Homework 11: Reliability and Safety Analysis

Due: Friday, April 4, at NOON

Team Code Name: ____Two Wheel Deal_______________________________________

Group No. __12____

Team Member Completing This Homework: ___Pete Dudash_________________________

E-mail Address of Team Member: ___pdudash____ @ purdue.edu

NOTE: This is the third in a series of four "professional component" homework assignments, each of which is to be completed by one team member. The completed homework will count for 20% of the individual component of the team member's grade. The body of the report should be 3-5 pages, **not** including this cover page, references, attachments or appendices.

Evaluation:

SCORE	DESCRIPTION
10	***Excellent*** *– among the best papers submitted for this assignment. Very few corrections needed for version submitted in Final Report.*
9	***Very good*** *– all requirements aptly met. Minor additions/corrections needed for version submitted in Final Report.*
8	***Good*** *– all requirements considered and addressed. Several noteworthy additions/corrections needed for version submitted in Final Report.*
7	***Average*** *– all requirements basically met, but some revisions in content should be made for the version submitted in the Final Report.*
6	***Marginal*** *– all requirements met at a nominal level. Significant revisions in content should be made for the version submitted in the Final Report.*
*	***Below the passing threshold*** *– major revisions required to meet report requirements at a nominal level.* ***Revise and resubmit.***

* *Resubmissions are due within* ***one week*** *of the date of return, and will be awarded a score of "6" provided all report requirements have been met at a nominal level.*

Comments:

1.0 Introduction

The Two Wheel Deal is a device used to balance and transport a single rider on two wheels. The design uses an accelerometer and gyroscope to sense when the center of gravity is not directly over the axis of the wheels. It then drives the motors in a precise way to balance the rider safely and smoothly. The rider leans forward to move this device forward, and similarly for reverse. Obviously, the main safety concern for this project is protecting the wellbeing of the rider and the system by avoiding injury and damage from falling over. The Two Wheel Deal will only be able to protect the user to a certain degree. It is still the rider's responsibility to be a safe and smart driver. A safety feature being designed utilizes a dead-man's switch to change The Two Wheel Deal between balancing by itself and balancing with a rider. With this implementation, if the user falls off during a ride, the device will theoretically come to a stop and balance itself. Also, if the rider is brave enough to drive near full speed or full tilt, the LCD screen will alert the rider that he/she is driving at a dangerous rate and the device may no longer be able to balance correctly. In order to best identify possible failures of high and low criticality and keep the user safe, the schematics for the motor controller and brain board have been broken into functional blocks and analyzed individually.

To be a successful and commercial product, the Two Wheel Deal also needs to be reliable. A few of the most critical components that will be analyzed in this report include the two LM340T Linear Voltage Regulators [1], the HRF3205 MOSFETs [2], ATmega32 microcontroller [3], ADXL203 dual-axis accelerometer [4], and the MLX90609E2 gyroscope [5]. The failure rate and mean time to failure (MTTF) are included in the tables below for each of the previously mentioned components.

2.0 Reliability Analysis

The components mentioned above have a high risk associated with them if they fail. They have been analyzed for reliability and the results can be seen in the tables below. The voltage regulators and power MOSFETs are the main components in the Two Wheel Deal that are most likely to fail as a result of over-heating, causing the entire transport device to stop working. The microcontroller is also highly critical because it is what calculates the necessary signal to send to the motors to balance the rider. If this component fails, then the entire system cannot operate. The accelerometer and gyroscope are responsible for measuring the current tilt angle and its derivative. Without these components functioning correctly, the balancing algorithm won't be able to produce the correct signal to stabilize the system.

The next couple sections are comprised of the necessary calculations to determine the number of failures per 10^6 hours and mean time to failure (MTTF) for each of the previously mentioned components. To compute the number of failures/10^6 hours, the components use the following model from page 25 of the Military Handbook—Reliability Prediction of Electronic Equipment [6]: $\lambda_P = (C_1\pi_T + C_2\pi_E)\pi_Q\pi_L$ and $MTTF = (\lambda_P)^{-1}$. In these equations, λ_P is the number of failures per 10^6 hours, C_1 is the die complexity, π_T is the junction temperature coefficient, C_2 is the package failure rate, π_E is the environmental constant, π_Q is the quality factor, and π_L is the learning factor associated with how long the particular component has been manufactured. Assumptions have been made in order to complete the following analysis. First of all, the Two Wheel Deal's components are operating at their respective maximum temperatures (π_T). Also, the system will be ground mobile (π_E) with commercially manufactured parts (π_Q) in production for over two years (π_L). The tables below are used to derive the failure rates and MTTF using information taken from the component datasheets.

