A10 - Reliability and Safety Analysis

Year: 2023 Semester: Fall Team: 16 Project: Air Hockey Robot

Creation Date: ­November 3, 2023 Last Modified: November 4, 2023

Author: Cameron McCutcheon Email: mccutchc@purdue.edu

1. Reliability Analysis

The components being analyzed are as follows:

* DM542T Stepper Motor Driver
  + Carries all current to and from each motor. High operating temperature associated with rapid, high current switching.
* NEMA 23 Stepper Motors
  + Each motor burns up to ~60W of power at max speed. High operating temperatures associated with rapid high current switching.
* STM32 Microcontroller
  + Complex IC w/ minimal heat ventilation
* AMS1117 5 to 3.3V LDO
  + Power supply for the microcontroller + most off-PCB peripherals. Although operating with near ideal input (5V), heat generation is inevitable for this component.

Model and Assumptions:

The model for failure rate per 106 hours and the mean time to failure (MTTF) come from the MIL-HDBK-217F handbook.

λP = (C1 x πT + C2 x πE) x πQ x πL

MTTF = 106/λP hours = 106/(λP \* 24 \* 365) years

Parameters constant across each component (and therefore excluded from the tables below) are: πE, πQ, πL. πE, the environmental constant, is fixed at 2.0 due to the constant environment each component is in (moderate airflow, uniform temperature, static position). πQ, the quality factor constant, is fixed at 10 for all commercial components as outlined in the MIL-HDBK-217F handbook. πL, the learning factor constant, is fixed at 1 as all components have been in production for more than 2 years.

Variable parameters are set and justified in the table below. All referenced documents are available on the course website.

|  |  |  |  |
| --- | --- | --- | --- |
| **Component:** STM32 Microcontroller | | | |
| **Parameter** | Description | Value | Justification |
| C1 | Die complexity coefficient | 0.56 | STM32 is a 32bit, CMOS-based microcontroller. From page 25 of 217F this yields a C1 die complexity rate of 0.56. |
| πT | Temperature Coefficient. | 1.8 | Assuming the temperature for the microcontroller is at absolute max of 105C. High assumption but this is the max junction operating temperature of the microcontroller. See page 35 of 217F and table 24 in the STM documentation. |
| **C2** | Pin constant/Package failure rate constant | .025 | The stm32f091 has 64 pins with the package type we have chosen. From the 217F handbook, this yields a coefficient of .025. See page 36 (of 205) |
| Constant Coefficients: πE = 2.0, πQ = 10, πL = 1 | | | |
| λP | Predicted number of failures per 106 hours | 10.58 | This number is quite high. Assumptions that the microcontroller is at absolute max and that the commercial quality is so low increase this number significantly. |
| MTTF | Mean Time to Failure (Hours) | 94517.95 = 10.79 years | Under worst case operating conditions, it would take just 10 years for the micro to fail. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Component:** DM542T Stepper Motor Driver | | | |
| **Parameter** | Description | Value | Justification |
| C1 | Die complexity coefficient | 0.14 | DM542T has an 8-bit microprocessor controlling the driver. Value from page 25 of 217F handbook. |
| πT | Temperature Coefficient. | 0.50 | Assuming the temperature is at absolute max of 65C. See page 35 of 217F and page 4 in the driver documentation. |
| **C2** | Pin constant/Package failure rate constant | .0048 | 14 pins accepting GPIO w/ external current driving elements. This value may need to be higher to accommodate the external transistors used to drive stepper currents. |
| Constant Coefficients: πE = 2.0, πQ = 10, πL = 1 | | | |
| λP | Predicted number of failures per 106 hours | .796 | DM542T is not a concern for failure in a reasonable time period. |
| MTTF | Mean Time to Failure (Hours) | 1256281.4 =  143.11 years |

|  |  |  |  |
| --- | --- | --- | --- |
| **Component:** AMS1117 | | | |
| **Parameter** | Description | Value | Justification |
| C1 | Die complexity coefficient | 0.02 | Based on 217F for components with 100 to 300 bipolar transistors. |
| πT | Temperature Coefficient. | 3.1 | Assuming the temperature is at absolute max of 125C for p-channel MOSFET transistors. See page 35 of 217F and page 4 in the driver documentation. |
| **C2** | Pin constant/Package failure rate constant | .0013 | 4 Functional pins. See page 36 of 217F. |
| Constant Coefficients: πE = 2.0, πQ = 10, πL = 1 | | | |
| λP | Predicted number of failures per 106 hours | .646 | The LDO is not a concern for failure over a reasonable time period. |
| MTTF | Mean Time to Failure (Hours) | 1547987.61 =  176.71 years |

