A10 - Reliability and Safety Analysis

Year: Spring 2025 Team: 15 Project: αCassiopeiae 8800

Creation Date: ­April 3, 2025 Last Modified: April , 2025

Author: Nathan Huang Email: huan1811@purdue.edu

Assignment Evaluation: See the Rubric in the Brightspace Assignment

1. Reliability Analysis

RP2350

The RP2350 was chosen because of its ubiquitous use in all our PCBs. We have over 20 of these chips, each completely controlling a separate system of the software, and we are essentially using all the pins in this microcontroller. Clearly, this microcontroller needs to function properly. The failure per hours ( and the mean time to failure were both calculated using the formulas outlined in MIL-HDBK-217F [1]. To calculate the mean-time failure, the digital CMOS IC microprocessor model was used. The formula used is as below:

After completing all the calculations as seen in the table below, it was determined that the MTTF and are within an acceptable range. A failure of the microcontroller would not cause serious harm to the user, just the IO pins and internal circuitry.

Table 1: Microcontroller Analysis

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter name | Description | Value | *Comments* |
| C1 | Die Complexity | *7.2* | Estimated for ARM Cortex-M0+ MCU. |
| C2 | Package Failure Rate |  | 48 Functional Pins |
| πT | Temperature Coefficient | *1.7* | At 40°C. |
| πQ | Quality Factor | *3.0* | Assumed commercial. |
| πE | Environment Factor | *1.0* | Ground benign. |
| πA | Device Application Factor | *1.0* | Low Noise and Power |
| πL | Learning Factor | *1.8* | .5 Years in Production |
| Entire design: | | | |
| λp | Failure Rate (F/10⁶ hrs) | 66.2 | λ = 0.5 × 1.7 × 3 × 1.0 |
| MTTF | Mean Time To Failure (hrs) | 15108 | MTTF = 1 / λ |

LM1117

The LM1117 is a low dropout linear voltage regulator used in the design to provide a regulated 3.3V rail. It is a critical component in the power delivery subsystem and typically operates above room temperature due to power dissipation. Its simplicity and thermal profile make it a likely candidate for long-term reliability analysis. The failure per hours ( and the mean time to failure were both calculated using the formulas outlined in MIL-HDBK-217F [1]. To calculate the mean-time failure, the CMOS Switch-mode regulator model was used. The formula used is as below:

After completing all the calculations as seen in the table below, it was determined that the MTTF and are within an acceptable range. A failure of the regulator would not cause serious harm to the user, because of how low the voltage is and the current limiter inside.

Table 2: Linear Regulator Analysis

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter name | Description | Value | *Comments* |
| C1 | Die Complexity | *0.015* | Low-complexity analog IC; standard value for linear regulators |
| πT | Temperature Coefficient | *1.7* | At an estimated operating temperature of 40°C |
| πQ | Quality Factor | *3.0* | Assumes standard commercial-grade component |
| πE | Environment Factor | *1.0* | Ground benign environment (MIL-HDBK-217F assumption) |
| Entire design: | | | |
| λp | Failure Rate (F/10⁶ hrs) | 0.0765 | λ = 0.5 × 1.7 × 3 × 1.0 |
| MTTF | Mean Time To Failure (hrs) | 13.07 | MTTF = 1 / λ |

MCP16331

The MCP16331 is a synchronous step-down DC-DC converter used to efficiently convert input voltage to 3.3V. Due to its internal switching transistor, control logic, and high-frequency operation, it generates more heat and is more complex than simple analog regulators, making it a strong candidate for failure analysis. The failure per hours ( and the mean time to failure were both calculated using the formulas outlined in MIL-HDBK-217F [1]. To calculate the mean-time failure, the CMOS Switch-mode regulator model was used. The formula used is as below:

After completing all the calculations as seen in the table below, it was determined that the MTTF and are within an acceptable range. A failure of the regulator would perhaps cause burns to the user, but nothing too severe, due to the voltage limiting.