Table 2.1: LM340T Linear Voltage Regulators

Parameter	Value	Assumptions
C_1	0.02	Linear, between 101-300 transistors
π_T	58	Linear, max temp of 125° C
C_2	0.0012	3 pins, Nonhermetic DIP
π_E	4.0	Ground Mobile on wheeled vehicle (G_M)
π_Q	10.0	Commercially manufactured component
π_L	1.0	More than 2 years in production
λ_P	11.648	Failures/10^6 hours
MTTF	**85,851.6484 hours = 9.794 years**	

Table 2.2: HRF3205 Power MOSFETs		
Parameter	**Value**	**Assumptions**
C_1	0.01	Linear, between 1-100 transistors
π_T	480	Linear, max temp of 175° C
C_2	0.0012	3 pins, Nonhermetic DIP
π_E	4.0	Ground Mobile on wheeled vehicle (G_M)
π_Q	10.0	Commercially manufactured component
π_L	1.0	More than 2 years in production
λ_P	48.048	Failures/10^6 hours
MTTF	**20,812.5208 hours = 2.374 years**	

Table 2.3: ATmega32 Micro		
Parameter	**Value**	**Assumptions**
C_1	0.14	8 bit, CMOS
π_T	58	Linear, max temp of 125° C
C_2	0.019	40 pins, Nonhermetic
π_E	4.0	Ground Mobile on wheeled vehicle (G_M)
π_Q	10.0	Commercially manufactured component
π_L	1.0	More than 2 years in production
λ_P	81.96	Failures/10^6 hours
MTTF	**12,201.074 hours = 1.393 years****	

**According to the microcontroller datasheet [3], "Reliability Qualification results show that the projected data retention failure rate is much less than 1 PPM over 20 years at 85°C or 100 years at 25°C."

Table 2.4: Accelerometer		
Parameter	**Value**	**Assumptions**
C_1	0.01	Linear, MOS device, between 1-100 transistors
π_T	58	Linear, max temp of 125° C
C_2	0.0016	4 functional pins, Nonhermetic
π_E	4.0	Ground Mobile on wheeled vehicle (G_M)
π_Q	10.0	Commercially manufactured component
π_L	1.0	More than 2 years in production
λ_P	5.864	Failures/10^6 hours
MTTF	**170,532.06 hours = 19.467 years**	

Table 2.5: Gyroscope		
Parameter	**Value**	**Assumptions**
C_1	0.01	Linear, MOS device, between 1-100 transistors
π_T	21	Linear, max temp of 110° C
C_2	0.0043	10 pins, Nonhermetic
π_E	4.0	Ground Mobile on wheeled vehicle (G_M)
π_Q	10.0	Commercially manufactured component
π_L	1.0	More than 2 years in production
λ_P	2.272	Failures/10^6 hours
MTTF	**440,140.845 hours = 50.244 years**	

These results and calculations are derived for the worst case scenario for each component. To get these results, π_T is assumed to be at the maximum operating temperature before the component burns up and no longer works. That is why the MTTF is relatively low. If we operate the voltage regulators at a more realistic temperature of 65° C ($\pi_T = 2.0$), the MTTF would increase to nearly 255 years. If temperature is an issue in the future, heat sinks can be added to help dissipate that energy and increasing the lifetime and reliability of that component. That is exactly what the fan on each motor controller board does for the MOSFETs. It continuously circulates cool air directly onto the components. If these parts operated at a more realistic temperature of 35° C ($\pi_T = 0.23$), the MTTF would increase to nearly 1,608 years. If the microcontroller also operates near 35° C, then the MTTF improves to about 400 years. By using values for π_T that are within a more reasonable temperature range that our system will be operating in, the MTTF for these critical components drastically increases. Based on the operation at lower temperatures, the reliability of each of the critical components is acceptable.