\*This section uses a different equation for failure rate calculation:

λP = λB \*πS \*πN\*πE

|  |  |  |  |
| --- | --- | --- | --- |
| **Component:** NEMA23 Stepper Motors | | | |
| **Parameter** | Description | Value | Justification |
| πS | Die complexity coefficient | 1.5 | Larger than size 18 with resolver windings. |
| λB | Temperature Coefficient. | .74 | Assuming worst case internal temperature of 130C. |
| πN | Number of brushes factor | 1 | 217F was written before brushless motors were common. Assuming 1 as no brushes. |
| πE | Environment Factor | 1 | Assuming static environment at room temp. See page 150 for details on all parameters |
| λP | Predicted number of failures per 106 hours | 1.11 | Motors are very reliable and long-lived. No failure concerns under normal usage. |
| MTTF | Mean Time to Failure (Years) | 102.8425 |

Reliability Analysis:

Overall, the system seems to be very reliable in the long term. The core assumptions made for the shortest lived element, the microcontroller, should not reflect the reality of the system. Assuming an operating temperature of 105C and a commercial quality factor of 10 is simply not representative of reality. In actuality, the operating temperature for all on-PCB components will likely not exceed 70C in worst-case conditions.

That being said, preserving the longevity of the system would potentially be as simple as adding additional cooling for the PCB and DM542T. Should this system be produced in greater volume, airflow to the surface of the table could be redirected to cool these systems (doing so would even increase the fluidity of the game, as hotter air yields better motion).

Furthermore, as it is likely only one of these systems will be produced, it is unnecessary to have a very low failure rate. With only one system in existence with a minimal operating period, failure rates in the electrical systems likely won’t be a concern. Rather, the mechanical systems are likely to be the source of the greatest failure.

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

Acceptable risk Levels:

* 10-6: Average Risk. Cases where users have minimal to no chance of injury.
* 10-7: Above Average Risk. Cases where it is unlikely but possible to have user injury
* 10-9: High Risk. Cases where user injury is likely in this failure case.
* 10-10: Extreme Risk. Cases where user injury and large damage possible with failure.

System Divisions:

To give a better idea of the system diagram for this project, I have attached a more readable version as appendix C.

