JOURNAL OF GUIDANCE, CONTROL, AND DYNAMICS
Vol. 31, No. 5, September–October 2008

Safe Trajectories for Autonomous Rendezvous of Spacecraft

Louis Breger* and Jonathan P. How†
Massachusetts Institute of Technology, Cambridge, Massachusetts 02139

DOI: 10.2514/1.29590

Autonomous spacecraft rendezvous is an enabling technology for many future space missions, but anomalies in recent flight experiments suggest that safety considerations will play an important role in the success of future missions. This paper presents a method for online generation of safe, fuel-optimized rendezvous trajectories that guarantee collision avoidance for a large class of anomalous system behaviors. We examine the cost of imposing safety as a problem constraint and of additional constraints that guarantee infinite horizon passive collision avoidance while enabling future docking retries. Tradeoffs between passive and active approaches to safety are examined. A convex formulation of the collision avoidance algorithm is introduced and shown to provide much faster solutions with only a small additional fuel expense. Numerous examples using both rotating and nonrotating targets are presented to demonstrate the overall benefits of incorporating these safety constraints when compared to nominal trajectory design techniques.

I. Introduction

AUTONOMOUS spacecraft rendezvous is an enabling technology for many future space missions [1]. Autonomous rendezvous has been used for docking with Mir [2], and more recently on the Engineering Test Satellite VII (ETS-VII) [3] and Demonstration of Autonomous Rendezvous Technology (DART) [4,5] missions. However, anomalies occurred during both of these last two missions. In the case of ETS-VII, multiple anomalies caused entries into safe mode over the course of the mission, at least one of which resulted in a preprogrammed maneuver to move the spacecraft 2.5 km from its target. The anomaly in the DART mission is thought to have resulted in excess fuel expenditures and appears to have caused an on-orbit collision [5–7]. These recent experiences suggest that autonomous rendezvous and docking would greatly benefit from the inclusion of additional safeguards to protect the vehicles in the event of failures. Designing approach trajectories that guarantee collision avoidance for some common failures could simultaneously decrease the likelihood of catastrophic failures in which one, or both, of the spacecraft are damaged and increase the likelihood that future attempts at docking succeed. This paper introduces a method for generating fuel-optimized rendezvous trajectories online that are safe with respect to a large class of possible spacecraft anomalies.

Numerous methods of generating and analyzing rendezvous trajectories exist in the literature and encompass a wide range of rendezvous scenarios [8–13]. These papers consider rendezvous from many perspectives, often taking into account complicated collision avoidance constraints, nonlinear rotational dynamics, and fuel efficiency. Another perspective to be considered when designing trajectories is safe behavior [12,14–16]. Safety in the context of spacecraft rendezvous and docking is typically with respect to collision avoidance following some type of failure. Drifting or passive fault tolerance is a safety technique used in both manual (human-in-the-loop) and autonomous rendezvous missions [12]. For example, the approach in [16] creates trajectories which naturally tend to drift away from the target spacecraft in the absence of thrusting, but which are not fuel optimized. Alternately, [12,14] develop the *safety ellipse* method, in which a nearby orbit with a relative trajectory with minimal secular drift is established that allows safe long-term observation before docking; however, this approach is not fuel optimized and does not propose a specific docking path. A method proposed in [15] optimizes both safety and fuel using genetic algorithms. This approach treats safety as a goal rather than a constraint and thus, cannot assure that the resulting trajectory would be safe. Roger and McInnes [11] plan passively safe trajectories using potential functions, but their approach is computationally intensive and limited to static obstacles. Various types of safety have been considered in the design of autonomous aircraft trajectories, but these focused on creating trajectories that are safe under nominal operating conditions (e.g., safety from adversaries, uncertain terrain) [17,18].

This paper defines a safe trajectory as an approach path that guarantees collision avoidance in the presence of a class of anomalous system behaviors. Similarly, a passive safe trajectory guarantees collision avoidance with no thrusting required for safety and an active safe trajectory requires that inputs be applied to keep the system safe in the event of a failure. Note that this definition of safety is more restrictive than guaranteeing nominal collision avoidance because it guarantees that no collisions will occur for a range of faults. In particular, for a passive safe trajectory, safety is guaranteed even if the chaser spacecraft cannot use thrusters, computers, or communications equipment. The rationale behind choosing a passive abort strategy is threefold: 1) passive abort can protect against a large set of possible system failures simultaneously; 2) an abort trajectory that does not require fuel use guarantees that remaining fuel will not be expended rapidly to increase spacecraft separation distance, thereby increasing the likelihood that future docking attempts can occur; and 3) passive abort guarantees thrusting will not be used in close proximity to the target during an anomaly, thereby eliminating the danger of plume impingement during an automatic safe-mode maneuver. Active safety is less restrictive than passive safety, but it requires that the types of any failures be identified in real time and that some components of the control system remain operational so that a sequence of control inputs can be applied.

The following sections review a method for generating fuel-optimized trajectories from linearized relative dynamics and develop a novel approach for guaranteeing those trajectories will be safe. Several examples of safe trajectories generated for docking with both rotating and nonrotating target spacecraft establish that adding safety constraints does not result in significantly increased fuel use. Next, we examine additional constraints to guarantee desirable infinite horizon passive collision avoidance and ease of future docking attempts. To address online implementation considerations, a convex formulation of the safety problem is introduced that trades

Received 4 January 2007; revision received 30 July 2007; accepted for publication 2 August 2007.

*Research Assistant, Department of Aeronautics and Astronautics; lbreger@mit.edu.

†Associate Professor, Department of Aeronautics and Astronautics; jhow@mit.edu.

some performance for large computation reductions. An active form of safety is then considered as a means of reducing fuel costs while still remaining safe for a large set of possible failure modes.

II. Online Trajectory Optimization for Autonomous Rendezvous and Docking

A trajectory generated through online optimization can be designed by choosing the system inputs that produce that trajectory. For a linear system, methods for incorporating and propagating the effects of inputs are well known. The trajectory optimization formulation in this section is presented in the context of linear time-invariant dynamics, but there is no inherent restriction in the formulation preventing the use of time-varying dynamics [19]. Given a chaser satellite whose state is $\mathbf{x}_k$ at time k, the linearized dynamics of the system can be written as

$$\mathbf{x}_{k+1} = A_d \mathbf{x}_k + B_d \mathbf{u}_k \tag{1}$$

where A_d is the state transition matrix for a single time step, B_d is the discrete input matrix for a single time step, and $\mathbf{u}_k$ is the input vector at step k. Typically, in a rendezvous situation, spacecraft would be in sufficiently close proximity to enable the use of the Hill–Clohessy–Wiltshire (HCW) equations [20], but approaches such as [21] can be used for more widely separated situations. Examples in this paper will use the HCW equations and hence the state $\mathbf{x}$ is defined as

$$\mathbf{x} = [\,x \quad y \quad z \quad v_x \quad v_y \quad v_z\,]^T \tag{2}$$

where x, y, z, v_x, v_y, and v_z are the positions and velocities of a chaser satellite in the radial, in-track, and cross-track axes, respectively, of a local–vertical/local–horizontal (LVLH) frame positioned on the center of gravity of a passive target vehicle. The input is defined as

$$\mathbf{u} = [\,u_x \quad u_y \quad u_z\,]^T \tag{3}$$

where u_x, u_y, and u_z are the inputs of the chaser vehicle in the axes indicated by the subscripts in the LVLH frame.

