1.1 Requirements and Constraints

Functional - how should the product work?

The Mobile Vehicle Security Bridge will be able to detect instructions sent by a malicious user, whether they be replayed instructions that a hacker reads while sniffing on the local CAN network, or artificial. These fraudulent messages will be ignored which will allow the vehicle to keep functioning normally.

Resource - what external resources can this system use?

We will need access to cryptography libraries to implement the AES encryption system, and socket CAN libraries.

Physical - weight, size, shape etc

The product is a box that needs to be durable, able to withstand any situation, holding the technology inside. The box is roughly 8x5x2 inches. We think approximately between 5-10 pounds max is suitable for this project.

Aesthetic - How should the product look?

It is just a simple monocolored box. It is not something a user physically sees inside of their vehicle; it's a hidden component. The product is comparable to any other part for a car and will most likely remain untouched unless the user intends to find it.

User experiential - How should the user experience be?

The user shouldn't have to worry about their car being hacked due to this device and have one less stress while driving. The user doesn't need to activate anything. The product passively sits, defending any cyber attack against the user's vehicle that may come its way. If the user attempts to hack their own car, this device will prevent that.

Environmental - How will we have to design this product based on the environment?

The product is mainly electronic, so it will have to be in an internal part of the car and immune to any weather conditions. Additionally, it will have to be secured snuggly so any bumps in the road or a minor accident wouldn't dislodge it from its installed location. It will have to be securely screwed onto the vehicle in such a way to ensure that it stays in place, but can still be unscrewed so any replacement parts or physical updates required by the product can be applied with relative ease.

1.2 Engineering Standards

What Engineering standards apply to your project? (some standards might be built into your requirements and others might fall out of design)

- AES-128 (Advanced Encryption Standard for 128 bits)
    Justification: Our project leader (John Potter) introduced us to AES128 and thought it could be good for us to use it due to it being very secure and efficient, so it should fit within any time constraints we have for communication to happen

    Within AES-128 we are currently looking at these specific modes:
    - AES-128 ECB (Electronic Codebook)
    - AES-128 CTR (Counter)
    - AES-128 CMAC (Cipher Message Authentication Code)

- J1939
    - Standard developed by Society of Automotive Engineers (SAE)
    - Designed for Controller Area Network (CAN) for quick data communication between Electronic Control Units (ECUs)
        - Commonly used in heavy duty tractors, cars, and buses