A10 - Reliability and Safety Analysis

Year: 2023 Semester: Fall Team: 5 Project: Smart Air Hockey Table

Creation Date: October 30, 2023 Last Modified: November 4, 2023

Author: Ben Owen Email: owen67@purdue.edu

1. Reliability Analysis

In this design, the components most likely to fail are the STM32U575 microcontroller, the DRV5033 hall effect sensors, the WS2812B individually-addressable LEDs, and the 1TDP7 centrifugal blower. The STM32U575 was selected because it is connected to most external devices, and is constantly in operation during use. The DRV5033 hall effect sensors were chosen due to the number (512) present in our design, as well as their constant operation switching between different logic outputs. The WS2812 LEDs were chosen due to the number (512) present in our design, as well as the constant data processing and heat generation they will be subject to. Lastly, the 1TDP7 blower was chosen due to the constant operation, high power consumption, and moving parts present.

The models used to calculate the failure rate and mean time to failure (MTTF) of the various electronic components evaluated was found in the Military Handbook for Reliability Prediction of Electronic Equipment (MIL-HDBK-217F) [1]

For our digital logic-based devices, the following equations are used:

For our motor, different equations are used:

For our LEDs, different equations are used:

For all equations, units for λp are in failures/106 hours and units for MTTF are in years, respectively.

From these equations, several of the coefficients are constant for analysis of all the electronic parts listed. The learning factor, πL, is set to 1.0 as all of our components have been in production for at least two years (according to their respective datasheets) [2, 3, 4, 5]. The quality factor, πQ, is set to 10 (for all components except the LEDs), as all of our components are consumer/commercial grade, and are not military rated. The environmental factor, πE, is set to 2.0, as our design falls under the “Ground, Fixed” environment, as the table is not in a completely controlled environment, but is also not subject to constant movement.

**1.1 STM32U575 Reliability Analysis**

For our microcontroller, the remaining coefficients are determined from the military handbook. For C1, the die complexity failure rate, the value is 0.56. This is a result of the STM32U575 being a 32-bit MOS microprocessor [2]. Furthermore, the temperature factor, πT, was set to 0.98. This is a result of the microcontroller supporting a maximum junction temperature of 85℃. Lastly, for package failure rate, C2, the value was 0.052. This was calculated as a result of the microcontroller being a nonhermetic 100-pin SMT device. All other coefficients were already determined earlier.

**STM32U575 Microcontroller** [2]

|  |  |  |  |
| --- | --- | --- | --- |
| **Parameter name** | **Description** | **Value** | **Comments** |
| C1 | Die complexity failure rate | 0.56 | 32-bit MOS microprocessor |
| πT | Temperature factor | 0.98 | Max junction temperature of 85℃ |
| C2 | Package failure rate | 0.052 | Nonhermetic 100-pin package |
| πE | Environment factor | 2.0 | Ground, fixed |
| πQ | Quality factor | 10 | Commercial-grade |
| πL | Learning factor | 1.0 | >2 years old |
| λp | Failure rate per million hours | 6.528 |  |
| **MTTF** | Mean time to failure | 17.487 years |  |

**Table 1: STM32U575 reliability analysis**

**1.2 DRV5033 Reliability Analysis**

Texas Instruments provides reliability characteristics for many of their devices. For the DRV5033, they offer a mean time between failures (MTBF) of 7.47E9 [4]. Based on their comments, this is a result of testing over 87,000 devices for a period of 1,000 hours [4, 5]. This value is equivalent to a MTTF of 855,000 years.

For our implementation, however, we also must consider the 512 sensors used. This results in a MTTF of closer to 1,670 years.

**1.3 WS2812B Reliability Analysis**

Due to the fact that these LEDs are essentially just 3 LEDs combined with a microcontroller, we will consider MTTF for both aspects independently.

For the LEDs, the remaining coefficients are determined from the military handbook. For λb, the base failure rate, a value of 0.0013 was chosen for “Light Emitting Diode” (LED). For πT, the temperature coefficient, a value of 4.3 was chosen due to the maximum junction temperature of 80°C. For πQ, the quality factor, we do not use the same chart as the other components. We instead choose a value of 8.0, as our package is plastic. This is different from the other devices which focused on consumer/military rating instead.

