Homework 11: Reliability and Safety Analysis

Due: Friday, April14, at NOON

Team Code Name: Digital Real Time Intelligent Networked Kegerator Group No. 4

Team Member Completing This Homework: Dustin Poe
E-mail Address of Report Author: depoe@purdue.edu

NOTE: This is the third in a series of four "professional component" homework assignments, each of which is to be completed by one team member. The completed homework will count for 10% of the team member's individual grade. It should be a minimum of five printed pages.

Evaluation:

Component/Criterion	**Score**	**Multiplier**	**Points**
Introduction and Summary	0 1 2 3 4 5 6 7 8 9 10	X 1	
Reliability Analysis	0 1 2 3 4 5 6 7 8 9 10	X 2	
Failure Mode, Effects, and Criticality Analysis	0 1 2 3 4 5 6 7 8 9 10	X 3	
Appendix A	0 1 2 3 4 5 6 7 8 9 10	X 1	
Appendix B	0 1 2 3 4 5 6 7 8 9 10	X 1	
List of References	0 1 2 3 4 5 6 7 8 9 10	X 1	
Technical Writing Style	0 1 2 3 4 5 6 7 8 9 10	X 1	
		TOTAL	

Comments:

___

___

___

___

1.0 Introduction

This document provides the Reliability and Safety information for the Digital Real Time Intelligent Network Kegerator. The Digital Real-Time Intelligent Networked Kegerator is a modular addition to an existing beverage dispensing device. The DRINK system provides the owner with complete beverage control, allowing owners to monitor user's consumption, set consumption limits, or completely restrict access. In this reliability analysis, components with a high likelihood of failure were identified. For these components, the number of failures per hour and the mean time to failure (MTTF) were determined. Also provided in this document is the Failure Mode, Effects, and Criticality Analysis (FMECA) for each modular block of the DRINK system. This Analysis gives insight into the failure modes of the system. The majority of the failure modes will result in a loss of functionality which is a major inconvenience to the user, but would not result in injury. However, there are a few failure modes identified as being potentially hazardous to the user and the entire system. These failures and potential solutions will be discussed in detail.

2.0 Reliability Analysis

2.1 Component Selection

Several components were identified in this system that could contribute to increased failure rates of the system. These components were chosen because of their elevated temperatures and/or frequency of use. The components are the compressor contactor (MGM Power Relay), power MOSFETS (TIP122), switching regulators (LTC1265-3.3, -5), and the flow solenoids. For each component, the numbers of failures per hour was calculated using MIL-HDBK-217F. [1] For all components λ_b represents the base failure rate. The base failure rate was then adjusted using environmental and manufacturing parameters to get λ_p the number of failures per hour. The mean time to failure (MTTF) was then calculated using the inverse of the number of failures per hour. [2]

2.1.1 Compressor Contactor

The failure rate for the contactor can be determined using the following formula from MIL-HDBK-217F Section 13.1.

$$\lambda_p = \lambda_b \pi_L \pi_C \pi_{CYC} \pi_F \pi_Q \pi_E \text{ Failures}/10^6 \text{ Hours}$$

Factor	Description	Value	Explanation
λ_b	Base Failure Rate	0.0066	Based on Internal worst case temperature in Compressor Compartment, 50 degrees C, and assuming rated temperature of contactor is 125 degrees C. However, contactor is rated for 155 degrees C. [3 1]
π_L	Load Stress Factor	1.04	Ratio of Load Current to Rated Current is .16666 and load is an inductive motor. [3 1]
π_C	Contactor Form factor	1	Value for Single Throw Single Pole Relay [3 1]
π_{CYC}	Cycling Factor	1	10 cycles per hour and lower quality [1]
π_F	Application and Construction Factor	6	The signal current was assumed to be 5Amps, with medium power rating, and it is magnetically latching [3 1]
π_Q	Quality Factor	3	The quality factor is not established. Assuming worst case [1]
π_E	Environmental Factor	5	Assuming Moderately controlled environment and non mil grade part [1]
λ_p	**Failure Rate**	**0.618 Failures in 10^6 Hours**	
MTTF	**Mean time to Failure**	**1.62 x 10^6 Hours or 185 years**	

Table 2.1.1 Reliability Parameters for the Compressor Contactor

The compressor contactor was chosen to have a high likelihood of failure for several reasons. First, because the contactor is located in the compressor compartment it will have higher ambient temperatures than any other component in the design. Second, due to temperature regulation it is estimated that the contactor will switch frequently, an estimated 10 times an hour. In addition if this contactor fails closed there could be potential harm to the system and user. In this failure mode the compressor would be continuously driven. The MTTF rate for this device needs to be 1 x 10^9 to have complete control over the compressor. It is highly recommended that owners keep the original temperature circuit in series with this device but set at a much higher temperature level. Finally in future models, an inclusion of an auxiliary contact for feedback purposes would greatly increase detecting of failure. This would allow for a software comparison of the drive signal with the feedback signal.

