

**Work Plan**

Project Team

**Fall Semester**

Robert Cyprus (S)

Aishvarya Korde (S)

Zayra Lobo (J)

Paige Rinnert (Fall TL)

Project Advisor: Professor Christopher Clark

Project Liaisons: Ken Dreshfield ‘80

Ian Jimenez ‘11

Ron P. Smith ‘83

Stephanie Tsuei (Lead)

October 2016

ABSTRACT

The Northrop Grumman Corporation Clinic Team at Harvey Mudd College will build a quadrotor, then implement and test a secure state estimation (SSE) algorithm for autonomous control. This workplan presents the specifications and design alternatives for the device. It describes the quadrotor’s states, sensors, onboard hardware, and the SSE algorithm. At the end of the fall semester, the team will have realized an SSE in Matlab simulations and have constructed a quadrotor with functioning sensors. Throughout the spring semester, the team will implement the SSE on the quadrotor using ROS, modifying the SSE algorithm and hardware as necessary in support of the software to hardware transition.

TABLE OF CONTENTS

ABSTRACT ii

1. Introduction 2

1.1. Northrop Grumman 2

1.2. Project Statement 2

1.2.1. Objectives 3

1.2.2. Constraints 3

1.2.3. Functions 3

1.3. Deliverables 4

2. Background 6

2.1. Literature Review 7

3. Technical Approach 9

3.1. Design Alternatives 9

3.1.1. States of the Quadrotor 9

3.1.2. Sensors 10

3.1.3. Algorithm 10

3.1.4. Quadrotor 12

3.2. Detailed Design 13

3.3. Testing 14

4. Project Management 16

4.1. Work Breakdown Structure 16

4.2. Schedule 17

4.3. Division of labor 18

5. References 19

APPENDIX A: team member profiles 20

# Introduction

Northrop Grumman (NG) is sponsoring a 2016-2017 Clinic Project to test sensor robustness from cyber attacks on autonomous vehicles, specifically aircraft. This section describes NG, presents the project statement, and defines the deliverables for the project.

## Northrop Grumman

Northrop Grumman is a leading global security company that innovates in the fields of autonomous vehicles, cyber security and communications, and air and space systems. NG is committed to preserving freedom and advancing human discovery. This Clinic Project is sponsored by NG’s Aerospace Systems sector, NGAS. NGAS is based in Redondo Beach, CA and provides next-generation solutions for military aircraft and land vehicles, autonomous systems, and space systems for its customers worldwide. NG holds world records in many fields, with technology integrated in products ranging from cell phones to space satellites. NGAS’s Research and Development department is sponsoring this project to test sensor robustness in autonomous aircraft.

## Project Statement

The Northrop Grumman Clinic Team will implement a secure state estimator in software and then experimentally validate the estimator in hardware. The team will demonstrate that the addition of the SSE algorithm to the control loop in real time bounds the tracking error from a set flight path based on data from compromised onboard sensors.

### Objectives

Objectives for the quadrotor state estimator include:

* Demonstrate quadrotor altitude tracking control with minimal tracking error [m]
* Maximize the number of compromised sensors for which the SSE can be tested
* Minimize cost

### Constraints

The design must meet the following constraints:

* The root-mean-square absolute tracking error when all sensors are functioning and there is no SSE algorithm will be referred to as e\*, and the team allows for an increase in error of up to 1.2e\* when adding the SSE algorithm to the control loop. When compromised sensors cause the absolute error to exceed 5e\* without the SSE, the addition of the SSE should keep errors below 1.2e\*.
* Final implementation of the SSE must be on the Robot Operating System (ROS) platform
* Quadrotor must fly for 10 minutes on a single battery charge
* Must estimate states at a minimum rate of 25 Hz
* All equipment purchased must be less than $7,000, according to the team’s budget proposal

### Functions

The design should perform the following functions:

* Quadrotor should complete pre-planned flight path with compromised sensors
* Quadrotor should perform real time state estimation and correction
* The SSE must be configurable to receive correct data from sensors or overwrite data from specified sensors to simulate hacking
* The SSE should accurately estimate the state of the quadrotor (position [m], velocity [m/sec], orientation [°])

## Deliverables

By the end of the fall semester, the team will complete the following:

* Implement and simulate a state estimator in Matlab with all sensors functioning and with some sensors compromised
* Log sensor data
* Produce a quadrotor with onboard computer, controllers, and sensors capable of altitude tracking
* Project documentation and presentations including:
  + Workplan
  + Midyear Report
  + Lab visit and presentation at Northrop Grumman in October
  + Three internal Clinic presentations

