Homework 11: Reliability and Safety Analysis

Due: Friday, April14, at NOON

Team Code Name: RFID Xpress Group No. 10

Team Member Completing This Homework: Jennifer Tietz

E-mail Address of Report Author: jtietz @ 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

RFID Xpress is a state-of-the-art self-checkout station utilizing RFID technology to enhance the retail store customer's checkout experience. Once the customer is finished shopping, he or she simply swipes a key fob with an embedded RFID tag within a few inches of the mouse pad-like receiver. The unique serial number on the key fob is used to query an external database and obtain the customer identification and pertinent information. The customer is then prompted to input his or her PIN on a 16-key keypad as an added security measure. Then, the customer can begin scanning products past the receiver as the RFID tags with unique serial numbers will return the product's name and price from a similar external database. As products are scanned, the information and total price appears on the LCD screen for the customer to view. After all of the product scanning is complete, the customer chooses whether to print a receipt or just receive one via email.

As the RFID Xpress is designed for interaction with the general public on a frequent basis, safety and reliability are a serious concern. The system needs to be manufactured reliably, including selection of well-tested components. It must be properly enclosed so as to minimize the probability of harm to the customer should a malfunction occur. The system must also adequately verify customer identification to decrease the likelihood of identity theft. These considerations will be discussed in this report, which includes a detailed Reliability Analysis of several main components in the design and their respective Mean Time to Failure (MTTF) based on parameters and equations obtained in the Military Handbook of Reliability and Prediction of Electronic Equipment [1]. This report also details a Failure Mode, Effects, and Criticality Analysis (FMECA) of each functional block in the schematic.

2.0 Reliability Analysis

In order to determine the reliability of the overall system, it is necessary to identify those components that are most likely to fail. This decision is based largely upon the common operating temperature of the components, as those that operate above room temperature are more likely to fail sooner, as well as the use of the components, since those found in power circuits are stressed more heavily.

The team identified the following four components and utilized the MIL-HDBK-217F Military Handbook to calculate each component's failure rate per 10^6 hours and the component's MTTF:

1. MC9S12NE64 Microcontroller
2. REG1117A 1 A LDO 3.3 V and 5.0 V Voltage Regulators
3. MC33063A 1.5 A Peak Boost/Buck/Inverting 12 V Switching Regulator
4. SMD High Frequency 25 MHz Crystal Unit

The following tables outline the reliability analysis of these four components. Each provides a specific equation for that component to compute the part failure rate, λ_p. MTTF is calculated according to the equation 1/ λ_p. The 3.3 V and 5.0 V regulators are evaluated as one component since they are the same part and have the same parameter values. The operating environment for each component is assumed to be ground benign since RFID Xpress is intended for use within a grocery or retail store, which is a non-mobile and temperature and humidity controlled environment. Any other assumptions made in the calculations are clearly stated. Useful parameter definitions are found below in Table 1.

λ_p = part failure rate
λ_b = base failure rate
C_1 = die complexity failure rate
C_2 = package failure rate (utilizes N_p)
N_p = number of functional pins
π_T = temperature factor
π_E = environment factor
π_Q = quality factor
π_L = learning factor

Table 1 – MTTF Parameter Definitions

For failure analysis, two levels of criticality were identified for RFID Xpress. Those levels, along with their explanation and maximum allowable probability, are detailed below in Table 2 and are discussed at length in the reliability analysis and FMECA.

Criticality Level	Description	Maximum Probability
High	Customer identification or safety compromised	$\lambda_p < 10^{-9}$
Low	Possible customer dissatisfaction	$\lambda_p < 10^{-5}$

Table 2 – Criticality Levels

2.1 – MC9S12NE64 microcontroller [2]

$$\lambda_p = (C_1\ \pi_T + C_2\ \pi_E) \text{ x } \pi_Q \text{ x } \pi_L \text{ failures per } 10^6 \text{ hours}$$

Parameter	Value	Justification
C_1	0.28	16-bit MOS microcontroller (MIL-HDBK-217F, Section 5.1)
C_2	0.041	80-pin SMT package $C_2 = 3.6 \text{ x } 10^{-4}\ (N_p)^{1.08}$, $N_p = 80$ (MIL-HDBK-217F, Section 5.9)
π_T	3.1	Digital MOS device, maximum operating temperature, T_j = 125°C (MIL-HDBK-217F, Section 5.8)
π_E	0.50	Assumes ground benign environment, G_B (MIL-HDBK-217F, Section 5.10)
π_Q	10	Commercial product screening level (MIL-HDBK-217F, Section 5.10)
π_L	1.0	Generic device in production ≥ 2 years (MIL-HDBK-217F, Section 5.10)

