Reliability and Safety Analysis

Year: 2019 **Semester:** Spring **Team:** 2 **Project:** The Guard DAWG System
Creation Date: 3/24/19 **Last Modified:** March 29, 2015
Author: Ian Sibley **Email:** isibley@purdue.edu

1.0 Reliability Analysis

XRCGB48M000F0L00R0 Oscillator (Quartz Crystal, pg. 170)

$$\lambda_p = \lambda_b \cdot \pi_Q \cdot \pi_E \text{ Failures}/10^6 \text{ Hours}$$

The XRCGB48M000F0L00R0 is used in a handful of timing aspects of our product. Though no major systems issues should arise from its failure in the current design, there's still potential to stall out the process should the timer be needed for that section. Currently, this can potentially result in the user being locked out indefinitely should 3 invalid keypad inputs be given. Its reliability rating was chosen for this reason, as even the lightest use case can have cause for concern. Using the Quartz Crystal model in the MIL-HDBK-217F [1], both λ_p and MTTF were calculated using the respective equation, shown above. This falls well within our expected range, as it'd take more than a lifetime for this component to fail. A failure of this oscillator would not directly cause harm to the user.

Table 1: *Oscillator reliability evaluation*

Variable	Variable Name		Value	Comments
λ_b	Base failure rate		0.032	48 MHz frequency
π_Q	Quality Factor		2.100	Non-Military grade
π_E	Environmental Factor		10.000	G_m
Component Results				
	λ_p	=	0.665	Failures/1e6 hours
	MTTF	=	1.504	1e6 hours

C1Q3751206 Fuse (pg. 173)

$$\lambda_p = \lambda_b \cdot \pi_E \text{ Failures/1e6 hours}$$

Our C1Q3751206 fuse is used to protect our power regulator from power surges from its supply. Should it fail at a critical time, our power regulator won't be protected, and the whole circuit is liable to stop working, or worse, become damaged. This makes a strong case for its need for reliability, as it's on the front lines for the functioning of our entire circuit. The Fuse model in the MIL-HDBK-217F [1] was used to calculate both λ_p and MTTF, using the respective equation shown above. This would take more than a lifetime for this component to fail, so it easily falls within our expected rating range. A failure of this fuse would not directly cause harm to the user.

Table 2: *Fuse reliability evaluation*

Variable	Variable Name		Value	Comments
λ_b	Base failure rate		0.010	Base rate for all types
π_E	Environmental Factor		8.000	G_m
Component Results				
λ_p		=	0.080	Failures/1e6 hours
MTTF		=	12.500	1e6 hours

LT3668EMSEPBF Power Switch Regulator (pg. 25)

$$\lambda_p = (C_1 \cdot \pi_T + C_2 \cdot \pi_E)\, \pi_Q \cdot \pi_L \text{ Failures/1e6 hours}$$

The power switch regulator is a focal point for our entire microcontroller-based section of the project to function, as without it no component is able to receive the appropriate power. If the power regulator were to fail, there's potential for either no power or too much power to propagate throughout the PCB, and therefore put the rest of the product in danger of being irrecoverable. The reliability rating was chosen for this reason, and the "Microcircuits, Gate/Logic Arrays and Microprocessors" section was used for its evaluation. This component exceeds our preferred reliability range by significant margins, and furthermore, any potential failure of this power regulator would not directly cause harm to the user.

Table 3: *Power Switch Regulator reliability evaluation*

Variable	Variable Name		Value	Comments
C_1	Die Complexity 1		0.004	assume 0.3k - 1k gates
π_T	Temperature Factor		0.100	~85℉ max use
C_2	Package Failure Rate		0.006	16 pins
π_E	Environment Factor		4.000	G_m

π_Q	Quality Factor		2.000	Consumer Quality
π_L	Learning Factor		1.000	+2 years in production
Component Results				
		λ_p	=	0.046	Failures/1e6 hours
		MTTF	=	21.930	1e6 hours

RFD3055 Power MOSFET to Door Motor

$$\lambda_p = \lambda_b \cdot \pi_T \cdot \pi_A \cdot \pi_Q \cdot \pi_E \text{ Failures/1e6 hours}$$

The MOSFET is the hinge point that takes the result of our hardware and software readings, processings, and communications, and facilitates its desired purpose for the user. Furthermore, should it fail, the user has potential to be locked out of their home if they don't have the means to engage the manual override, i.e. if they don't have their house or building key (as commonly only higher-level employees and parents carry keys for business and home buildings, respectively). This makes the failure rate of this component very important, both for the convenience of our consumer body and potentially their safety from weather and other conditions, so it was chosen for these reasons. The "Transistors, Low Frequency, Si Fet" section was used for this analysis. this component piece fails in about 10 or 11 years, by these calculations, lower than our preferred range. A failure of this power regulator would not directly cause harm to the user.