By the end of the spring semester, the team will complete the following:

* Run the state estimator on real sensor data with some corrupted measurements, both offline and in real time
* Fly the quadrotor on a set vertical trajectory with real time data logging and state estimation
* Project documentation and presentations including:
  + Final Report
  + Spring semester presentation at HMC
  + Projects Day presentation
  + Final Presentation at Northrop Grumman

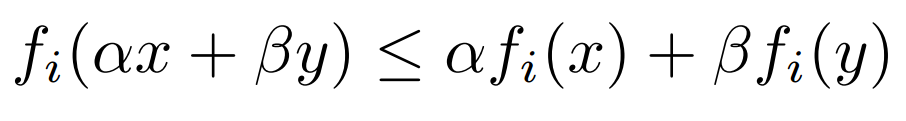
# Background

Flying an unmanned aerial vehicle like a quadrotor requires a robust control system to ensure that the vehicle follows the user’s desired trajectory as accurately as possible. Most control systems use feedback control, where previous system outputs are fed back into the system as inputs. State space control, or modern control, is a mathematical model where an estimate of the system states is fed into the controller to calculate the necessary inputs to maintain the desired trajectory. However, a control system is only as good as the states fed into the controller.

Estimating the states of a real system, like location and orientation, is a challenge given that the exact state cannot be determined simply by observation. Instead, the state needs to be estimated given a set of measurable parameters of the system. The goal of state estimation is to provide an estimate of the system state given the inputs and outputs of the real system; this state can then be fed into a standard controller to maneuver the vehicle.

The focus of this project is primarily on implementing a *secure* state estimator. Cyber-physical attacks can cause an estimator to fail to produce an accurate estimate of the state of the system. A cyber attack can be a malicious virus introduced to the system or a signal that is intercepted and altered by a hacker. Physical attacks on the actual hardware can also affect the accuracy of sensor outputs, the behavior of the controller, and even the actuators that provide control input. Both cyber and physical attacks will compromise the accuracy of the state estimator if they alter the sensor outputs. The potential for these types of attacks motivates the need for a secure state estimator that is robust in the face of attacks. Given the scope of this project, the team will focus only on attacks on sensors, in the form of broken sensors, compromised signals, or noisy outputs.

One of the techniques used to make a state estimator robust against attacks is convex optimization. A convex optimization problem is a special class of nonlinear optimization problems where the function to minimize and each of the constraint functions are all convex, which means they satisfy Equation 1:



Equation 1 | Convex optimization inequality.

While convex optimization solvers are not as widely used as least squares or linear solvers, the field is mature and there are a number of reliable methods. The benefit of convex optimization is that once a problem has been identified as such, the solution can be found using software [2].

Another approach to secure state estimation is satisfiability modulo theory (SMT), which is a method of determining whether a Boolean formula is solvable. Like for convex optimization, there are many SMT solvers that can be used to find a solution once the problem is described by a Boolean formula.

## Literature Review

An important step in making a robust state estimator is detecting if any of the sensors are not working properly. Compromised sensors can be identified by comparing sensor measurements to an analytical model using the residual signal of the system [1], [3]. Although this method works in some contexts, Fawzi et al. claim it is not effective for large errors in sensor measurements and only works for bounded disturbances. Another method of securing the state estimator is to assume that the disturbances follow a stochastic process. Stochastic disturbances are predictable but, this model is not an accurate representation of real world disturbances. Centralized and decentralized filters have also been introduced to detect and identify attacks but these filters are difficult to implement and computationally expensive [1].

The problem of secure state estimation has been posed as secure state reconstruction, where the goal is to reconstruct the state of the system from functional sensor outputs. Shoukry et al. focused on reconstructing the state of a nonlinear system given that some sensors are compromised. They posed the secure state reconstruction problem as a Boolean formula and developed a lazy SMT procedure to solve this problem that uses an SAT solver as a subroutine [3].