2.1.2 Power MOSFETS

The failure rate for the contactor can be determined using the following formula from MIL-HDBK-217F Section 6.4.[1]

$$\lambda_p = \lambda_b \pi_T \pi_A \pi_Q \pi_E \text{ Failures}/10^6 \text{ Hours MIL Section 6.4}$$

Factor	Description	Value	Explanation
λ_b	Base Failure Rate	0.012	Value for MOSFET [1]
π_T	Temperature Factor	6.7	Based on Absolute max ratings from data sheet.150 degrees C [4 1]
π_A	Application Factor	4	5W ≤ 12W < 50W [1] Power MOSFET 12V*1A=12W [4 1]
π_Q	Quality Factor	8	Assuming worst quality Factor Plastic [1]
π_E	Environmental Factor	6	Assume GF since located in moderately controlled. Potential for excess heating, or humidity [1]
λ_p	**Failure Rate**	**15.44 = Failures in 10^6 Hours**	
MTTF	**Mean time to Failure**	**648 x 10^6 Hours or 7.39 years**	

Table 2.1.2 Reliability Parameters for the Power MOSFETS

The power MOSFETS in this design were chosen because they are operating above room temperature. In this analysis, a worst case junction temperature of 150 degrees C was used.[3] In reality, the junction temperatures will probably never approach 100 degrees C. The MTTF for this part is unacceptable. Since this device won't function without this component, the failure rate should be at least 1 x 10^6 Hours until failure. It is recommended that higher quality parts be used in commercial use. Failure of this component will result in the solenoids remaining open or closed. If this part fails on the contactor, the compressor will be continually forced on or off. It is also recommended that two of these MOSFETS be used in series. This provides the ability to still shutoff the compressor if one fails closed.

2.1.3 Switching Regulator 3.3V and 5V

The failure rate for the regulars can be determined using the following formula in MIL-HDBK-217F Section 5.1. [1]

$$\lambda_p = (C_1\pi_T + C_2\pi_E)\pi_Q\pi_L \text{ Failures}/10^6 \text{ Hours}$$

Factor	Description	Value	Explanation
C_1	Die Complexity Failure Rate	0.02	Assuming worst case there no more than 300 transistors in device. [1]
π_T	Temperature	58	Absolute worst Junction Temperature is 125 Degrees C [5] For a Linear Device [1]
C_2	Package Failure Rate	.0048	14 Pin Surface Mount Plastic Package [5] [1]
π_E	Environmental Factor	2	Assuming moderately controlled environment and non mil grade part [1]
π_Q	Quality Factor	10	Assuming unknown quality level [1]
π_L	Learning Factor	1	Product has been in Market since 1995 [5] [1]
λ_p	**Failure Rate**	**0.111 Failures in 10^6 Hours**	
MTTF	**Mean time to Failure**	**8.96 x 10^6 Hours or 102 years**	

Table 2.1.3 Reliability Parameters for the Switching Regulators

This component was chosen because it's high junction temperature. In this design there are two switching regulators each powering different sources in the system. In either case of failure, the system will be virtually useless. Most failure modes of this device will not cause harm to the user or system. However, if this device has a short to ground it could cause a potential fire. The MTTF for this part is somewhat high for being a critical part in this design. It should be noted that the junction temperature will probably never exceed 100 degrees C in this design. To increase reliability /it is recommended that an external fuse be placed inline with each power supply to prevent a fire from occurring.

2.1.4 Solenoid Valve

The failure rate for solenoids can be modeled from the relay section 13.1 of the MIL-HDBK-217F. [1]

$$\lambda_p = \lambda_b\pi_L\pi_C\pi_{CYC}\pi_F\pi_Q\pi_E \text{ Failures}/10^6 \text{ Hours}$$

Factor	Description	Value	Explanation
λ_b	Base Failure Rate	0.0066	Based on Operating Temperature, 49 degrees C [6 1]
π_L	Load Stress Factor	1	Virtually No Load only actuating contactor [6 1]
π_C	Contactor Form factor	3	Value for Double Throw Double Pole Relay [6 1]
π_{CYC}	Cycling Factor	6	Worst Case Scenario 60 cycles per hour and lower quality [1]
π_F	Application and Construction Factor	12	General Purpose Solenoid with 1.2A Signal [6 1]
π_Q	Quality Factor	3	The quality factor is not established. Assuming worst case [1]
π_E	Environmental Factor	5	Assuming Moderately controlled environment and non mil grade part [1]
λ_p	**Failure Rate**	**21.4 Failures in 10^6 Hours**	
MTTF	**Mean time to Failure**	**468 x 10^6 Hours or 5.33 years**	

Table 2.1.4 Reliability Parameters for the Solenoid Valve

This component was chosen because of its frequency of use, up to 60 cycles an hour. In addition, the solenoids require 1.2 Amps at 12V to power the actuation. This will cause heating in the component that may lead to more failures. The MTTF failure for this part is unacceptable because without fundamental operation cannot occur. A failure rate of 1 x 10^6 is necessary for component in commercial operation. To increase the reliability for this component the number of cycles an hour should be reduced.

3.0 Failure Mode, Effects, and Criticality Analysis (FMECA)

3.1 Division of Functionality

A Failure Mode Effects and Criticality Analysis was performed on the entire DRINK system. To simply this analysis the system was broken into functional blocks. This division can be seen in Appendix A. In the blocks shown below each border color and letter correspond to a section in Appendix A.