Given an initial state $\mathbf{x}_0$, the state at any future step k is [22]

$$\mathbf{x}_k = A_d^k \mathbf{x}_0 + [\,A_d^{k-1}B_d \quad A_d^{k-2}B_d \quad \cdots \quad A_d B_d \quad B_d\,] \begin{bmatrix} \mathbf{u}_0 \\ \vdots \\ \mathbf{u}_{k-1} \end{bmatrix} \tag{4}$$

$$= A_d^k \mathbf{x}_0 + \Gamma_k \begin{bmatrix} \mathbf{u}_0 \\ \vdots \\ \mathbf{u}_{k-1} \end{bmatrix} \tag{5}$$

where Γ_k is the discrete convolution matrix. Because the effects of the control on the states are readily expressed as linear combinations of the inputs, a linear optimization can be formed that optimizes the constrained control commands and constrains the states of the system. The cost function for this optimization will exclusively penalize fuel use. In an actual maneuver implementation, it may be preferable to optimize both the fuel use and the maneuver duration (see [23]); however, in this paper only fuel use will be considered to simplify presentation and cost comparisons. The cost of the optimization J is given by

$$J = \sum_{i=0}^{N-1} \|\mathbf{u}_i\|_1 \tag{6}$$

where the 1-norm cost is used to capture the expenditure of fuel used, which is proportional to acceleration and ΔV, from axial thrusters. The optimal cost is then given by

$$J^* = \min_{\mathbf{u}_0,\ldots,\mathbf{u}_{N-1}} \sum_{i=0}^{N-1} \|\mathbf{u}_i\|_1 \tag{7}$$

At each step k, it is possible to constrain the state at that time to lie inside a convex region

$$\bar{A}_k \mathbf{x}_k \le \bar{b}_k \tag{8}$$

where $\bar{A}_k$ is a matrix and $\bar{b}_k$ is a vector that together capture a set of linear constraints on the state. Note that the costs and constraints in Eqs. (6) and (8) show an example linear implementation of a trajectory optimization, but in general the same concepts that will be presented hold for nonlinear costs and constraints as well. Alternately, the state $\mathbf{x}_k$ could be constrained to lie outside a region through the use of binary variables [8]

$$\bar{A}_k \mathbf{x}_k \le \bar{b}_k + M\mathbf{y}_k \tag{9}$$

$$\|\mathbf{y}_k\|_1 \le m - 1 \tag{10}$$

where $\mathbf{y}_k$ is a vector whose elements are constrained to be 0 or 1, and M is a large number on the scale of values taken by elements of $\mathbf{x}$. This "Big M" method of collision avoidance works by allowing, at most, all but one of the collision avoidance constraints to be relaxed. A constraint is relaxed when the binary variable associated with it is set to 1, thereby making the right-hand side of the inequality very large and guaranteeing constraint satisfaction. Because at least one constraint is always guaranteed to not be relaxed, collision avoidance is assured (e.g., knowing that one is outside of one side of a box is sufficient information to guarantee that one is not in the box).

The inputs at each time step can also be directly constrained using

$$\mathbf{u}_{\min_k} \le \mathbf{u}_k \le \mathbf{u}_{\max_k} \tag{11}$$

where $\mathbf{u}_{\min_k}$ and $\mathbf{u}_{\max_k}$ are vector bounds on the values of $\mathbf{u}_k$. Typically, the minimum thrust at all times would be $-\mathbf{u}_{\max_k}$. A detailed description of the full matrix forms used in linear trajectory optimizations for space vehicles can be found in [8,19].

This section reviewed an approach for creating fuel-minimizing trajectories that satisfy time-varying position, velocity, and thrusting constraints. Applications of these constraint types can insure that a spacecraft remains inside a line-of-site cone, and arrives at a docking port position at a particular time with a particular speed range. In addition, the control authority available over the course of the trajectory can be varied according to desired pattern.

III. Safety Formulation

The trajectories generated by the constraints in Sec. II will satisfy docking requirements and use minimal fuel to arrive at a rendezvous location. However, as is typical of optimal paths, the trajectories will approach constraint boundaries and generally be sensitive to uncertain behavior. Richards [23] and Tillerson and How [24] describe computationally feasible methods of generating trajectories online that are robust to process and sensing noise expected under nominal operating conditions. That type of robustness to uncertainty is distinct from the definition of safety for off-nominal conditions considered herein. This section presents an approach for generating trajectories that are safe with respect to a class of system failures. Although it would be desirable to avoid collisions and successfully complete docking in the presence of any system failure, it is unlikely that such a scenario is possible. Instead, a large subset of all possible failures is used, including guidance system shutdowns, which encompasses thruster failures, computer anomalies, and loss of sensing. The response to these types of failures would be a guidance system shutdown in which the chaser vehicle would go into a safe mode with all its thrusters turned off. Safety to this class of failures is called *passive abort safety*, because any rendezvous can be aborted using no thrusting. Passive abort safety guarantees collision avoidance for any failure that can be identified and responded to by disabling thrusters before the spacecraft trajectory is affected. This type of safety does not include failures in which a thruster fails on (see Sec. VIII).

A consequence of passive abort is that if thrusters are disabled at any step T, counted from the start of the plan, during the trajectory implementation, then the thrusters will remain failed until the last

step N of the plan. Clearly if $N - T$ is small (i.e., only constraining steps toward the end of the horizon are safe), fewer constraints will be on the trajectory optimization than for a large value, but this assumes that more of the plan will be successfully implemented. Conversely, a large $N - T$ is a more conservative approach to safety and more tightly constrains the optimization. The choice of which steps in the plan that are constrained to be safe depends on the specific characteristics of the spacecraft and the mission requirements. The objective of this paper is to present a systematic way of embedding the safety goals into the path planning problem so that the designer can evaluate the tradeoffs associated with choosing a segment of a trajectory that is guaranteed safe.

Note that enabling passive safety abort at the end of a trajectory can eliminate potential plume impingement conflicts that may result from last-minute safe-mode maneuvers. A further benefit of guaranteeing safety at the end of the trajectory is that it gives controllers an immediate safe exit from the docking procedure during the period when the spacecraft are in the closest proximity and there is the least time available to plan emergency maneuvers.

