Reliability and Safety Analysis

Year: 2019 Semester: Fall Team:10 Project: Gesture Controlled Remote for Smart Home Devices

Creation Date: 10/24/2019 Last Modified: 10/25/2019

Author: Tsung Lin Hsia Email: thsia@purdue.edu

Assignment Evaluation:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **Score (0-5)** | **Weight** | **Points** | **Notes** |
| **Assignment-Specific Items** | | | | |
| **Reliability Analysis** | 3.5 | x2 | 7 | Details needed |
| **MTTF Tables** | 4.5 | x3 | 13.5 | Good |
| **FMECA Analysis** | 5 | x2 | 10 | Good |
| **Schematic of Functional Blocks (Appendix A)** | 5 | x2 | 10 | Good |
| **FMECA Worksheet (Appendix B)** | 4.5 | x3 | 13.5 | Good. Adding concluding remarks would have been nice. |
| **Writing-Specific Items** | | | | |
| **Spelling and Grammar** | 4 | x2 | 8 | A few typos and grammatical errors. |
| **Formatting and Citations** | 5 | x1 | 5 |  |
| **Figures and Graphs** | 5 | x2 | 10 |  |
| **Technical Writing Style** | 5 | x3 | 15 |  |
| **Total Score** | 92 | | |  |

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

Comments:

*Comments from the grader will be inserted here.*

1. Reliability Analysis

Microcontroller: STM32F407VGT6[2]

The model to determine the failure rate is from the Military Handbook MIL-HDBK-217f [1]

The failure per *106* hours is calculated by 𝜆𝑃 = (C1 · πt + C2· πe) · πL · πQ

Mean time to failure in years is shows as MTTF =*106* / (24 x 265 x 𝜆𝑃) years A

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter name | Description | Value | *Comments regarding choice of parameter value, especially if you had to make assumptions.* |
| C1 | Die complexity | 0.18 | datasheet for device with 100 to 300 bipolar transistor |
| πT | Temperature coeff. | .93 | worst case temperature of 125C on worst junction temp of the regulator |
| C2 | Package failure rate | 0.02 | 3-pin SMD |
| πe | Environment factor | 1 | mobile device |
| πl | Learning Factor | 1 | number used for devices older than 2 years in production |
| πq | Quality factor | 8 | commercial part |
| λP | Failures rate per million hours | 1.58239 |  |
| MTTF | Mean Time To Failure | 618273.2342 | Approximately 68 years to a failure for one device |

Table 1, microcontroller analysis

LM317 Voltage Regulator[3]

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter name | Description | Value | *Comments regarding choice of parameter value, especially if you had to make assumptions.* |
| C1 | Die complexity | 0.02 | datasheet for device with 100 to 300 bipolar transistor |
| πT | Temperature coeff. | 5.8 | worst case temperature of 125C on worst junction temp of the regulator |
| C2 | Package failure rate | 0.00092 | 3-pin SMD |
| πe | Environment factor | 2.0 | mobile device |
| πl | Learning Factor | 1.0 | number used for devices older than 2 years in production |
| πq | Quality factor | 10.0 | commercial part |
| λP | Failures rate per million hours | 1.1784 |  |
| MTTF | Mean Time To Failure | 848608.2824 | approximate 97 years to a failure for one device |

Table 2, Voltage Regulator analysis

Battery 18650

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter name | Description | Value | *Comments regarding choice of parameter value, especially if you had to make assumptions.* |
| C1 | Die complexity | 0.14 | datasheet for device with 100 to 300 bipolar transistor |
| πT | Temperature coeff. | 0.98 | worst case temperature of 125C on worst junction temp of the regulator |
| C2 | Package failure rate | 0.023 | 3-pin SMD |
| πe | Environment factor | 0.3 | mobile device |
| πl | Learning Factor | 1 | number used for devices older than 2 years in production |
| πq | Quality factor | 10 | commercial part |
| λP | Failures rate per million hours | 1.534 |  |
| MTTF | Mean Time To Failure | 102.4985 | 500 cycles |

Table 3,

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

The schematic for our senior design can be divided into five subsections. These subsystems are power circuit, sensor circuit, LCD connector, and microcontroller circuits. The division of our design is based on the diagram of our software development.

For the gesture sensor, there are two failure modes. One is when the gesture sensor fails to detect gestures, and the other one is when the gesture sensor decodes the gestures incorrectly. Both modes could lead to sending wrong information to the WiFi module and therefore executing wrong commands. As a result of miscommunications, the smart home devices will behave differently than what users expect. In addition to sensor’s failures, the LCD will also display incorrect information to the user.

