Reliability and Safety Analysis

Year: 2019 Semester: Fall Team: 1 Project: IntelliFace

Creation Date: 10/27/2019 Last Modified: 12/09/2019

Author: Pratyaksh Sharma Email: sharm235@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** | 5 | x2 | 10 |  |
| **Formatting and Citations** | 4 | x1 | 4 |  |
| **Figures and Graphs** | 5 | x2 | 10 |  |
| **Technical Writing Style** | 5 | x3 | 15 |  |
| **Total Score** | 99 | | |  |

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

Comments:

1.0 Reliability Analysis

The components of the Interface that are most likely to fail are the following:

* STM32F051R8T6 Chip, due to static discharge
* NVIDIA Jetson Nano, due to overheating and component wear down
* LD1117AV33 Power Regulator, for miscellaneous reasons as detailed below

**1.1 Models and Functions:**

The model we used to calculate the failure rate, λP, was derived from the document MIL-HDBK-217F [1] as:

λP = (C1 πT + C2 πE) πQ πL

The Mean Time To Failure (MTFF) is calculated as:

MTTF = 106 / (24 \* 365 \* λP) years

**1.2 STM32F051R8T6:**

The chip in use, the STM32F051R8T6[2] is susceptible to failure due to the discharge of static electricity due to improper handling. If handled poorly, a discharge from the user’s hands or from other sources during production will damage the internal workings of the chip, in most cases rendering it unusable and possibly a fire hazard. An infinitesimally low risk of chip damage from prolonged run times in unsuitable conditions does exist, but with proper handling and storage can be avoided entirely. To avoid all risk of chip damage during production, it is recommended that work is performed on a grounded mat, as well as proper casing to prevent accidental discharge from the end user.

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter | Description | Value | Comments |
| C1 | Die complexity | 0.56 | Failure rate for 32 bit microcontroller |
| πT | Temperature coefficient | 0.35 | Temperature Factor for TA = 35oC |
| C2 | Package failure rate | 0.0425 | 64 pin LPFQ package |
| πE | Environment factor | 0.5 |  |
| πQ | Quality factor | 10 | Commercial Product |
| πL | Learning factor | 1 | Part older than 2 years |
| Overall Design: | | | |
| λP | | 2.7125 | |
| MTTF | | 52.55 | |

**1.2 NVIDIA Jetson Nano**

The NVIDIA Jetson Nano Developer Kit [3] runs the Face ID system, the Dashboard, PySerial Parser, and API calls to weather, stock, email and news services in parallel. As a result, multiple threads are run and can be intensive on the processor. However, as the device was built to handle computationally intensive deep learning processes, the probability of failure due to heat is low, especially due to the presence of a dedicated heat sink.

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter | Description | Value | *Comments* |
| C1 | Die complexity | 0.56 | *64 Bits* |
| πT | Temperature coefficient | 0.98 | *-25 to 85 C Range* |
| C2 | Package failure rate | 0.017 | *J41 41 Pinout header* |
| πE | Environment factor | 0.5 | *In place component* |
| πQ | Quality factor | 10 | *Commercial component, widely available* |
| πL | Learning factor | 1 | *Device has been produced for the last 2 years.* |
| Overall Design: | | | |
| λP | | 8.573 | |
| MTTF | | 23.5 | |

**1.3 LD1117V33 Power Regulator:**

The LD1117V33 [4] is a crucial component of our project and it is extremely paramount that it does not fail at any point. The power regulator gets the voltage to drop to 3.3V which is further used to power the STM32F0 chip on the PCB. If in the scenario that something would happen and the power regulator fail, the chip will not receive any power and thus, nothing would be turned on. Since nothing would be turned on, the user will not be able to wake up the smart mirror as the IR sensor would also not be on since we are using the IR sensor to wake up the smart mirror. In that case, the user would not be able to see the UI and essentially the smart mirror would just become a normal mirror. It would be great if the power regulator acted as an open instead of a short since this would hinder the current flow and would also stop any kind of shorting to happen that could further cause the chip to fry or explode.

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter name | Description | Value | Comments |
| C1 | Die complexity | 0.02 | For devices with 100 to 300 bipolar transistors |
| πT | Temperature factor | 5.8 | Worst case junction temperature of the LD1117 of 125˚C |
| C2 | Package failure rate | 0.00092 | 3 pins |
| πE | Environment factor | 2.0 | Mobile Device |
| πQ | Quality factor | 10 | Commercial |
| πL | Learning factor | 1 | More than 2 Years in Production |
| λP | Failures rate per million hours | 1.1784 |  |
| MTTF | Mean time to failure | ~97 | Years to Failure |

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

IntelliFace has 4 major subsystems which are listed as:

* Barrel Jack Power Connector and Power Regulator
* STM32F0 Microchip
* NRST Circuit
* Sensor Board

The schematic diagrams of the subsystems have been broken down into detail in Appendix A.