**WS2812B LED** [6] (LED analysis)

|  |  |  |  |
| --- | --- | --- | --- |
| **Parameter name** | **Description** | **Value** | **Comments** |
| λb | Base failure rate | 0.0013 | LED |
| πT | Temperature factor | 4.3 | Max junction temperature of 80°C |
| πQ | Quality factor | 8.0 | Plastic |
| πE | Environment factor | 2.0 | Ground, fixed |
| λp | Failure rate per million hours | 0.26832 | Accounted for 3 LEDs per component |
| **MTTF** | Mean time to failure | 425.44 years | Accounted for 512 total LEDs present |

**Table 2: WS2812B LED reliability analysis**

For the microcontroller part of the LEDs, the remaining coefficients are determined from the military handbook. For C1, the die complexity failure rate, the value is 0.14. Since we don’t know the exact number of gates present in the device, we instead consider it an 8-bit microcontroller. This is due to the fact that each LED color can handle 8-bit resolution [6]. Furthermore, the temperature factor, πT, was set to 0.98. This is a result of the microcontroller supporting a maximum junction temperature of 85℃. Lastly, for package failure rate, C2, the value was 0.00249. This was calculated as a result of the microcontroller being a nonhermetic 6-pin SMT device. All other coefficients were already determined earlier.

**WS2812B LED** [6] (Microcontroller analysis)

|  |  |  |  |
| --- | --- | --- | --- |
| **Parameter name** | **Description** | **Value** | **Comments** |
| C1 | Die complexity failure rate | 0.14 | 8-bit MOS microprocessor |
| πT | Temperature factor | 0.98 | Max junction temperature of 85℃ |
| C2 | Package failure rate | 0.00249 | Nonhermetic 6-pin package |
| πE | Environment factor | 2.0 | Ground, fixed |
| πQ | Quality factor | 10 | Commercial-grade |
| πL | Learning factor | 1.0 | >2 years old |
| λp | Failure rate per million hours | 1.4218 |  |
| **MTTF** | Mean time to failure | 80.29 years |  |

**Table 3: WS2812B microcontroller reliability analysis**

**1.4 1TDP7 Reliability Analysis**

For the motor, the remaining coefficients are determined from the military handbook. For A and B, constants based on the motor type, values of 1.9 and 1.1 were chosen, respectively. This is due to the fact that the motor falls under the “Electrical (General)” motor type. For LC, the life cycle of the motor, we chose one year (8760 hours), due to the length of the manufacturer warranty. For αB and αW, the bearing and winding characteristic life (respectively), the values were set to 7.8E4 and 8.9E5 hours (respectively). This is based on an estimated ambient temperature of 30°C, which is higher than typical room temperature to account for generated heat of other nearby components.

From these values, λ1 and λ2 can be determined based on the following calculations:

,

Using the calculated values of x and y, λ1 is found to be 0.15, and λ2 is found to be 0.13. These values are simply the result of a lookup table found in the handbook. Finally, the final failure rate can be calculated.

**1TDP7 Motor** [7]

|  |  |  |  |
| --- | --- | --- | --- |
| **Parameter name** | **Description** | **Value** | **Comments** |
| A | Constant | 1.9 | General motor |
| B | Constant | 1.1 | General motor |
| LC | Life cycle (hours) | 8,760 | 1 year mfg. warranty |
| αB | Bearing characteristic life | 78,000 | 30°C ambient temperature |
| αW | Winding characteristic life | 890,000 | 30°C ambient temperature |
| λ1 | Intermediate constant | 0.15 | Lookup table |
| λ2 | Intermediate constant | 0.13 | Lookup table |
| λp | Failure rateper million hours | 1.145 |  |
| **MTTF** | Mean time to failure | 99.7 years |  |