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

The schematics for the Two Wheel Deal's brain board and motor controller boards have been broken down into functional blocks. This illustration can be seen in Appendix A. These blocks include Section A for the brain board's signal outputs to the motor controller boards, Section B for the microcontroller and related components, Section C for the 5V and 12V Linear Voltage Regulators, Section D for the brain board's ADC inputs from the accelerometer, gyroscope, battery detection level, and joystick for steering (not shown), Section E for the motor controller's MOSFET H-Bridge, and Section F for the H-Bridge driver module. All the possible failure conditions for each functional block and the possible causes are included in Appendix B.

To determine the reliability of the entire system, two different degrees of criticality have been defined. Any failure that concerns the system's main balancing and maneuvering functions is defined as being a *high* criticality with $\lambda_P < 10^{-9}$. These failures could result in system instability, damage to the device, or injury to the rider. On the other hand, failures that affect the auxiliary aspects of the system, but still allow device functionality, are defined as being *low* criticality with $\lambda_P \geq 10^{-4}$. For example, the LCD screen malfunctions or displays incorrect information, the dead-man's switch or alarm buzzer doesn't work, or other similar supplementary functions. For failures of low criticality, there is no definite threat of injury to the user or damage to the device. It just serves as an inconvenience to the user and may cause customer dissatisfaction.

The completed FMECA charts are included in Appendix B. If the user falls off the Two Wheel Deal, it is assumed that it is dangerous and harmful. Also, it's assumed that the device has been damaged or broken due to the crash. That is why this situation is defined as high criticality.

4.0 Summary

After completing the analysis, observation is crucial in identifying the failures and the resulting effects. The components that were analyzed are very important because failures in those particular functional blocks have high criticality. This report also provides a good idea about how long the components will live. The lifetime of the components can be increased by proper heat sinking, therefore significantly lowering the temperature coefficient (π_T). With regards to the FMEC analysis, the most critical failures occur in Sections B & E which contain the microcontroller circuitry and the MOSFET H-Bridge circuit, respectively. Precautions have been taken to protect these sections from failures in the design, but accidents do happen. The MOSFETs have a fan to minimize heat and the microcontroller is safe from over-voltage and noise by two linear voltage regulators. Also, the brain board and two motor controller boards are safely secured under the base plate to prevent damage from collisions with objects on the ground and crashes. Overall, the Two Wheel Deal is a safe and reliable product.

List of References

[1] National Semiconductor, Linear Voltage Regulators, LM340T series Datasheet
http://www.national.com/ds/LM/LM340.pdf

[2] Fairchild Semiconductor HRF3205 100A, 55V N-Channel MOSFET Datasheet
http://www.tranzistoare.ro/datasheets3/fairchild/HRF3205.pdf

[3] Atmel ATmega32 Datasheet
http://www.atmel.com/dyn/resources/prod_documents/doc2503.pdf

[4] Analog Devices ADXL203 ±1.7g Dual-Axis Accelerometer
http://www.analog.com/UploadedFiles/Data_Sheets/ADXL103_203.pdf

[5] Melexis ±150 °/s MLX90609E2 Angular Rate Sensor (Gyroscope)
http://www.melexis.com/prodfiles/0005359_MLX90609_standard_datasheet.pdf

[6] MIL-HDBK-217F Military Handbook—Reliability Prediction of Electronic Equipment
http://cobweb.ecn.purdue.edu/~dsml/ece477/Homework/CommonRefs/Mil-Hdbk-217F.pdf