3.1.1 Common Beverage Interface

A picture of the common beverage interface is shown below. Due to the symmetry of this interface, only one beverage line is shown. This interface provides all the necessary signals for each beverage. Each interface has six signals: three for the flow meter, two for the solenoid valve, and one to indicate a beverage is connected. The failure mode\ analysis for this block can be found in Appendix B.

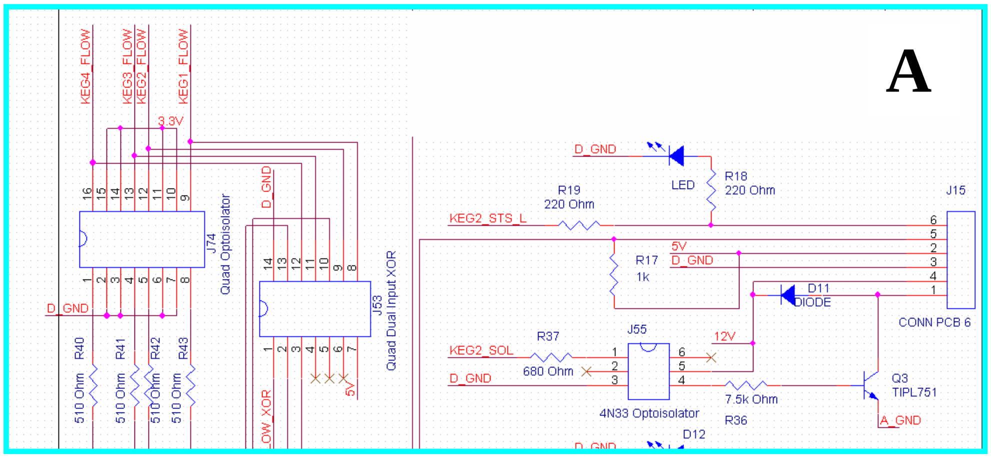


Figure 3.1.1 Common Beverage Interface for One Line

3.1.2 3.3V LCD and RPG Interface

Figure 3.1.2 shows a picture of the functional block for the LCD. This block contains the RS-232 chip which converts a 3.3V Signal into ± 15V. In addition, this interface contains all the necessary headers for the LCD and Rotary Pulse Generator. The failure mode analysis for this block can be found in Appendix B.

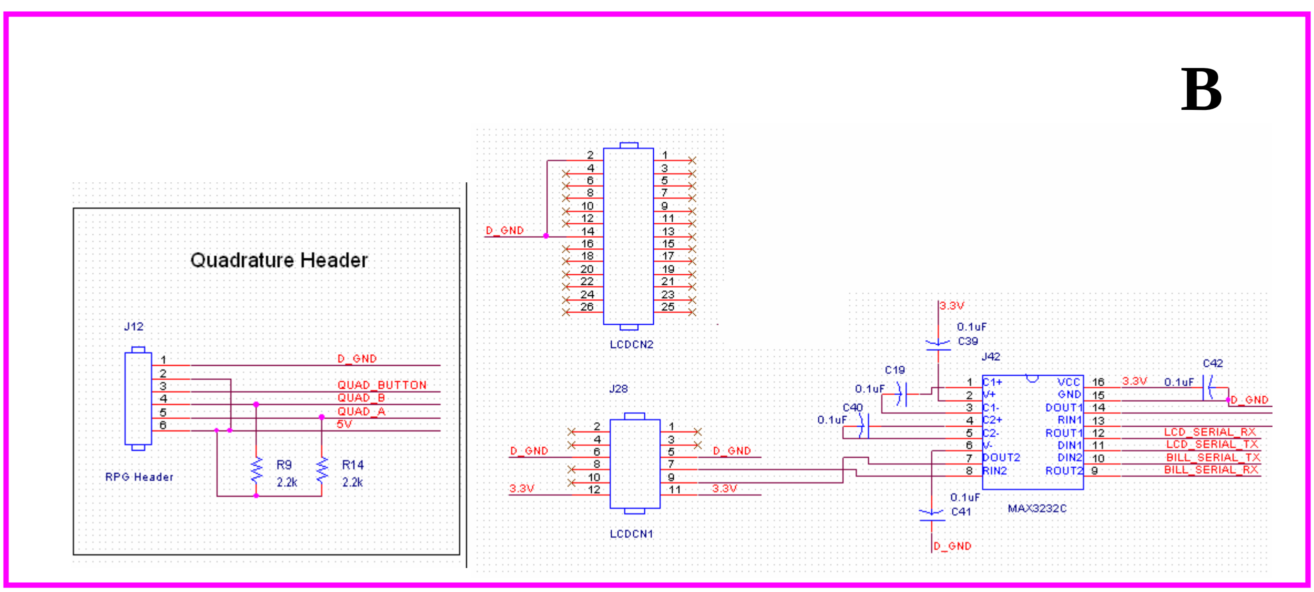


Figure 3.1.2 LCD and RPG Interface

3.1.3 Temperature Control Interface

A picture of the temperature control interface is shown below in Figure 3.1.3. This interface contains the headers to two temperature probes, and the driver for the compressor contactor. One probe is located inside the refrigerator, while the other is ambient temperature. The compressor contactor interrupts the AC power to the refrigerator compressor. The failure mode analysis for this block can be found in Appendix B.