**Table 4: 1TDP7 reliability analysis**

**1.5 Reliability Analysis Summary**

All components considered have a failure rate in the same order of magnitude, and the earliest MTTF calculated was over 17 years (STM32 microcontroller). Since this system is still a prototype-level product, higher failure rates are acceptable. Even considering this fact, the evaluated components have a very low failure rate. To improve the reliability of the design, a simpler microcontroller could be considered. It is likely possible to design the firmware around an 8- or 16-bit microcontroller, allowing for more reliable part selection. Since this component was the most unreliable during analysis, this would most increase the overall reliability of our device. This may also have the added benefit of a lower cost, as simpler microcontrollers are typically cheaper.

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

The master PCB schematic can be divided into 8 sections, and the sensor PCB can be divided into 3 sections. For the master PCB, these sections include the power supply, microcontroller, encoder, LED level shifters, EEPROM, OLED displays, goal detection, and ESD protection. For the sensor PCB, these sections are LEDs, hall effect sensors, and digital logic propagation.

In addition to the PCBs, there is an externally-powered motor. This is directly connected to 120V logic. There isn’t a schematic for this design, as the only interfacing is turning the motor on and off, but it will be mentioned in the criticality analysis.

The power supply for the master PCB is very simple. We take a 5V supply and use a buck converter to drop down to 3.3V. Although a buck converter is more complex than an LDO, the design pulls very low current, so heat dissipation and reliability shouldn’t be a concern. The possible failures for this schematic is a failed buck converter or failed passives. Either of these could result in a lower output voltage (buck converter output not connected correctly) or a higher output voltage (output shorted to input). Both of these will cause a failure in the operation of the device. A higher output voltage will damage the microcontroller (medium criticality), while a lower output voltage will not damage anything (low criticality).

The microcontroller, although connected to many things, is actually very simple. It simply is connected to external sensors and devices such as OLED displays and an EEPROM. Although these devices can still fail, microcontroller-related failures are relatively harmless. The most common failures would be a failed decoupling capacitor, leading to unstable power supply voltages (low criticality). Additionally, the external oscillator could fail, but since our design utilizes the internal oscillator, this is also a low criticality failure. If the microcontroller itself fails, this could lead to an unplayable device, which is a medium criticality failure.

The menu encoder is very simple. It is connected directly to timer pins on the microcontroller. The only failure that could occur would be mechanical. This could include a disconnection to the PCB (low criticality), or physical damage to the encoder. Since physical damage would result in an inability to interact with the software menu system, this would fall under medium-criticality.

The LED level shifters are also simple. Utilizing purely analog components, they shouldn’t fail completely at a given moment in time. Possible failures include MOSFET failure, which would result in an inability to communicate correctly with the sensor PCB LEDs. Because the game should still operate, this failure is of low criticality.

The onboard EEPROM is also simple. It is directly connected to the microcontroller SPI lanes. Although reliable due to little use, a failed decoupling capacitor could cause the device to stop working. However, our system relies very little on this component, so this failure would only be considered low criticality.

The OLED displays are also relatively simple. These are simply connected to the microcontroller through ESD-protected SPI lanes. An ESD failure to the OLED displays would be a low-level failure, as the table should still work almost entirely. Additional sources of failure include a connector disconnect between the PCB and the display, resulting in no output. This is a low-criticality failure, since no permanent damage should occur to any component.

The goal detection circuit is more complex, since it is an analog device. However, the components involved are very simple, only using an LED, LDR, and comparator. Possible failures would be mechanical failure to the LED/LDR pair due to the puck. This is mitigated with redundant LED/LDR pairs, but this failure would fall under either low- or medium-criticality, depending on if the redundant pair is still working. Another failure would include a failure of a passive component connected to the comparator. This could lead to incorrect goal detection. Since this would affect the majority of gameplay, this would fall under a medium-criticality failure.

The ESD protection is completely passive. If they fail, it will simply increase the risk of other failures for various components. Because of this, these failures would be low criticality. Since there are no passives connected to these protection chips, the only failure would be internal failures.

