on page 43 of the MIL-Hdbk 217f [5] for Hermetic packages with 128 pins to hold a value of .053. From that the mean time to failure was calculated to be 127.6333308 years.

For the RFM95W-868S2 LoRa Transceiver [3], the microcircuit section in the handbook is the best fit section. From that I found the Temperature Factor (π_T) based on the MIL-Hdbk 217f [5] for microcircuits with a temperature range of 155^C(RFM95W's worst case) to hold a value of 0.9999999983385419. After that I found the Complexity Failure Rate(C_1) based on the MIL-Hdbk 217f [5] for devices with 1,001 to 10,000 linear bipolar transistors to hold a value of 0.060. I then found the Package Failure Rate(C_2) based on page 43 of the MIL-Hdbk 217f [5]

for Hermetic packages with 16 pins to hold a value of .0056. From that the mean time to failure was calculated to be 692.6900510 years.

For the MTK3339 GPS, the microcircuit section in the handbook is the best fit section. From that I found the Temperature Factor (π_T) based on the MIL-Hdbk 217f [5] for microcircuits with a temperature range of 85^C(RFM95W's worst case) to hold a value of 0.98. After that I found the Complexity Failure Rate(C_1) based on the MIL-Hdbk 217f [5] for devices with 1,001 to 10,000 linear bipolar transistors to hold a value of 0.060. I then found the Package Failure Rate(C_2) based on page 43 of the MIL-Hdbk 217f [5] for Hermetic packages with 20 pins to hold a value of .0079. From that the mean time to failure was calculated to be 631.3896634 years.

LT1129 Voltage Regulator [1], Table 1

Parameter	Description	Value	Comments
C_1	Die Complexity Failure Rate	0.02	Based on the MIL-Hdbk 217f [5] for devices with 100 to 300 bipolar transistors. (page 32).
π_T	Temperature Factor	4.7	Based on the MIL-Hdbk 217f [5] for devices with Aluminum Metallization, T_J of 150^c and V_S of 0.45 (page 65).
C_2	Package Failure Rate	0.0026	Based on the MIL-Hdbk 217f [5] for Hermetic packages with 8 pins (page 43).
π_E	Environmental Factor	4.0	Based on the MIL-Hdbk 217f [5] for devices in Ground, Mobile (page 25, 39).
π_Q	Quality Factor	2.0	Based on the MIL-Hdbk 217f [5] for Class B-1 Devices (page 44).
π_L	Learning Factor	1.0	Based on the MIL-Hdbk 217f [5] for devices in production for more than 2 years (page 44).
λ_P	Failure Rate Per 10^6 Hours	0.2088	(0.02*4.7+0.0026*4.0)2.0*1.0
MTTF	Mean Time to Failure	546.7205514 years	10^6/(24*365* 0.2088)

STM32L4 Microcontroller [2], Table 2

Parameter	Description	Value	Comments
C_1	Die Complexity Failure Rate	0.24	Based on the MIL-Hdbk 217f [5] for Bipolar 32-bit Microprocessors (page 31).
π_T	Temperature Factor	.98	Based on the MIL-Hdbk 217f [5] for microciruits with temperature range of 85^C(worst case).
C_2	Package Failure Rate	.053	Based on the MIL-Hdbk 217f [5] for Hermetic packages with 128 pins while the STM has 100 (page 43).
π_E	Environmental Factor	4.0	Based on the MIL-Hdbk 217f [5] for devices in Ground, Mobile (page 25, 39).
π_Q	Quality Factor	2.0	Based on the MIL-Hdbk 217f [5] for Class B-1 Devices (page 44).
π_L	Learning Factor	1.0	Based on the MIL-Hdbk 217f [5] for devices in production for more than 2 years (page 44).
λ_P	Failure Rate Per 10^6 Hours	0.8944	(0.24*0.98+0.053*4.0)*2.0*1.0
MTTF	Mean Time to Failure	127.6333308 years	10^6 / (24 * 365 * 0.8944)

