Risk Audit

Project FishWorks / ECET 291 / 9.24.20XX
Sebastien, Eric, Kayleb and Braden

MANIFESTED RISKS

Risk #5 – LEDs Overheating

After testing on the lighting system, we determined that running the LEDs at or near 100% power can lead to premature failure of the diodes. However, we performed these tests while the system was being monitored in-person, therefore we were able to replace damaged LEDs quickly, so we never had failures when we were not around that could have left the lights off for an externed period, potentially risking life in the tank. Also, we configured the LED drivers in a way so that if the control system goes down, they revert to a safe power level. While this risk was close to manifesting, our risk management strategies in place prevented a failure that could cause risk to tank life.

Risk #14 – PCB Design/ Nonworking boards

We did have several small issues on both of our PCBs. Luckly our risk mitigation strategy of having the boards designed and manufactured as soon as possible meant that we had ample time to find solutions to these issues. Because of this extra time, we were able to find solutions that did not involve creating a second revision of either of the two boards, saving us from extra expenses and time delays. In retrospect, we likely underestimate this chance of this risk, as with the complexity of these two boards, having no issues would be unlikely. Appendix #1 contains a more detailed breakdown of the most significant of these issues.

Risk #16 – Ordering/ Deliveries Delayed

This risk did manifest when our order of an Atlas Scientific pH sensor placed early in the semester had not shipped in time for us to complete its development on schedule. Our risk mitigation strategy of leaving enough time to accommodate for a worst-case scenario delivery time proved ineffective as this order was promised in October but still had not been delivered by mid-November. We addressed this scenario by putting in an EC to cancel the Atlas Scientific order and placing an order for another pH sensors from a different company that would deliver in time for development. We also discussed alternative devices to implement if we were not able to get any pH sensors in time. Looking back, we should have had product alternatives planned earlier on in case of this scenario. This would have resulted in a less rushed pivot to the other pH sensor.

Risk #17 – Camosun College Flooded

While we were not personally affected by the great TEC 204 flood of 2024, we could have easily been if we had picked 204 instead of 229 for our capstone workspace. Our risk mitigation strategies

for this risk focused on alternative workspaces in case of an issue on Campus. While these strategies are still valid, we should have also addressed the possibility of damage to our project due to a weather event on campus. Also, we did plan for the fact that we ended having a fully functioning fish tank in the second half of the semester and how we would deal with having to move it to another location in case of issues.

UNEXPECTED RISKS

Living Organisms

The added difficulty and associated risks of introducing life into the tank was not something we had originally planned for as it was not something we had in our original scope. However, as it will be a large part of the Symposium Presentations, the life in our tank can be now considered “mission critical”. A large portion of the mitigation for this risk is Fish Sense itself, and so far, it has proven reliable in allowing us remote control of the tanks system. We have also purchased and installed a “pet camera” that uses WiFi to allow us to monitor the tank while off campus.

CONCLUSION

We are happy with our initial risk assessment. What was missed was acceptable given our level of experience, and the risks that manifested which we had planned for were well handled. In the future we should spend more time understanding the individual requirements and risk on a per PCB component level to decrease likelihood of damaging PCB components.

APPENDIX #1

CAN Bus Transceiver IC Failure

This is a detailed breakdown of the most significant reliability issues that we had with our circuit boards. The first instance of these issues came about when a high-speed data signal was applied to the power switch for the CAN Bus network on the base station. This resulted in the power supply to the attached node controller being turned on and off rapidly. Following this instance the node controller would not communicate with devices on the CAN Bus network. This led us to believe that the IC responsible for the CAN Bus communication had been damaged.

This issue manifested again on two other node controllers when plugging and unplugging node controllers from a powered network. Full functionality was regained for the effected nodes when the CAN Bus transceiver IC was replaced. The exact cause of this issue is not fully known; however, a strong theory has been developed. The fact that all other components on the board besides the CAN transceiver were functional after these incidents and that the only component on the 5V power rail was the transceiver led us to the 24V to 5V switching power supply. If this supply had outputted a higher-than-normal voltage during these rapid input voltage on/off events (such as the contact bounce when plugging on our RJ45 connector or when the data signal was applied to the power switch) this could have damaged the CAN Bus transceiver. But since there is a linear regulator between the 5V rail and the 3.3V, the rest of the devices on the board could have been left undamaged.

Preliminary testing showed some validity to this theory. Short (microsecond scale) voltage spikes on the output of the switching power supply were observed at as high as 8V during rapid switching of

the input voltage. Time constraints meant that we haven't been able to do any further testing on this matter. More testing would need to be conducted before using this component in further board revisions.

Two main mitigation strategies were implemented to attempt to address this issue. First, a policy was implemented to never plug or unplug devices from the network when it was powered. This means that the only way the devices would be powered on would be using the clean edge of the power switch on the base station. Second, two protections were added to the base stations and some devices: a 8V varistor to clamp the voltage on the 5V rail and a TVS diode to add additional protection to the 24V power rail. Since implementing these measures, no additional failures have occurred.