According to Lee et al., there are three main approaches to the problem of error correction: geometric, greedy, and combinatorial. In the geometric approach, linear programming techniques are used to formulate the problem as a convex optimization problem (this is the approach used in [1]). The greedy approach uses an iterative process to approximate signal coefficients, and the combinatorial approach identifies different combinations of parameters that could produce the measured sensor outputs to restrict the solution space. Lee et al. take the combinatorial approach to reduce computational intensity of the optimization problem. To create a secure state estimator, they consider a separate observer for each output and combine the state estimates from each observer [4]. Mishra et al. also use the combinatorial approach to produce a state estimator by looking at the residues of all possible sets of sensors with the size of the number of sensors known to be functional [5]. This approach, like many of the models discussed, assumes an upper bound on the number of sensors that are compromised.

# Technical Approach

The team compared different ways of approaching the physical hardware and software implementation of the state estimation algorithm. Section 3.1 enumerates the alternatives considered by the team and the selections the team has made by the time of writing. Section 3.2 describes how the team plans to complete a detailed design of the preferred alternative, and Section 3.3 addresses testing.

## Design Alternatives

The team is considering many options for the states of interest, the sensors to measure these states, the algorithm to perform state estimation using the sensor outputs and the type of quadrotor to house the sensors and onboard algorithm.

### States of the Quadrotor

This subsection delineates the states that the team is considering. The states the team is most interested in are states necessary to control the quadrotor and track a flight path. The team will need sufficient states in order for the quadrotor to perform autonomous navigation. The proposed states are included in Table 1:

|  |  |  |
| --- | --- | --- |
| Position | Each of X, Y, and Z in a global frame | Note: The global origin will be set to the take-off position. |
| Velocity | Each of X, Y, Z directional velocities |  |
| Orientation | Each of Roll, Pitch, and Yaw |  |
| Angular Velocity | Each of Roll, Pitch, and Yaw time derivatives |  |

Table 1 | Quadrotor states.

### Sensors

The team must select sensors to measure the states mentioned in Section 3.1.1, and these sensor outputs will be input to the SSE. The list of sensors the team considered is included in Table 2 (underlined sensors are sensors that the team selected to purchase):

|  |  |  |
| --- | --- | --- |
| **Position** | **Velocity** | **Orientation** |
| Accelerometers (3)  Radar  Laser scanner  Optical flow sensor  Pressure sensor  OptiTrack Camera tracking system | Airspeed sensor | 3DOF compass  Gyroscopes (3) |

Table 2 | Possible sensors.

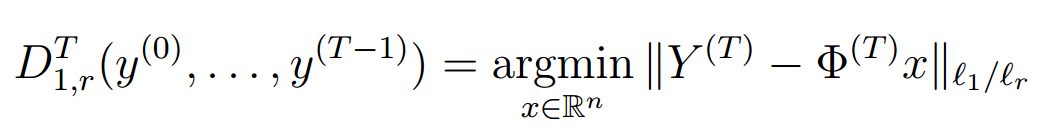
The accelerometers and gyroscopes will likely be combined on a 6DOF IMU (inertial measurement unit). The team is considering using an OptiTrack camera system to determine the true states of the quadrotor or to transmit the position measurements to the computer onboard the quadrotor.

### Algorithm

The team is considering two main approaches for the secure state estimation algorithm, based on literature suggested by the liaisons. The first algorithm uses concepts from compressed sensing and error correction over the reals to pose the estimation problem as a convex optimization problem [1]. The other algorithm uses Satisfiability Modulo Theory to perform state estimation on nonlinear systems [3]. Both algorithms will be described here.

#### Convex Optimization

This secure state estimation algorithm is presented in Equation 2 as a convex optimization problem:

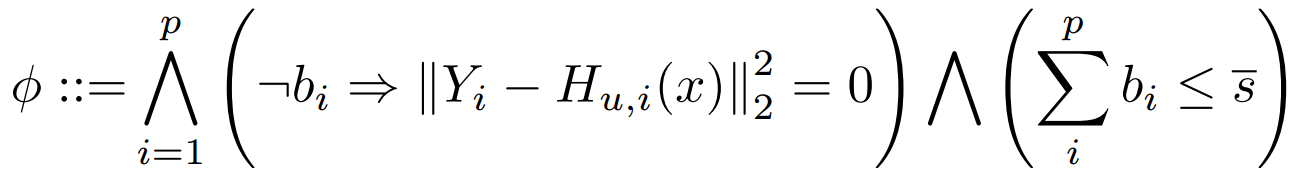


Equation 2 | Compressed sensing algorithm.

where is a decoder whose inputs are the sensor output column vectors (1 by the number of sensors); *argmin* for a vector of real values denotes the states for which the argument is minimized; is the matrix of outputs (number of time steps by number of sensors); is the linear transformation that maps to using the system matrices and ; and the notation is the sum of the norms (also known as a -norm) of the rows of matrix [1]. The team has decided to use this approach to secure state estimation because of the team’s familiarity with state space control and the notation used in the paper.