Appendix A: Schematic Functional Blocks

Figure 1 – Brain Board

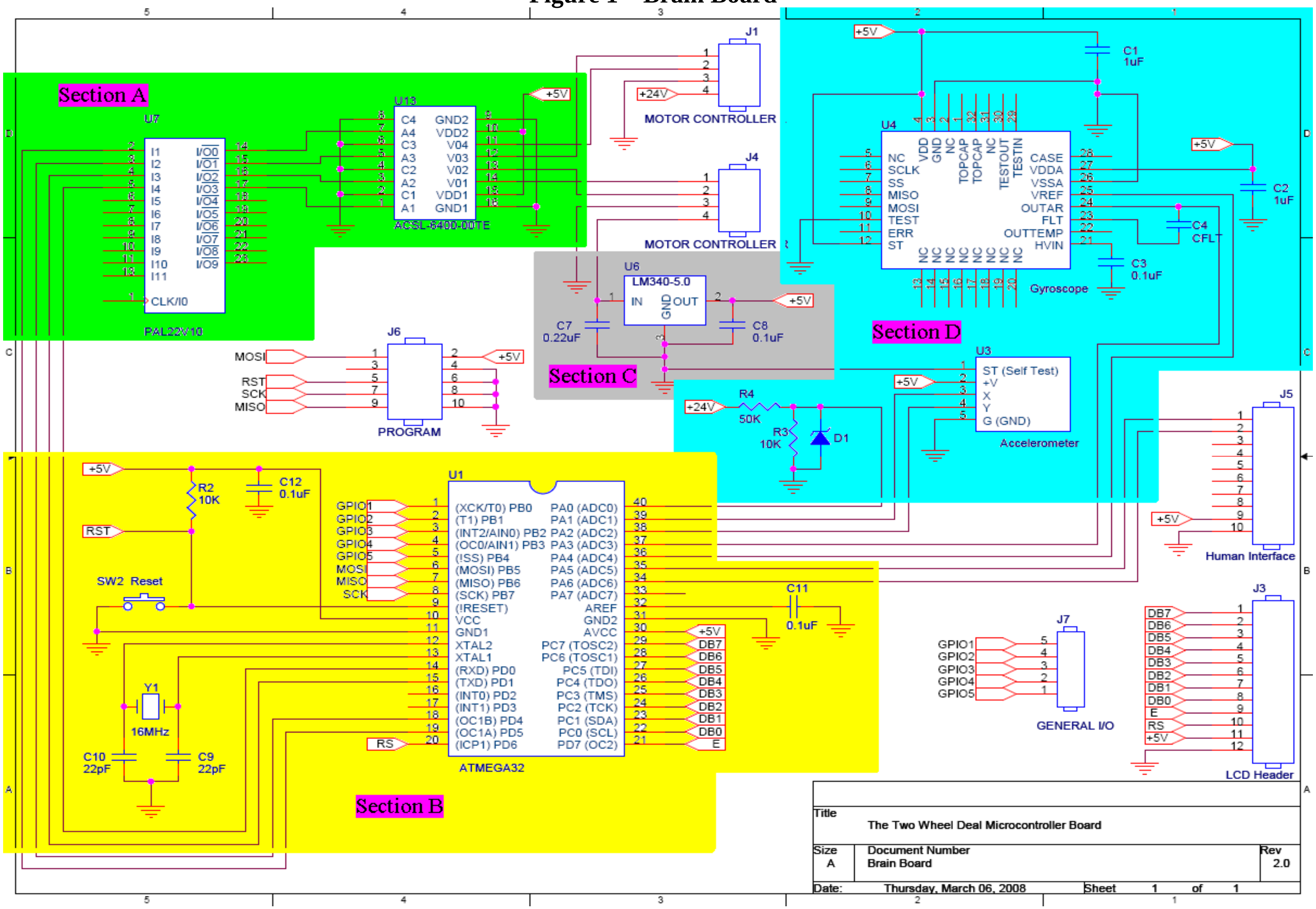
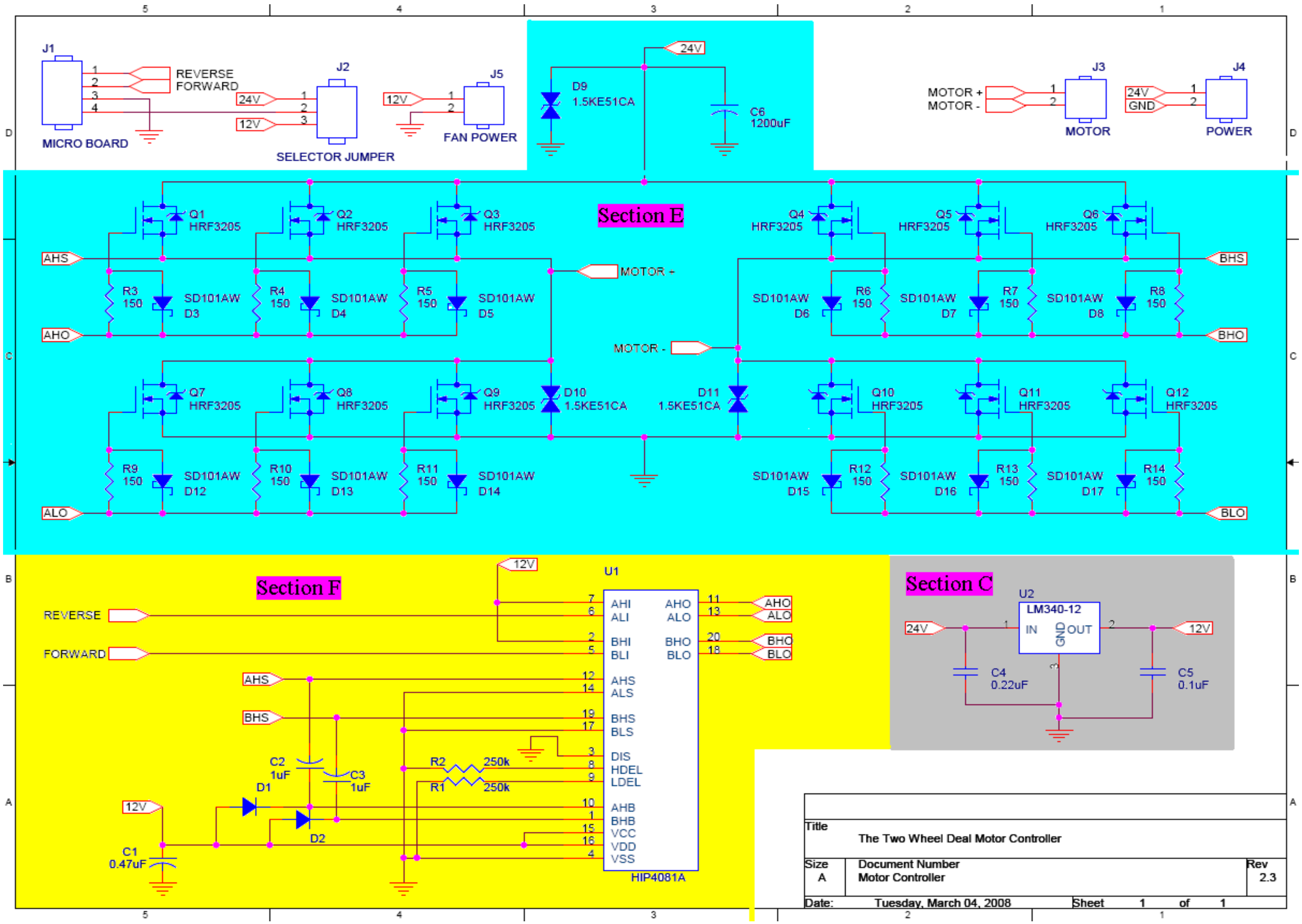