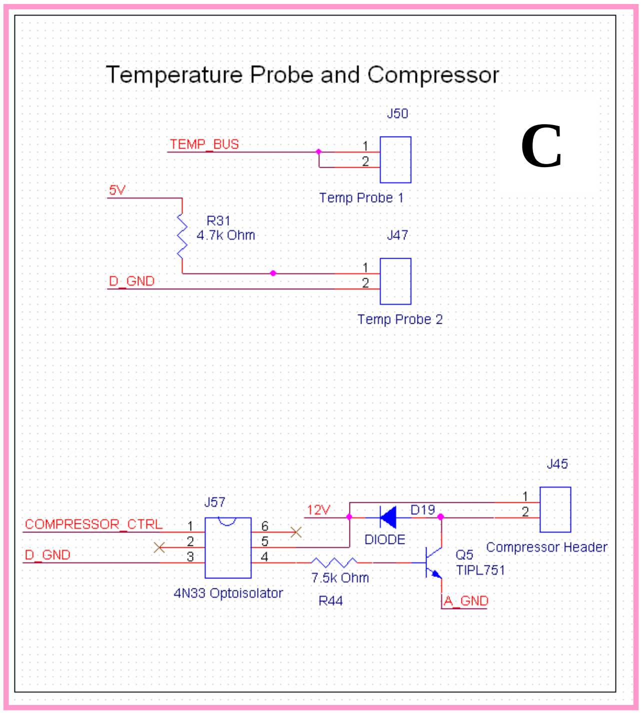


Figure 3.1.3 Temperature Control Interface

3.1.4 5V Power Circuit

Figure 3.1.4 shows the 5V Power Circuit. This circuit is responsible for powering the RFID module, the flow meters, biometric sensor, and the temperature probes. The failure modes for this block can be found in Appendix B.

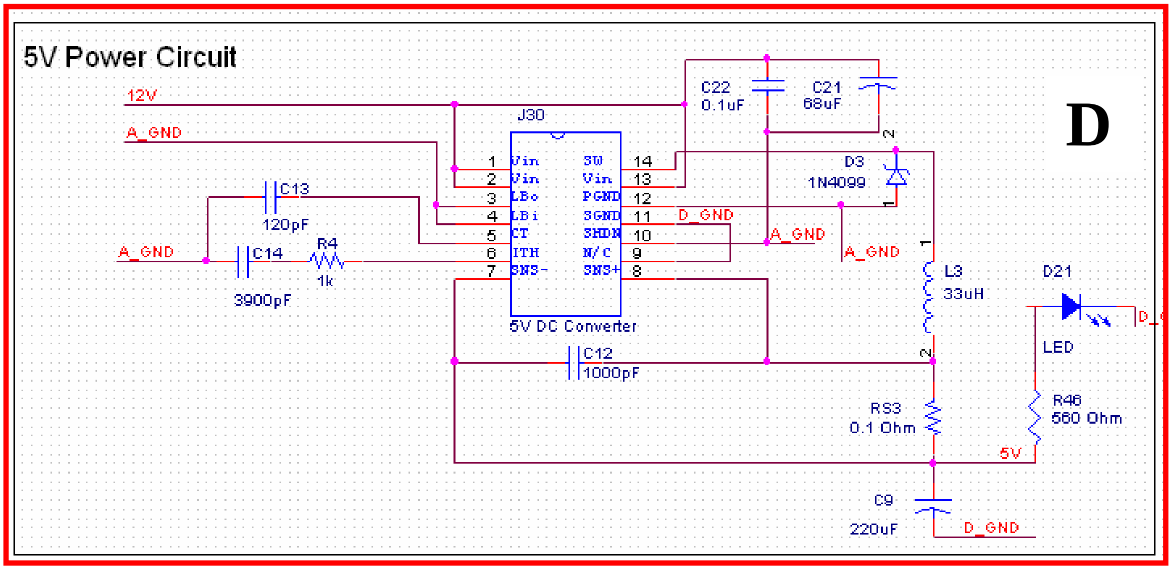


Figure 3.1.4 - 5V Power Circuit

3.1.5 3.3V Power Circuit

Shown below in Figure 3.1.5 is the 3.3V power supply and circuit. This circuit is responsible for powering the Rabbit microprocessor, and the RS-232 translator chips. The failure mode analysis for this block can be found in Appendix B.