Table 4: *Door Motor's Power MOSFET reliability evaluation*

Variable	Variable Name		Value	Comments
λ_b	Base Failure Rate		0.012	MOSFET group
π_T	Temperature Factor		3.000	~85℉ max operation
π_A	Application Factor		4.000	24W max power
π_Q	Quality Factor		8.000	Assume plastic quality
π_E	Environment Factor		9.000	G_m
Component Results				
		λ_p	=	10.368	Failures/1e6 hours
		MTTF	=	0.096	1e6 hours

MSP432[P401RIPZR] Microcontroller for Guard DAWG System

$$\lambda_p = (C_1 \cdot \pi_T + C_2 \cdot \pi_E) \cdot \pi_Q \cdot \pi_L \text{ Failures/1e6 hours}$$

The MSP432 is our microcontroller, which is in charge of all the logic for our door-related operations. Should it fail, there's potential for anything from continuous activation of the motor to locked or unlocked, or vacillation between, though this will only provide inconvenience for the user; the motor driver we're using won't break or fry from this actuation, though obviously extended use of the electrical components involved may increase their wear over time. This component doesn't pose any danger to a user, especially if contained, besides whatever inconvenience the lock/unlocking behavior might pose. This component falls well within our range of reliability, 6+ million hours is excessively reliable.

Table 3: *MSP432 Microcontroller reliability evaluation*

Variable	Variable Name		Value	Comments
C_1	Die Complexity 1		0.560	32 bit Micro
π_T	Temperature Factor		0.100	~85℉ max use
C_2	Package Failure Rate		0.040	Hermetic category
π_E	Environment Factor		4.000	G_m
π_Q	Quality Factor		2.000	Consumer B-1 Quality
π_L	Learning Factor		1.000	+2 years in production
Component Results				
	λ_p	=	0.157	Failures/1e6 hours
	MTTF	=	6.378	1e6 hours

Summary

While this is shorter than desirable, as the minimum reliability rating states, 10 years is still a good lifespan for a product like this. It's likely that there's a newer and more advanced model or competitive product by then, and the users would replace the unit by then anyways. Since this product would likely be a relatively cheap security measure, 10 years for even one or two hundred dollars is fairly reasonable; even $20 a year for a dynamic security product that's the first to use facial recognition for user access becomes a fairly reasonable price, though we will still be aiming to make a product at a competitive price in the market. Our strongest alterations to the design to allow for higher longevity include getting a higher quality MOSFET, operating it under less power by using a different motor with lower requirements, or investigating potential MOSFET alternatives that yield better wear resistance under our desired conditions.

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

Failure modes were divided into 4 grouped sections: Power, State LEDs and Auxiliary Inputs, Bluetooth, and Microcontroller. This is a relatively straightforward sectioning of our design into four general categories, though our schematic has them divided even further. Though some have more effects than others, all have failure cases that are worth considering.

Our criticalities were rated Very High, High, Moderate, or Low, with Very High rating at $\lambda_p <$ 0.5 Failures/1e9 hours, for only one component with the potential to "pop", though this state should be impossible for it to reach without highly significant wear. High describes a potential full-system propagation of failure and damage to significant components, and was rated at $\lambda_p <$ 0.01 Failures/1e6 hours, as they'd make a board at least partially irrecoverable. Moderate was a rating assigned to components that failed locally and stopped some functionality, but were fixable with replacements, and given a $\lambda_p < 0.1$ Failures/1e6 hours. Low criticality components were designated a $\lambda_p < 10$ Failures/1e6 hours, to which the only components it applies to is the likely unused external Oscillator, where a failure wouldn't change the functioning of any other component or need to be replaced, unless design plans change.