Table 3: Linear Regulator Analysis

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter name | Description | Value | *Comments* |
| C1 | Die Complexity | *0.06* | Low-complexity analog IC; standard value for linear regulators |
| πT | Temperature Coefficient | *1.7* | At an estimated operating temperature of 40°C |
| πQ | Quality Factor | *3.0* | Assumes standard commercial-grade component |
| πE | Environment Factor | *1.0* | Ground benign environment (MIL-HDBK-217F assumption) |
| Entire design: | | | |
| λp | Failure Rate (F/10⁶ hrs) | 0.306 | λ = 0.06 × 1.7 × 3 × 1.0 |
| MTTF | Mean Time To Failure (hrs) | 3.27 | MTTF = 1 / λ |

Summary:

The MTTF of all three components—LM1117, MCP16331, and RP2350—are above several hundred thousand hours, which is sufficient for the expected lifetime of our machine. To further improve system reliability, we can consider simplifying the microcontroller or replacing it with a lower-complexity alternative. As a sidenote, the actual MTTF for the Raspberry Pi Pico W – 182000 hours, was given in the datasheet, and as a similar part, it was important to keep that value in mind. Additionally, implementing a basic thermal management solution, such as passive heat sinking or airflow ventilation, could help reduce the operating temperature and improve the temperature coefficient across all power-related components. Cooling within the aluminum assembly could also be another option we could explore.

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

There are three defined criticality levels for this project: low, medium, and high. High criticality includes failures that could lead to serious injury to users, such as electrical fires or overheating components causing burns. Medium criticality covers failures that might indirectly cause discomfort or minor harm, such as exposed hot surfaces or small electrical sparks under abnormal conditions. Low criticality refers to failures that only affect the function of the system, such as an automatic shutdown due to voltage drop or regulation failure, with no risk of injury. In general, no substantial risk is posed to the user except for heat effects of the linear regulator. The acceptable failure rate for high criticality components is 10⁻¹⁰ per hour, while medium and low criticality components are allowed to be a maximum rate of 10⁻⁶ per hour. For this analysis, we assume users have read the user manual thoroughly and will operate the system under normal indoor conditions. It is also assumed that the electrical system will not be exposed to water, snow, or other severe environmental factors. Therefore, we define two criticality levels for this project:

* High Criticality: Failures that could pose a direct safety risk to the user, such as overvoltage causing burns or damaging exposed components. Acceptable failure rate: λ < 10⁻⁹/hour.
* Low Criticality: Failures that only impact functionality, such as a system shutdown or unreliable readings, without any physical risk to the user. Acceptable failure rate: λ < 10⁻⁶/hour.

These levels are assigned based on the nature of interaction with the system. We assume the user follows the operation manual and uses the system indoors under normal conditions.

3.0 Sources Cited:

[1] MIL-HDBK-217F, Reliability Prediction of Electronic Equipment, U.S. Department of Defense, Dec. 1991.

[2] Texas Instruments, LM1117 Low-Dropout Linear Regulator, [Online]. Available: https://www.ti.com/product/LM1117

[3] Raspberry Pi Ltd., Raspberry Pi Pico W Datasheet, [Online]. Available: https://datasheets.raspberrypi.com/picow/pico-2-w-datasheet.pdf

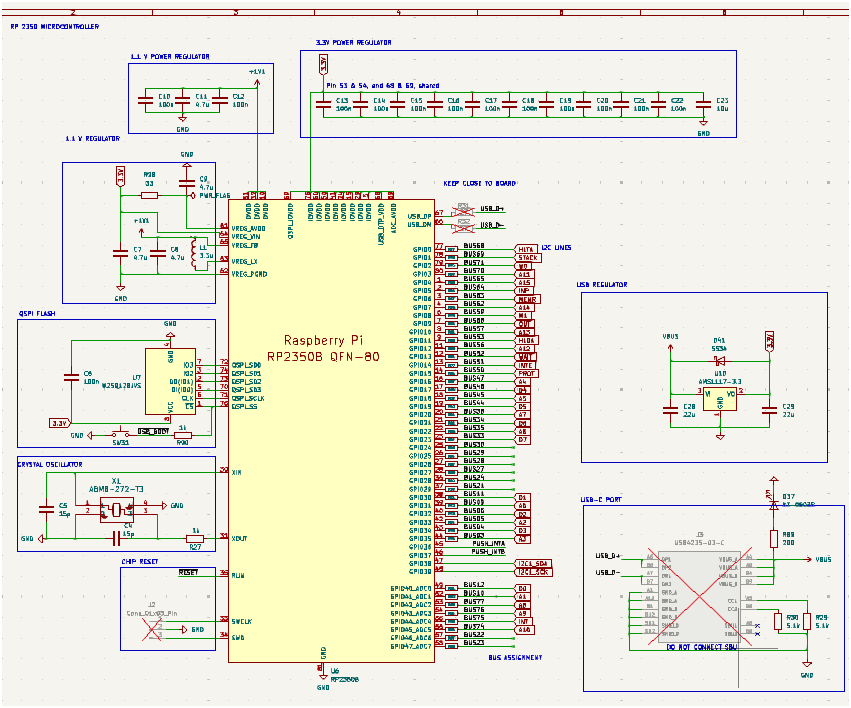
[4] Microchip Technology Inc., MCP16331/MCP16331T High-Efficiency, Low Input Voltage DC-DC Converter Datasheet, [Online]. Available: https://ww1.microchip.com/downloads/en/DeviceDoc/20005308C.pdf