FMECA Analysis

* Subsystem A: Power Distribution
  + Failure Condition 1: 5V Supply failure
    - Effect 1: 5 to 3.3V LDO will fail. Power across most of the PCB will fail. May present as brown out condition.
    - Effect 2: 3.3V to 5V logic IC’s will fail. As these IC’s are supplied by the 5V, the logic translation (if 3.3V logic is still being sent given the micro runs on the 5V translated to 3.3V) will fail. May present as unpredictable motion by the motors.
    - Potential Causes:
      * Shorted barrel jack. Will present as significant hot spot on the board.
      * Failed 5V wall wart supply. No present failure conditions on PCB
    - Acceptable Risk Level: 10-7. It is unlikely for a 5V drop to cause the motors to move due to the control logic of the motor controllers. However, as there is still potential for injury this must be better-than-average failure rate.
  + Failure Condition 2: 5 to 3.3V LDO Failure
    - Effect 1: Power across most of PCB will fail. May present as brown out condition.
    - Effect 2: May damage microcontroller if highly variant voltages are generated.
    - Potential Causes:
      * Broken LDO. Likely to cause damage to microcontroller and other IC’s running on 3.3V supply.
      * Shorted Bypass capacitor. From experience, this will cause a highly time variant voltage of varying magnitude.
    - Acceptable Risk Level: 10-7. It is unlikely for a 3.3V drop to cause the motors to move due to the control logic of the motor controllers. However, as there is still potential for injury this must be better-than-average failure rate.
  + Failure Condition 3: 24V Supply Failure (Not shown in appendix A as not on board)
    - Effect 1: Motor failure. The DM542 will fail and the motors will not move.
    - Potential Causes: Internal elements on the 24V supply or motor controllers fail.
    - Acceptable Risk Level: 10-9. There is potential here for the motor to move unpredictably through brown out conditions. User injury is high and thus must be very low failure rate.
* Subsystem B: External Sensors/UI
  + Failure Condition 1: Camera Failure
    - Effect 1: Puck detection failure
    - Effect 2: PC stops sending data to microcontroller.
    - **Potential Causes:** Camera failure, software failure, camera connector failure.
    - **Acceptable Risk Level: 10-6.** The microcontroller is designed to hold current position if data is no longer sent. Low probability of user injury therefore high probability of failure accepted.
  + Failure Condition 2: General Sensors
    - Effect 1: Goal Detection Failure
    - Effect 2: Game Control Failure
    - **Potential Causes:** Sensor Failure, microcontroller software failure, sensor connector failure.
    - **Acceptable Risk Level: 10-6.** Failure of game state does not present significant change of injury therefore high levels of risk acceptable.
  + Failure Condition 3: Limit Switch Failure
    - Effect 1: Gantry System attempting to move past established limits.
    - **Potential Causes:** Limit switch, limit switch connections, or microcontroller detection of limit switches fail.
    - Acceptable Risk Level: 10-9. There is potential here for the motor to move unpredictably. User injury is high and thus must be very low failure rate.
* Subsystem C: Microcontroller + Other IC’s
  + Failure Condition 1: Dead microcontroller
    - Effect 1: No control signals sent to external systems.
    - Effect 2: Potential short across pins. Hot spot on PCB.
    - **Potential Causes:** Shorted Pins, shorted bypass capacitor, burned silicon.
    - Acceptable Risk Level: 10-6. A dead micro will present no active control signals (in most cases) so it is acceptable to have higher risk.
  + Failure Condition 2: Dead translator IC’s
    - Effect 1: USB->UART communication disrupted. May present as unpredictable motor motion as a result of microcontroller receiving unpredictable signals.
    - Effect 2: Level translation failure. May present as brown out conditions and unpredictable off-PCB behavior
    - **Potential Causes:** Shorted Pins, shorted bypass capacitor, burned silicon.
    - Acceptable Risk Level: 10-7. It is unlikely these dead IC’s will produce active control signals for the motors. As it is possible, we must lower our acceptable risk slightly.
* Subsystem D: Motion Control + Drivers
  + Failure Condition 1: DM524T Failure (Not shown in appendix A)
    - Effect 1: Unpredictable motor motion.
    - Effect 2: High energy short. Will present as *significant* heat source.
    - **Potential Causes:** Failed wiring, burned silicon.
    - Acceptable Risk Level: 10-8. While it is unlikely a dead controller will produce active control signals, this condition still presents possibility of user injury and is therefore low risk accepted.
  + Failure Condition 2: Dead Stepper Motor
    - Effect 1: Unpredictable motor motion
    - Effect 2: High energy short. May cause fire.
    - **Potential Causes:** Failed internal wiring
    - Acceptable Risk Level: 10-10. A dead motor will burn massive amounts of current if allowed to. This must not be the case as a fire is likely. Very low risk accepted here.

Observation Techniques:

Hopefully most failures will be readily apparent to the user/engineer. In general, the on board debugging systems are enough to determine and fix potential sources of failure. For less visibly apparent failures, an oscilloscope will need to be used to find the exact points where signals break down.

3.0 Sources Cited:

DM542T full Datasheet Digital Stepper driver 1.0-4.2a ... - STEPPERONLINE. (n.d.-a). <https://www.omc-stepperonline.com/download/DM542T.pdf>

*NEMA 23 high temp stepper motor 1.85nm(256.9oz.in) insulation class H 180C*. Nema 23 Stepper Motor. (n.d.). <https://www.omc-stepperonline.com/nema-23-high-temp-stepper-motor-1-85nm-256-9oz-in-insulation-class-h-180c-23hs30-2804s-h>

Advanced Monolithic Systems. (n.d.-a). <http://www.advanced-monolithic.com/pdf/ds1117.pdf>

"MIL-HDBK-217F: Military Handbook - Reliability Prediction of Electronic Equipment," U.S. Department of Defense, Nov. 1991.

"STM32F091xC, STM32F091xD, STM32F091xE Datasheet," STMicroelectronics, Jan. 2022.