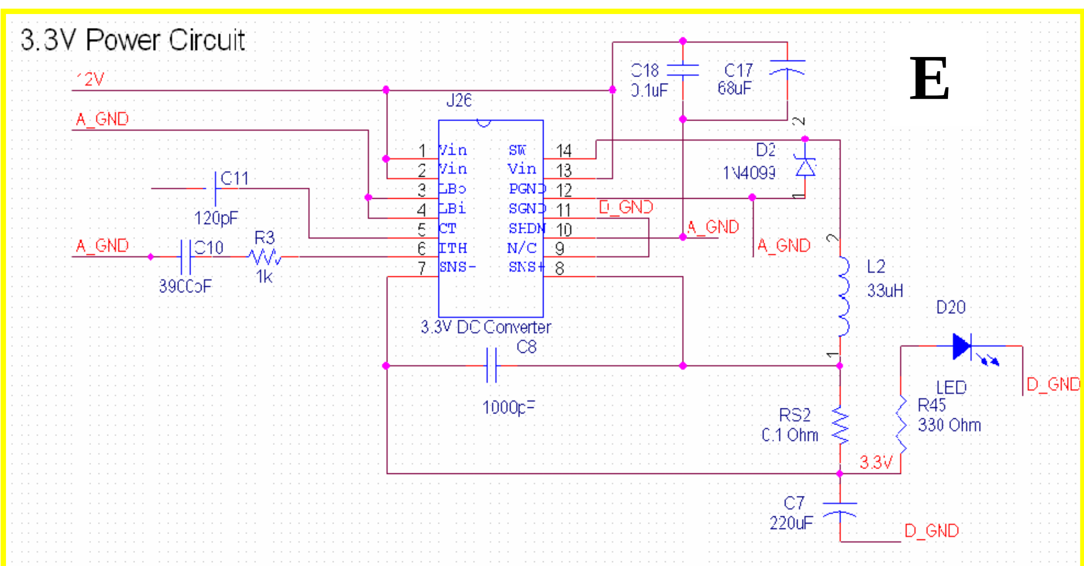


Figure 3.1.5 - 3.3V Power Circuit

3.1.6 User Identification Interface

The User Identification Interface is shown in Figure 3.1.6. Within this interface is the RFID reader which will be used to determine cup size, and the header to the Biometric Thumb print reader which will be used to recognize users in the system. The failure mode analysis for this block can be found in Appendix B.

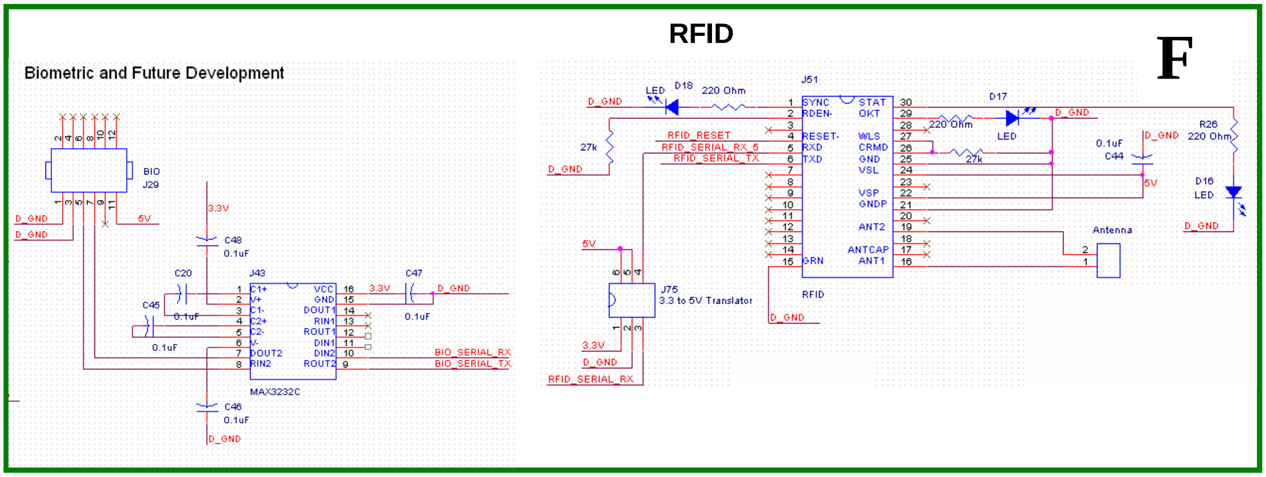


Figure 3.1.6 User Identification Interface

3.1.7 Currency Acceptor Interface

Figure 3.1.7 shows the Currency Acceptor Interface. This section features an RS-232 level translator along with signal and power headers to the Currency Acceptor. The failure mode analysis for this block can be found in Appendix B.