Table 3 – MC9S12NE64 Microcontroller MTTF Parameters

λ_p = 8.89 failures per 10^6 hours

MTTF = 112549.24 hours ≈ 12.85 years

The microcontroller was selected for reliability analysis due to its central role in the entire system. It is responsible for controlling the integrated peripherals such as the RFID reader, thermal printer, LCD, Ethernet, and keypad, as well as containing all of the software logic for the design. Therefore, proper operation of the microcontroller is integral to the success of RFID Xpress. While the microcontroller is relatively important compared to other components, the system does not pose any serious safety hazards to the customer should a failure occur. It is therefore considered a low criticality level, and a part failure rate of 8.89 x 10^{-6} hours is adequate. Also, taking into consideration the fact that the microcontroller will not be in continuous intensive operation during idle states and that it will normally be operating below the maximum rated temperature, this calculated MTTF is an upper-bound that will likely not pose a serious threat to system operation, and failure is reparable.

2.2 – REG1117A 1A LDO 3.3 and 5.0 V Voltage Regulators [3]

$$\lambda_p = (C_1\ \pi_T + C_2\ \pi_E) \text{ x } \pi_Q \text{ x } \pi_L \text{ failures per } 10^6 \text{ hours}$$

Parameter	Value	Justification
C_1	0.01	Assumes 1 to 100 transistors in linear MOS device (MIL-HDBK-217F, Section 5.1)
C_2	0.0012	3-pin SMT package $C_2 = 3.6 \text{ x } 10^{-4}\ (N_p)^{1.08}$, $N_p = 3$ (MIL-HDBK-217F, Section 5.9)
π_T	58	Linear MOS device, maximum operating temperature, $T_j = 125°C$ (MIL-HDBK-217F, Section 5.8)
π_E	0.50	Assumes ground benign environment, G_B (MIL-HDBK-217F, Section 5.10)
π_Q	10	Commercial product screening level (MIL-HDBK-217F, Section 5.10)
π_L	1.0	Generic device in production ≥ 2 years (MIL-HDBK-217F, Section 5.10)

Table 4 – REG1117A Voltage Regulator MTTF Parameters

$\boldsymbol{\lambda_p}$ = 5.81 failures per 10^6 hours

MTTF = 172235.62 hours ≈ 19.66 years

The 3.3 V and 5.0 V regulators were selected for reliability analysis because they provide two of the three supply voltages to system components and they are known to operate at higher than ambient temperatures. A thin copper strip was added to the heat dissipation pad of the 3.3 V regulator to decrease its operating temperature, as it increases noticeably when the circuit draws more current. The 3.3 V signal powers the microcontroller and RS-232 level translator, and the 5.0 V signal powers the LCD. Due to the fact that failures on either voltage regulator would simply result in improper operation (potentially including no operation at all) of the microcontroller, serial communication, and LCD, this component is rated at a low criticality level that would cause customer dissatisfaction. Therefore, the part failure rate of 5.81 x 10^{-6} is acceptable.

2.3 – MC33063A 1.5 A Peak Boost/Buck/Inverting 12 V Switching Regulator [4]

$$\lambda_p = (C_1 \pi_T + C_2 \pi_E) \text{ x } \pi_Q \text{ x } \pi_L \text{ failures per } 10^6 \text{ hours}$$

Parameter	Value	Justification
C_1	0.01	Assumes 1 to 100 transistors in linear MOS device (MIL-HDBK-217F, Section 5.1)
C_2	0.0034	8-pin DIP package $C_2 = 3.6 \text{ x } 10^{-4} (N_p)^{1.08}$, $N_p = 8$ (MIL-HDBK-217F, Section 5.9)
π_T	180	Linear MOS device, maximum operating temperature, $T_j = 150°C$ (MIL-HDBK-217F, Section 5.8)
π_E	0.50	Assumes ground benign environment, G_B (MIL-HDBK-217F, Section 5.10)
π_Q	10	Commercial product screening level (MIL-HDBK-217F, Section 5.10)
π_L	1.0	Generic device in production ≥ 2 years (MIL-HDBK-217F, Section 5.10)

Table 5 – 12V Switching Regulator MTTF Parameters

$\boldsymbol{\lambda_p}$ = 18.02 failures per 10^6 hours

MTTF = 55503.14 hours ≈ 6.34 years

The 12 V switching regulator was selected for reliability analysis because it provides power for the RFID receiver, which is an integral part of the design. It also operates at higher than ambient temperatures, which makes it a greater candidate for failure. The relatively large number of resistors, capacitors, and inductors associated with the 12 V power circuit (compared to the other power circuits) also increases the opportunity for failure. If power somehow became shorted to ground in the circuit, excessive heat may be generated that could possibly overheat components and cause a fire, resulting in injury to the customer. In this high criticality situation, a part failure rate of $18.02 \text{ x } 10^{-6}$ is unacceptable. However, in the more likely event that the voltage regulator fails to output the proper voltage or shuts down entirely, the RFID reader would simply cease to operate. While this would render the entire unit useless until it was repaired and would result in customer dissatisfaction, it poses no serious risk to the customer. In this low criticality situation, the calculated part failure rate is acceptable.

