**Reliability and Safety Analysis**

**Year: \_\_2019\_\_\_\_ Semester: \_\_\_Fall\_\_ Team: \_\_8\_\_\_ Project:\_\_\_Condiment Express\_\_**

**Creation Date: \_\_\_\_\_Nov/1/2019\_\_\_\_\_\_ Last Modified:** March 25, 2019

**Author: \_\_\_\_Chengming Zhang\_\_\_\_ Email: \_\_\_\_zhan2568@purdue.edu\_\_\_\_\_**

**Assignment Evaluation:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **Score (0-5)** | **Weight** | **Points** | **Notes** |
| **Assignment-Specific Items** | | | | |
| **Reliability Analysis** | 5 | x2 | 10 |  |
| **MTTF Tables** | 5 | x3 | 15 |  |
| **FMECA Analysis** | 5 | x2 | 10 |  |
| **Schematic of Functional Blocks (Appendix A)** | 5 | x2 | 10 |  |
| **FMECA Worksheet (Appendix B)** | 5 | x3 | 15 |  |
| **Writing-Specific Items** | | | | |
| **Spelling and Grammar** | 4 | x2 | 8 |  |
| **Formatting and Citations** | 5 | x1 | 5 |  |
| **Figures and Graphs** | 5 | x2 | 10 |  |
| **Technical Writing Style** | 5 | x3 | 15 |  |
| **Total Score** | 98 | | |  |

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

**Comments:**

*Comments from the grader will be inserted here.*

**Nice detailed effort. A few spellings and grammatical errors here and there could have been avoided.**

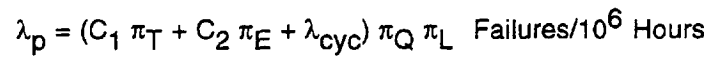
1. **Reliability Analysis**

### **Component to be included**

* Voltage Regulator 5v to 3v3, MP2541EN
  + Reason for Selection: This is a buck converter which provides power for the entire 3v3 bus which the microcontroller and other sensor are relied on. Failure of this component could result in the end of operation for the entire machine.
* Voltage Regulator 12v to 5v, MP1584EN
  + Reason for Selection: This is a buck converter that provides power for the entire 5v bus which the servo motors and stepper motor driver are relied on, as well as the MP2541 Voltage Regulator. Failure of this component could result at an end of operation for the entire machine. Things like heat generated during the process might cause a problem.
* ESP32 Microcontroller
  + Reason for Selection: This is the brain of the entire operation. A failure in this component will result at an end of operation for the entire machine. This microcontroller contains many IOs which could be damaged by power surges or in proper EM shielding.

### **Model**

Models used for the failure rate in the analysis is from the Military Handbook (MIL-HDBK-217f) [1]:



Models used for the MTTF in the analysis is also from the Military Handbook (MIL-HDBK-217f) [1]:

*MTTF = 106 / (24 \* 365 \* λP) yrs*

### **Assumption**

From the guideline in the Military Handbook, **the component quality factor is 10** for our component. We just assume that the part we get from the manufacturer is genuine and error-free since they have their own error checking system. **For the Learning Factor**, **we use a value of 1** since all of our components have been on the market for more than 2 years. Since the entire PCB is mounted in our machine, which is also mounted in the kitchen, our **Environment coefficient is 2**.

### **Failures per 10^6 and MTTF**

#### **ESP32 Microcontroller:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Parameter name** | **Description** | **Value** | *Comments regarding the choice of the parameter value, especially if you had to make assumptions.* |
| C1 | Die complexity | 0.56 | Based on the MIL-Hdbk217f [1] for 32-bit microcontrollers |
|  | Temperature Coeff. | 3.1 | Based on ESP32 Datasheet [2], the **worst-case junction temperature** is 125 degrees C |
| C2 | Package failure rate | 0.015 | ESP32 have a pin number of 48, the closest reference is a package of 40 pins. |
|  | Environment factor | 2 | Mounted PCB on a non-moving object |
|  | Quality factor | 10 | Commercial products widely adopted by many electronic companies. |
|  | Learning factor | 1 | The device is on the market for more than 2 years |
|  | Failures rate per million hours | 17.66 |  |
| **MTTF** | Mean Time To Failure | 6.46405 | It takes around 6 and a half years on average for the device to fail. **IN WORST CASE** |

#### 

#### **MP1584EN Buck Convertor:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Parameter name** | **Description** | **Value** | *Comments regarding the choice of the parameter value, especially if you had to make assumptions.* |
| C1 | Die complexity | 0.01 | Based on the MIL-Hdbk217f [1] for 1 Digital Gate MOS [3] |
|  | Temperature Coeff. | 180 | Based on MP1584EN Datasheet [3], the **worst-case junction temperature** is 150 degrees C, for a Linear MOS Device |
| C2 | Package failure rate | 0.0026 | MP1584 have a pin number of 8 |
|  | Environment factor | 2 | Mounted PCB on a non-moving object |
|  | Quality factor | 10 | Commercial products widely adopted by many electronic companies. |
|  | Learning factor | 1 | The device is on the market for more than 2 years |
|  | Failures rate per million hours | 18.052 |  |
| **MTTF** | Mean Time To Failure | 6.3236 | It takes around 6 and a half years on average for the device to fail. **IN WORST CASE** |

