A10 - Reliability and Safety Analysis

Year: 2024 Semester: Spring Team: 5 Project: Dodgebot

Creation Date: ­March 30, 2024 Last Modified: March 30, 2024

Author: Ayman Motoda Email: aelnamr@purdue.edu

1. Reliability Analysis

The STM32F207VGT6 [1] is the main microcontroller onboard that is used to interface with the motor controllers, and the main computation system making it a very critical component of this system. Because of its very high complexity, and its relatively higher operating temperature compared to most components on the board, it was selected for this analysis.

The model used to find the failure rate of the STM32F2 chip is referred to as a microcircuit in the MIL-HDBK-217f [2] handbook since the Cortex M3 chip has more than 60k gates [3]. The environment this system is in is relatively controlled and isolated, so not a lot of environmental factors play a huge role in its failure rate. Most of the failure points come from its inherent design and manufacturing scheme, which is not in our control, but we can always add redundancy if the insane number of hours needed to fail the chip was reached.

The TLV1117LV LDO [4] is a relatively simple chip, but it will also produce the most heat on the board, so it also has a higher chance of failing due to heat stress compared to most of the other components on the board. It is also critical for the operation of a lot of microchips on board, so its operation is vital to safe operation. This is classified as a linear microcircuit in the MIL-HDBK-217f [2] handbook, and has a relatively low transistor count, so most of the failure rate is going to be determined by its operating temperatures and its manufacturing tolerances.

The LM2678 Buck controller is also a relatively simple chip, but it will also produce a decent mount of heat which is also the reason it has a giant pad on the back of the package to dissipate the heat that is produced by the transistor. It is the most critical component of this board because ALL the ICs on board are in some way powered from this chip. Many of the chips use 5V power as well as many chips use the 3.3V power which is sourced from the LDO which sources its power from this buck controller. This is classified as a linear microcircuit in the MIL-HDBK-217f [2] handbook, and has a relatively low transistor count, so most of the failure rate is going to be determined by its operating temperatures and its manufacturing tolerances in the same way as the LDO.

*Table 1: STM32F207VGT6 Analysis*

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter name | Description | Value | *Comments regarding choice of parameter value, especially if you had to make assumptions.* |
|  | Die Base Failure Rate | *0.16* | *Logic Chip* |
|  | Manufacturing Process Correction Factor | *0.55* | QPL Chip |
|  | Die Complexity Correction Factor | *A = 1.96cm2 [1]*  *Xs = 0.80*  *πcd = 0.36 [3]* |  |
|  | Package Base Failure Rate | *.0039* | 100 Pins |
|  | Environment Factor | *0.50* | Nonmobile, controlled environment use. |
|  | Quality Factors | *10* | Commercial Part |
|  | Electrical Overstress Failure Rate | *.065* | Limited to 1000V [1] |
| Entire design: |  |  |  |
|  | *Failures per million Hours Rate* | *0.11618* |  |
| MTTF | *Mean Time to Failure* | *8607333.4* |  |

*Table 2: TLV1117LV Analysis*

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter name | Description | Value | *Comments regarding choice of parameter value, especially if you had to make assumptions.* |
|  | Die Base Failure Rate | *0.2* | *Linear Bipolar Chip* |
|  | Manufacturing Process Correction Factor | *5.8* | Can reach a temperature junction of 150C in operation |
|  | Die Complexity Correction Factor | *0.0013* | 4 Pin Device |
|  | Environment Factor | *0.50* | Nonmobile, controlled environment use. |
|  | Quality Factors | *10* | Commercial Part |
|  | Learning Factor | *1* | In production for more than a decade. |
| Entire design: |  |  |  |
|  | *Failures per million Hours Rate* | *11.6065* |  |
| MTTF | *Mean Time to Failure* | *86158.6* |  |

*Table 3: LM2678 Analysis*

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter name | Description | Value | *Comments regarding choice of parameter value, especially if you had to make assumptions.* |
|  | Die Base Failure Rate | *0.2* | *Linear Bipolar Chip* |
|  | Manufacturing Process Correction Factor | *5.8* | Can reach a temperature junction of 125C in operation |
|  | Die Complexity Correction Factor | *0.0026* | 8 Pin Device |
|  | Environment Factor | *0.50* | Nonmobile, controlled environment use. |
|  | Quality Factors | *10* | Commercial Part |
|  | Learning Factor | *1* | In production for more than 20 years. |
| Entire design: |  |  |  |
|  | *Failures per million Hours Rate* | *11.613* |  |
| MTTF | *Mean Time to Failure* | *86110.4* |  |

Many of the components for the system are commercial parts which are fit for our application, but if we want to increase the rating on things like the power regulation circuits, we will need to purchase ICs that are rated for military operation.