IntelliFace is designed to be a part of our everyday lives and is built using parts that can be easily purchased online. The parts were chosen after thorough research regarding safety and credibility and thus, IntelliFace should be considered as a very safe and reliable product.

**Criticality Level Breakdown:**  
It is crucial that the FMECA model has a system to classify the successes and failures of the design output. Below is the criteria by which the failures of the design will be calculated:

* **Low**: Criticality level “Low” failures are relatively unimportant and won’t affect the user and basic functioning of the product as a whole.
* **Medium**: Criticality level failures categorized as “Medium” will affect the basic usable cause of the product and may also pose a risk to the safety of the user. These failures can be defined with a failure rate of roughly 10^-6.
* **High**: Failures with a “High” Criticality level will pose a definite high risk to the safety of the user and affect the electrical components of IntelliFace as well. These failures can be defined with a failure rate of roughly 10^-10.

3.0 Sources Cited:

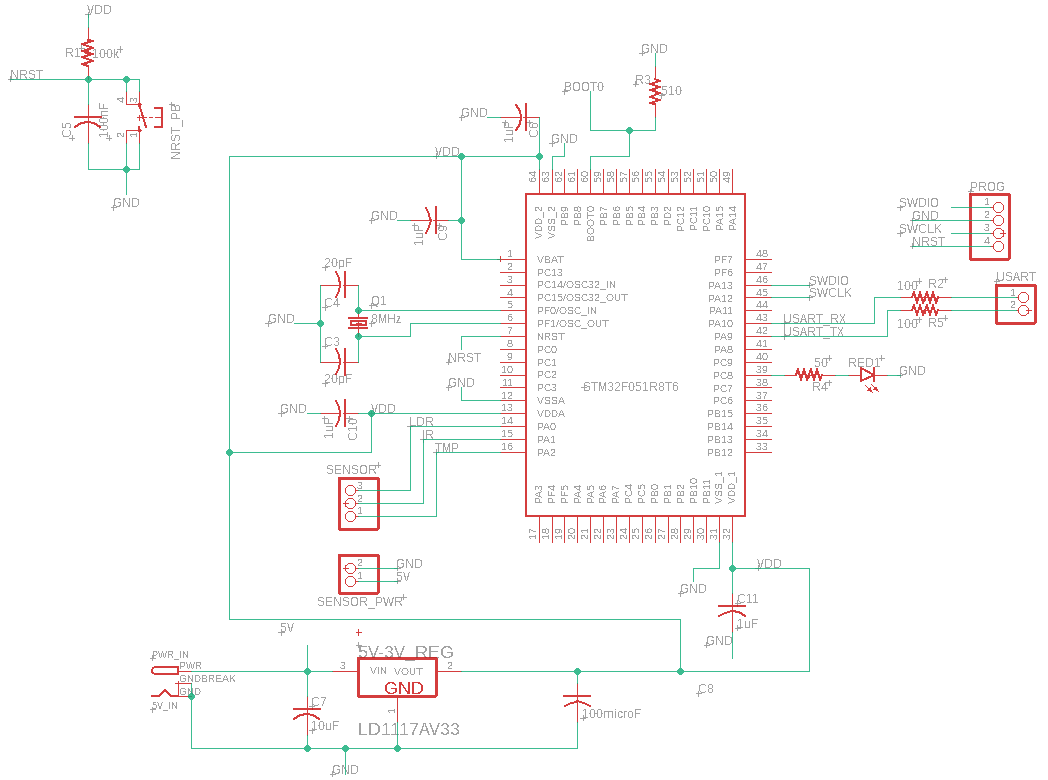
[1] Snebulos.mit.edu, 2019. [Online]. Available: https://snebulos.mit.edu/projects/reference/MIL-STD/MIL-HDBK-217F-Notice2.pdf. [Accessed: 02- Nov- 2019].

[2] St.com, 2019. [Online]. Available: https://www.st.com/resource/en/datasheet/stm32f051c4.pdf. [Accessed: 02- Nov- 2019].