2.4 – SMD High Frequency 25 MHz Crystal Unit [5]

$\lambda_p = \lambda_b \text{ x } \pi_Q \text{ x } \pi_E$ failures per 10^6 hours

Parameter	Value	Justification
λ_b	0.027	25 MHz (MIL-HDBK-217F, Section 19.1)
π_Q	2.1	Assumes lower than MIL-SPEC (MIL-HDBK-217F, Section 19.1)
π_E	1.0	Assumes ground benign environment, G_B (MIL-HDBK-217F, Section 19.1)

Table 6 – 25 MHz Crystal MTTF Parameters

$\boldsymbol{\lambda_p}$ = 0.0567 failures per 10^6 hours

MTTF = 17636684.30 hours ≈ 2013.32 years

The 25 MHz crystal unit was selected for reliability analysis due to its sensitivity and the sensitivity of the components within the oscillator circuit. It is possible that simply probing the traces in the oscillator circuitry could cause permanent damage and result in erratic operation of the microcontroller. However, should a failure actually occur with the crystal unit, the effects would be limited to the microcontroller and the components that depend on proper timing. It is likely that the internal bus clock would not operate properly, thereby distorting the baud rate and causing serial communication to break down. The customer would not be at serious risk in this situation, so the failure rate of 0.0567 x 10^{-6} is not only acceptable, but results in the longest MTTF out of all the components identified as high-risk.

2.5 – Conclusion

The results of this reliability analysis are organized in Table 7. The shortest MTTF is clearly the 12 V switching regulator, which seems logical. The microcontroller, 3.3 V, and 5.0 V regulators all have relatively similar MTTF values. Should a failure occur in the system, it is clear that these components are most likely to be at fault. The 25 MHz crystal, on the other hand, is estimated to be orders of magnitude more reliable than the other components and won’t be any more likely to experience failure than any other random minor component in the design. While the failure rate for the microcontroller and voltage regulators may seem high, it is important to remember that the worst-case operating temperatures were used in these calculations and that measures have already been taken to increase heat dissipation in necessary components. Therefore, it is believed that the calculated MTTF of the overall design is reasonable and safe.

Component	**λ_p per 10^6 hours**	**MTTF (hours)**
MC9S12NE64 microcontroller	8.89	1.12549×10^5
REG1117A 3.3 V, 5.0 V regulator	5.81	1.72235×10^5
12 V switching voltage regulator	18.02	5.5503×10^4
25 MHz crystal unit	0.0567	1.7636684×10^7

Table 7 – RFID Xpress Reliability Analysis Results

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

For the Failure Mode, Effects, and Criticality Analysis, the overall schematic was partitioned into seven functional blocks: 5.0 V Power Circuit (A), 3.3 V Power Circuit (B), 12 V Power Circuit (C), Microcontroller and Oscillator Circuit (D), Ethernet and Physical Transceiver Circuit (E), RFID and Printer RS-232 Circuit (F), and Keypad and LCD Interface Circuit (G). Schematics of each block can be found in Appendix A. The potential failure modes of each block are examined in the FMECA worksheet in Appendix B, including possible causes and effects of failure, methods of detection, and criticality.

The criticality levels in this analysis correspond to those mentioned previously in Table 2. A failure with a criticality level of "high" ($\lambda_p < 10^{-9}$) either compromises customer safety or customer identity. A failure with a criticality level of "low" ($\lambda_p < 10^{-5}$) is likely to cause customer dissatisfaction.

4.0 Summary

Analyzing the safety and reliability of RFID Xpress is an integral part of the design process. This paper has identified those components believed most likely to fail and calculated their part failure rates, λ_p, and mean time to failure (MTTF). The values obtained were within acceptable limits for the predefined levels of criticality. This paper also analyzed potential modes of failure by functional blocks and identified causes and effects for those problems. The

RFID Xpress system was designed to improve the customer's retail shopping experience, all the while maintaining adequate levels of customer safety and security.