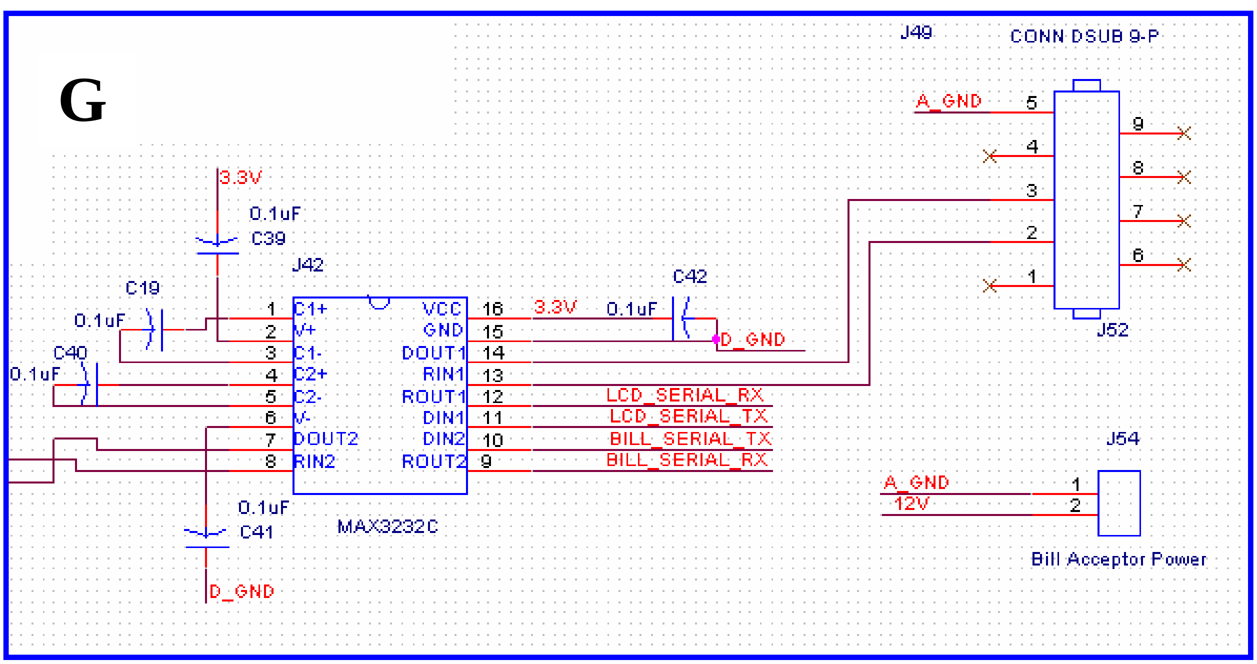


Figure 3.1.7 Currency Acceptor Interface

3.1.8 Rabbit Module Circuit

Figure 3.1.8 shows the Rabbit Module Circuit. Within this circuit are the headers to the Rabbit Microprocessor, and audio transducer, reset switch, and backup battery for memory. . The failure mode analysis for this block can be found in Appendix B.

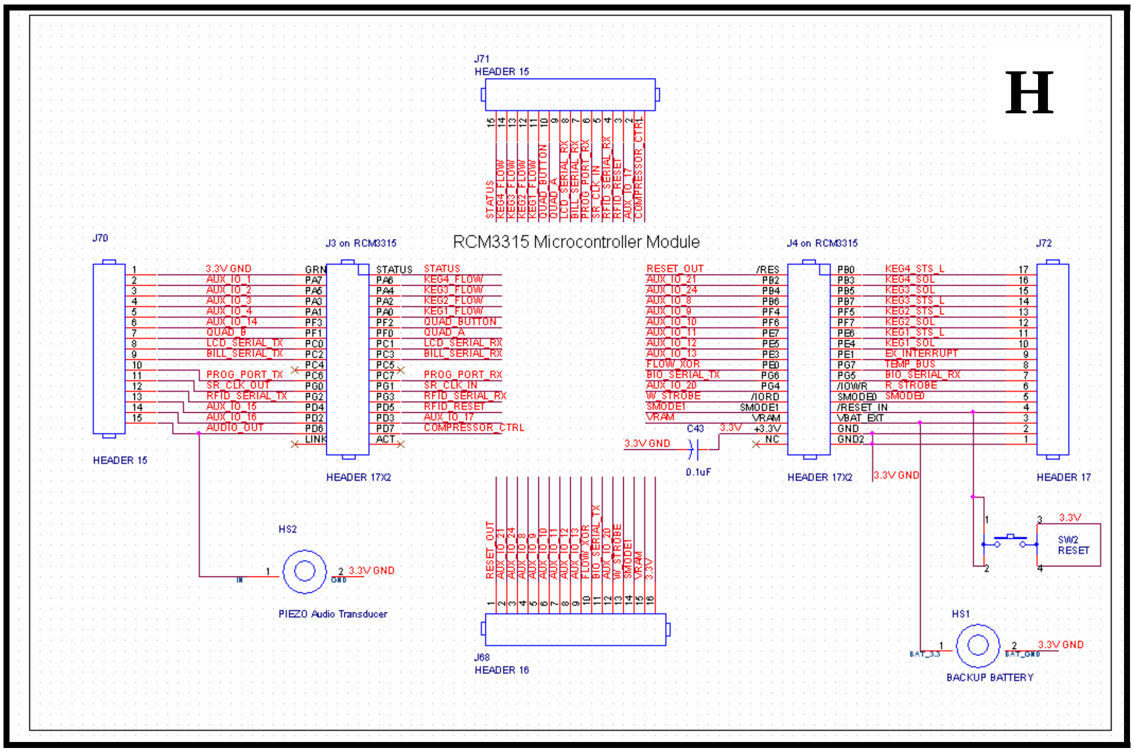


Figure 3.1.8 Rabbit Module Circuit

3.2 Definitions of Criticality Levels

The criticality levels, their definition and the acceptable failure rates are shown in Table 3.2.

Level	Description of Failure	Acceptable Reliability Rates (Hours until Failure)
Low	Minor inconvenience, little or not affect on system performance	1×10^5
Med	Harmless to User but results in Major Loss of Functionality	1×10^6
High	This failure can potentially cause heavy damage to the system and the user	1×10^9

Table 3.2 Definition of Criticality Levels.

4.0 Summary

In this document, the reliability of the Digital Real-Time Intelligent Networked Kegerator was analyzed. For components identified as higher likelihood of failure the number of failures in an hour, and mean time to failure was also calculated. It was found the reliability of any of the parts was not acceptable. Further design or inclusion of a backup system will be necessary to meet the required reliability rates. In the second part of this analysis the schematic was divided up into functional sections. In each section every failure mode was identified along with its criticality on the overall system. The criticality was split into three levels. Low levels criticality failures were associated with errors that have little or not effect on performance. Medium criticality failures were associated with a major loss of functionality, but would result in no harm to user. Finally, high criticality failures were associated with failures that would result in potential harm to the user, and the entire system.