The discrete convolution approach used in Eq. (4) can be used to predict the state of the chaser at step k in the planning horizon in the event of a failure at time T, by considering all inputs after and including the input at time T to be zero

$$\mathbf{x}_{FT_k} = A_d^k \mathbf{x}_0 + \begin{bmatrix} A_d^{k-1}B_d & A_d^{k-2}B_d & \cdots & A_d^{T-2}B_d & 0 \times A_d^{T-1}B_d & \cdots & 0 \times A_d B_d & 0 \times B_d \end{bmatrix} \begin{bmatrix} \mathbf{u}_0 \\ \vdots \\ \mathbf{u}_{k-1} \end{bmatrix} \tag{12}$$

where $\mathbf{x}_{FT_k}$ is the state of the chaser spacecraft at some step $k < N$ in the planning horizon after a failure occurred at step T. The value of a failure state after the planning horizon is found through open-loop propagation of the state at time N

$$\mathbf{x}_{FT_k} = A_d^{k-N} \mathbf{x}_{FT_N} \quad \text{for } k \geq N \tag{13}$$

Passive collision avoidance is achieved by adding constraints on the failure states of the spacecraft. Define the set of position states occupied by the target as $\mathcal{T}_k$, which can describe any polytopic region of position states, convex or otherwise. The safety horizon is the period of time after a failure during which both spacecraft are guaranteed not to collide. The safety horizon lasts S steps after the end of the nominal trajectory and is guaranteed by introducing the set of constraints

$$\mathbf{x}_{FT_k} \notin \mathcal{T}_k \quad \forall\ k \in \{T+1 \cdots N+S\} \tag{14}$$

The constraints in Eq. (14) are then imposed for $T \in \mathcal{F}$ where $\mathcal{F}$ is the set of every potential failure time at which the system must guarantee collision avoidance for guidance shutdowns. The parameters to be chosen in this safety formulation are $\mathcal{F}$ and S. This choice of parameters is highly dependent on the requirements of a particular space mission. The advantage of choosing to be safe for a large number of steps and for a long safety horizon is the improved likelihood of preventing a catastrophic failure scenario in which the chaser and target collide. However, imposing many safety constraints greatly reduces the number of potential solution trajectories and as a result, likely reduces fuel efficiency. The tradeoff between safety and fuel efficiency is discussed in the scenarios in Secs. IV.A and IV.B.

Remark 1: Mitigating Effects of Process Noise and Navigation Error. The safety formulation in Eqs. (12) and (14) assumes that the state of the chaser spacecraft relative to the target spacecraft is precisely known. In practice, this relative state is only known to within the accuracy provided by the navigation system. Likewise, the propagation used in Eq. (12) is only as accurate as the linear dynamics used to formulate that equation, because the actual vehicle would be subject to nonlinear dynamics, and disturbances from effects such as drag, J_2, separation distance, and eccentricity. Equation (12) can also be rewritten to enable time-varying dynamics or an additional vector of modeled disturbances can be added to the problem without increasing the complexity of the resulting optimization [19]. This permits a more sophisticated dynamics model to be used, which could reduce some of the effects of the modeling error [25]. To account for navigation error, the constraints in Eq. (14) can be made robust by posing them multiple times for a representative sampling of possible initial states that cover the space of likely navigation errors. Breger et al. [26] introduce such an approach and an algorithm for minimizing the effect of robustness constraints on the size of the resulting optimization.

IV. Scenarios

The rendezvous and docking scenario to be examined in this paper involves a chaser spacecraft maneuvering to achieve docking with a target spacecraft. Figure 1 shows a target spacecraft that lies at the center of a local frame. A line-of-sight (LOS) cone protrudes from the target spacecraft and it is required that the rendezvous remain within this LOS cone for vision-based sensing. At the interface between the LOS cone and the target is a docking port (rectangular platform). In the rotating case (Fig. 2) the axis of rotation is the long axis of the spacecraft and the rotation rate is orbital. The choice of rotation axis and rate was arbitrary and only enters the optimization through their effect on the time-varying constraints imposed for LOS requirements, docking, and safety. The LOS requirements are

$$A_{\mathrm{LOS}_k} \mathbf{x}_k \leq b_{\mathrm{LOS}_k} \quad \forall\ k = 1 \cdots N \tag{15}$$

where A_{LOS_k} and b_{LOS_k} describe the states within the LOS cone at a step k in the planning horizon. The terminal constraint is

$$A_{\mathrm{Term}_N} \mathbf{x}_N \leq b_{\mathrm{Term}_N} \tag{16}$$

where A_{Term_k} and b_{Term_k} describe the states the spacecraft must occupy at the end of the planning horizon to achieve safe docking. These constraints can be both on position (e.g., enter a region within reach of a grappling arm) and on velocity (e.g., dock within a velocity range that produces acceptable stress on the docking port). In addition, time-varying bounds are introduced on the maximum thrusting levels to ensure large thrusts are not planned for the period immediately before docking. The safety constraints in Eq. (14) are imposed for the last quarter of the planning horizon. In the examples, an orbit with frequency $n = 0.001$ rad/s is used and is discretized into 20 steps and the set of inputs that can fail is $T \in \{14 \cdots 19\}$. The planning horizon is a full orbit. The chaser spacecraft, modeled after the mission in [27], has a mass of 45 kg and a maximum acceleration of 10^{-3} m/s^2 during the first 17 steps of the plan and 10^{-5} m/s^2 for the last three steps to prevent trajectory solutions with large terminal

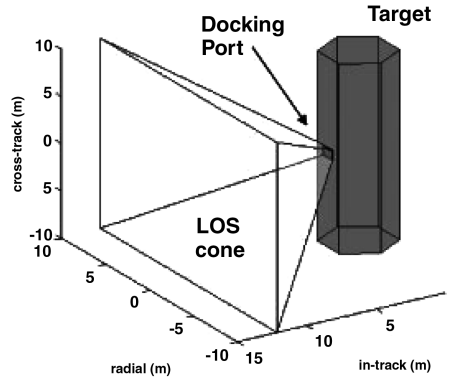

Fig. 1 Target spacecraft and docking configuration.

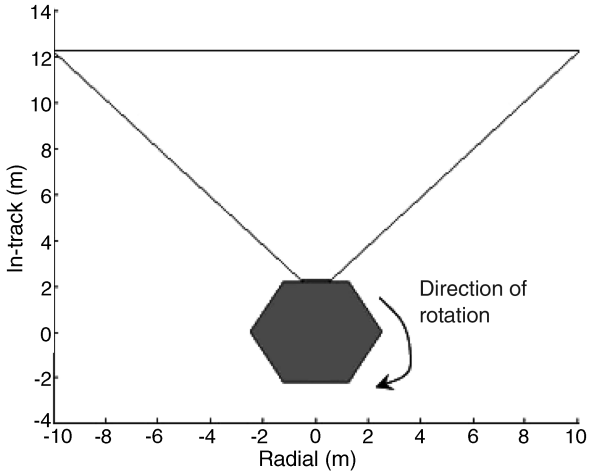

Fig. 2 Radial/in-track view of rotating target spacecraft and docking configuration.

thrusts. In addition, the docking constraint specifies that the velocity of the spacecraft at the time of docking be less than 1 mm/s. In summary, the safety algorithm used in this section minimizes the 1-norm of fuel consumption subject to thrust magnitude constraints, line-of-sight constraints, rendezvous constraints, and safety constraints. This algorithm can be stated as the optimization

$$\begin{aligned} \min_{\mathbf{u}_0,\ldots,\mathbf{u}_{N-1}} \quad & \text{Eq. (6)} \\ \text{s.t.} \quad & \text{Eq. (11)} \quad \forall\ k \in \{0,\ldots,N-1\} \\ & \text{Eq. (15)} \\ & \text{Eq. (16)} \\ & \text{Eq. (14)} \quad \forall\ T \in \mathcal{F} \end{aligned} \tag{17}$$

In these examples, the safety horizon is a full orbit. Any of the design parameters in the safety implementation can be easily adjusted and in practice one would likely conduct a simulation study or analysis [28] to find the best combination for minimizing fuel use and guaranteeing feasible solutions.