The motor driver's R10 failure would lead to an increased likelihood that the D1 MOSFET fails, which in turn would prevent the door motor from being actuated. The R9 failure case would, contrarily, prevent the door motor from being actuated but without any damage to the other parts of the actuating circuits themselves. The D1 MOSFET failure itself would of course mean the door motor couldn't be actuated, but this is particularly vulnerable to parasitic inductance from the motor currently. However, a schottky diode will soon be placed on the wire line leading to the motor, minimizing the exposure of the MOSFET to this parasitic inductance.
The C16 capacitor failing would potentially require more power to be pushed through the PCB than the traces can handle, but this would be our only expected "active" failure possibility, resulting in a popcorning effect. Housed in the protective case, and again requiring a potentially impossible scenario, this becomes extremely unlikely, though its damage to the rest of the PCB and physical blow itself are both highly undesirable, as contained as they may be by the product housing.
The Buck Converter requires a reference voltage to operate properly, and if either C11 fails, or the pair R15 and R14 fail, the reference voltage will become inaccurate and damage the buck converter. Should the Buck Converter fail, damage propagation becomes unpredictable, and either just removes power from the rest of the non-24V system (i.e. everything not powering the door motor), or possibly pushes higher power through the rest of the system than the system is capable of handling. Since nothing outside of the door powering circuitry is made to withstand 24V, full system failure is possible, and undesirable. Failure of the fuse, on the other hand, likely implicates lack of power to the system, though this would be fixed by the replacement of the fuse. Should the fuse short, it cannot protect the system from power surges and the Buck Converter potentially failing as well, though if detected it can also be fixed by a replacement of the fuse.

Should any of the resistors associated with the Keypad or State LEDs fail, the system would experience partial failure: for every resistor that fails on the keypad a column will stop registering input, while an LED with a failed resistor will likely eventually burn out, and the system state won't be accurately displayed. The Keypad failure is the more concerning here, and may leave the user with only the physical bypass option left should they find the facial recognition system inoperable or falsely registering their face.
The Hall Effect sensor's R11 failure could potentially blow the HES, which would leave the system unable to tell when the door is open or closed and potentially damage the GPIO pin associated with the sensor's reading. This would leave the system incapable of locking the door, and require a replacement of the hall effect sensor and resistor, and potentially a replacement of the MSP432 if an alternate pin couldn't be used (likely not an option for the average consumer).
Capacitor failures C1 and C2 on the External Oscillator could result in enough noise that the readings from it become completely unreliable, and speed up any systems relying on it. Failure of the oscillator itself would mean its clock signal remains indefinitely low, so any system reading and relying on that clock signal would hang indefinitely as well.

Failure of the capacitors C8 and C7 of the Bluetooth module shouldn't have too much effect, since the HC-05 has its own internal protective circuitry, though may leave it more vulnerable to power oscillations. This makes these capacitors failing less than crucial for system operating, though still good practice to have.

Finally, the MSP432 decoupling capacitors C3, C4, C5, and C6 failing would result in the failure of the MSP432 itself, and obviously a full stop of the entire system, with unpredictable behavior of related systems as the outputs given to them will vary. Ideally, nothing will propagate failure, though the door lock could be stuck open or locked.

3.0 Sources Cited:

[1] Military handbook: reliability prediction of electronic equipment. Washington, D.C.: U.S. Dept. of Defense, 1990.

[2] “LT3668 40V 400mA Step-Down Switching Regulator with Dual Fault Protected LDOs.” 1630 McCarthy Blvd., Milpitas, CA.

[3] “MSP432P401R, MSP432P401M SimpleLink™ Mixed-Signal Microcontrollers.” . Device Data Sheet.

[4] “12A, 60V, 0.150 Ohm, N-Channel Power MOSFETs.” 2AD. Device Data Sheet.