[5] Raspberry Pi Ltd., RP2350 Microcontroller Datasheet, [Online]. Available: https://datasheets.raspberrypi.com/rp2350/rp2350-datasheet.pdf

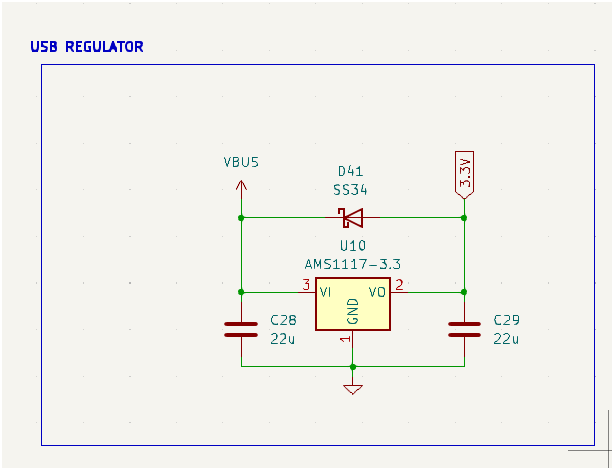
[6] J. Keane and C. H. Kim, "Transistor Aging: Measuring the degradation of microprocessors is tricky. Doing it better would unleash more processing power," IEEE Spectrum, May 2011. [Online]. Available: https://spectrum.ieee.org/transistor-aging