List of References

[1] MIL-HDBK-217F – Military Handbook of Reliability Prediction of Electronic Equipment
http://shay.ecn.purdue.edu/~dsml/ece477/Homework/Spr2006/Mil-Hdbk-217F.pdf

[2] Novak, George. Designing for Reliability, Maintainability, and Safety Circuit Cellar. Dec 2000
http://shay.ecn.purdue.edu/~dsml/ece477/Notes/PDF/4-Mod13_ref.pdf

[3] Omron Heavy Duty Power Relay Datasheet
http://shay.ecn.purdue.edu/~477grp4/documents/specs/MGN0305PowerRelay.pdf

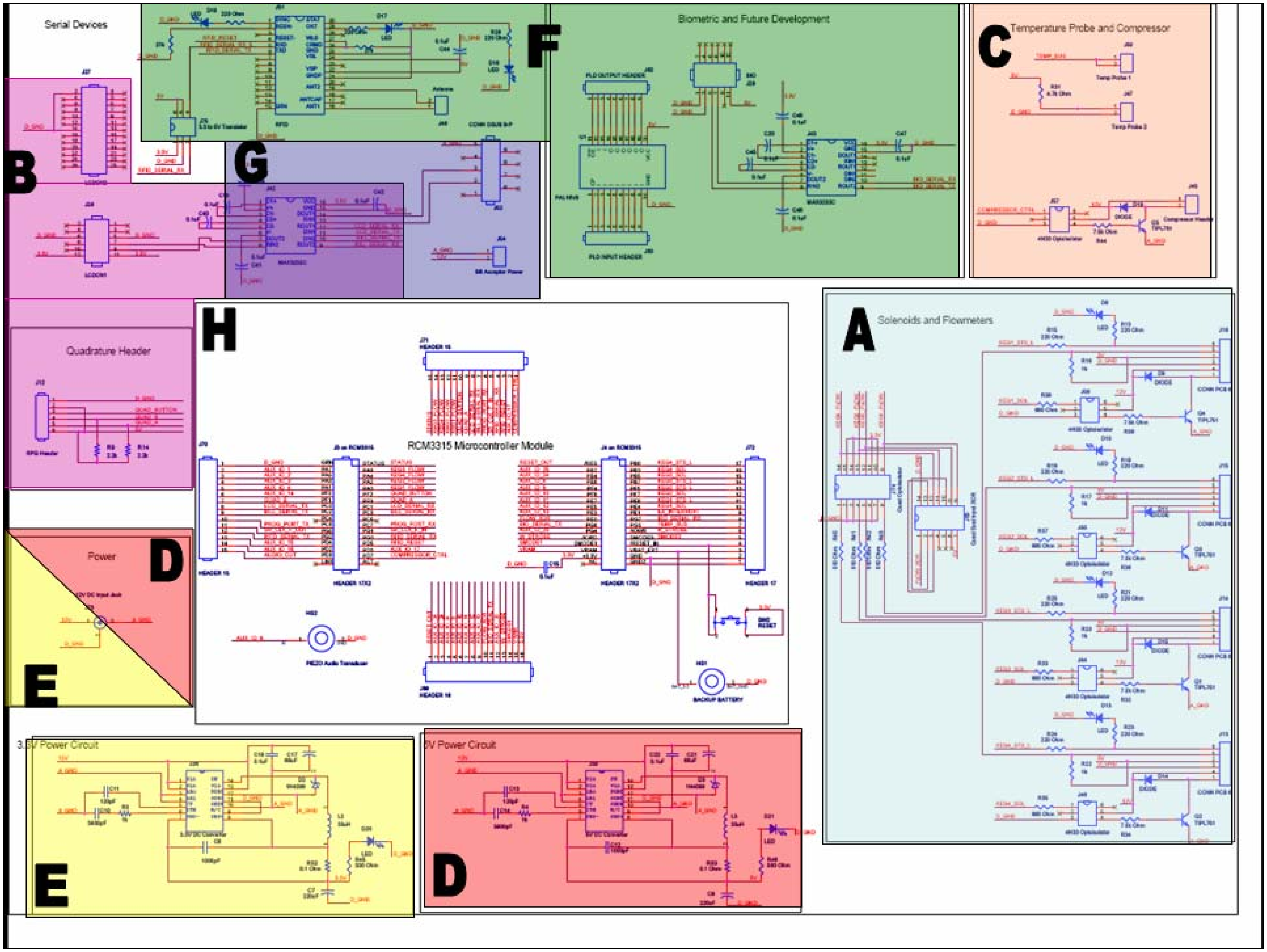
[4] Fairchild NPN Epitaxial Darlington Transistor Datasheet
http://shay.ecn.purdue.edu/~477grp4/documents/specs/TI-TIP122-1.pdf

[5] Linear Technologies Step Down DC/DC Converter Datasheet
http://shay.ecn.purdue.edu/~477grp4/documents/specs/LTC1265.pdf

[6] Evolutionary Concepts Inc Series 2200 Specifications
http://www.ecivalves.com/specs/SpecsS2200.htm

IMPORTANT: One of these should be *MIL-HDBK-217F*. Use standard IEEE format for references, and CITE ALL REFERENCES listed in the body of your report. Any URLs cited should be "hot" links.