#### 

#### **MP2451EN Buck Convertor:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Parameter name** | **Description** | **Value** | *Comments regarding the choice of the parameter value, especially if you had to make assumptions.* |
| C1 | Die complexity | 0.01 | Based on the MIL-Hdbk217f [1] for 2 Digital Gate MOS[4] |
|  | Temperature Coeff. | 180 | Based on MP2451 Datasheet [4], the **worst-case junction temperature** is 125 degrees C, for a Linear MOS Device |
| C2 | Package failure rate | 0.0019 | MP1584EN have a pin number of 6 |
|  | Environment factor | 2 | Mounted PCB on a non-moving object |
|  | Quality factor | 10 | Commercial products widely adopted by many electronic companies. |
|  | Learning factor | 1 | The device is on the market for more than 2 years |
|  | Failures rate per million hours | 18.038 |  |
| **MTTF** | Mean Time To Failure | 6.3285 | It takes around 6 and a half years on average for the device to fail. **IN WORST CASE** |

### **Failure Analysis Summary**

Although the MTTF for all the components above shows an average of 6 and a half year lifetime, the component is still very reliable consider it is a worst-case calculation. From simple observations, one can tell that the biggest reason for such a high failure rate is the high junction temperature. The component such as ESP32 has a heat sink on its shield preventing it from overheating. With proper heat dissipation from the pad and via, the temperature on both buck convertor, ideally should not exceed over 50 degrees C, from experiences and measurement from the past. If during the inspection phase, the component such as the Buck Convertor excess such temperature limit often, a passive or active heat sink will be considered to drive the temperature coefficient down furthermore.

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

The schematic for Condiment Expressed is divided into these subsections, Power Circuit, Microcontrollers, Sensors, and Drivers.

Power Circuit contains a switching power supply IC, resistors, inductors, and capacitors. From 12V DC supply that connected to the PCB, the MP1584EN is coverts the 12V DC to 5V DC. The MP2451EN converts 5V to 3v3 for the microcontrollers and the sensors. A possible point of failure could include:

* A saturated Inductor causing a meltdown of the inductor that will lead to a full machine shut-down. Since both buck converter is connected in series, any failure in these two buck convertor could cause a stall in operation and memory loss. The method of detection for this failure mode is by observation of the inductor. High Criticality.
* A shorted filter capacitor that could cause a sudden drop in uC supply voltage. This will not cause a shutdown of the machine as long as the drop in supply voltage duration is short and not-aggressive (low voltage drop). This, however, could permanently damage the microcontroller if the voltage surges are high in amplitude. The method of detection for this failure mode is by observation of the power indicator LED or status of the debugger window. High Criticality.
* A high junction temperature that causes a shutdown of the switching power supply IC. Since both buck converter is connected in series, any failure in these two buck convertor could cause a stall in operation and memory loss. The method of detection for this failure mode is by observation of the package condition of the IC if anything is burnt or very hot. High Criticality.

The sensors include an accelerometer and a temp-humidity sensor. These sensors are equipped with its own filtering capacitor that prevents sudden voltage drop. A possible point of failure could include:

* Memory or Register Block fails to cause loss of information, it will not stall the operation since these sensors will not be mission-critical. This can be observed by eyes during the debugging process. Medium Criticality.

The Microcontroller is the brain of the operation and the possible point of failure includes:

* Memory or Register Block fails to cause loss of information for the status of the operation. This will stall the operation and cause a problem for user experiences. This can be observed by eyes during the debugging process. High Criticality.
* A shorted filter capacitor that could cause a sudden drop in uC supply voltage. This will not cause a shutdown of the machine as long as the drop in supply voltage duration is short and not-aggressive (low voltage drop). This, however, could permanently damage the microcontroller if the voltage surges are high in amplitude. The method of detection for this failure mode is by observation of the power indicator LED or status of the debugger window. High Criticality.

**Levels of Criticality**

In our circumstance, the “Low” criticality is defined for that failure mode which will not obstruct the core functionality of the machine. For example, if the BLE module stop working, the user can simply switch to our OLED interface and continue. This might hurt the user experience, but not stop the core functionality. The “Medium” criticality is defined for that failure mode where the core functionality might be obstructed, but a simple restart could fix the problem. For example, many memory failures could be resolved by restart because of the volatile nature of the system RAM. Some of the minor heat issues could also be resolved by a restart. The “High: criticality is defined for that failure mode where all the functionality is disabled. The problem cannot be resolved by a software reset, but the complete replacement of the PCB or the machine. This failure mode could also cause danger to the user, such as causing a fire hazard.