A. Case 1: Stationary-Target Satellite

An optimized trajectory with no safety constraints [i.e., Eq. (17) without constraints using Eq. (14)] for the stationary-target (i.e., not rotating or translating in the local frame) case is shown in Fig. 3. The initial trajectory to the docking port roughly corresponds to a two-impulse V-bar (in-track) [12] approach. The nominal trajectory is marked with ● and the failure trajectories with ×. Failure trajectories, the paths followed by the spacecraft in the event of a guidance shutdown, are shown for the last five possible inputs. Several of the failure trajectories overlap, a condition which

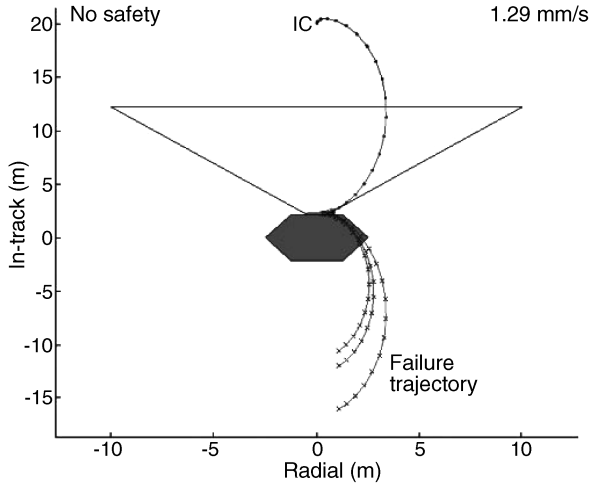

Fig. 3 Nominal trajectory planning with no safety: constraint violations occur for trajectory failures. The nominal trajectory is marked with ● and the failure trajectories with ×. The failure trajectories all result in collisions with the target spacecraft.

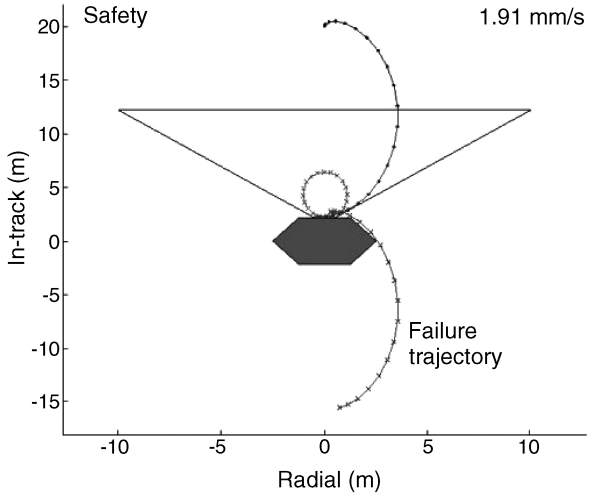

Fig. 4 Trajectory planning with safety: failed trajectories deviate around the target spacecraft, preventing collision. The nominal trajectory is marked with ● and the failure trajectories with ×.

corresponds to the nominal input at a step already being set to zero thrust. All of the failure trajectories clearly impact the target spacecraft. Figure 4 shows the same rendezvous situation for trajectories generated with safety constraints. In this case, none of the failure trajectories impact the target spacecraft. As in the case without safety, several of the failure trajectories overlap. The fuel costs (measured in ΔV) of the trajectory with no safety guarantees and the trajectory with safety are 1.29 and 1.91 mm/s, respectively. Hence, in this case, imposing safety results in a 48% increase in fuel use. To put these numbers in context, an optimized approach constrained to follow a V-bar trajectory (strictly in-track) would use 37.7 mm/s of fuel.

An approximate method for overbounding the optimized numbers would be to consider an approach based on introducing in-track drift and arriving at the docking port after a full planning horizon, with no other constraints. In this case, the planning horizon is a full orbit, with no initial radial offset and no initial velocity; an initial thrust in the in-track direction will introduce a secular drift into the relative orbit. Over the course of an orbit this secular drift causes the in-track position to shift by

$$\Delta y = \Delta v_y 6\pi/n \tag{18}$$

according to the in-track solution for Hill's equations [29]. For the example in this section, the amount of fuel required for this maneuver would be 0.93 mm/s. An approximate upper bound on the fuel number could be obtained by forming a constrained problem similar to the linear program (LP), but forced to follow a strict in-track (V-bar) trajectory. If the 2-norm of fuel use is minimized as an approximation instead of the correct 1-norm metric and the thruster inputs are not constrained, this problem can be solved using a pseudoinverse. By constraining the radial position state at each step k in the planning horizon to be zero and the final in-track position to lie on the edge of the docking port, the following equality constraints are formed:

$$A_Q \begin{bmatrix} \mathbf{u}_0 \\ \vdots \\ \mathbf{u}_{k-1} \end{bmatrix} = b_Q \tag{19}$$

with

$$A_Q = \begin{bmatrix} H_x\Gamma_1 & 0 & \cdots & 0 & 0 \\ H_x\Gamma_2 & 0 & \cdots & 0 & \\ H_x\Gamma_{N-1} & 0 & & & \\ H_x\Gamma_N & & & & \\ H_y\Gamma_N & & & & \end{bmatrix}, \quad b_Q = \begin{bmatrix} -H_xA_d^1\mathbf{x}_0 \\ -H_xA_d^2\mathbf{x}_0 \\ \vdots \\ -H_xA_d^N\mathbf{x}_0 \\ -H_yA_d^N\mathbf{x}_0 + y_{\text{des}} \end{bmatrix} \tag{20}$$

where H_x is a row vector that extracts the scalar radial component, H_y is a row vector that extracts the scalar in-track component, and y_{des} is the desired in-track component at step N. This form has $N+1$ constraints and $3N$ input variables to choose. The trajectory that minimizes the 2-norm of the input vectors and meets those simple constraints is given by the pseudoinverse solution [30] of

$$\begin{bmatrix} I_{3N} & A_Q^T \\ A_Q & 0_{N+1} \end{bmatrix} \begin{bmatrix} \mathbf{u}_0 \\ \vdots \\ \mathbf{u}_{k-1} \\ \mathbf{z} \end{bmatrix} = \begin{bmatrix} 0_{3N,1} \\ b_Q \end{bmatrix} \tag{21}$$

where $\mathbf{z}$ is a vector of $N+1$ Lagrange multipliers, Ip is a $p \times p$ identity matrix, 0_q is a $q \times q$ matrix of zeros, and $0_{p,1}$ is a $p \times 1$ vector of zeros. The fuel cost of the trajectory found using this method is 39.1 mm/s, which is very close to the optimized cost of following a strict V-bar trajectory.