#### Satisfiability Modulo Theory for nonlinear systems

The other state estimation algorithm is formulated in Equation 3 as a Boolean equality:



Equation 3 | SAT algorithm.

where is a pair that satisfies the following Boolean expression; is the number of sensors; is a Boolean value indicating whether sensor is compromised ( indicates that the sensor has been attacked); is a column vector of sensor measurements from the sensor where the first element is the measurement from the beginning of the window (at time ) and the final element is at the end of the window (at time ); is the system transfer function; the notation is the norm of the matrix squared; and the upper bound on the number of compromised sensors [3].

### Quadrotor

The team needs a quadrotor that is lightweight and customizable in order to incorporate the sensors necessary for state estimation. The team also needs to be able to simulate different sensor outputs to test how the estimator responds to faulty inputs. The Northrop Grumman liaisons suggesting buying the QAV400 Quadrotor frame shown in Figure 1.

Figure 1 | Quadrotor frame.

The QAV400 quadrotor frame fits the requirements for the project – it is lightweight (375g) and durable and can be purchased individually, allowing the team liberty in choosing the flight control unit, sensors, actuators, and on-board computer [6].

Since the team will implement the algorithm using ROS, the Northrop Grumman liaisons suggested using the Jetson TK1 computer board. The Jetson TK1 runs the Linux operating system and is equipped with 2 USB, 1 HDMI, 1 RS232, expansion I/O, 1 Ethernet, and SD card reader ports, which will help the team implement and test different sensors [7].

Having a controller on board is essential to being able to fly the quadrotor. Since the main focus of the project is the implementation of the secure state estimation algorithm, the team decided to use an off-the-shelf controller for the quadrotor. The 3DR Pixhawk flight controller is appropriate for the project’s needs. The Pixhawk is a fitting option because of the open-source software and firmware. This open-source availability is necessary for multiple reasons; the team must be able to integrate the SSE software with the quadrotor and its flight controller, and ensure that the existing controller does not interfere with the results of the estimator [8].

## Detailed Design

The team will select an implementation of the state estimator algorithm from the papers provided by the liaisons. The selected state estimator will then be implemented in simulation using MATLAB with consideration for the objectives and constraints outlined in the project statement (Section 1.2). The team will then implement the state estimator in hardware, using a ROS platform instead of MATLAB. The quadrotor and sensors used for the hardware implementation will be selected, purchased, and assembled by the team. To evaluate the performance of the state estimator in the hardware implementation, the team will program a set flight path for the quadrotor to follow. Using the OptiTrack camera system, the team will record how closely the quadrotor follows the set path with all sensors functioning and also test the quadcopter performance with different subsets of sensors compromised. Successful hardware implementation will be defined by the constraints outlined in the constraints section of the problem statement (Section 1.2.2).

## Testing

The team will first test the secure state estimation algorithm in software by implementing the algorithm using the Matlab Robotics package and simulating different subsets of sensors being compromised. Once the algorithm is successfully tested in software, the team will begin to implement the controller and state estimator in hardware. Rather than physically hacking any sensors, the team will simulate a non-functioning sensor by passing compromised signals to the SSE. The team will design a test platform with OptiTrack Motion ground sensors for ground truth values to compare against the results of the state estimator.

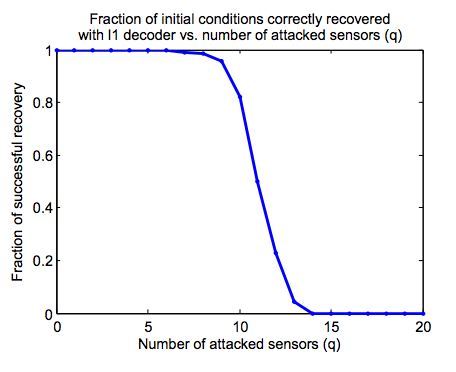


Figure 2 | Simulation results using SSE algorithm [1].

To determine the success of the results, the team will compare the simulation and hardware results to the expected results from the algorithm literature. The literature contains results on the success rate of the algorithm as a function of number of compromised sensors, as seen in Figure 2.