Appendix A: Schematic Functional Blocks

Figure 1: Buck Converter

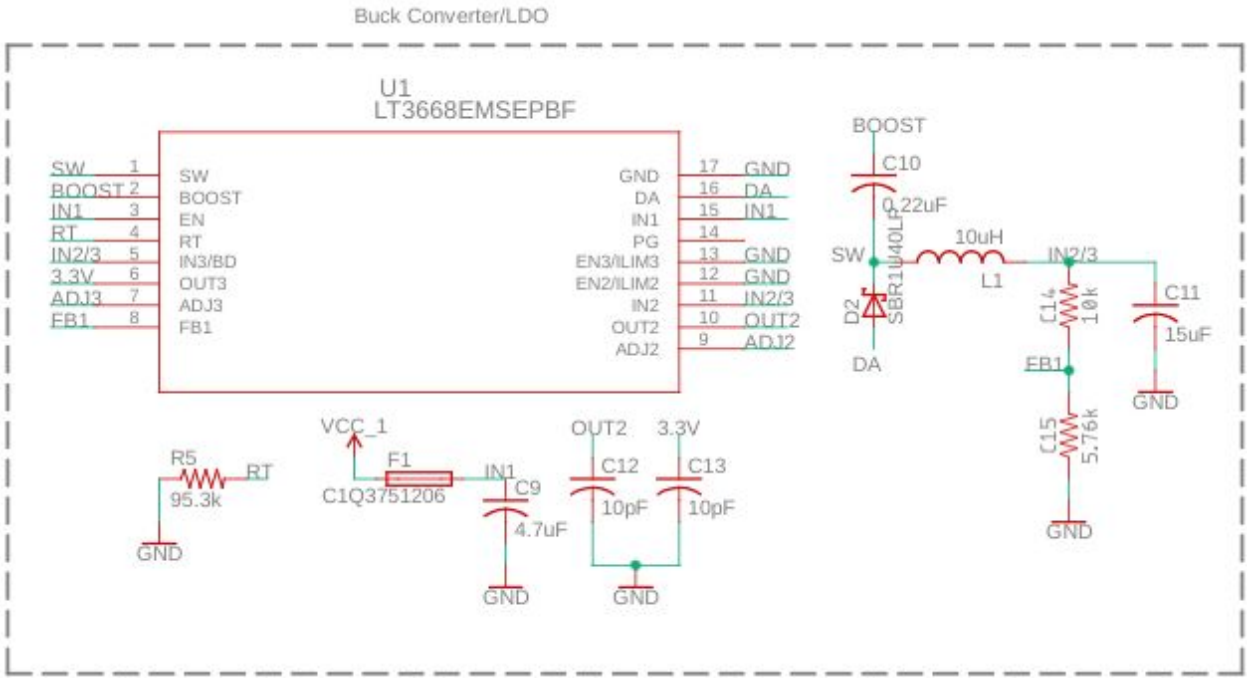


Figure 2: Power input section

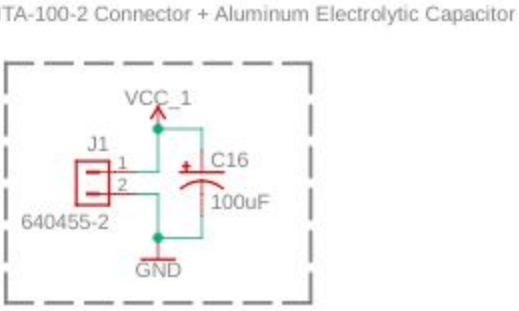


Figure 3: Motor Driver block

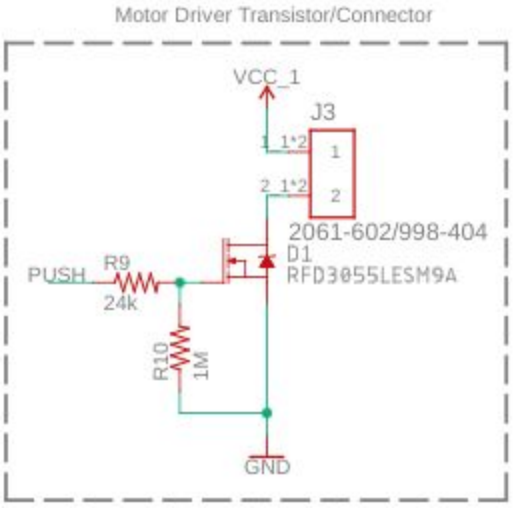