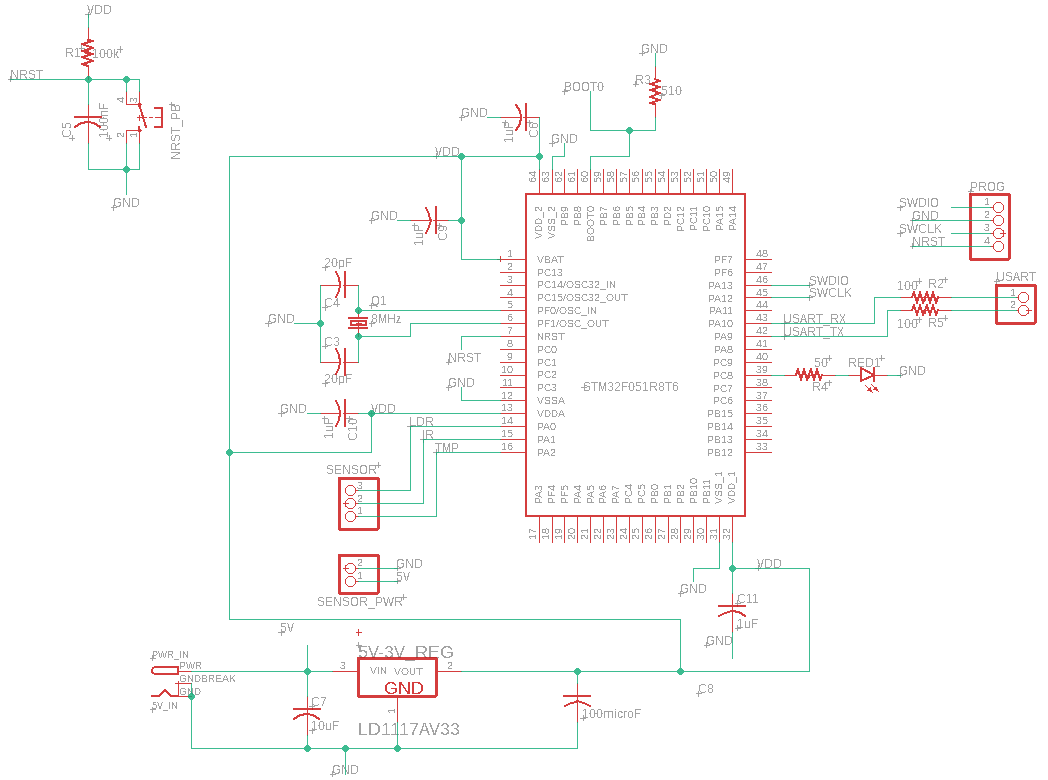
[3] "Jetson Nano Developer Kit", NVIDIA Developer, 2019. [Online]. Available: https://developer.nvidia.com/embedded/jetson-nano-developer-kit. [Accessed: 02- Nov- 2019].

[4] "LD1117AV33 STMicroelectronics | Mouser", Mouser Electronics, 2019. [Online]. Available: https://www.mouser.com/ProductDetail/STMicroelectronics/LD1117AV33?qs=hUhhBvpTJN9Rfx8G8TXH1A%3D%3D. [Accessed: 02- Nov- 2019].