List of References

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

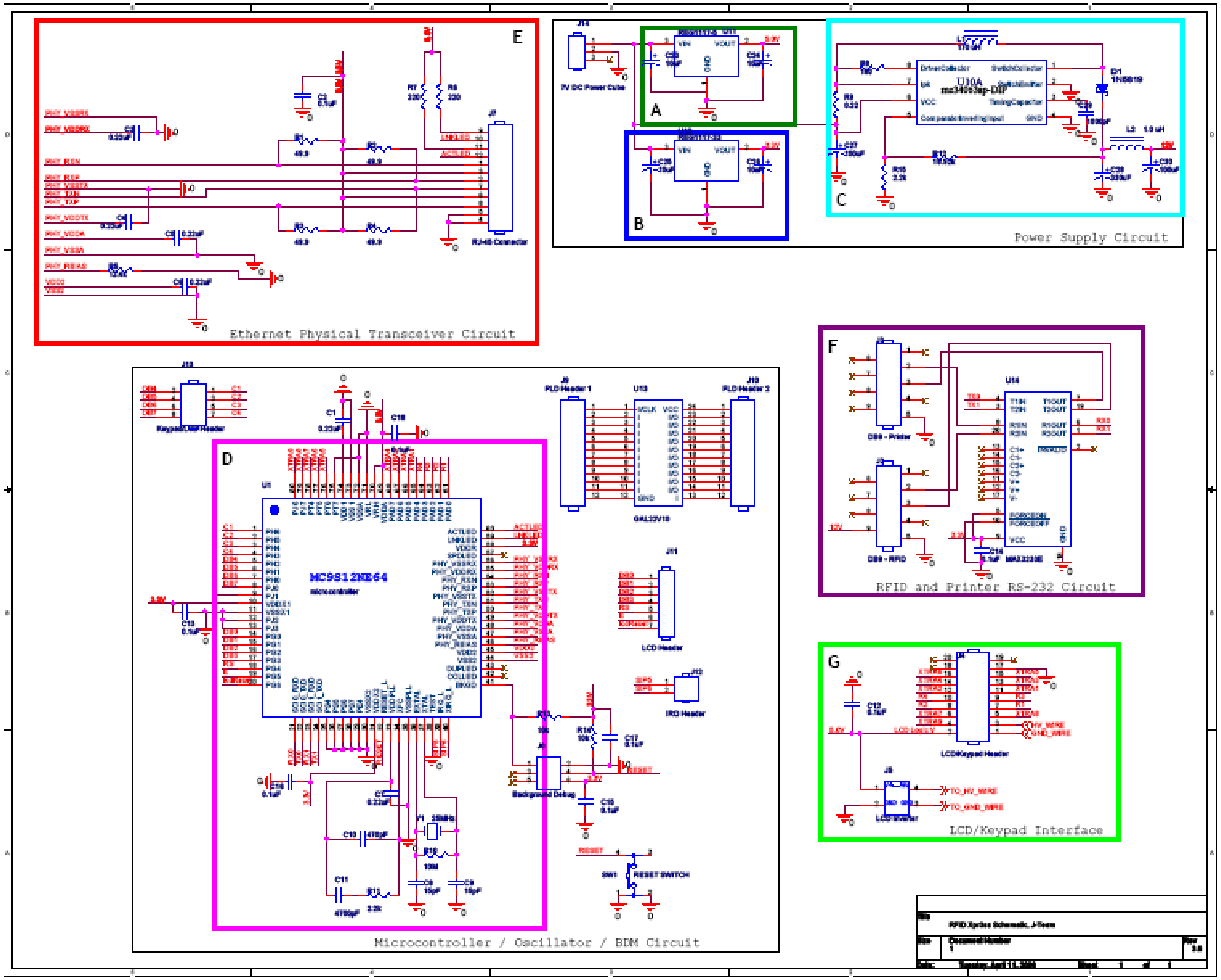
[2] Freescale MC9S12NE64 Microcontroller data sheet
http://www.freescale.com/files/microcontrollers/doc/data_sheet/MC9S12NE64V1.pdf

[3] REG1117A 1A LDO Voltage Regulator data sheet
http://focus.ti.com/lit/ds/symlink/reg1117.pdf

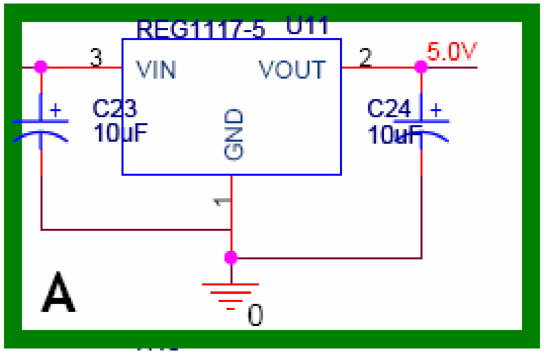
[4] MC33063A 1.5 A Peak Boost/Buck/Inverting Switching Regulator data sheet
http://focus.ti.com/lit/ds/symlink/mc33063a.pdf

[5] SMD High Frequency 25 MHz Crystal Unit data sheet
http://www.eea.epson.com/go/Prod_Admin/Categories/EEA/QD/Crystals/mhzSMD_Crystals/go/Resources/TestC2/MA406