For the sensor PCB sections, the reliability is increased by the fact that these boards were pre-assembled. This reduces the likelihood of failure due to poor soldering, heat exposure, or other common prototype-related reasons.

On the sensor PCB, LED failures are similar to the master PCB level shifter failures. If a decoupling capacitor fails short, these will be unable to work or transmit data to other LEDs, resulting in no under-table lighting. However, the game will still operate, so this is a low criticality failure.

The hall effect sensors are very simple, and the MTBF mentioned earlier is the highest of any component analyzed. The only source of failure other than internal failures would be a shorted decoupling capacitor. Likely, this would result in the hall effect sensor no longer working, which would cause indeterminate behavior. However, due to the digital logic aspect of these boards, this shouldn’t completely break the gameplay aspect of the device, so this is only a low criticality failure.

The digital logic gates on the sensor PCBs are also simple, only consisting of a few AND gates. Similar to the previous components, the only risk of external failure is a shorted decoupling capacitor. This would result in indeterminate behavior, likely not working. However, the other sensors and gates should allow for relatively normal gameplay, resulting in a low criticality failure.

Finally, the motor controls the airflow to the table. Failures would likely be due to power/heat issues, or failure of the power cables going to the motor. This failure is unlikely to happen due to the simplicity of the design. However, a shorted power cable could lead to massive power draw. This could result in failure of the motor, and, in the worst case, a possible fire hazard. This is a high-criticality failure, but should almost never happen. Likely, a fuse would trip in the power relay or source power circuit breaker before this would occur. Additionally, the chassis of the motor is grounded, further reducing the risk of this event.

**2.1 Levels of Criticality**

The levels of criticality defined will include “low,” “medium,” and “high.”

A criticality level of “low” means that although normal operation of the device may be disrupted, no cascading damage to other components or to the user will occur. This would include failures such as sensors reporting incorrect data or a loss of power to a component. These failures should have a failure rate of less than 10-6.

A criticality level of “medium” means that critical functions of the device will not work, and some components may be permanently damaged. However, the user would still be at no risk of harm. These failures would include overvoltage to electronic components or soldered components falling off due to vibration. These failures should have a failure rate of less than or equal to 10-6.

A criticality level of “high” means that significant damage to the device or harm to the user may occur. These failures include components catching on fire, or mechanical parts being ejected from their mounting points. These failures should almost never happen, and should have a failure rate of less than or equal to 10-9.

3.0 Sources Cited:

[1] Department of Defense. *Reliability Prediction of Electronic Equipment (MIL-HDBK-217F)*. Available: <https://s3vi.ndc.nasa.gov/ssri-kb/static/resources/MIL-HDBK-217F-Notice2.pdf> (accessed Nov. 4, 2023).

[2] STMicroelectronics, *Ultra-low-power with FPU Arm Cortex-M33 MCU with TrustZone, 160 MHz with 2 Mbytes of Flash memory*. Available: <https://www.st.com/en/microcontrollers-microprocessors/stm32u575vi.html> (accessed Nov. 4, 2023).

[3] Texas Instruments. *DRV5033 Digital-Omnipolar-Switch Hall Effect Sensor*. Available: <https://www.ti.com/lit/gpn/drv5033> (accessed Nov. 4, 2023).

[4] Texas Instruments. *Quality, reliability & packaging data download*. Available: <https://www.ti.com/quality-reliability-packaging-download/report?opn=DRV5033FAQDBZR> (accessed Nov. 4, 2023).

[5] Texas Instruments. *Reliability testing*. Available: <https://www.ti.com/support-quality/reliability/reliability-testing.html> (accessed Nov. 4, 2023).

[6] Worldsemi. *WS2812 Intelligent control LED integrated light source*. Available: <https://cdn-shop.adafruit.com/datasheets/WS2812.pdf> (accessed Nov. 4, 2023).

[7] Dayton. *Technical Specification 1TDP5\_TSREV0.DOC*. Available: <https://images-na.ssl-images-amazon.com/images/I/917ulOFWuWL.pdf> (accessed Nov. 4, 2023).