Figure 2 – Motor Controller Board



Appendix B: FEMCA Worksheet

Table 1-Brain Board Section A

Failure No.	Failure Mode	Possible Causes	Failure Effects	Method of Detection	Criticality	Remarks
A1	Cannot send PWM and direction signals to motor controller	PLD malfunction, optical isolator damaged	Wheels will not spin	Observation by oscilloscope	High	High Criticality because this could cause harm to both rider and device.

Table 2-Brain Board Section B						
Failure No.	**Failure Mode**	**Possible Causes**	**Failure Effects**	**Method of Detection**	**Criticality**	**Remarks**
B1	Micro remains in reset mode	Reset switch is broken and stays in "pressed" state.	Microcontroller fails to run program, also cannot reprogram FLASH memory	Observation with DMM	Low	Low criticality because user will realize the system won't balance after power up so user isn't in danger of falling off.
B2	V_{CC} shorted to ground	C_{12} fails and shorts out	No power to microcontroller—cannot drive motors	Observation with DMM	High	High criticality because if the micro is no longer powered, then the wheels stop and it could throw rider and damage the device.
B3	ADC inputs are all zero	C_{11} fails and shorts out	AREF for ADC channels is 0V causing all ADC outputs to be zero	Observation with DMM	High	If the micro no longer receives vital system feedback, then system becomes unstable which may injure rider and damage the device.

Table 3-Brain Board Section C						
Failure No.	**Failure Mode**	**Possible Causes**	**Failure Effects**	**Method of Detection**	**Criticality**	**Remarks**
C1	System performance seems random and erratic	Bypass capacitors C_4, C_5, C_7, C_8 became disconnected or failed	Introduces substantial amounts of noise which affects sensor outputs	Observation while riding	High	Medium criticality because system will still operate. If this isn't fixed right away, personal injury and device damage could occur.
C2	V_{CC} = 0V	Bypass capacitors C_4, C_5, C_7, C_8 became shorted or failed	No power to microcontroller stops the motors from turning.	Observation by DMM measurement	High	

Table 4-Brain Board Section D

Failure No.	**Failure Mode**	**Possible Causes**	**Failure Effects**	**Method of Detection**	**Criticality**	**Remarks**
D1	No response to changes in tilt	Either one or both axis of the accelerometer failed	System will not respond accurately, balancing alg. wont respond to small changes	Observation while riding	High	Depending on which axis fails, system may still balance. Could result in instability, injury, or damage to device.
D2	No response to quick changes in tilt	Failure of gyroscope, filter capacitor is disconnected or shorted out	System will respond the same way for quick and slow movements which may disrupt balancing	Observation while riding	High	The system should still balance itself but response may be slow. If rider changes angle quickly, they will fall off. Damage or injury may result.
D3	Incorrect battery voltage reading	Failure of zener protection diode, or resistors R_3 or R_4 burned up	The battery strength displayed on LCD is wrong	Observation of resistors on PCB or while riding	Low	Low criticality because system will still operate as expected. This failure won't harm user or device, but only be an inconvenience.

Table 5-Motor Controller Board Section E						
Failure No.	**Failure Mode**	**Possible Causes**	**Failure Effects**	**Method of Detection**	**Criticality**	**Remarks**
E1	Cannot control motors	The MOSFETs could have overheated and burned up	One or both motors stop working	Observation	High	High criticality because if the motor stops while the user is riding, injury and damage to device will occur.
E2	Operation is bumpy or unstable	Gate resistor and/or diode network may be destroyed	Shoot-through current may burn out components, rapidly discharge batteries.	Observation	High	High Criticality because the rider can fall off and get hurt and batteries/electronics could be destroyed.
E3	+24 voltage line is grounded	Reservoir capacitor, C_6, becomes shorted or spike suppression diodes D_9, D_{10}, or D_{11} become shorted.	Rapid battery discharge. Power wires heat up and melt, batteries begin to leak.	Observation	High	High criticality because of possible injury or damage to device by leaking batteries or hot wires.

Table 6-Motor Controller Board Section F

Failure No.	**Failure Mode**	**Possible Causes**	**Failure Effects**	**Method of Detection**	**Criticality**	**Remarks**
F1	+12 shorted to ground	Bypass capacitor, $C_{1,}$ shorts out.	H-bridge driver has no voltage and therefore cannot drive motors. Failure propagates to brain board too.	Observation	High	High criticality because the motors will not turn. This can cause injury to the user and possible damage to device.
F2	Cannot drive motors	High-pass capacitors C_2, C_3 are open circuited.	The PWM signal cannot pass into H-Bridge	Observation	High	High criticality because the motors may suddenly stop, injuring user and damaging device.
F3	Noisy or bumpy response	Pull down resistors R_1 and R_2 fail and are open circuited.	May get shoot-through current because of no dead-time between direction changes. Batteries may short, heat up, or leak.	Observation	High	Highly critical because if these fail, the device may suddenly stop operating; injury to rider or damage to batteries or device possible.