RFM95W-868S2 LoRa Transceiver [3], Table 3

Parameter	Description	Value	Comments
C_1	Die Complexity Failure Rate	0.060	Based on the MIL-Hdbk 217f [5] for devices with 1,001 to 10,000 linear bipolar transistors. (page 32).
π_T	Temperature Factor	0.9999999983385419	Based on the MIL-Hdbk 217f [5] for microcircuits with temperature range of 115^C(worst case). (page 40). (.1)^((-.8/8.63*10^(-5))*((1/(115+273))-(1/298)))

C_2	Package Failure Rate	0.0056	Based on the MIL-Hdbk 217f [5] for Hermetic packages with 16 pins (page 43).
π_E	Environmental Factor	4.0	Based on the MIL-Hdbk 217f [5] for devices in Ground, Mobile (page 25, 39).
π_Q	Quality Factor	2.0	Based on the MIL-Hdbk 217f [5] for Class B-1 Devices (page 44).
π_L	Learning Factor	1.0	Based on the MIL-Hdbk 217f [5] for devices in production for more than 2 years (page 44).
λ_P	Failure Rate Per 10^6 Hours	0.1647999	(0.060*0.99+0.0056*4.0)*2.0*1.0
MTTF	Mean Time to Failure	692.6900510 years	10^6 / (24 * 365 * 0.1647999)

MTK3339 GPS [4], Table 4

Parameter	Description	Value	Comments
C_1	Die Complexity Failure Rate	0.060	Based on the MIL-Hdbk 217f [5] for devices with 1,001 to 10,000 linear bipolar transistors. (page 32).
π_T	Temperature Factor	.98	Based on the MIL-Hdbk 217f [5] for microciruits with temperature range of 85^C(worst case).
C_2	Package Failure Rate	0.0079	Based on the MIL-Hdbk 217f [5] for Hermetic packages with 20 pins (page 43).
π_E	Environmental Factor	4.0	Based on the MIL-Hdbk 217f [5] for devices in Ground, Mobile (page 25, 39).
π_Q	Quality Factor	2.0	Based on the MIL-Hdbk 217f [5] for Class B-1 Devices (page 44).
π_L	Learning Factor	1.0	Based on the MIL-Hdbk 217f [5] for devices in production for more than 2 years (page 44).

λ_P	Failure Rate Per 10^6 Hours	0.1808	(0.06*0.98 + 0.0079*4.0) *2.0*1.0
MTTF	Mean Time to Failure	631.3896634 years	10^6 / (24 * 365 * 0.1808)

Reliability Summary

The tested systems overall prove that this project is reliable. The largest Mean Time Till Failure tested is 662.7 years, with the smallest being that of the STM32L4 [2] at 127.6 years. Worst case scenarios were considered for these tests and the parts have a similar scale of Failure Rate Per 10^6 Hours (λ_P). The best way to improve reliability of the overall design would be to buy more expensive parts or military grade parts. There is an additional voltage regulator we intend on putting in front of the GPS to deal with it's ripple limitations. Additionally, we could search for a microcontroller with a higher worst case maximum temperature, but our product is intended to be used in the high altitude elements. Purchasing better discrete components would be a good use of budget, but all other improvements to the product should go into the product's display limitations in order to gain more adopters.

2.0 Failure Mode, Effects, and Criticality Analysis (FMECA)

The schematic for the Snow-weAR Goggles can be divided into 7 subsections,These subsections are Power Supply/Management, LoRa Transceiver, GPS, User I/O, IMU Breakout and OLED Breakout. Two of these subsections, IMU and OLED Breakout, have little difference from an FMECA analysis standpoint than User I/O. The Power Supply and Management is a large point of emphasis in this analysis. <Concluding Sentence>

The Power Supply and Management is one of the most important components to do this sort of analysis on. This is because all the power flows freely from this point into all the other locations. For this system I added 4 failure modes: No supply voltage, a faulty voltage regulator, charging mistakes causing combustion, and charging mistakes that just fail to charge a battery. These criticalities range from low to high, the high being reserved to voltage regulator failure and issues in reverse charging the battery.