Appendix A: Schematic Functional Blocks



Appendix B: FEMCA Worksheet

Failure No.	Failure Mode	Possible Causes	Failure Effects	Method of Detection	Criticality	Remarks
A1	No Beverage Monitoring	Flow meters, Optocouplers (J74) XOR (J53) R40-R43, connector, wire, microprocessor, software	Inaccurate or Failure to Monitor BAC	Software, Observation on LCD	High	Could result in harm to user if consumption no properly monitored
A2	Solenoids won't open	Solenoids, MOSFETS (Q1, Q2, Q3, Q4) diodes (D14, D15, D11, D9), wire J56, J55, J44 J46, connectors, wire, microprocessor, software	Inability to dispense beverage	Observation,	Med	
A3	Solenoids won't close	Solenoids, MOSFETS (Q1, Q2, Q3, Q4) diodes (D14, D15, D11, D9), optocouplers, connectors, wire, microprocessor, software	Inability to control beverage flow. Unrestricted access to beer	Observation,	High	Could result in harm to user if consumption no properly monitored

A4	KEG Showing Not connected	connector, wire, R15, microprocessor, software	Inability to serve all beverages	Observation,	Low	
B1	Rotary Pulse Generator failure	RPG, wire, header, R9, R14, microprocessor, software	Inability to Navigate through menu	Observation on LCD	Low	
B2	LCD Improper Display	Wire, connector, Noise, microprocessor, software	Inability to see Menu	Observation on LCD	Med	
B3	LCD Failure	J42, connector, wire, microprocessor, software	Inability to See Menu	Observation on LCD	Med	
C1	Improper or No Temperature Monitoring	Temperature Probes, R31, Connector, Wire, microprocessor, software	Inaccurate Temperature Regulation, Compressor Failure, Overheating	Software, Observation on LCD	High	Could result in damage or fire to refrigerator. Recommended to use backup emergency temperature controller
C2	Contactor Driven Constant High	Contacts on relay melded ,shut, MOSFET Failure Q5, J57, microprocessor, software	Compressor Failure, Overheating	Observation,	High	Could result in damage or fire to refrigerator. Recommended to use backup emergency temperature controller
C3	Contactor Driven Constant Low	Relay Failure, MOSFET, Q5, J57, microprocessor, software	Inability to Cool Beverage,	Observation,	Med	Non Regulation of Temperature would result in warm beverage

D1	Voltage Output >5V	External PS, J30,D3	Unpredicted Behavior and potential damage to Serial Communications, RFID, flow meters temperature probes, also potential to damage Micro.	Observation,	High	Unpredictable may result in excess current/ Damage to micro is due to fact that some pins have 5V Input
D2	Voltage Output=0	Any component in Block D	Loss of RFID, and Biometric, ability to monitor temp and flow. Could result in fire due to short to ground	Observation,	High	TBD
D3	Out of Tolerance	Any component is Block D	Out of Spec Operating Voltage	Observation,	Med	TBD
E1	Voltage Output >3.3	External PS, J26,D2	Unpredicted Behavior and potential damage to RFID and Microprocessor	Observation,	High	
E2	Voltage Output=0	Any component in Block D, Power and Ground Short	Complete Loss of Functionality since Microprocessor is not powered. A short to ground could cause potential fire	Observation,	High	
E3	Out of Tolerance	Any component is Block D	Out of Spec Operating Voltage	Observation,	Med	

F1	Failure of RFID	Antenna, RFID chip(J51), Level Translator, J75 , microprocessor, software	Unable to Identify cup size cannot limit flow	Observation, Software	Low	
F2	Failure of Biometric	Thumb Print Reader, RS232 level translator (J43), microprocessor, software	Inability to Identify Users, therefore to serve beverage	Observation,	Med	
F3	Invalid RFID Match	Antenna, RFID chip(J51), Level Translator J75, RFID Transponder	Incorrect identification of cup size and incorrect flow limit	Observation, Software	Low	
F4	Invalid Finger Match	Thumb Print Reader, RS232 level translator (J43)	Incorrect identification of users, unauthorized pours	Observation, Software	High	Could result in harm to user if consumption is recorded for wrong user.
G1	Dollar Bill Acceptor Fails Off	RS-232 Cable, J42, Dollar Bill Acceptor, microprocessor, software	Inability to Buy Credits for Drinks	Observation,	Med	TBD
G2	Dollar Bill Acceptor Fails On	RS-232 Cable, J42, Dollar Bill Acceptor, microprocessor, software	Accepts Dollars/but doesn't give credits	Observation,	Med	
H1	Audio Transducer Stuck High	Microprocessor, software	Speaker has continuous noise	Observation	Low	

H2	Web server crashes	Microprocessor, software	Inability to remotely control Kegerator, view users statistics, add manage or users.	Observation	Med	

It is not necessary to calculate the probability of each failure mode. These numbers would usually be taken from the reliability analysis, but since you are not performing a complete analysis, they do not need to be included in your FMECA worksheet.