Appendix A: Schematic Functional Blocks

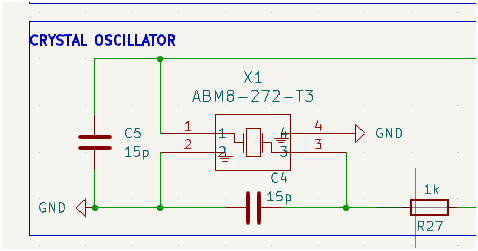
*Figure 1: Microcontroller Circuit*



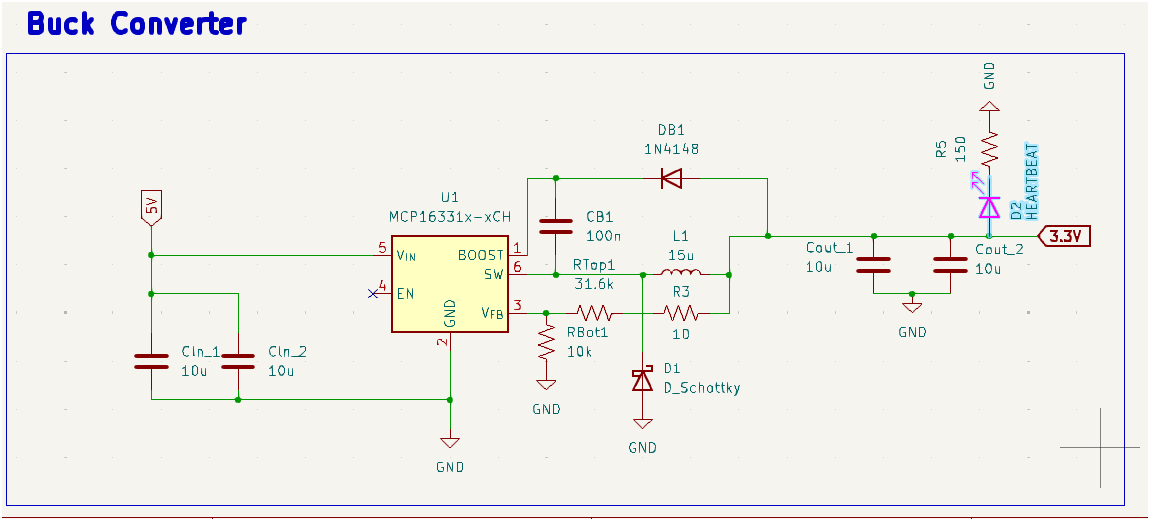
*Figure 2: LDO Circuit*



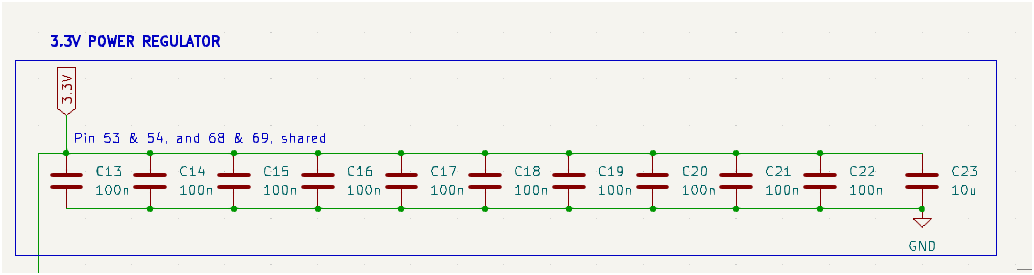
*Figure 3: Crystal Oscillator Circuit:*



*Figure 4: Buck Converter Circuit*



*Figure 5: 3.3 V Microcontroller Regulator*



*Figure 6: 1.1 V Microcontroller Regulator*

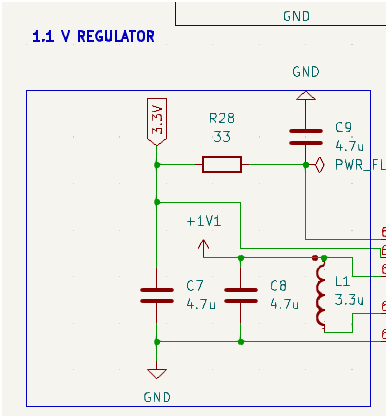
Appendix B: FMECA Worksheet

Table 4: Microcontroller Circuit FEMCA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| Failure No. | Failure Mode | Possible Causes | Failure Effects | Method of Detection | Criticality | Remarks |
| MC-1 | No power to MCU | Broken connection, faulty power rail | MCU doesn't turn on | Visual inspection, voltmeter | High | Check power supply paths |
| MC-2 | Stuck at boot | Bad flash, firmware error | MCU unresponsive | Serial debug output | High | Reprogram firmware |
| MC-3 | Overheating | Overvoltage, poor layout | Thermal damage to MCU | Infrared thermometer | High | Ensure correct voltage and cooling |

Table 5: LDO Circuit FEMCA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| LDO-1 | No output voltage | Open circuit, faulty LDO | Subsystems downstream don’t power | Voltmeter | High | Replace regulator, check input |
| LDO-2 | Output too high | Feedback failure, wrong resistor | MCU damage or misbehavior | Multimeter, oscilloscope | High | Verify resistor values |
| LDO-3 | Excess ripple | Bad bypass cap | MCU resets or glitches | Oscilloscope | Medium | Add or replace decoupling caps |

Table 6: Crystal Oscillator Circuit FEMCA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| Failure No. | Failure Mode | Possible Causes | Failure Effects | Method of Detection | Criticality | Remarks |
| XO-1 | Oscillator not starting | Improper load cap, cold joint | MCU won't clock/start | Oscilloscope, logic analyzer | High | Check capacitors, solder joints |
| XO-2 | Frequency drift | Temp change, wrong crystal | Communication errors, time drift | Frequency counter | Medium | Use temp-compensated crystal |

Table 7: Buck Converter Circuit FEMCA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| BUCK-1 | No output | Controller failure, blown MOSFET | System downstream won't power | Voltmeter | High | Replace component, check control PWM |
| BUCK-2 | Output too high | Feedback loop issue | Component overvoltage | Multimeter | High | Recalculate FB resistor divider |
| BUCK-3 | Excessive switching noise | Poor layout, missing snubber | EMI issues, MCU instability | Oscilloscope | Medium | Add filtering, improve layout |