The LoRa Transceiver Module is relatively simple when it comes to the FMECA analysis or at least in comparison to other items on this list. The first thing to think about when it comes to failure, is a failure for the component to be powered. This could be due to an unstable voltage source and the component will simply not function. This is a relatively low concern from a ciriciality standpoint. Another problem could arise from connectivity issues or if the Radio is constantly active. This could occur if the radio push button is pressed too often resulting in a higher power use and potentially damage the circuit. You will be able to observe this radio constantly sending requests, but never reports findings to the display. This is categorized under a medium criticality.

The GPS module is relatively similar to the LoRa Module, except with the addition of a voltage regulator for which holds a failure mode in the FMECA tables in Appendix B. That failure mode is if the GPS Voltage Regulator does not regulate the ripple coming in. This can be caused by shorted transistors in the voltage regulator. After that the method of detection would look something like the component not functioning. There are fail safes set up inside the GPS to prevent the GPS from breaking due to ripple, but the device can be rendered useless while the ripple is occuring. The GPS could also not be getting it's supply voltage. The GPS could also be located in an area where the satellite cannot be connected. Occasionally, the GPS takes a lot of time to connect. This can lead to sessions not activated and a waste of power and detected using a watchdog timer. This is a low criticality failure.

The User I/O, IMU Breakout and OLED Breakout are all the simplest components on the board. The User I/O module contains the following components: a radio push button, a session push button, a reset push button, and the JTAG Debugger. The IMU and OLED breakouts are connectors to connect the micro to extra boards like the OLED Driver and the BNO055. A failure mode that can face all the push buttons is the possibility that no supply voltage is reaching the button. This can be caused by an unstable voltage source and renders a push button inoperable. The method of detection can be seen if the action of that push button is exacerbated and the system begins to lag. Similarly if the JTAG Debugger is not wired properly then we will not be able to interface with the STM32L4 [2]. For the IMU and OLED Breakouts I am concerned about the failure mode of having noisy communication lines. This can cause

unpredictability, but can be noticed with faulty information coming in from the IMU or the OLED display having unexpected pixels on.

Lastly, the microcontroller, which is arguably the most at risk component or module and there are many issues that could arise. The first failure mode I assessed was that of: no signal coming out of the microcontroller. This issue could be caused from a damaged capacitor on a VDD pin. If that failure mode occurred then all the components would not function and you would be able to diagnose that issue from there. I addressed this as a 'Low' criticality assuming that there is no permanent damage to the system. The next failure mode I assessed was that of: no power going into the VCC pin of the micro. This could be caused by an unstable voltage source. Similar to the last failure mode, you would be able to see this problem by other components not functioning. Again, this is typically a low criticality. The last failure mode I addressed was a large amount of noise appearing in outputs of various pins. This issue has numerous potential causes: overheated internals, a memory stack overflow, or electrical interference. These failure rates are fairly unpredictable, but some or all components may not function properly. This has a medium amount of criticality because it could damage some devices permanently.

Levels of Complexity

The goal of assessing levels of complexity are done to understand the difference between different failure modes, helping us to know which failure modes are more harmful or less harmful.

'Low' criticality specifies that the failure mode is not harmful to the user or destructive of the rest of the board. For instance, sensor or communication failures would fall into this category. The product may still be unusable until the part is replaced. Low critical errors are intended to have a failure rate of 10-6 or less.

'Medium' criticality is defined as a failure that does not harm the user, but has a potential to damage the system. A failure in the power system could be medium criticality since it has the potential to damage the entire board. Medium criticality failures are aimed to have a failure rate of 10-7 or less.

'High' criticality is reserved for failures that present potential harm to the user. Related failures for this project would be the voltage regulator catching fire. While highly unlikely, it is still a possibility. High critical errors should only occur at a failure rate of 10-9 or less.

3.0 Sources Cited:

[1] Analog.com. 2020. SparkFun Electronics. [online] Available at: <https://www.analog.com/media/en/technical-documentation/data-sheets/112935ff.pdf> [Accessed 3 November 2020].