Appendix A: Schematic Functional Blocks

Subsystem A: Power Distribution

A screenshot of a computer

Description automatically generated

Subsystem B: External Sensors/ UI

A screenshot of a computer

Description automatically generated

Subsystem C: Microcontroller + other IC’s

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated A diagram of a circuit board

Description automatically generated

Appendix B: FMECA Worksheet

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| A1 | 5V Supply failure | Shorted barrel jack. Will present as significant hot spot on the board.  Failed 5V wall wart supply. No present failure conditions on PCB | Effect 1: 5 to 3.3V LDO will fail. Power across most of the PCB will fail. May present as brown out condition.  Effect 2: 3.3V to 5V logic IC’s will fail. As these IC’s are supplied by the 5V, the logic translation (if 3.3V logic is still being sent given the micro runs on the 5V translated to 3.3V) will fail. May present as unpredictable motion by the motors. | Observation w/ scope or visible brown out conditions | 10-7 | It is unlikely for a 5V drop to cause the motors to move due to the control logic of the motor controllers. However, as there is still potential for injury this must be better-than-average failure rate. |
| A2 | 5 to 3.3V LDO Failure | Broken LDO. Likely to cause damage to microcontroller and other IC’s running on 3.3V supply.  Shorted Bypass capacitor. From experience, this will cause a highly time variant voltage of varying magnitude. | Effect 1: Power across most of PCB will fail. May present as brown out condition.  Effect 2: May damage microcontroller if highly variant voltages are generated. | Observation | 10-7 | It is unlikely for a 3.3V drop to cause the motors to move due to the control logic of the motor controllers. However, as there is still potential for injury this must be better-than-average failure rate. |
| A3 | 24V Supply Failure | Potential Causes: Internal elements on the 24V supply or motor controllers fail. | Effect 1: Motor failure. The DM542 will fail and the motors will not move. | Observation | 10-9 | There is potential here for the motor to move unpredictably through brown out conditions. User injury is high and thus must be very low failure rate. |

Subsystem B: External Sensors/UI

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| B1 | Camera Failure | Camera failure, software failure in powerpc, camera connector failure. | Effect 1: Puck detection failure  Effect 2: PC stops sending data to microcontroller. | Observation in powerPC | **10-6** | The microcontroller is designed to hold current position if data is no longer sent. Low probability of user injury |
| B2 | General Sensor failure | Sensor Failure, microcontroller software failure, sensor connector failure. | Effect 1: Goal Detection Failure  Effect 2: Game Control Button Failure  General loss of game function. | Observation | **10-6** | Failure of game state does not present significant change of injury therefore high levels of risk acceptable. |
| B3 | Limit Switch Failure | Limit switch failure, limit switch connections, or microcontroller detection of limit switches fail. | Effect 1: Gantry System attempting to move past established limits. | Observation | 10-9 | There is potential here for the motor to move unpredictably. User injury is high and thus must be very low failure rate |

Subsystem C: Microcontroller + other IC’s

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| C1 | Dead microcontroller | Shorted Pins, shorted bypass capacitor, burned silicon. | Effect 1: No control signals sent to external systems.  Effect 2: Potential short across pins. Hot spot on PCB. | Observation.  Thermal Imaging | 10-6 | A dead micro will present no active control signals (in most cases) so it is acceptable to have higher risk. |
| C2 | Dead translator IC’s | Shorted Pins, shorted bypass capacitor, burned silicon. | Effect 1: USB->UART communication disrupted. May present as unpredictable motor motion as a result of microcontroller receiving unpredictable signals.  Effect 2: Level translation failure. May present as brown out conditions and unpredictable off-PCB behavior | Observation  Thermal Imaging | 10-7 | It is unlikely these dead IC’s will produce active control signals for the motors. As it is possible, we must lower our acceptable risk slightly. |

Subsystem D: Motion Control + Drivers

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| D1 | DM524T Failure | Failed wiring, burned silicon. | Effect 1: Unpredictable motor motion.  Effect 2: High energy short. Will present as *significant* heat source. | Observation | 10-8 | While it is unlikely a dead controller will produce active control signals, this condition still presents possibility of user injury and is therefore low risk accepted |
| D2 | Dead Stepper Motor | Failed internal wiring | Effect 1: Unpredictable motor motion  Effect 2: High energy short. May cause fire. | Observation Maybe a fire. | 10-10 | A dead motor will burn massive amounts of current if allowed to. This must not be the case as a fire is likely. Very low risk accepted here. |

Appendix C:

A computer screen shot of a diagram

Description automatically generated