Appendix A: Schematic Functional Blocks



Figure 1: Power supply circuit



Figure 2: Microcontroller circuit



Figure 3: Encoder circuit



Figure 4: LED level shifter circuit



**Figure 5: EEPROM circuit**



Figure 6: OLED display circuit



Figure 7: Goal detection circuit



Figure 8: ESD protection circuit



Figure 9: LED circuit



Figure 10: Hall effect sensor circuit



Figure 11: Digital logic propagation circuit

Appendix B: FMECA Worksheet

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 1 | Voltage drop | C13, C14, R4, R5 | Low output voltage on 3.3V rail | Observation, unresponsive device | Low |  |
| 2 | Output voltage short | U3 | 5V present on 3.3V rail | Observation, unresponsive device | Medium | May cause irreparable damage to microcontroller |

Table 5: Power supply circuit FMECA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 3 | Reset button failure | C1, R2, SW1 | Microcontroller stuck in reset state | Observation, unresponsive device | Low |  |
| 4 | BOOT0 jumper failure | R1, JP1 | Microcontroller stuck in bootloader | Observation, unresponsive device | Low |  |
| 5 | Oscillator failure | U5, C22 | No external oscillator | None | Low | If firmware stays consistent, this component has no effect on operation |
| 6 | Input power voltage drop | C3, C4, C5, C6, C7, C8, C9, C10, C11, C12, C21 | Low input voltage | Observation, unresponsive device | Low |  |

Table 6: Microcontroller circuit FMECA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 7 | Encoder connector disconnect | SW2 | No input from encoder | Observation, unresponsive device | Low | Can be fixed by end-user |
| 8 | Encoder physical damage | Repeated use, physical trauma | No input from encoder | Observation, unresponsive device | Medium | Lose ability to interact with menu until part replaced |

Table 7: Encoder circuit FMECA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 9 | No output voltage | Q1, Q2, Q3, Q4 | No valid output to LEDs | Observation, no LED output | Low | Won’t affect game functionality |

Table 8: LED level shifter circuit FMECA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 10 | Display connector disconnect | J15, J16 | No output on display | Observation, no output | Low | Can be fixed by end-user |
| 11 | Display physical damage | ESD, physical trauma | No output on display | Observation, no output | Low | Table can still work normally |

Table 9: OLED display circuit FMECA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 12 | Connector disconnect | J5, J6, J7, J8, J9, J10, J11, J12 | Incorrect goal detection | Observation, incorrect game operation | Medium | Can be fixed by end-user, but will affect core functionality until fixed |
| 13 | LED/LDR failure | LED/LDR pairs | Incorrect goal detection | Observation, incorrect game operation | Medium |  |
| 14 | Comparator voltage supply drop | C20 | Incorrect goal detection | Observation, incorrect game operation | Medium |  |

Table 10: Goal detection circuit FMECA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 15 | Internal failure | U6, U7, U8 | Higher risk of failure due to ESD |  | Low | Will not affect anything at time of failure, but will increase future failures |

Table 11: ESD protection circuit FMECA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 16 | Input voltage supply drop | D1, D2, D3, D4 | No LED output | Observation, no LED output | Low | Won’t affect game functionality |

Table 12: LED circuit FMECA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 17 | Input voltage supply drop | C3, C4, C5, C6 | Incorrect puck detection | Observation, incorrect LED display | Low | Won’t affect core game functionality |

Table 13: Hall effect sensor circuit FMECA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 18 | Input voltage supply drop | C1, C2 | Incorrect puck detection | Observation, incorrect LED display | Low | Won’t affect core game functionality |

Table 14: Digital logic propagation circuit FMECA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 19 | Input voltage supply drop | 120 VAC relay | No airflow | Observation | Medium | Game will work, but without air, core functionality is lost |
| 20 | Input voltage short circuit | Poor motor wire insulation, poor assembly, loose wire connections | Motor damage | Observation, circuit breaker | High | In the worst case (no circuit breaker), this could lead to excessive power draw and potential fire risk |

Table 15: Motor circuit FMECA