Figure 4: Programmer connector

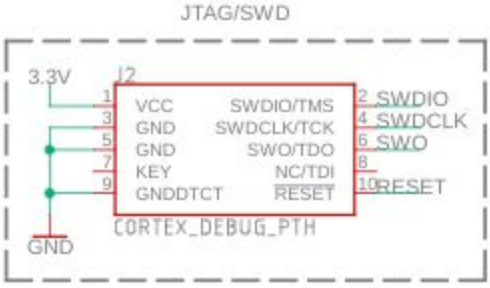


Figure 5: Software Debugging LEDs

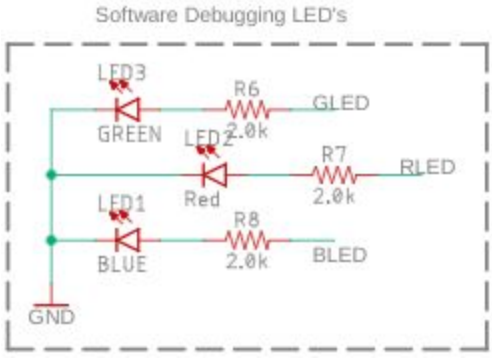


Figure 6: Keypad

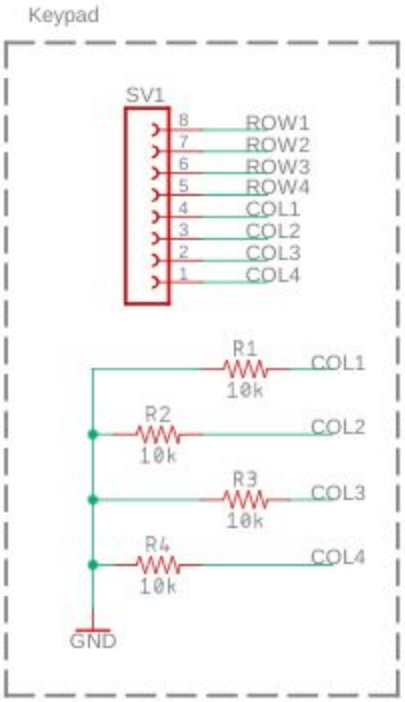


Figure 7: Hall Effect Sensor

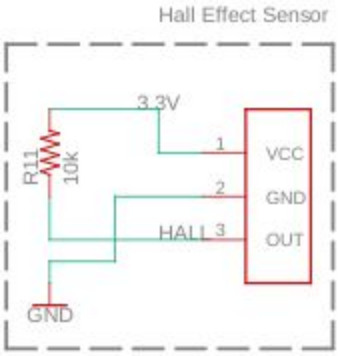