[2] digchip.com. 2020. SparkFun Electronics. [online] Available at: <https://www.digchip.com/datasheets/parts/datasheet/456/STM32L476-pdf.php> [Accessed 3 November 2020].

[3] Sparkfun.com. 2020. SparkFun Electronics. [online] Available at: <https://cdn.sparkfun.com/assets/learn_tutorials/8/0/4/RFM95_96_97_98W.pdf> [Accessed 3 November 2020].

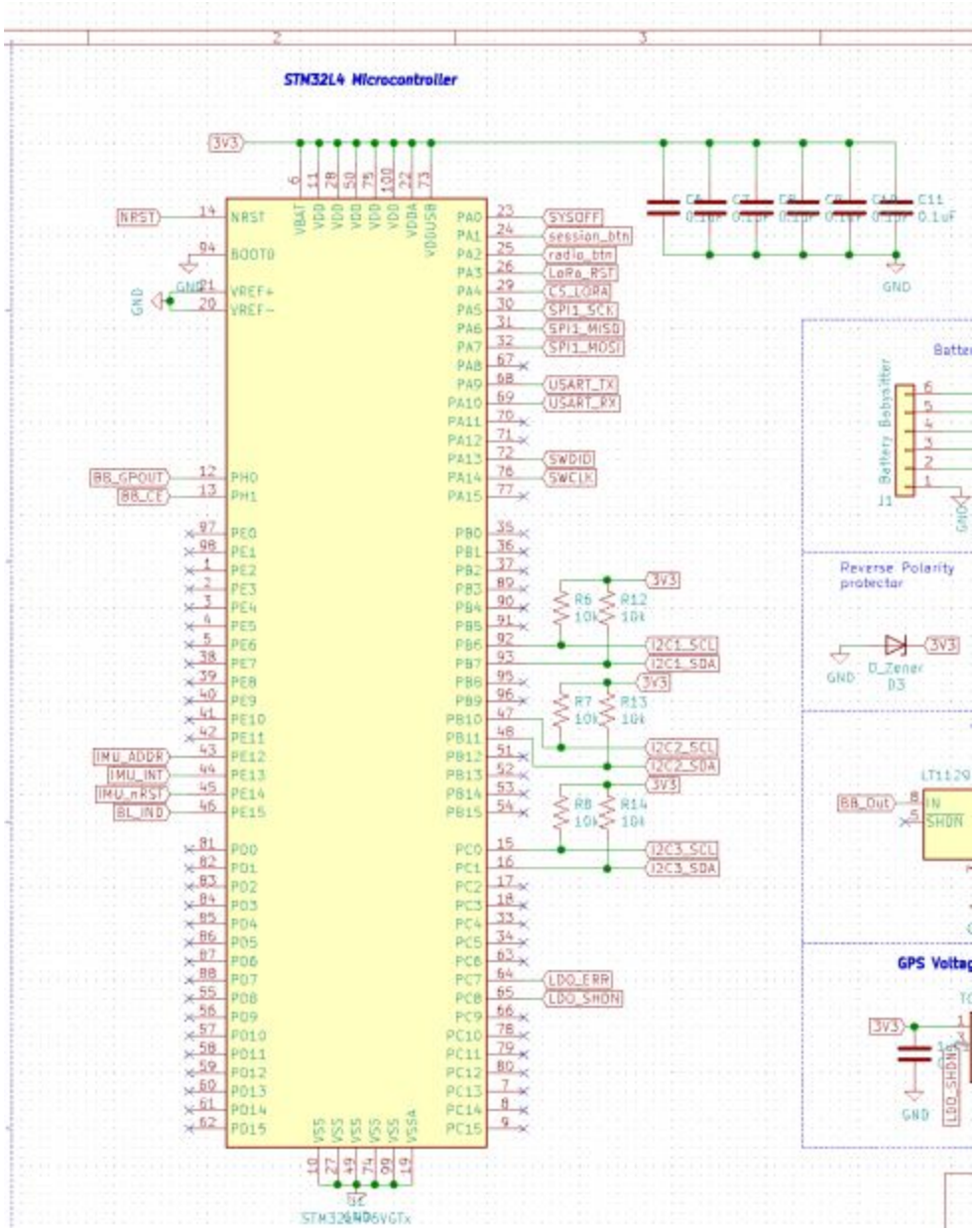
[4] mediatek.com. 2020. SparkFun Electronics. [online] Available at: <http://labs.mediatek.com/en/chipset/MT3339> [Accessed 3 November 2020].