B. Case 2: Docking Port Perpendicular to Spin Axis

The rotating docking port case uses an identical formulation to the stationary case, however, the constraint regions are time varying. In particular, in the stationary case, $A_1 = A_2 = A_k \forall\ k = 1 \cdots N$, but to formulate the rotating problem, the A_k and b_k matrices must be formed for each step of the planning horizon based on the rotation rate and, for more general cases, the motion of the target, the docking port, and the line-of-sight cone. One simple way to generate these constraints is to represent each side of an avoidance region as a plane that is specified by a sample of its constituent points. These points will remain in a plane through any reorientation of the original constraint. Thus, the rotated constraint side can be found by applying rotation matrices [31] to the points and then forming the equation of a new plane, which can then be used as an inequality constraint. The translation and rotation motion of the target spacecraft should be well characterized through observation or cooperation before starting a rendezvous maneuver, thereby allowing the prediction of its future trajectory to be used for forming constraints. All trajectory propagations of the target spacecraft used to create constraints are formed before the rendezvous maneuver is optimized. As a result, the propagation can be carried out using any method appropriate for the specific online implementation (e.g., simple linear propagation, high accuracy numerical integration). Robustness to uncertainty in target motion can be accommodated by guaranteeing that any optimized trajectory is valid for a range of representative target initial conditions [19].

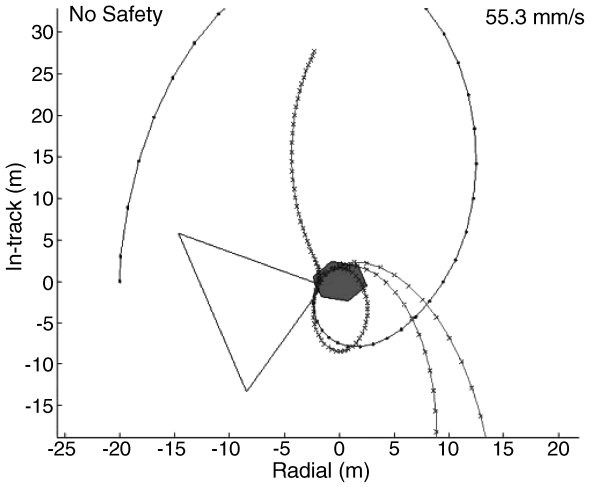

Fig. 5 Nominal trajectory planning with no safety in the rotating case: constraint violations occur for trajectory failures.

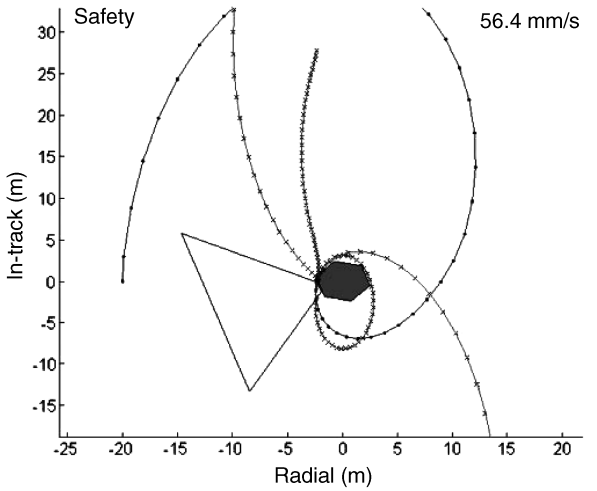

Fig. 6 Trajectory planning with safety in the rotating case: failed trajectories deviate around the target spacecraft, preventing collision.

For the rotation case examined in this section, the optimized trajectory no longer matches a two-impulse V-bar approach, but is instead forced to thrust regularly to stay within the rotating LOS cone. Figure 5 shows this optimized trajectory with no safety constraints. As in the stationary case, in the absence of safety constraints, the nominal trajectory collides with the target in the event of guidance shutdowns. An alternate form with safety constraints prevents collisions for failures occurring in the last quarter of the trajectory (Fig. 6). Note that in Fig. 6, the safe trajectory appears to pass through the target, but in actuality it avoids collision because of the rotational motion of the target. The fuel costs without and with safety constraints are 55.3 and 56.4 mm/s, respectively. In this case, the fuel cost of imposing safety as a constraint is only a 2% increase over the nominal cost. As in the nonrotating case, the increase in fuel needed to include the safety constraints is minimal and the advantage is guaranteed collision avoidance for passive abort in the last quarter of the nominal path.

C. Case 3: Stationary Docking Along a Radial Trajectory

Another example (safe trajectory in Fig. 7) using a stationary target with an initial radial offset required 104 mm/s of fuel with and without safety constraints. The safety constraints in this case were not necessary for creating a safe trajectory, because R-bar approaches tend to naturally drift away from the target satellite. However, the addition of the safety constraints would be appropriate for a radial approach if the target satellite has additional avoidance constraints (e.g., solar panels).

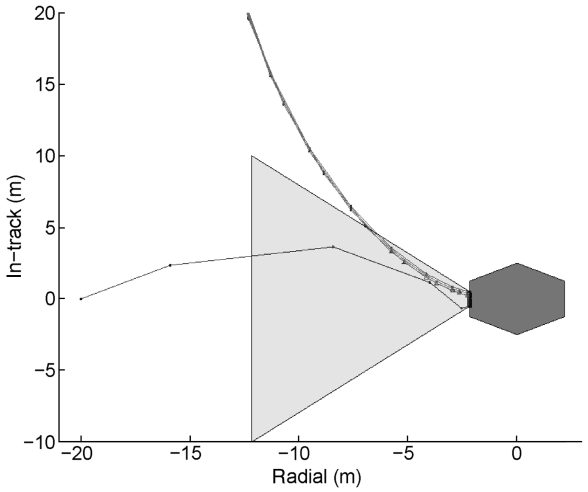

Fig. 7 Radial trajectory with passive safety.

V. Probability of Collision

To judge the effectiveness of the safety algorithm introduced in Sec. III, define a probability of the collision metric P_{col}, which is the probability of a failure at any time step during a maneuver resulting in a collision between the target and chaser spacecraft. The probability of collision is given by

$$P_{\text{col}} = \sum_{i=1}^{N} P(\text{failure at } i \mid \text{no failure before } i) \cdot P(\text{collision occurs} \mid \text{failure at } i) \tag{22}$$

where the probability $P(\text{collision occurs} \mid \text{failure at } i)$ is either 1 or 0 and is evaluated by examining the trajectory followed if thrusters are disabled at step i and checking for future collisions. Assuming that the probability of a failure at any step in the trajectory is f, then

$$P(\text{failure at } i \mid \text{no failure before } i) = (1-f)^{i-1} f \tag{23}$$

Using the metric P_{col}, the effectiveness of the safety approach was investigated by creating a series of safe trajectories starting from different initial conditions near the target. The initial condition positions were chosen to create a range of nearby starting points. The velocity vector for each position was chosen according to the conditions in [14] to create a safety ellipse. This creates a situation where each rendezvous trajectory begins from a safe, invariant orbit within range of a final approach rendezvous trajectory.