Figure 8: External Oscillator

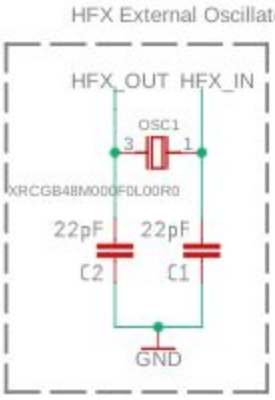


Figure 9: Bluetooth Module

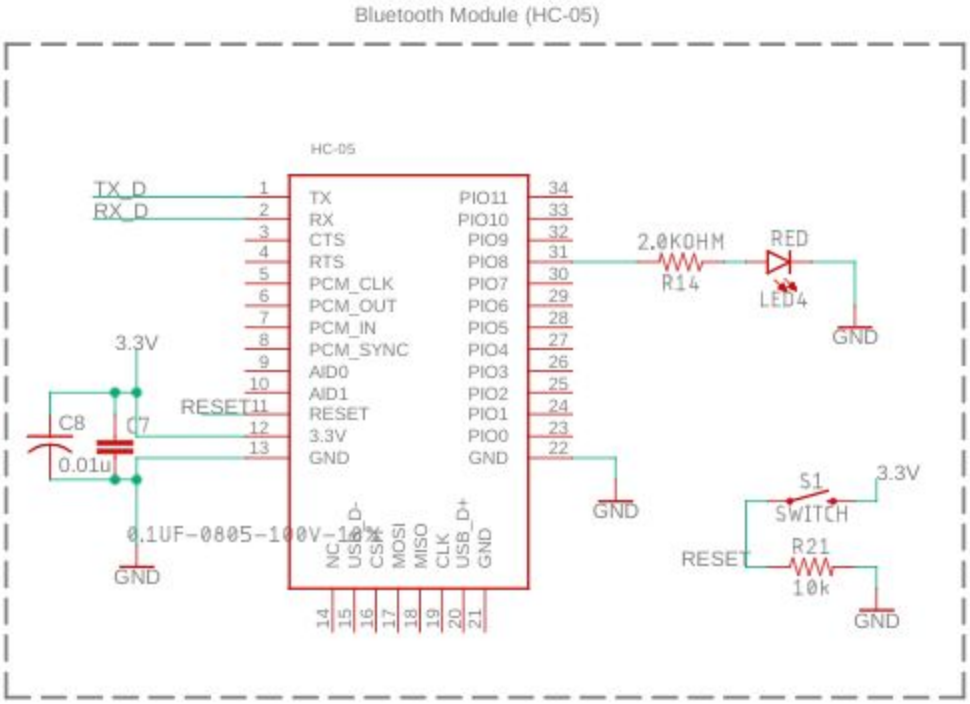


Figure 10: Micro Decoupling Capacitors

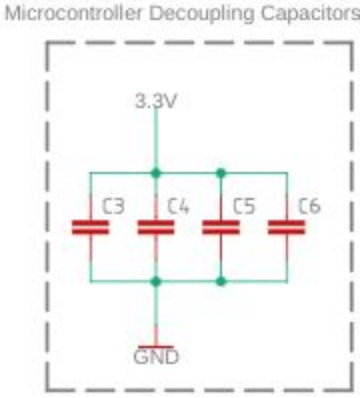
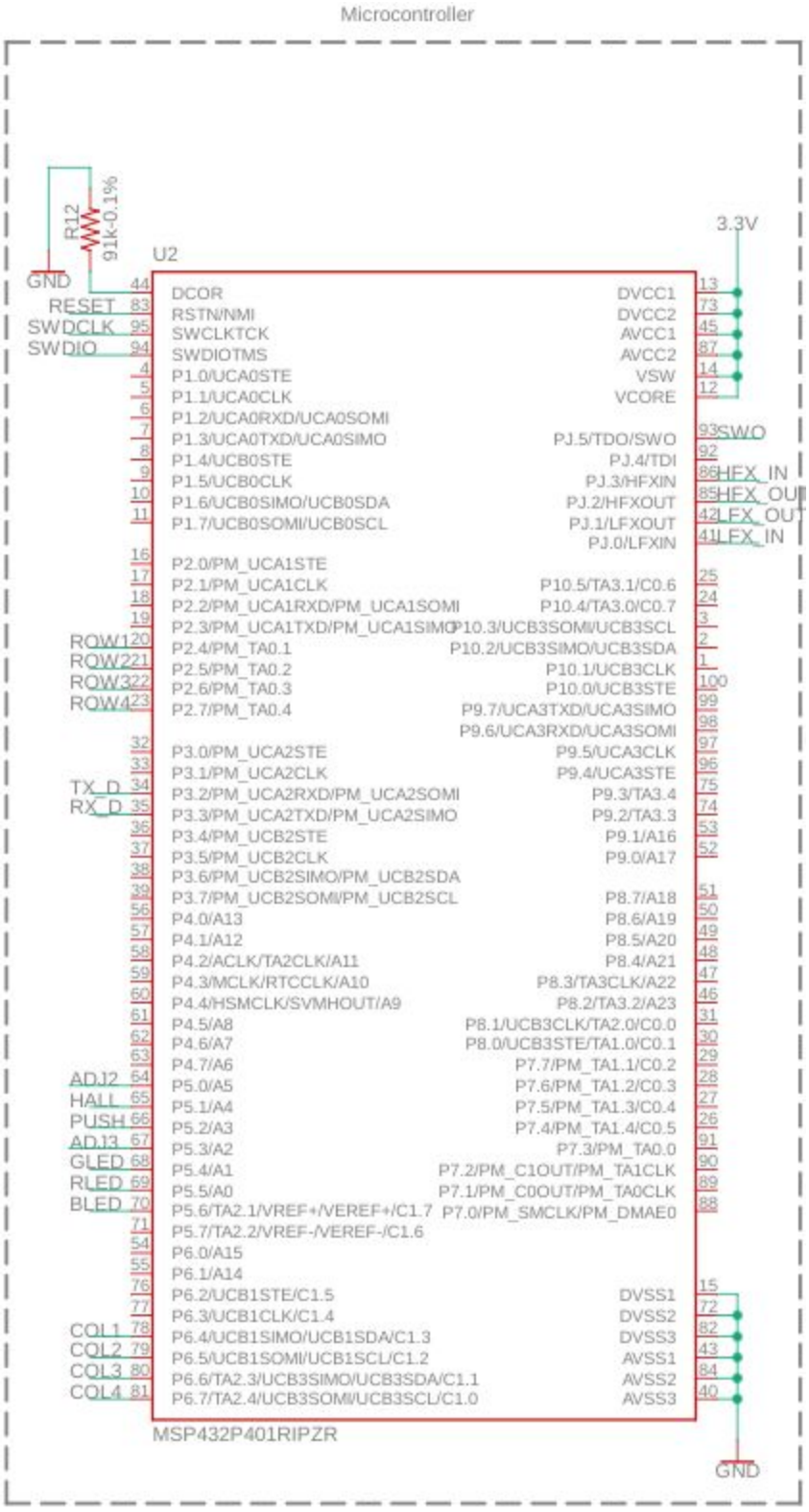