[5] mit.edu. 2020. United States Department of Defense. [online] Available at: <https://snebulos.mit.edu/projects/reference/MIL-STD/MIL-HDBK-217F-Notice2.pdf > [Accessed 3 November 2020].

Appendix A: Schematic Functional Blocks

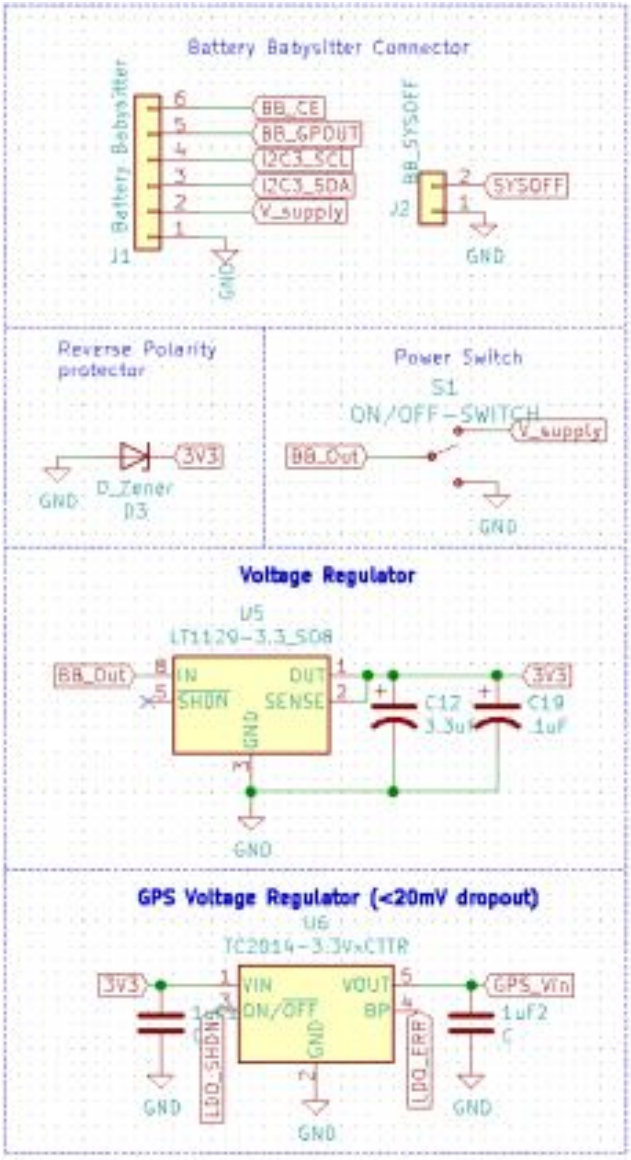
Microcontroller

Figure 1



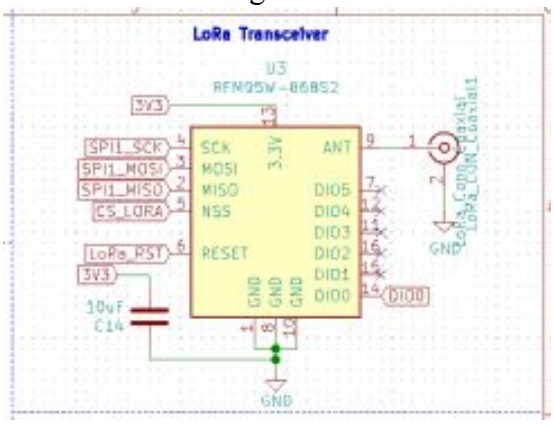
Power Supply/Management

Figure 2



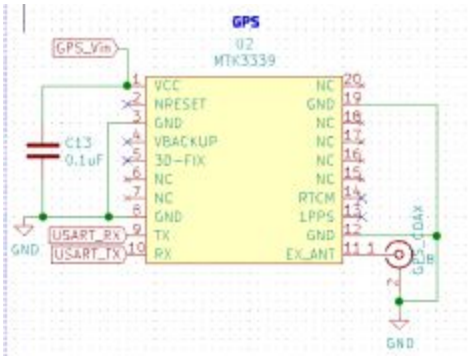
LoRa Transceiver

Figure 3



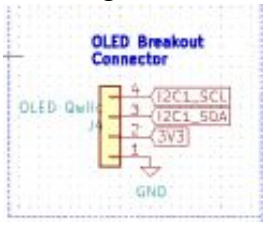
GPS

Figure 4



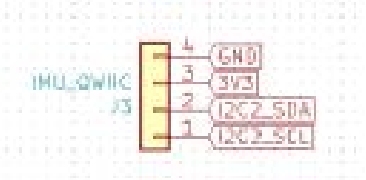
OLED Breakout

Figure 5



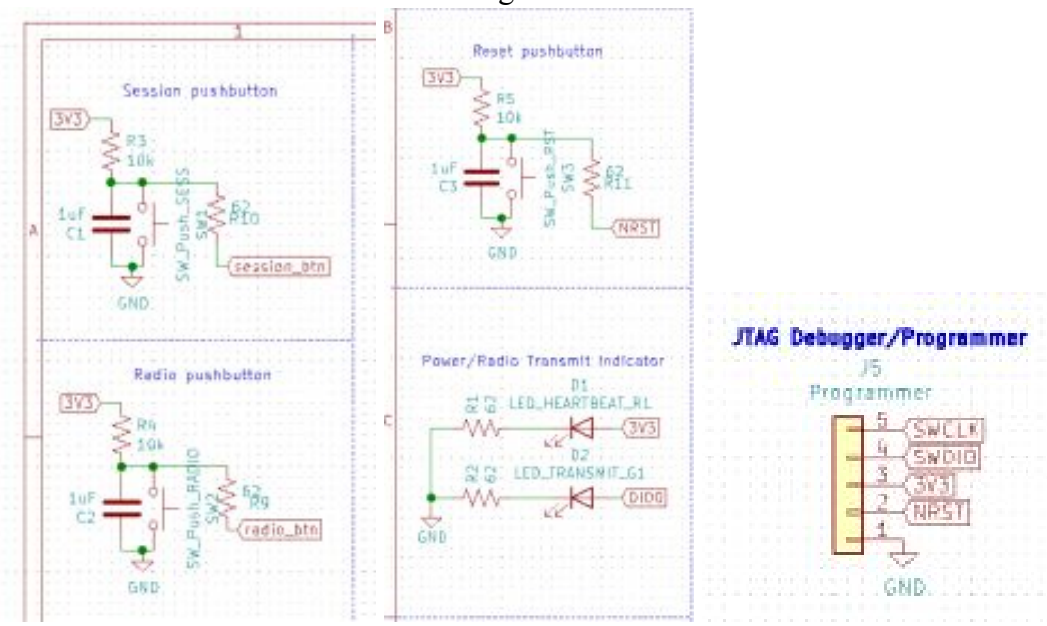
IMU Breakout

Figure 6



User I/O

Figure 7



Appendix B: FMECA Worksheet

Microcontroller FRMCA, Table 5

Failure No.	Failure Mode	Possible Causes	Failure Effects	Method of Detection	Criticality	Remarks
1	No signal coming out of the microcontroller	Damaged capacitor on VDD pin	All components do not function	All components do not function	Low	None
2	No supply voltage going into VCC pin	Unstable voltage source	All components do not function	All components do not function	Low	Assuming supply voltage is being applied
3	A large amount of noise appears in the outputs of various pins	Internals over-heated, Memory Stack Overflow, Electrical Inter-ference	Unpredicta ble	Some components may not function properly	Medium	Assuming supply voltage is being applied