The LCD has very good reliability. It just displays whatever information given by the microcontroller. However, the flickering screen and can be the failure mode. This mode can lead to user gets the incorrect status update and harms user’s eyes.

The microcontroller can have numerous failure modes. One can be reset incorrectly triggered and the microcontroller accidentally being reset. Another can be that the incorrect behavior of capacitors and resistors affect the microcontroller’s behavior. (An example can be that the decoupling capacitor gets shorted and causes the microcontroller may get overheated.) The failure mode of microcontroller would affect the whole design not functioning properly. (Decoding the wrong information, displaying incorrect status update, and wrong communication among all components.)

The failure mode of battery can be overheating, false alarm inside the built-in integrated circuit that checks the battery charging and current. Overheating may harm the user and the false alarm would lead to the whole device not functioning (no power).

2.1 Criticality Analysis

There are three criticality levels, which are low, medium, and high.

Low level of criticality specifies that the failure of the project will only cause the system to shut down without producing any damage to users or environment.

Medium criticality level refers to failures which does not harm the user but has some potential to damage the components and system. For medium and low level failure, the failure rate is 10^-6.

High criticality level refers to failures which can cause injury to users, such as voltage regulator catching fire. The acceptable failure rate for high level failure is 10^-9 or less.

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 5 2014].

[2]STM32F407 datasheet. (2019) Available: https://www.st.com/resource/en/datasheet/dm00037051.pdf

[3]Life.argmented, “Adjustable and fixed low drop positive voltage regulator,” 4 2004.

[Online]. Available:

http://www.st.com/web/en/resource/technical/document/datasheet/CD00000544.pdf [Accessed 4

4 2013].

*NOTE: MIL-HDBK-217F should be among the sources teams cite, as well as relevant component datasheets*

Appendix A: Schematic Functional Blocks

Subsystem A

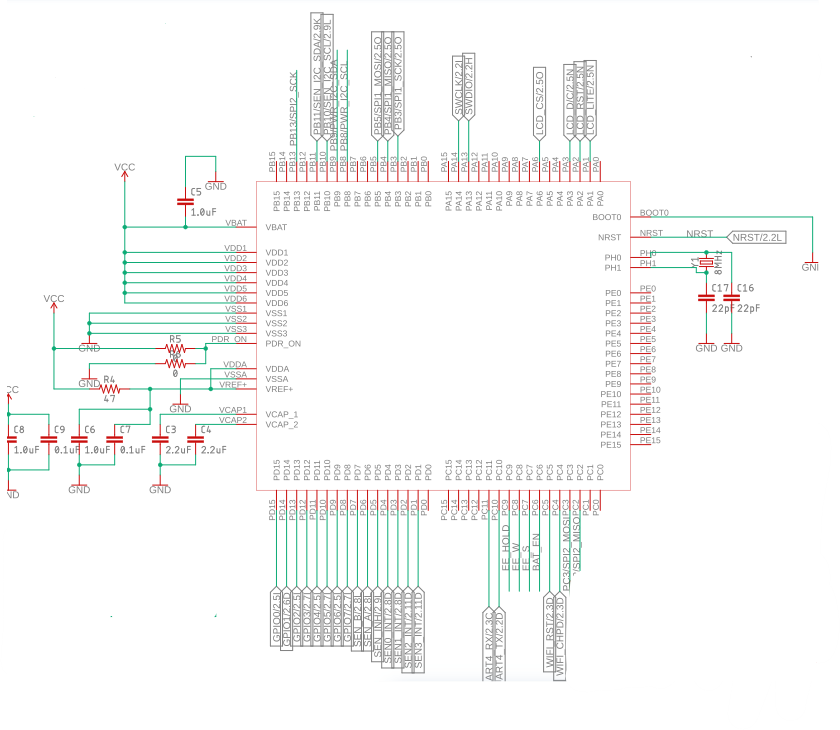
**

Figure 1, Microcontroller

Subsystem B

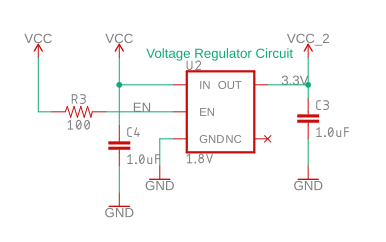


Figure 2, Voltage Regulator Circuit

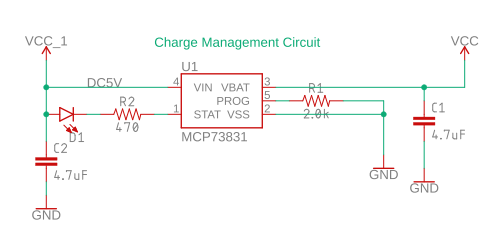


Figure 3, Charge Management Circuit

Subsystem C

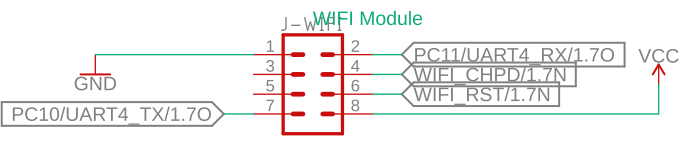


Figure 5, WIFI module

Subsystem D:

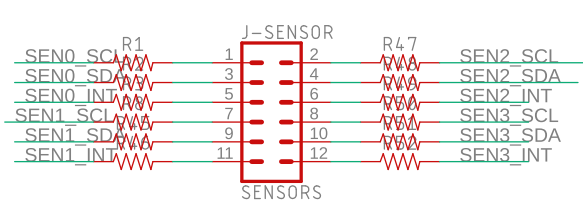


Figure 6, J-Sensor

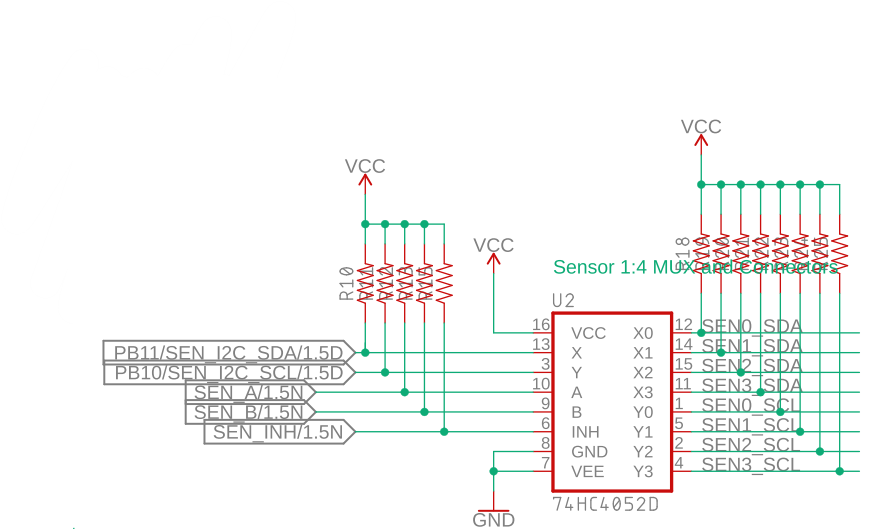


Figure 7, 74HC4052D

Appendix B: FMECA Worksheet

Subsystem A: Microcontroller

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| A1 | The stm32F4 does not executing instructions | Software bugs,  Power,  Broken components  (Resistors) | Unpredictable | Observation | Low |  |
| A2 | No supply voltage goes to VCC | Shorted bypass capacitors | Unpredictable | Observation | Low |  |

**Table 4, Microcontroller chart**

Subsystem B: Power Supply

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| B1 | Voltage Drop | Voltage regulator failure, battery IC problem | Some or all components will turn off | Observation | Low | by checking the voltage constantly |
| B2 | Voltage regulator fails short | 2 voltage regulator, battery IC failure | Protection from battery so all components will turn off or else components might burned | Observation | High | by checking the voltage constantly |

Table 5, Power Supply chart

Subsystem C: Wifi Module(ESP8266)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| C1 | ESP8266 not able to communicate with the microcontroller | Different baud rate or parity,  Wrong configuration of UART | Not able to send or receive instructions from other | Oscilloscope to detect TX and Rx data sending and receiving | Low |  |
| C2 | ESP8266 not able to connect to Wifi | Wifi authentication,  Wifi connection issue | Not able sending or receiving information to IFTTT | Observation | Low |  |
| C3 | ESP8266 not able to communicate with IFTTT applets | Wifi connection,  Applet triggering issue, IFTTT service issue | Not able to send or to receive instruction or feedback from IFTTT | Observation | Low |  |

Table 6, Wifi Module chart

Subsystem D: Sensor Network

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| D1 | Sensor sending back inaccurate data | Broken sensor, I2C communication problem, software | Detection and Instruction are inconsistent | Observation | Low |  |
| D2 | Sensor not able to send data back | Sensor shorted to ground, I2C pin in microcontroller failed | It’s not detect anything | Observation | Low |  |

Table 7, Sensor network chart