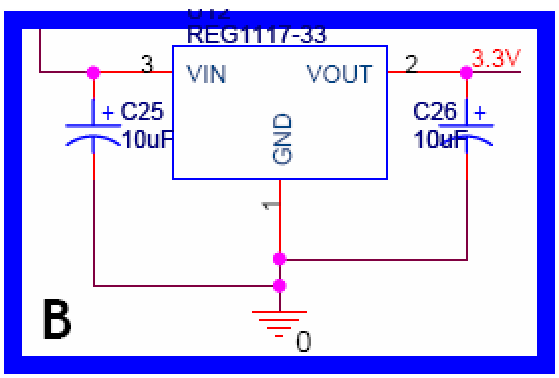
Appendix A: Schematic Functional Blocks



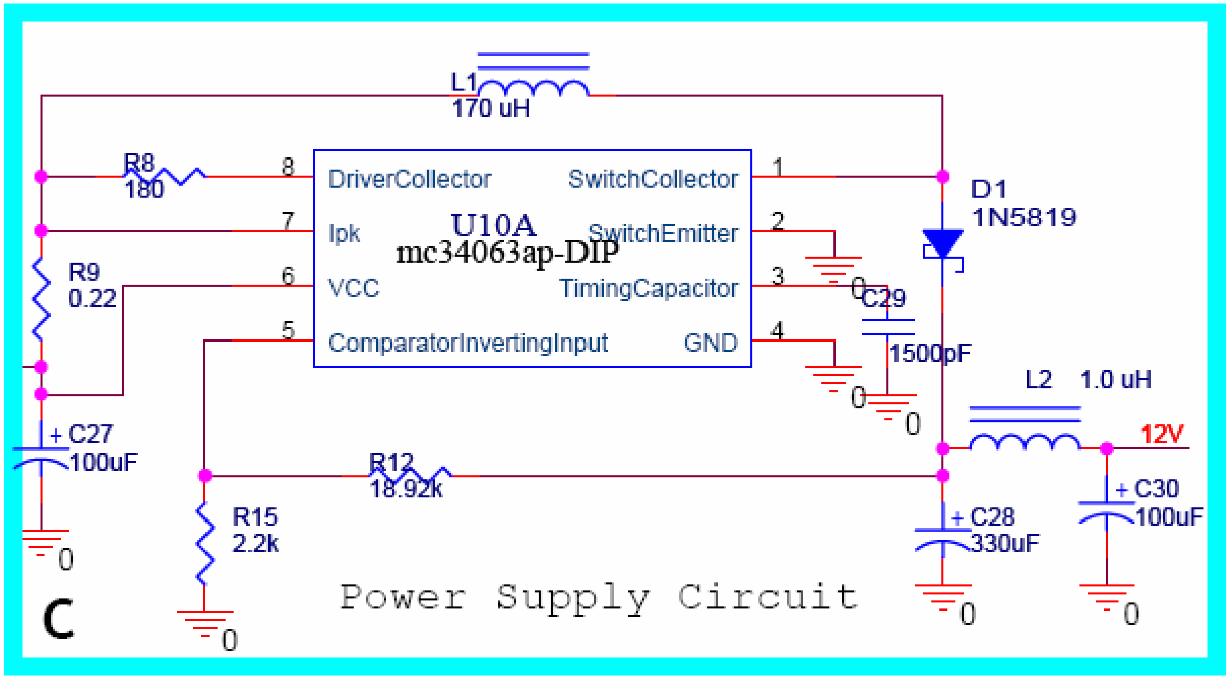
Overall Design Schematic



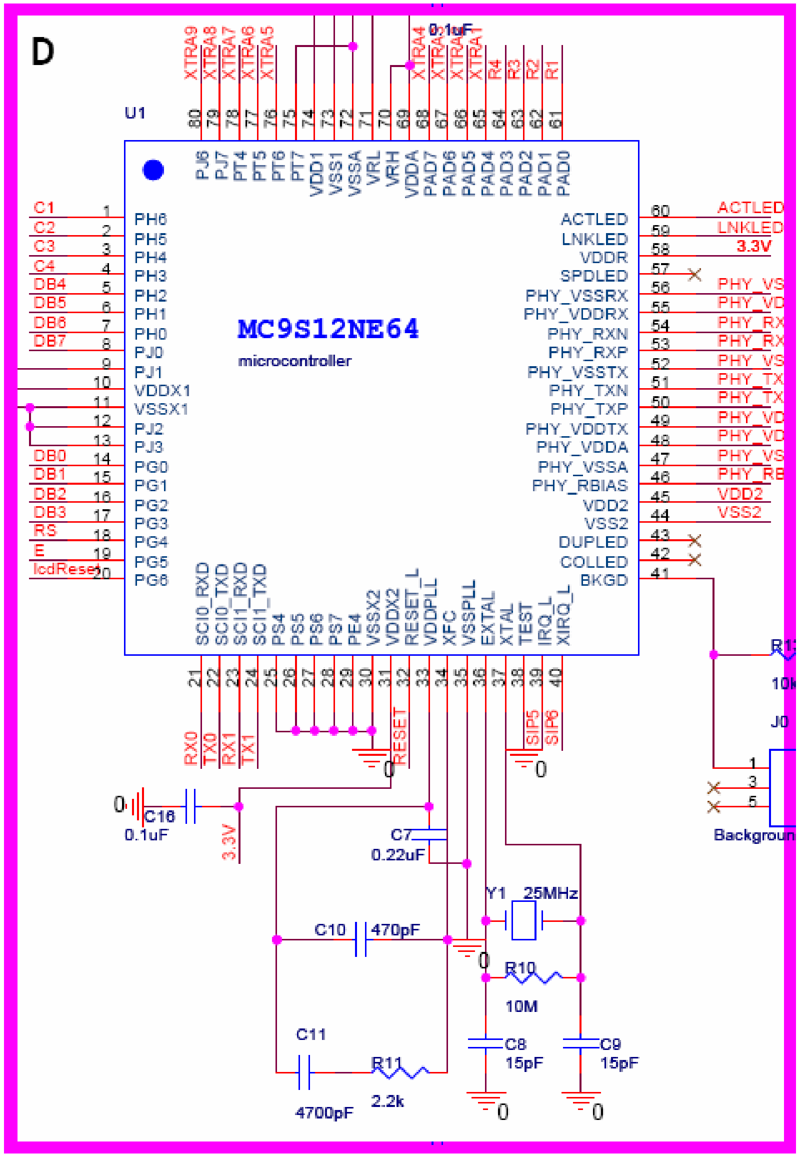
Block A: 5.0 V Power Circuit



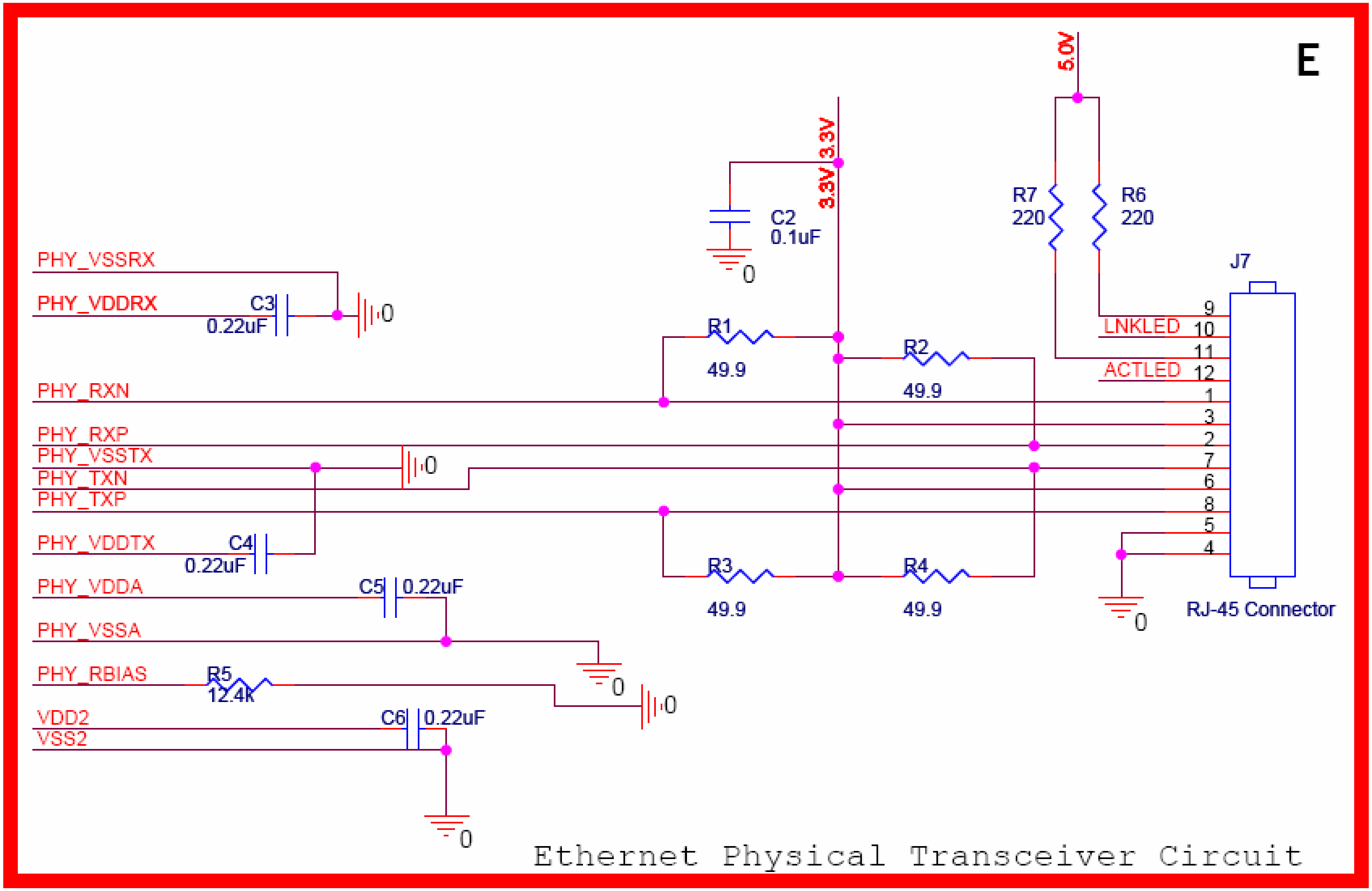
Block B: 3.3 V Power Circuit



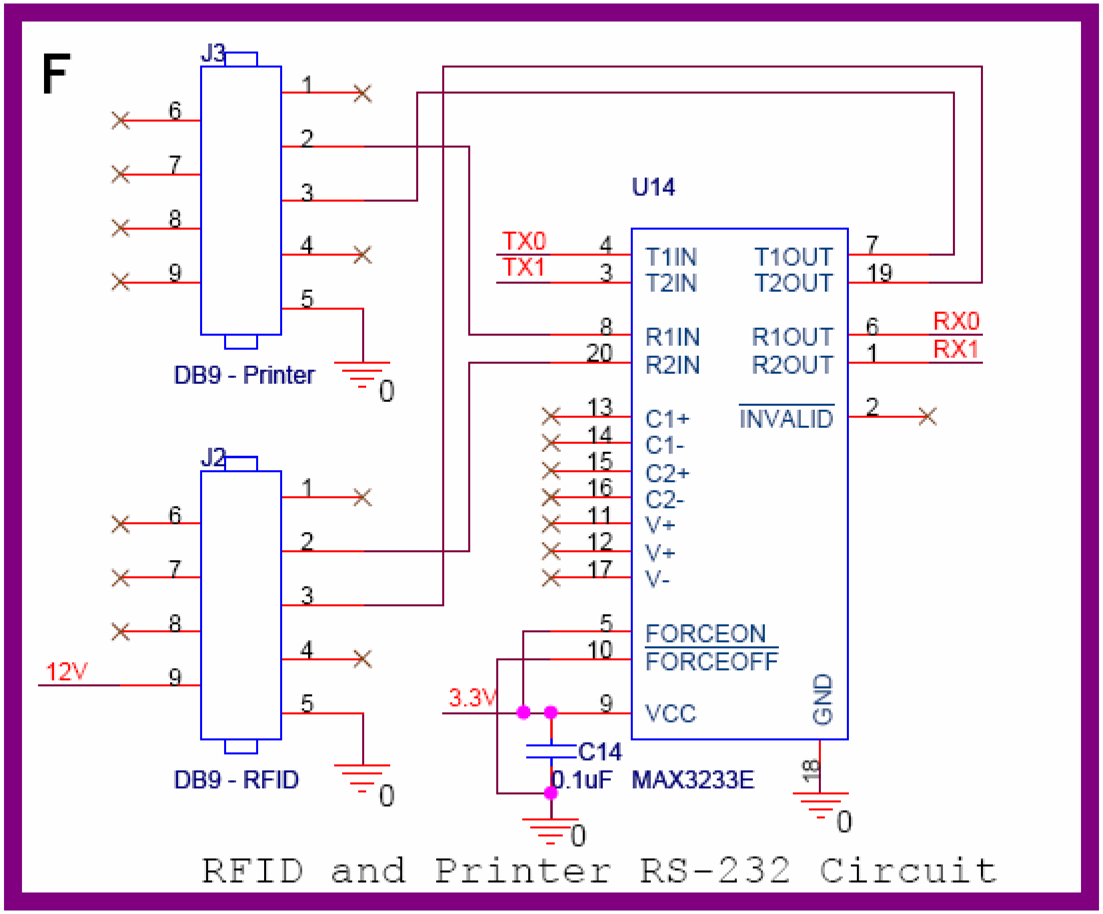
Block C: 12 V Power Circuit



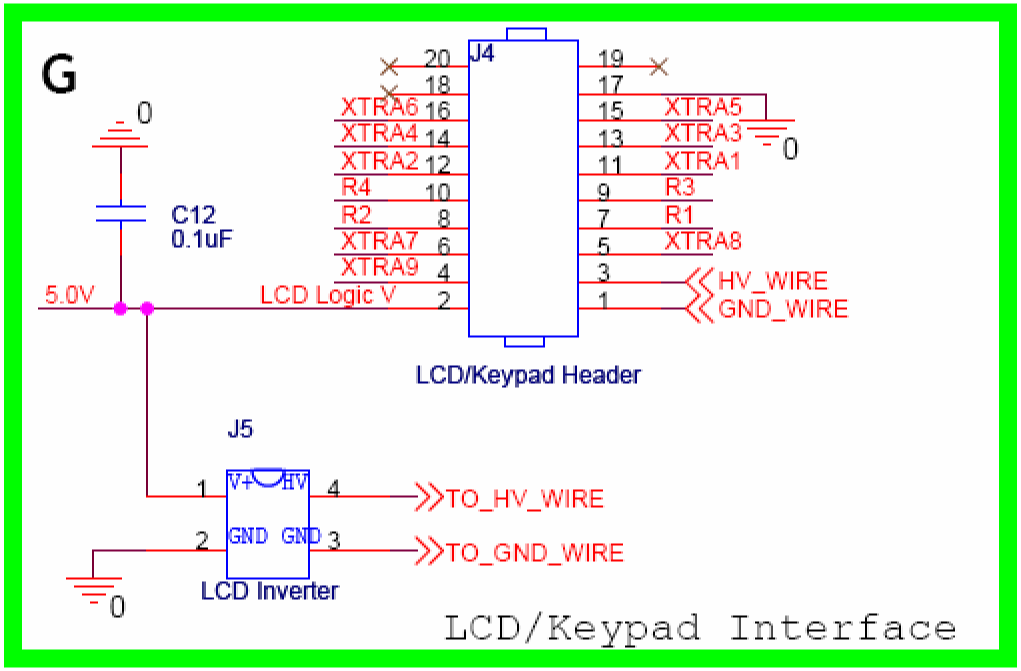
Block D: Microcontroller and Oscillator Circuit



Block E: Ethernet Physical Transceiver Circuit



Block F: RFID and Printer RS-232 Circuit



Block G: Keypad and LCD Interface Circuit

Appendix B: FMECA Worksheet

Failure No.	Failure Mode	Possible Causes	Failure Effects	Method of Detection	Criticality	Remarks
A1	Output = 0 V	Failure of any component in A or an external short to ground	LCD ceases to function, short could potentially cause overheating	Observation	High	Customer could potentially be injured if component overheating leads to fire