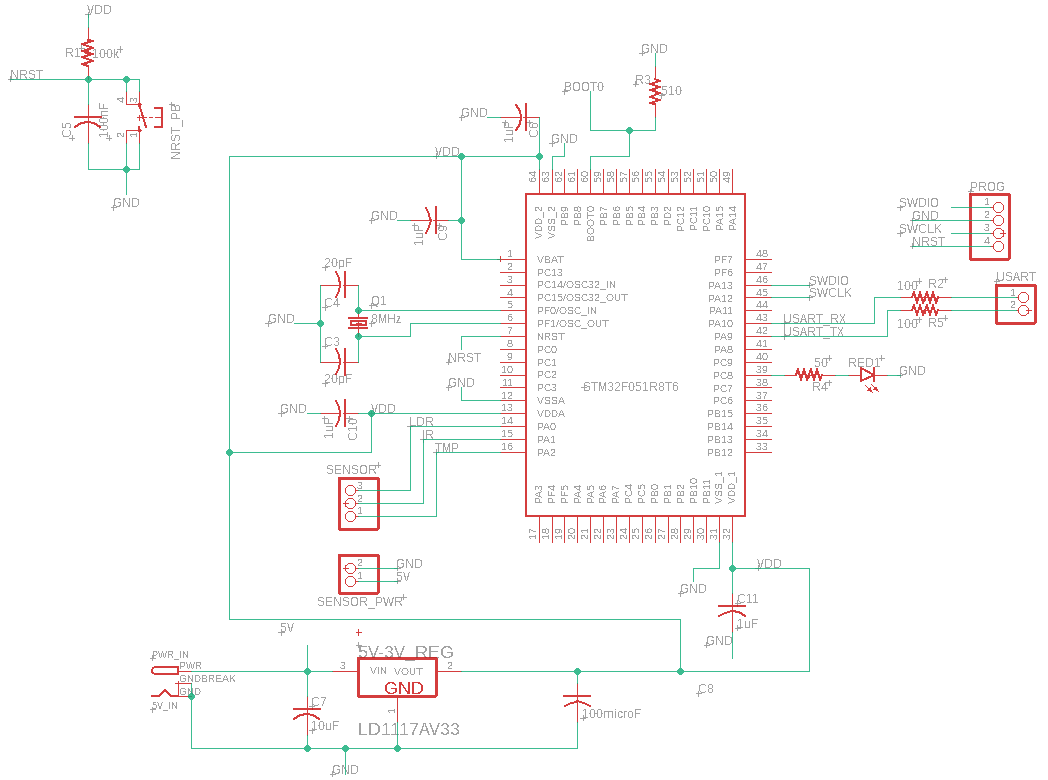
Appendix A: Schematic Functional Blocks



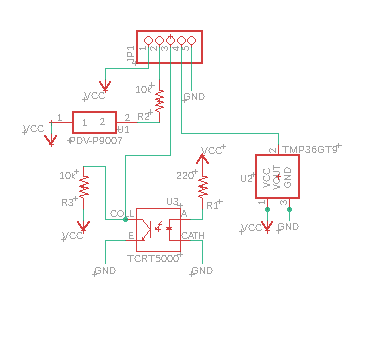
*Subsystem 1. Barrel Jack Power Connector and Power Regulator*



*Subsystem 2. STM32F0 Microchip*



*Subsystem 3. NRST Circuit*



*Subsystem 4. Sensor Board*

Appendix B: FMECA Worksheet

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 1.1 | No supply voltage (12V) | Damaged barrel jack connector | Main board and sensors have no power, LED indicators off | Observation of microchip inactivity | Low | No damage |
| 1.2 | Incorrect 5V Vin | Switching regulator failed | Sensors and microchip may get damaged | Observation | Medium | May cause power regulator to fail |
| 1.3 | Incorrect 3.3V Vout | LDO failed | Sensors and microchip may get damaged | Observation | Medium | May damage other components |
| 1.4 | High supply voltage (>12V) | Damaged wall adapter | Board will get damaged and components may smoke up | Observation of smoke or hot components | High |  |

*Subsystem 1. Barrel Jack Power Connector and Power Regulator*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 2.1 | Microchip stops running code | Incorrect power supplied or software is wrongly flashed | No executable instructions. | Observation | Low |  |
| 2.2 | Not able to boot microchip | BOOT0 not pulled low, resistor damage or insufficient power | MCU cannot boot up | Observation | Low |  |
| 2.3 | Reset Triggered | Stuck push button or damaged decoupling capacitor | Continuous reboot of microchip | Observation of erratic MCU behavior | Low |  |
| 2.4 | Non functional microchip pins | Static damage or physical damage | Loss of functionality of PCB | Observation of faulty functionality | Low |  |
| 2.5 | Not able to flash microchip | Insufficient power or damaged SWD headers | Microchip cannot be programmed | Observation of absent program activity | Low | Need to consider alternative programming  methods |
| 2.6 | Noisy analog sensor data | Dysfunctional RC filter or incorrect ADC | Unuseable sensor readings | Observation of noisy data | Low |  |
| 2.7 | No sensor data on dashboard | Damaged UART connector or low power | No sensor data for user to read | Observation of absent readings | Low |  |

*Subsystem 2. STM32F0 Microcontroller Chip*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 3.1 | Reset always asserted | Damaged push button | MCU cannot run program | Observation | Low | Button will need to be removed |
| 3.2 | Reset never asserted | Shorted capacitor | MCU can never reset | Observation | Low |  |

*Subsystem 3. NRST Circuit*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 4.1 | Inactive sensors | Insufficient power available to board | Inability to display sensor data on dashboard | Observation of volatile serial input | Low |  |
| 4.2 | Erratic light sensor data | Damaged sensor or insufficient power | Dashboard brightness will fluctuate | Observation of volatile serial input | Low | Replace sensor |
| 4.3 | Erratic IR data | Damaged sensor or insufficient power | System will toggle between wake and sleep state | Observation of volatile serial input | Medium | Replace sensor |
| 4.4 | Incorrect temperature data | Damaged sensor or insufficient power | Dashboard will display incorrect temperature | Observation of incorrect serial input | Low | Replace sensor |

*Subsystem 4. Sensor Board*