# A Brief Discussion of Project Constraints

## Economic Constraints

Since this project is being personally funded, the budget for acquiring equipment and material is rather limited. The current estimate for the project's budget is $100 with a max budget of $200. As a result, hobbyist electronics will be used for the project's hardware. The project's software will also use free and open source software to help cut costs. Luckily, there are plenty of options available for both hardware and software that are affordable and meet project requirements. Since this is a personal project, no economic development or benefit will result from this project.

## Professional Constraints

This project will require that I utilize most of the technical and soft skills I've developed during my career thus far. Technical skills to be applied will include software development, IoT device development/set up, and knowledge of cybersecurity defense practices. Soft skills to be applied will include technical communication (both spoken and written), presentation design, and collaboration with technical advisors. Since this project is rather all encompassing in nature, it will be a great resume builder.

## Legal Constraints

To mitigate any licensing issues during the development and deployment of the data pipeline, the project will use software with permissive licenses. The project itself will also be licensed under the MIT license. Note that the MIT license is one of the more permissive open source licenses currently available.

## Security Constraints

Data being sent to and from the facility's message broker must be authenticated and encrypted. Authentication will prevent threat actors from spoofing sensor data to overwhelm the system or tamper with the analysis of stored sensor data. Encryption will ensure that any authentication credentials being sent will remain confidential. Additionally, encryption can prevent threat actors from learning what message format the system accepts. That way, spoofing sensor data becomes more difficult.

In addition to securing message broker communication, the local servers will utilize database users with restrictive permissions. The API will also use its own restricted database user. That way, a compromised user can only inflict limited damage to the database. Every user will also access the database via SSL to ensure the confidentiality of any credentials, along with API usernames and passwords.

Lastly, the API will require a JSON Web Token (JWT) signed by the API with a private key to be sent with each request. That way, threat actors will have increased difficulty forging valid JWTs. This ensures that only authorized users can query and analyze the collected senor data. Note that communication between the API and its users will be encrypted over HTTPS to prevent a threat actor from obtaining a valid JWT via a man-in-the-middle (MITM) attack. Each JWT will also have a time-to-live of 5 minutes to further mitigate the risk of a MITM attack.