A2	Output > 5.0 V	Failure of U11	Potential damage to LCD	Observation	Low	Regulator should have automatic shutdown if voltage or current get too high
A3	Output out of tolerance	Failure of C23, C24, U11	Out-of-spec operating voltage; unpredictable	Observation	Low	
B1	Output = 0 V	Failure of any component in B or an external short to ground	μC and RS232 line driver cease to function, potential overheating	Observation	High	Customer could potentially be injured if component overheating leads to fire
B2	Output > 3.3 V	Failure of U12	Potential damage to μC and/or RS232 line driver	Observation	Low	Regulator should have automatic shutdown if voltage or current get too high

B3	Output out of tolerance	Failure of C25, C26, U12	Out-of-spec operating voltage; unpredictable	Observation	Low	
C1	Output = 0 V	Failure of any component in C or an external short to ground	RFID reader ceases to function, short could potentially cause overheating	Observation	High	Customer could potentially be injured if component overheating leads to fire
C2	Output > 12 V	Failure of U10	Potential damage to RFID reader	Observation	Low	Regulator should have automatic shutdown if voltage or current get too high
C3	Output out of tolerance	Failure of L1, L2, D1, R8, R9, R12, R15, C27, C28, C29, C30, U10	Out-of-spec operating voltage; unpredictable	Observation	Low	
D1	Output continuously 0	U1, Y1, C1, C7, C8, C9, C10, C11, C13, C16, C17, C18, R10, R13, R14, reset circuitry, software	LCD, printer may display erratic output, keypad, Ethernet may not function properly	Observation	Low	
D2	Output continuously 1	U1, Y1, C1, C7, C8, C9, C10, C11, C13, C16, C17, C18, R10, R13, R14, software	LCD, printer may display erratic output, keypad, Ethernet may not function properly	Observation	Low	

D3	User information not validated correctly	Failure of U1, software	Incorrect PIN accepted, wrong user authenticated	Observation	High	Could compromise user’s identity, allow purchases on others’ accounts
E1	Ethernet doesn’t work	Failure of any component in E, U1, software	Email, database lookups, time synchronization unsuccessful	Observation	Low	ACTLED and LNKLED provide Ethernet status notification
F1	Receipt fails to print	Failure of U14, J3, U1, software	Receipt printing unsuccessful, default to email receipt	Observation	Low	Could also be caused by failure of printer itself
F2	RFID reader fails to detect tags	Failure of U14, J2, U1, software	RFID tag not acknowledged, unable to scan items or user key fobs	Observation	Low	Could also be caused by failure of RFID reader itself
G1	LCD display functioning improperly	Failure of U1, J5, C12, software	LCD displays incorrect or no information, unable to view cart or status	Observation	Low	Could also be caused by failure of LCD or inverter module itself
G2	LCD backlight too bright or off	Failure of J5	LCD backlight failing, possible problem with inverter	Observation	High	Customer could potentially be injured if inverter malfunction leads to fire

G3	Keypad entries not detected	Failure of U1	Key presses not recognized, unable to enter PIN or make menu selections	Observation	Low	Could also be caused by failure of keypad itself