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

The criticality of this project realistically for all the MAIN components shown here are high or low. This is because many failure of the components that are displayed in the index below can result in catastrophic loss of control of the robot which can cause extremely violent mechanical results that could fatally injure or kill someone. All electrical failures that occur on the board will also be enclosed, so the risk is not very high if components fail catastrophically for the user since it is also very far away. The only low criticality is related to power loss since a loss of power guarantees that the operation of the robot halts. Since our risks are very high for this project, our failure rate for a high level is 10-10. For any of the low level failures, the acceptable failure rate is 10-6. Everything shown in the appendix from the schematic is necessary for necessary operation of the robot, so not every subcircuit was shown since they are not required or effect the operation of the robot. Many of the control schemes are redundant, and some of them give extra operations in case our demands change.

3.0 Sources Cited:

[1] STMicroelectronics, “STM32F205xx STM32F207xx,” Jul. 2020. Accessed: Mar. 31, 2024. [Online]. Available: https://engineering.purdue.edu/477grp5/Files/refs/stm32f207vg.pdf

[2] “Military Handbook Reliability Prediction of Electronic Equipment” Department of Defense. Washington DC. MIL-HDBK-217F, Dec. 2, 1991.

[3] A. Mittal, “Which ARM Cortex-M Processor?,” *www.vlsiip.com*, 2020. http://www.vlsiip.com/soc/soc\_0003.html#:~:text=ARM%20Cortex%20M3%20Gate%20Count (accessed Mar. 31, 2024).

[4] Texas Instruments, “TLV1117LV 1-A, Positive Fixed-Voltage, Low-Dropout Regulator,” Jan. 2023. Accessed: Mar. 31, 2024. [Online]. Available: https://engineering.purdue.edu/477grp5/Files/refs/tlv1117lv.pdf

[5]Texas Instruments, “LM2678 SIMPLE SWITCHER ® High Efficiency 5-A Step-Down Voltage Regulator,” Jan. 2023. Accessed: Mar. 31, 2024. [Online]. Available: https://engineering.purdue.edu/477grp5/Files/refs/lm2678.pdf

Appendix A: Schematic Functional Blocks

A diagram of a circuit

Description automatically generated

Figure 1: Power Topology

A diagram of a power supply

Description automatically generated

Figure 2: STM32 Power Supply Scheme

A diagram of a computer

Description automatically generated

Figure 3: Servopack Output Topology

A white board with green text and red and green text

Description automatically generated

Figure 4: Inputs to Servopack Topology

Appendix B: FMECA Worksheet

Table 4: Power Topology & STM32 Power Topology FEMCA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 1 | Voltage Drops on STM32 | C15-C29 | Can cause pulsations on outputs of pins which can cause extra pulse movements in motor commands | Encoder Feedback Count | High |  |
| 2 | Voltage Loss | TLV1117LV & LM2678 | Shuts off the microcontrollers and ICs | Loss of robot operation, Power LEDs off. | Low | Robot will automatically stop moving at the loss of the enable signals and pulsations. |
| 3 | High Voltage Fluctuation | LM2678 | Exceeds the maximum voltage output of the LDO which will burn it out which will kill power. | 3.3V LED Power detector off, maybe small amounts of smoke coming from the LDO IC | Low | With any of the main ICs off, the operation of the robot will be none since there are no control schemes that are operational. The box is also enclosed, so it is not a huge danger for the user if it occurs. |

Table 5: Outputs from Servopack FEMCA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 3 | Line Receiver IC (Pulse Encoding)  Signal Loss | SN65LBC175A Failure | Lose the ability to read the encoder, will throw off the positional reading to the computer which will cause movements that are unexpected. | Wild Movement, Large Delta between camera and motor position. | High |  |
| 4 | Line Receiver IC (Pulse Encoding) Level Shifter  Signal Loss | RS0104 Failure | Lose the ability to read the encoder, will throw off the positional reading to the computer which will cause movements that are unexpected. | Wild Movement, Large Delta between camera and motor position | High | Same result as the line-receiver IC, but with another point of failure since it’s also required to read the pulses. |
| 5 | Photocoupler IC (Alarm Notification) Signal Loss | ASCL-6400 | Lose the ability to read the alarm code from the servo pack making diagnosis trickier. | Loss of robot movement without any apparent or obvious reason. | Low | Robot will shutoff when an alarm notification is sent, so even if we can’t read the notification, it is safe. |

Table 6: Power Topology & STM32 Power Topology FEMCA

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 6 | Line Driver IC (Pulse Transmission) Control Signal Loss | SN75ALS174 | Can cause pulse losses on the output side to the servo pack which can deviate the commands from the encoder which could throw off calculations | Encoder Feedback Count, Camera Detection Position and motor differential calculation. | High | Can eventually lead to robot drifting towards the edges of the operating range which can then collide with objects or other people around the robot. |
| 7 | NPN Transistor Array Short | SN75468 | Lose the ability to turn off the control of the servopacks which could lead to unexpected motor movements based on microcontroller signals. | Random robot movements that are being sent even when the microcontroller shows that the enable signal is not being sent to the NPN array | High | Random movement of random amounts can eventually lead to exiting the operating range without any feedback system which can then collide with people and objects. |