# Project Management

The Northrop Grumman Clinic Team has developed a work breakdown structure identifying the tasks to be performed, a Gantt chart laying out the milestones and the critical path through the project, and an initial partitioning of the labor among team members.

## Work Breakdown Structure

The work breakdown structure in Figure 1 shows how the project has been hierarchically subdivided into more manageable tasks.

**Activity Time (Hours)**

Background research

Algorithms 15

Sensors 5

Quadcopter 5

Drone regulations 5

Conceptual Design

Brainstorming, sketching, component research 10

Software 15

Hardware 15

Comparison of Alternatives 4 × 4 = 16

Detailed Design

Coding the algorithm 26

Simulation 50

Quadcopter assembly 15

Sensor setup (offline) 10

Sensor setup (on quadcopter) 12

Test Plan

Initial Test Plan 15

Revised Test Plan 10

Testing

Software integration onto quadcopter 5

Testing software on quadcopter (calibration) 20

Indoor testing 8

Field testing 30

Team Meetings

Teleconferences 1 x 28 = 28

Internal Team Meetings 5 x 28 = 140

Tuesday Presentations 1 x 28 = 28

Team Leader Meetings 1 x 6 = 6

Planning 1 x 28 = 28

Logistics

Register to drive clinic van 2

Presentation and Preparation

Orientation Day 3 × 4 = 12

Fall Review #1 2 × 4 = 8

Fall Review #2 3 × 4 = 12

Fall Review #3 3 × 4 = 12

Fall Site Visit 6 × 4 = 24

Spring Presentation 6 x 4 = 24

Projects Day Presentation 6 x 4 = 24

Spring Site Visit 6 x 4 = 24

Reports

Work Plan

Background 6

Design Alternatives 6

Project Management

Work Breakdown 1 x 3 = 3

Schedule 2

Division of Labor 1

Other Sections 4

Writing Center review 2

Midyear Report 40

Final Report 80

Total Time 803

Figure 2 | Work Breakdown Structure.

## Schedule

The Gantt chart in Figure 3 shows that the critical path for the fall involves conceptual design, selection of a preferred alternative, detailed design for that alternative, and sending the design for manufacturing. The team anticipates testing, redesign, and further testing in the spring; the details will be flushed out in the Midyear Report based on the fall progress.

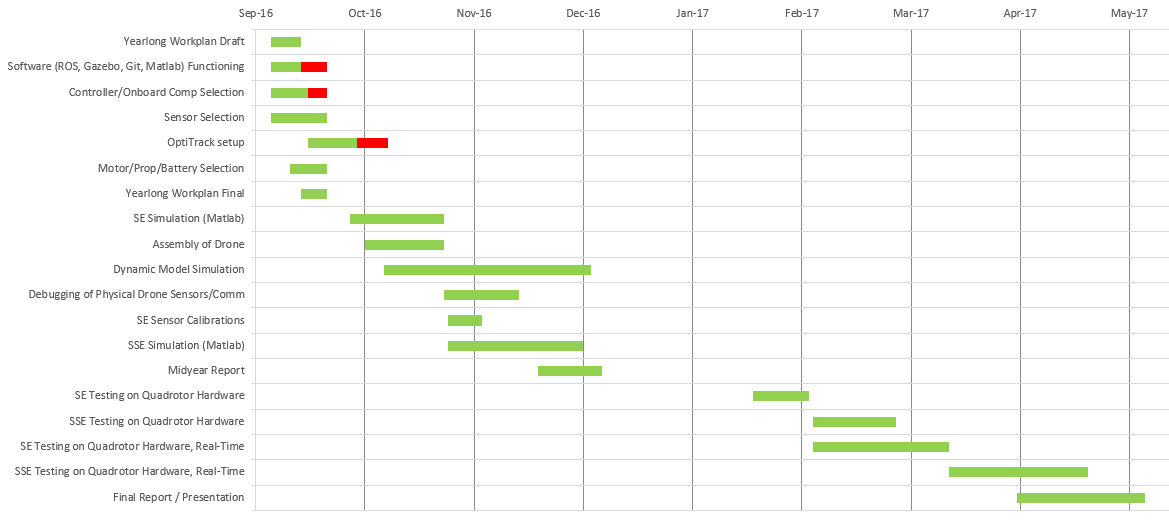


Figure 4 | Gantt chart.