**Observation Techniques**

The board is equaled with many feedback loop to detect malfunctions. The onboard temperature sensor could provide feedback on the machine temperature anomaly. Most of the sensor and functionality have a backlog to our debug port and potentially uploaded to the cloud. For failure mode that has a medium or low criticality, observation should not be necessary as most of the backlog can provide insight to that problem, such as low or high supply voltage or temperature. For failure mode that has a high criticality, a visual inspection is very necessary as many of the burned chips can be only detected via visual inspection. A photo of the PCB by any modern smartphone should be sufficient to diagnose most of the problems by any electronic expert.

**3.0 Sources Cited:**

[1] “Military Handbook,”1 1990. [Online]. Available: <http://snebulos.mit.edu/projects/reference/MIL-STD/MIL-HDBK-217F-Notice2.pdf> [Accessed 11 1 2019].

[2] “ESP32 Series”1 2019. [Online]. Available: <https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf>[Accessed 11 1 2019].

[3] “MP1584”1 2014. [Online]. Available: <https://www.haoyuelectronics.com/Attachment/MP1584/MP1584.pdf>[Accessed 11 1 2019].

[4] “MP2451”1 2014. [Online]. Available: <https://www.mouser.com/datasheet/2/277/MP2451_r1.33-477967.pdf>[Accessed 11 1 2019].

Appendix A: Schematic Functional Blocks

##### **Functional Blocks A - Power Circuits**

*A close up of a map

Description automatically generated*

*A close up of a map

Description automatically generated*

##### **Functional Blocks B - Microcontrollers**

*A close up of text on a white background

Description automatically generatedA close up of a map

Description automatically generated*

##### **Functional Blocks C - Sensors**

*A close up of a map

Description automatically generated*

*A close up of a map

Description automatically generated*

**Appendix B:  FMECA Worksheet**

**Subsystem A for Power Circuits**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| A1 | Supply Voltage High for 3V3 Bus | Inductive Load current resurgent | The microcontroller cannot properly work. Logic Level messed up causing incapability of communicating with sensors | Observation | Medium | May Damage Microcontroller and sensors |
| A2 | Supply Voltage Low for 3V3 Bus | Sudden draw in current for ESP32 | Microcontroller not functioning. Sensor not functioning | Observation | High |  |
| A3 | Supply Voltage High for 5V Bus | Inductive Load current resurgent | The microcontroller cannot properly work. Logic Level messed up causing incapability of communicating with sensor. Stepper and servo motor driver cannot work properly | Observation | Medium | May Damage Microcontroller and sensors. Both Drivers. |
| A4 | Supply Voltage Low for 5V Bus | Sudden draw in current for Stepper Motor or Servo Motor | Microcontroller not functioning. Sensor not functioning. Stepper Motor Controller, Servo Motor Controller not functioning. Entire PCB not working | Observation | High |  |
| A5 | Supply Voltage shutdown for 3V3 Bus | Switching IC burned, Inductor melted, Capacitor Shorted | Microcontroller not functioning. Sensor not functioning | Observation | High | Memory Failure might occur for ESP32 |
| A6 | Supply Voltage shutdown for 5V Bus | Switching IC burned, Inductor melted, Capacitor Shorted | Microcontroller not functioning. Sensor not functioning. Stepper Motor Controller, Servo Motor Controller not functioning. Entire PCB not working | Observation | High | Memory Failure might occur for ESP32 |

**Subsystem B for Microcontroller**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| B1 | Memory Failure | Power Regulators Fails | The entire machine stop operation. Peripheral will stop working or on repeat command. | Observation | HIGH | May Damage Microcontroller and sensors |
| B2 | BLE Failure | EM Interference strong | Microcontroller not functioning. Sensor not functioning | Observation | LOW | It will cause bad user experience but will not stop the core functionality of the machine. |
| B3 | Chip Nonresponsive | Not Powered Corrected, Not incorrect operating temperature, Program halted. | The microcontroller cannot properly work. Logic Level messed up causing incapability of communicating with sensor. Stepper and servo motor driver cannot work properly | Observation | HIGH | It cannot perform core functionality. |

**Subsystem C for Sensors**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| C1 | Register Failure or Nonresponsive | Power Regulators Fails or Power Surges | The program will skip this information and used the last available sensor data. | Observation | LOW | The machine can still function correctly if it just simply stop working. |
| C2 | Corrupted Data | Strong Inertia Interference for Accelerometer. Logic Voltage not corrected set by the power supply. | Incorrect command send to drivers cause potential mechanical failure. | Observation | HIGH | This will cause Mechanical failure which could be perminate. |