Figures 8 and 9 show the values of P_{col} for full-orbit optimized final approach trajectories, discretized into $N = 20$ steps. The trajectories are generated using $\mathcal{F} = \emptyset$ (no safety constraints) and $\mathcal{F} = \{9, \ldots, 19\}$ (guaranteed safe for the last 10 steps of the trajectory), respectively, where $f = 0.001$. These plots show that without safety, the probability of collision for a given rendezvous trajectory tends to fall between 0.005 and 0.015. However, the addition of safety for half of the trajectory brings the collision probability for most of the trajectories below 0.001. The same optimizations were performed and analyzed for a range of other $\mathcal{F}$ ranges and the results are summarized in Fig. 10. The dashed line indicates an overbound, $\bar{P}_{\text{col}}$, for the maximum possible probability of collision, which is the case where every failure during the course of the trajectory when safety is not guaranteed (i.e., steps not in $\mathcal{F}$) would result in a collision, which is given by

$$\sum_{\{0,\ldots,N-1\}\{\mathcal{F}} P(\text{failure at } i \mid \text{no failure before } i) \tag{24}$$

The line marked with ◆ shows the largest probability encountered in the optimized trajectories for all initial conditions considered. This is equivalent to finding the maximum height (z value) in a plot of the type in Fig. 9 for each different set of $\mathcal{F}$ used to create Fig. 10. The minimum (line marked by ○) shows that in each case, there were

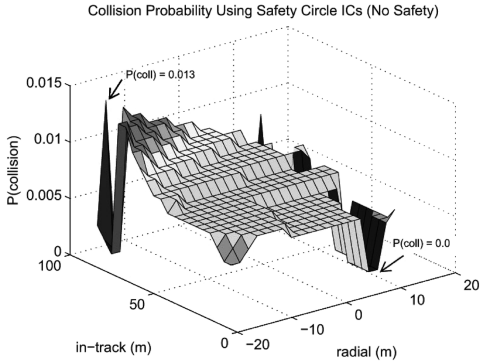

Fig. 8 Probability of a collision occurring for a range of initial conditions with $\mathcal{F} = \emptyset$ (no safety guarantees).

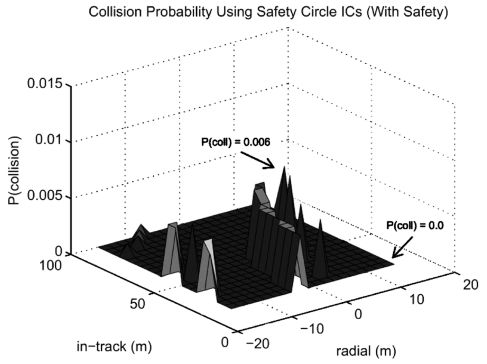

Fig. 9 Probability of a collision occurring for a range of initial conditions with $\mathcal{F} = \{9, \ldots, 19\}$ (latter half of trajectory guaranteed safe).

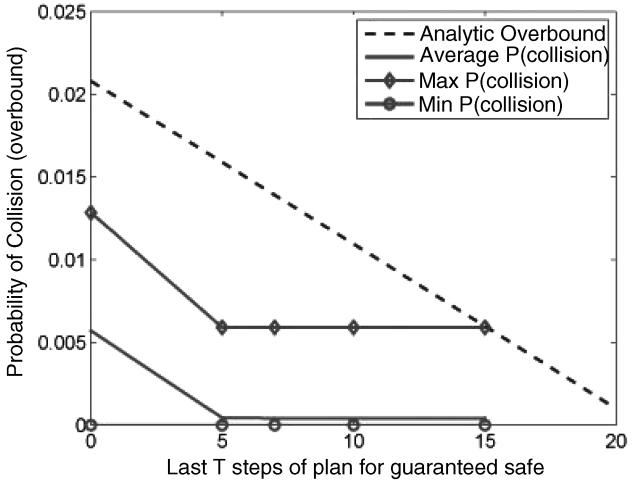

Fig. 10 Probability of collision occurring for various values of $\mathcal{F}$.

some initial conditions that did not result in collision, regardless of the steps in $\mathcal{F}$. In those cases, the fuel-optimal rendezvous trajectory is safe. The average P_{col} (solid line), equivalent to averaging the probability heights over an area of the type in Fig. 9, followed a similar trend to the largest P_{col}, but was significantly lower. This indicates that although some initial conditions are particularly prone to collision, on average the collision probabilities are significantly improved by safety and in no case has the addition of safety made collisions more likely than in the fuel-optimal case ($\mathcal{F} = \emptyset$). Furthermore, for this particular case, the trends indicate that guaranteeing more than the last five steps safe does not significantly decrease the probability of a collision. This conclusion would be valuable from a mission planning perspective, because each

additional plan step that is guaranteed safe represents a tradeoff in which computation time and nominal fuel use potentially increase.

Equation (24) indicates that the overbound $\bar{P}_{\text{col}}$ decreases with increasing length of the safe region (i.e., fewer steps in $\mathcal{F}$). For the purposes of worst-case safety guarantees, the overbound could be used as an analytic rule of thumb for mission design studies.

VI. Invariant Formulation

The safety formulation introduced in Sec. III only guarantees passive collision avoidance until the end of the safety horizon. In previous examples, the safety horizon has been fixed at one orbit. Figure 11 shows a stationary-target case where a collision would occur soon after the end of a one orbit safety horizon. If the safety horizon is extended to multiple orbits, the resulting failure trajectories will tend to either drift away from target spacecraft or create invariant orbits that neither drift toward nor away from the target spacecraft. Drifting away from the target orbit is preferable to collision; however, it means that fuel will need to be expended to bring the chaser near the target for any future docking attempts. Furthermore, the longer the controllers wait to cancel the drift, the farther apart the two spacecraft will become, thereby creating an additional timing consideration during an anomalous event. It is preferable for the chaser to drift into an invariant orbit that is near the target, but can never, under the assumptions of Keplerian dynamics, collide. The preference for invariant failure orbits can be captured by constraining a state in the failure trajectory at some step k to be the same one full orbit after k using a linear state transition matrix to propagate the state forward. This constraint is written as

$$\mathbf{x}_{FT_k} = A_d^{N_o}\mathbf{x}_{FT_k} \quad \text{for } k \geq T \tag{25}$$

where N_o is the number of steps in an orbit. By imposing this constraint for all possible failure times in $\mathcal{F}$, all failure orbits are guaranteed to be invariant with respect to the target. The safety algorithm in Eq. (17) is only altered by the addition of the new constraints in Eq. (25).

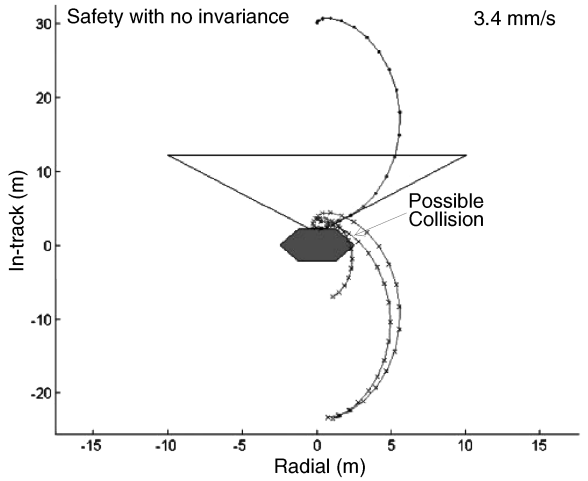

Fig. 11 Case where the end of the safety horizon is followed by a collision.