Power Supply/Management *FMECA* , Table 6

Failure No.	Failure Mode	Possible Causes	Failure Effects	Method of Detection	Criticality	Remarks
4	No supply voltage going into VCC pin	Unstable voltage source, dead battery	All components do not function	All components do not function	Low	Assuming supply voltage is being applied
5	Voltage is not regulated down to a 3.3V output	Internals NPN pass transistor is shorted and fail-safes fail.	Unpredictable	All components do not function	High	Assuming supply voltage is being applied
6	Battery Babysitter charges battery in reverse	Internal Body Babysitter Malfunctions	Unpredictable, Possible combustion	Hot battery or smoke	High	
7	Battery Babysitter does not switch on when in charging mode.	Batter Babysitter Fails to Charge Battery	Unpredictable	Unable to turn on device	Medium	

LoRa Radio Transceiver *FMECA* , Table 7

Failure No.	Failure Mode	Possible Causes	Failure Effects	Method of Detection	Criticality	Remarks
8	No supply voltage going into VIN pin	Unstable voltage source	component does not function	component does not function	Low	Assuming supply voltage is being applied
9	LoRa Radio constantly on and active	Radio Push Button is continuously pressed	Higher power use, potential damage to the circuit	Radio constantly sending requests, but never reports findings	Medium	

GPS *FMECA* , Table 8

Failure No.	Failure Mode	Possible Causes	Failure Effects	Method of Detection	Criticality	Remarks
10	No supply voltage going into VIN pin	Unstable voltage source	component does not function	component does not function	Low	Assuming supply voltage is being applied
11	GPS Voltage Regulator does not regulate ripple coming from Micro	Internals NPN pass transistor is shorted.	Unpredictable	component does not function	Medium	
12	GPS and device located in a location unreach-able by satellite	GPS Takes longer time than expected to get a satellite fix	Session not activated for extended period of time	Watchdog Timer	Low	

OLED Breakout *FMECA* , Table 9

Failure No.	Failure Mode	Possible Causes	Failure Effects	Method of Detection	Criticality	Remarks
13	No supply voltage going into VIN pin	Unstable voltage source	component does not function	component does not function	Low	Assuming supply voltage is being applied
14	Noisy communication lines going to OLED	Traces nearby causing interference	Unpredictable	OLED displays unexpected information	Medium	

IMU Breakout *FMECA* , Table 10

Failure No.	Failure Mode	Possible Causes	Failure Effects	Method of Detection	Criticality	Remarks
15	No supply voltage going into VIN pin	Unstable voltage source	component does not function	component does not function	Low	Assuming supply voltage is being applied
16	No commun-ication coming from I2C lines	Incorrect pull-up resistor values	Micro cannot interpret IMU data	Uninterpretable I2C1 lines	Low	

I/O *FMECA* , Table 11

Failure No.	Failure Mode	Possible Causes	Failure Effects	Method of Detection	Criticality	Remarks
17	No supply voltage going into 3V3 Session Push Button	Unstable voltage source	Session Push Button is inoperable	Sessions continue to restart	Medium	
18	No supply voltage going into 3V3 Radio Push Button	Unstable voltage source	Radio Push Button is inoperable	Radio interrupt continues to restart	Medium	
19	No supply voltage going into 3V3 Reset Push Button	Unstable voltage source	Reset Push Button is inoperable	Reset interrupt continues to restart	Medium	
20	No ground going into GND JTAG Debugger	Poor manufacturing or fabrication	Unpredictable	Read and Write Signals are uninterpretable between devices	Medium	

It is not necessary to calculate the probability of each failure mode. These numbers would usually be taken from the reliability analysis, but since you are not performing a complete analysis, they do not need to be included in your FMECA worksheet.