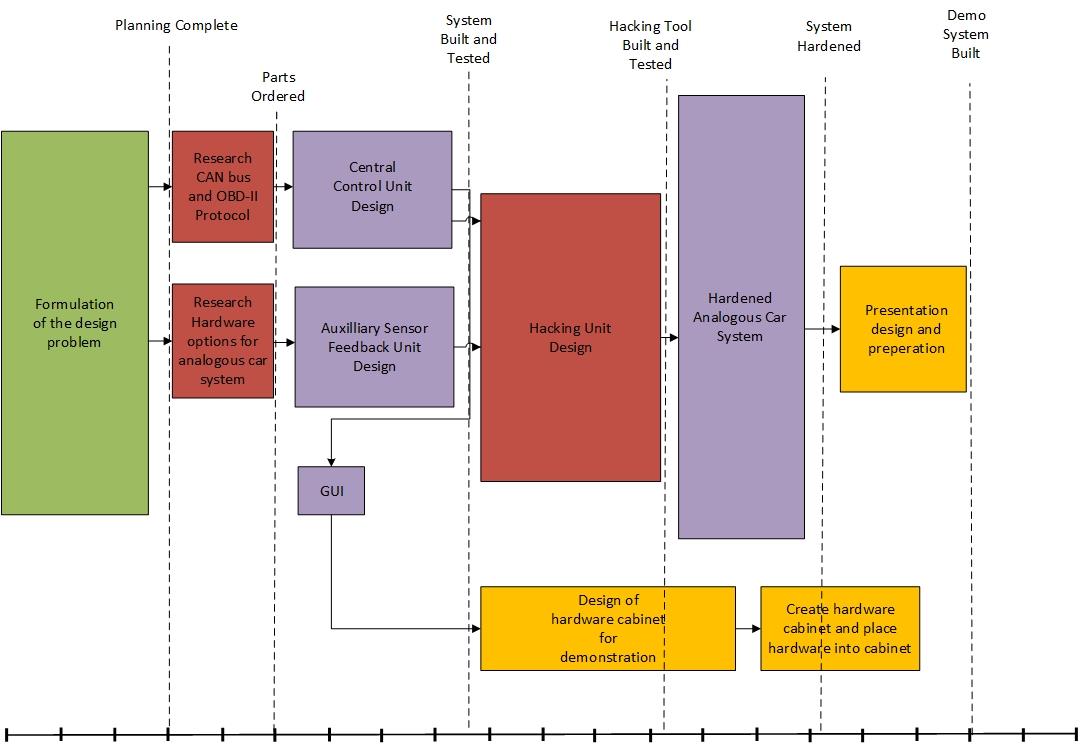
Project Implementation Plan: Team 16

# Executive Summary

It is well known that these days’ new technologies are being developed at a faster rate than at any other point in human history. We are creating new technologies faster than we can master the old technologies that have already been developed. Even industries that have been notorious for being slow to implementing new technologies are starting to change quicker than ever before, such as the automotive industry. Cars have had more technological advancements done to them in the last 15 years than all the years previous. Cars are becoming more fuel efficient and environmentally safe, both from during manufacturing and emissions from being ran. Cars are made safer for the passengers. This includes during collisions and with features such as line departure detection, better headlights, distance locking cruise control, and other similar features. These advancements are fantastic for everyone, but these technologies are being sometimes being implemented without thinking about the repercussions. With new technologies comes new ways for dangerous people to be able to hack in these connected devices. It goes without saying that there a huge safety concern if someone were to be able to hack into a vehicle, especially if it were moving. This is where our project comes into focus.

We are tasked with designing a control system that is an adequate analogy for a modern control system in today’s cars. Then once our system is designed, we must think of different ways to hack into the system and compromise the signals being sent and received. Once we have identified multiple security risks, we then need to devise and document cheap and effective ways to harden the system from these attacks. The documentation and reasoning behind the attacks we chose to isolate is one of the most important aspects of our project, because the overall purpose of this project is to be a useful educational tool for our clients to use to educate their system designers and what types of security risks they could easily avoid while designing a new system.

# PERT Chart



# Major Milestones

1. **System Proposal Document Signed Off**

Having our System Proposal Document signed off by both our client and supervisors mean that we have a well-defined project and universally agreed upon deliverables at the end of the project.

1. **Hardware Ordered**

This far into the project there should be a clear understanding of what the actual system should look like and how all the subsystems interact with each other. There should be enough detail in the design that when the hardware does come in there should be no questions as to what the next steps are with using the hardware.

1. **Analogous Car System Built and Tested**

All the hardware for the Analogous Car System (ACS) should be fully functioning and can be ran in a manner that would simulate the actions of a running vehicle. For a more detailed understanding about which features this Cay system should be able to demonstrate, please reference the Function Architecture Diagram in the System Proposal Document.

1. **Hacking Tool Built and Tested**

The Hacking Tool should be able to properly perform multiple malicious attacks on the ACS in a way that highlights various vulnerabilities in the system and presents these vulnerabilities in a way that shows how dangerous they could be for user of the system.

1. **Hardened Analogous Car System (HACS) Built and Tested**

The Hardened version of our ACS should be able to repel or adequately deal with any malicious attacks that were previously demonstrated by our Hacking Tool. If it is impossible to completely repel an attack from the Hacking Tool then the hardened ACS should be able to identify if it being attacked and adjust in a way that ensures the safety of the user.