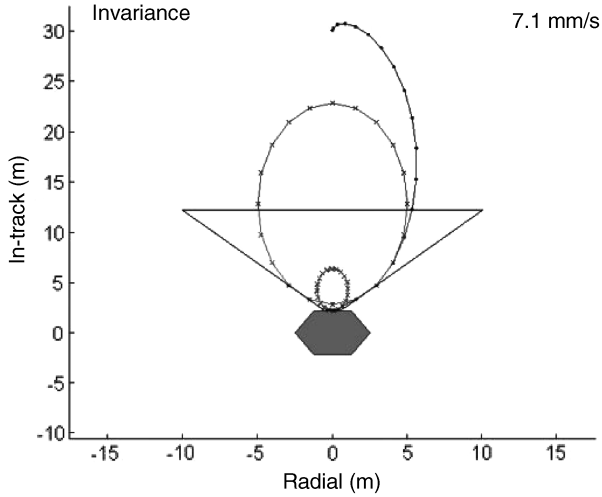

Fig. 12 Use of invariance constraints guarantees infinite horizon passive collision avoidance and prevents failure trajectories from drifting away from the target.

Figure 12 shows the same rendezvous problem from Fig. 11, but with additional invariance constraints on failures occurring in the last quarter of the rendezvous trajectory. Imposing invariance constraints yields circular trajectories relative to the target, which are traversed once per orbit with no fuel expenditure. Some of the six failure trajectories shown in Fig. 12 overlap each other where the optimized trajectory did not require fuel inputs. The safe trajectory with no invariance constraint used 3.4 mm/s of fuel and the safe trajectory with invariance used 7.1 mm/s of fuel. In this case, the invariance constraints have roughly doubled fuel requirements. However, this tradeoff may be beneficial when there is a danger of collision after the safety horizon or when the fuel requirements for canceling drift after a failure are taken into account. The cost of using an optimized rendezvous trajectory with no safety constraints is 3.1 mm/s (versus 3.4 mm/s with safety), making safety roughly 10% more expensive. The cost of using a strict V-bar approach (59.2 mm/s) is roughly 18 times more expensive than the optimized safe approach and 8.6 times more expensive than the optimized safe invariant approach. Thus, when compared to the cost of using a standard nonoptimized maneuver, the fuel premium for using safety with invariance is small.

The examples using invariance constraints presented in this section used Hill's dynamics [20], meaning that the particular type of invariance achieved is effectively equivalent to constraining the relative semimajor axes of the target and chaser spacecraft to be zero. Alternate equations of motion exist which model additional orbital perturbations. For example, the dynamics presented in [32] could be used for rendezvous and docking trajectory generation to create invariant orbits that account for the effects of differential J_2. Likewise, the effects of differential drag can also be taken into account using the method in [19].

VII. Convex Safety Formulation

The safety constraints introduced in Sec. III guaranteed that the chaser states would not collide with the target in the event of a failure. The collision avoidance in those constraints is accomplished using binary variables to capture the nonconvexity of the problem. The problem with binaries was formulated as a mixed-integer linear program (MILP) and posed to a commercial solver. Solving a MILP can be a computationally intensive task and the time required to solve tends to grow very quickly with the number of discrete variables in the problem [33]. The trajectory shown in Fig. 4 required 8.92 s to solve on a 3-GHz computer. That problem had a 20-step safety horizon, an avoidance region with eight sides, and six inputs that were safe (i.e., the last quarter of the trajectory) in the event of guidance shutdown. Each avoidance region side requires a binary variable at each step of the safety horizon and those constraints are included 6 times, each propagating forward from a different failed thruster step. Thus, implementing collision avoidance over the safety horizon for that simple example required 960 binary variables. Solving the same trajectory for a two orbit safety horizon required 24.6 s. Using the same horizon duration with a finer discretization step would further increase the required computation time. It is likely that online implementations would need to be solved with limited computer resources and that a nonconvex implementation may be impractical for implementations requiring short discretization steps.

An alternative to the nonconvex formulation is to use a more restrictive form of collision avoidance that is convex. Instead of requiring the chaser to remain outside an avoidance region, the

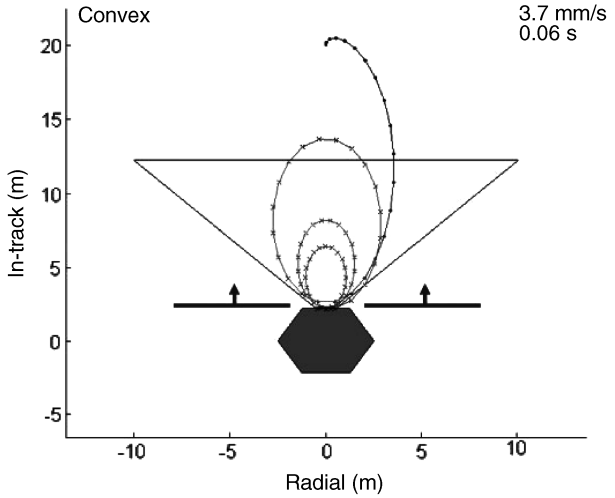

Fig. 13 Collision avoidance for failure trajectories using convex constraints indicated by arrows.

failure trajectories are instead constrained to remain inside a region that is known to not contain the target. This is similar to the type of convex passively safe trajectory examined for rotating satellite capture in [16]; however, the approach in this paper explicitly minimizes fuel use. Figure 13 shows an example of the optimized trajectory for the rendezvous problem in Fig. 4, but instead solved as a LP using the convex safety constraints

$$H_y \mathbf{x}_{FT_k} \geq y_{\min} \quad \forall\ k \in \{T+1, \ldots, N+S\} \tag{26}$$

where $y_{\min}$ is the maximum in-track position of the target spacecraft. The nonconvex case results in failure trajectories that are not permitted in the convex case and as a result, there is a fuel penalty for imposing convexity. Using the convex formulation in Eq. (26) does not require altering the basic safety algorithm in Eq. (17). Instead, only the target geometry, given by the set $\mathcal{T}$ in Eq. (14), needs to be altered to ensure that its complement is convex. The nonconvex case requires 1.5 mm/s of ΔV and the convex case requires 3.7 mm/s. The more restrictive area in which failure trajectories can lie caused the required fuel to increase by more than a factor of 2. However, the amount of time required to compute the convex trajectory was only 0.06 s, a decrease from the nonconvex case by a factor of 150. In cases where it is impractical to dedicate significant computational resources to planning, it may be desirable to trade the fuel optimality of the more general MILP formulation for the speed of the LP formulation. In addition, the convex solution is often similar to the invariant given in Eq. (25). For the example in Fig. 13, the trajectory cost when invariance and convexity are imposed is 4.2 mm/s, which is the same as the cost of using invariance in the fully nonconvex problem.