## Division of labor

The team anticipates the following division of the major tasks in the project:

**Task Manager**

Background

Algorithm research PR

Sensor design ZL

Quadrotor hardware AK

Software RC

Conceptual Design

Brainstorming, sketching, component research ZL and AK

Software RC and PR

Hardware RC

Detailed Design

Coding the algorithm All

Simulation PR

Test bed setup RC

Quadcopter assembly RC

Sensor setup (offline) ZL

Sensor setup (on quadcopter) AK

Test Plan AK

Testing All

Presentation and Preparation All

Reports All

# References

[1] H. Fawzi, P. Tabuada, and S. Diggavi, “Secure estimation and control for cyber-physical systems under adversarial attacks,” *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1454–1467, Jun. 2014.

[2] S. P. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge, UK ; New York: Cambridge University Press, 2004.

[3] Y. Shoukry, P. Nuzzo, N. Bezzo, A. L. Sangiovanni-Vincentelli, S. A. Seshia, and P. Tabuada, “Secure state reconstruction in differentially flat systems under sensor attacks using satisfiability modulo theory solving,” in *2015 54th IEEE Conference on Decision and Control (CDC)*, 2015, pp. 3804–3809.

[4] C. Lee, H. Shim, and Y. Eun, “Secure and robust state estimation under sensor attacks, measurement noises, and process disturbances: Observer-based combinatorial approach,” in *Control Conference (ECC), 2015 European*, 2015, pp. 1872–1877.

[5] S. Mishra, Y. Shoukry, N. Karamchandani, S. Diggavi, and P. Tabuada, “Secure state estimation: Optimal guarantees against sensor attacks in the presence of noise,” in *2015 IEEE International Symposium on Information Theory (ISIT)*, 2015, pp. 2929–2933.

[6] “QAV400.” [Online]. Available: http://www.lumenier.com/products/multirotors/qav400. [Accessed: 23-Sep-2016].

[7] “Jetson TK1 - eLinux.org.” [Online]. Available: http://elinux.org/Jetson\_TK1. [Accessed: 23-Sep-2016].

[8] “3DR Pixhawk - 3DR.” [Online]. Available: https://store.3dr.com/products/3dr-pixhawk. [Accessed: 23-Sep-2016].

1. team member profiles

|  |  |
| --- | --- |
| Robert Cyprus is a senior engineering major at Harvey Mudd College. His interests are RF, Systems, and Computer Engineering. Robert has taken three systems engineering courses, multiple analog and digital electrical engineering courses, and coding classes in Python, Java, and Matlab. Currently, Robert is enrolled in a C++ programming class. Last summer, Robert worked for Northrop Grumman on a Chaos Communications project in the NG-Next department. Upon graduation, he is seeking employment in systems or computer engineering. His other interests include machine learning and hiking. | C:\Users\Paige\Downloads\IMG_3730.JPG |
| Aishvarya Korde is a senior engineering major at Harvey Mudd College. She is currently working in a robotics lab that focuses on underwater robotics. Her project included improving AUV hardware and implementing autonomous shark tracking algorithms. She worked at the Jet Propulsions Laboratory (JPL) for two summers working on satellite calibration for the OCO2 satellite. Aishvarya is planning on entering the field of robotics after graduation and is considering getting a job in industry before pursuing a Masters or Ph.D. Some of her other interests include traveling, playing tennis, and enjoying different types of foods. | ../../IMG_1004.JPG |

|  |  |
| --- | --- |
| Zayra Lobo is a junior engineering major at Harvey Mudd College. She is a member of an underwater robotics lab on campus, and as part of her work with the lab, she traveled to Malta this past summer to program and deploy an AUV for data collection of underwater archaeological sites. The previous summer, she worked as a biomedical engineering intern at City of Hope. She has taken a technical elective in autonomous robot navigation and would like to either study robotics in graduate school or get a job in the robotics field. Her other interests include woodworking, filmmaking, and playing guitar. | C:\Users\Paige\Downloads\photo.JPG |
| Paige Rinnert is a senior engineering major at Harvey Mudd College. She has taken two technical electives in dynamics (Dynamics of Elastic Systems and Advanced Structural Dynamics) and was a Vehicle Engineering intern at SpaceX last summer in Dynamics and Loads. On campus, she does coarse grained modeling of nanocomposite gas separation membranes and is an active member of Engineers for a Sustainable World. After graduation, she will return to SpaceX as a Loads Engineer. In addition to running coupled loads analyses, her hobbies include playing the flute and reading Discover magazines. | C:\Users\Paige\Pictures\2016\me\Paige_Rinnert.JPG |