Figure 11: MSP432 Microcontroller



Appendix B: FMECA Worksheet

Subsystem A: Power System Sections (Buck Converter, Motor Driver, Power Input)

Failure No.	Failure Mode	Possible Causes	Failure Effects	Method of Detection	Criticality	Remarks
1	Popcorn, exploding capacitor	C16	Unpredictable, possible loss of system power or further propagated damage	Audible capacitor failure, likely system failure as well	Very High	This is highly unlikely, as it would require putting more power through our board than the traces should be able to handle
2	Inability to actuate the door motor	R9, D1, R10	Inability to actuate lock on door motor, likely continuously pulled open	Door unable to lock, and/or change position	Moderate	The MSOFET is susceptible to flyback current from the motor, and therefore failure, but a schottky diode is planned to be added to minimize that risk
3	False buck converter reference voltage	R15, R14, C11	Leads to buck converter failure and unpredictable fallout through the system	Whole system failure	High	This will either just shut the system off, or load the system with too high of a voltage and fry components
4	Either open and complete power denial, or short and lack of protection from power vacillation	F1	Either system shuts off, or no change with normal power input. If power input surges, potential system failures	Whole system failure if open. If shorted, potentially no noticeable difference	High	It is less likely that a fuse fails to a short circuit, in all likelihood the power will go out in the system and the fuse should then be checked.

Subsystem B: Debugging LEDs & External Inputs (Hall Effect Sensor, Keypad, Oscillator)

Failure No.	Failure Mode	Possible Causes	Failure Effects	Method of Detection	Criticality	Remarks
5	Keypad input column fails to read	R1, R2, R3, R4	Parts or all of the keypad become unable to register input, user bypass becomes limited to mechanical	Keypad input doesn't register on 1 or more columns	Moderate	Fixed by replacement of failed resistor(s)
6	LED failure to operate properly for debugging or user signalling	R6, R7, R8	One or more debug/use case signalling LEDs fails to signal the current system status	Normal operating states not accurately reflected by state LEDs	Moderate	Fixed by replacing components, no propagation of failure elsewhere
7	Noisy oscillator signals	C1, C2	Signal coming from the oscillator could become noisy enough that it no longer becomes reliable	Inconsistent timer based operations, in the time they take to run.	Low	Potentially don't need the external oscillator, was put on the design for potential Software uses.
8	Full low oscillator signal (period → ∞)	OSC1	Any process requiring the oscillator signal will hang indefinitely	Freezing of any processes relying on the oscillator	Low	No current plans to use external oscillator
9	Failure of contact for JTAG connector	J2	Inability to interface with and update the MSP432, potential scrambling of whatever pre-existing code exists on it already	Inability to write desired code and get desired behavior	Moderate	This should be a minimal concern outside of production, though also an easy solder fix if an update is desireable

Subsystem C: Bluetooth Module

Failure No.	Failure Mode	Possible Causes	Failure Effects	Method of Detection	Criticality	Remarks
10	Failure of noise regulation to HC-05 input	C8, C7	HC-05 has internal circuitry for input noise, though failure is possible if they're not adequate. Inability to communicate via Bluetooth worst case.	Raspberry Pi is unable to connect to the HC-05 via Bluetooth	Moderate	Though it makes the facial recognition system unavailable if the HC-05 should fail, keypad bypass should still be operable

Subsystem D: MSP432 & related decoupling capacitors

Failure No.	Failure Mode	Possible Causes	Failure Effects	Method of Detection	Criticality	Remarks
11	MSP432 fails in turn	C3, C4, C5, C6	Whole system failure, as the Microcontroller also fails in response to a decoupling capacitor failure	Whole system becomes unresponsive	High	