1. **Demo System Built**

Since the primary purpose of this project is to bring awareness to engineers and designers of embedded system that could potentially threaten the life of the users, having our ACS, Hacking Tool, and HACS all bundled into a single streamlined and easy to present demonstration kit is an essential aspect of our project. This demo kit should allow for quick setup and transportation, with no risk of damaging or dislodging any portion of the system. The final form of this demo kit should complement our presentation in such a way that concisely presents the different classifications of potential hacks to systems of this type and also educates the watchers on how best to defend against the hacks.

# Division of Labor

The work for this project will be divided among the members based on the competency level of everyone for tasks needed to be accomplished. If an individual already has a task assigned to them when a new task comes up that falls under their particular specialty, then the task falls to the next person who is most competent in the necessary skills needed for a timely completion of that task.

* **Paul Earhart:** Has the most technical knowledge and hands-on experience with CAN bus protocol and vehicle ECUs and thus will be the team's main source of knowledge with regards to either of those topics. Also, has been exposed to Cyber Security concepts as a member of Rose’s Cyber Security club.
* **Haoran Geng:** Most comfortable with the embedded coding and software development. Has strong familiarity with Arduino embedded design and FPGA. Will have responsibility when it comes to the embedded software design. Also, Haoran Geng can help other team members to finish the task.
* **Dustin Kline:** Most comfortable of the group when it comes to soldering and is meticulous when it comes to physical layout of the hardware. Will have main responsibility when it comes to designing and building the hardware cabinet and making sure it translates well to a demonstration platform. Also is currently taking an Embedded Linux course that teaches skills that will be useful with designing and creating the different systems of this project.
* **Larry Kozlowski:** Has strong familiarity with FPGA and SBCs and will be a useful asset when it comes to creating the ACS and making sure the connections between the Central Control Unit and Auxiliary Sensor Feedback Units are properly designed and implemented.

**Portions of the project that will be done in parallel:**

* Designing and building of the Central Control Units, Auxiliary Sensor Feedback Units
* Designing and Testing the Hacking Tool and the Hardware cabinet
* Designing and Testing the HACS and the Hardware cabinet

**Potential Bottlenecks:**

* Both the creation of the Hacking Tool and the designing/building of the hardware cabinet hinge on the completion of the ACS. We cannot design a hacking system until the system that is going to be hacked into is fully functioning. Likewise, the hardware cabinet cannot be built until the final system that is going to be housed in the cabinet is finalized.
* The HACS cannot be designed and tested until the Hacking Tool is finalized. We would not know what aspects of our ACS to harden until the Hacking Tool is fully functioning and capable of demonstrating dangerous attacks on the ACS.
* The presentation that is to be delivered cannot be properly planned out and prepared for unless the hardware cabinet is fully completed. The hardware cabinet is to ensure safe transport of our system and to allow for quick setup for demonstration purposes.

**V. Training Plan**

**Fields of Required Knowledge:**

A solid understanding of how the electronic components of a vehicle work and communicate with each other is fundamentally the most important aspect of this project since one of our main tasks is creating a system that is expected to act and behave in the same manner as the vehicle’s system. Another major field of knowledge that will be needed for the successful completion of this project is familiarity and ability to implement different types of malicious attacks to hack into potentially safety critical portions of the system that was mentioned above. Likewise, complementary knowledge on how to harden systems to protect from different types of malicious attacks is equally as important since this knowledge is truly what we as a team are trying to inform our clients on with our demonstration.

**Description of Relevant Strengths:**

This information can be found in section IV, Division of Labor. We found it most pertinent to present that information there because the skills of each individual team member heavily influence what work they are assigned for this project.

**Specific Actions Needed to Acquire Missing Knowledge:**

|  |  |  |
| --- | --- | --- |
| Assigned to: | Tasks: | Due Date: |
| Dustin Kline | Gain a better understanding of how electronic components in a vehicle communicate with each other. This is to be done by creating and maintaining a Research Memo on CAN bus protocol and OBD-II. | 10.11.2017 |
| Paul Earhart | Share some hands-on experience with Arduinos by bringing in some hardware and performing a live demo to teammates and allowing them to play around with the platform. Facilitate discussion on how some of these skills and concepts can be applied to our ACS and/or Hacking Tool. | 10.11.2017 |
| Haoran Geng | Research and have a better understanding of the Beaglebone and Raspberry Pi. We may only need to use one of it, but I’m not familiar with both. This is done by play around with these platforms and conducting a research memo with them. | 10.11.2017 |
| Larry Kozlowski | Since cyber security is a major portion of our project, maintaining a research memo on the topic will be useful so when we get to that portion of the project we can start working on the Hacking Tool right away. It is known that Professor Estrada has knowledge on this subject, therefore setting up a meeting with him is in the team’s best interest. | 10.11.2017 |

# Budget

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Category | Cost | Equipment/Tools | On-campus Resource | Real Cost |
| ECU System (multiple SBCs) | $350 | N | N |  |
| Hacking System (One SBC) | $75 | N | N |  |
| PCB Fabrication | $200 | Y | Y |  |
| Hardware Cabinet | $50 | N | Y |  |
| Personnel Hours | $16,000 | N/A | N/A |  |
| Soldering Kit | $125 | Y | Y |  |
| Wires/Connectors | $10 | N | Y |  |
| Hardening Components | $40 | N | N |  |
| Total Cost | $16,850 |  |  |  |