VIII. Active Safety

An alternative to passive safety is *active safety*, in which a set of thruster inputs is applied to ensure rendezvous safety. The active response is a set of input sequences that is used instead of passive safety. The *safe input sequence* can be designed a priori (e.g., thrust in-track, thrust radially) and chosen in real time or optimized at the time the nominal rendezvous maneuver is optimized. In either case, the safe inputs are known at all times during the maneuver and no additional optimization is required in the event of a failure. The advantages of active safety over passive safety are significant: by allowing thrusting in the event of a failure, a significantly larger portion of the nominal trajectory can be guaranteed safe and the fuel costs of guaranteeing the safety of the nominal trajectory are reduced. Passively safe trajectories can be considered a subset of active safe trajectories in which the active input sequence has no thrusting. The primary limitation of active safety is that it provides safety guarantees for a smaller set of possible system malfunctions than passive safety. In the case of passive safety, any anomaly in which the thrusters can be disabled can be made safe. Safety guarantees resulting from an active safety trajectory require that some thrusters continue to work properly and in the correct directions in the event of a failure. An extension at the end of this section will show how active safety can be modified to provide safety guarantees for single thruster failures.

To create an active safety constraint, the optimization from Sec. III is altered to allow the possibility of using a safe input sequence by introducing an additional discrete convolution matrix. Rewriting Eq. (12) for a predetermined safe input sequence

$$\begin{aligned}\mathbf{x}_{FT_k} = {} & [A_d^{k-1}B_d \quad A_d^{k-2}B_d \quad \cdots \quad A_d^{T-2}B_d \quad 0\times A_d^{T-1}B_d \quad \cdots \quad 0\times A_dB_d \quad 0\times B_d]\begin{bmatrix}\mathbf{u}_0\\ \vdots \\ \mathbf{u}_{k-1}\end{bmatrix} + A_d^k\mathbf{x}_0 \\ & + [A_d^{k-T-1}B_d \quad \cdots \quad A_dB_d \quad B_d]\begin{bmatrix}\mathbf{v}_0\\ \vdots \\ \mathbf{v}_{k-T-1}\end{bmatrix}\end{aligned} \tag{27}$$

where $T < k < N$, $k - T < N_s$, N is the number of steps in the nominal plan, and N_s is the number of steps in the safe input sequence. If $k \leq T$, then $\mathbf{x}_{FT_k} = \mathbf{x}_k$, because no potential failure could have occurred at that time. Equation (27) can be written more generally as

$$\mathbf{x}_{FT_k} = \begin{cases} \Gamma_k S(T,k)\mathbf{U}_k + A_d^k\mathbf{x}_0 + \Gamma_{k-T}S(k-T,N_s)\mathbf{V}_k, & T < k \leq N, T < k-T \leq N_s \\ A_d^{k-N}\Gamma_N S(T,N)\mathbf{U}_N + A_d^k\mathbf{x}_0 + \Gamma_{k-T}S(k-T,N_s)\mathbf{V}_k, & k > N, k-T \leq N_s \\ \Gamma_k S(T,k)\mathbf{U}_k + A_d^k\mathbf{x}_0 + A_d^{k-N_s}\Gamma_{N_s}\mathbf{V}_{N_s}, & k \leq N, k-T > N_s \\ A_d^{k-N}\Gamma_N S(T,N)\mathbf{U}_N + A_d^k\mathbf{x}_0 + A_d^{k-N_s}\Gamma_{N_s}\mathbf{V}_{N_s}, & k > N, k-T > N_s \end{cases} \tag{28}$$

where k is the time step that the failure trajectory is propagated forward to, $S(q,N_q) = \mathrm{diag}(\mathbf{I}_{3(q)}, \mathbf{0}_{3(N_{q-q})})$, $\mathbf{I}_n$ is an $n \times n$ identity matrix, $\mathbf{0}_n$ is an $n \times n$ matrix of zeros, the decision variables for the nominal input are the vector $\mathbf{U}_k^T = [\mathbf{u}_0^T \quad \cdots \quad \mathbf{u}_{k-1}^T]$, and the predetermined safe input sequence $\mathbf{V}_k^T = [\mathbf{v}_0^T \quad \cdots \quad \mathbf{v}_{k-1}^T]$. The possible ranges in Eq. (28) correspond to the steps before the nominal plan has ended and before the end of the safe input sequence ($k \leq N$, $k \leq k-T$), the times after the nominal plan has ended and before the end of the safe input sequence ($k > N$, $k \leq k-T$), times before the

nominal plan has ended and after the end of the safe input sequence ($k \leq N, k > k - T$), and the times after the both the nominal plan and the safe input sequence have ended ($k > N,\ k > k - T$). All four cases must be considered to allow for safe input sequences that are longer or shorter than the nominal plan length. Active safety can be guaranteed by introducing the set of constraints

$$\mathbf{x}_{FT_k} \notin \mathcal{T}_k \quad \forall\ k \in \{T+1, \ldots, N+S\} \tag{29}$$

The set of constraints in Eq. (29) is applied for each step T at which safety should be guaranteed in the event of a failure.

An alternate approach to active safety where the safe input sequence is optimized online can be implemented by moving the safe input sequence $\mathbf{V}_{N_s}$ into the decision vector of Eq. (28)

$$\mathbf{x}_{FT_k} = \begin{cases} [\Gamma_k S(T,k) \ \ \Gamma_{k-T} S(k-T, N_s)] \begin{bmatrix} \mathbf{U}_k \\ \mathbf{V}_k \end{bmatrix} + A_d^k \mathbf{x}_0, & T < k \leq N, T < k - T \leq N_s \\ [A_d^{k-N} \Gamma_N S(T,N) \ \ \Gamma_{k-T} S(k-T, N_s)] \begin{bmatrix} \mathbf{U}_N \\ \mathbf{V}_{N_s} \end{bmatrix} + A_d^k \mathbf{x}_0, & k > N, k - T \leq N_s \\ [\Gamma_k S(T,k) \ \ A_d^{k-N_s} \Gamma_{N_s}] \begin{bmatrix} \mathbf{U}_N \\ \mathbf{V}_{N_s} \end{bmatrix} + A_d^k \mathbf{x}_0, & k \leq N, k - T > N_s \\ [A_d^{k-N} \Gamma_N S(T,N) \ \ A_d^{k-N_s} \Gamma_{N_s}] \begin{bmatrix} \mathbf{U}_N \\ \mathbf{V}_{N_s} \end{bmatrix} + A_d^k \mathbf{x}_0, & k > N, k - T > N_s \end{cases} \tag{30}$$

such that the safe input sequence $\mathbf{V}_{N_s}$ is optimized at the same time as the nominal rendezvous trajectory. The weighting on the fuel inputs in $\mathbf{V}_{N_s}$ relative to those in $\mathbf{U}_N$ is made small to minimize the fuel required for the more likely nominal case. Active safety uses the same safety algorithm in Eq. (17), but with Eq. (14) replaced by Eq. (29) using the active failure trajectory given by Eq. (28) for a priori known safe input sequences or Eq. (30) for safe input sequences optimized online.

The implementation of an active safe trajectory would be similar to that of a safe trajectory. Before entering the trajectory, the spacecraft is assumed to be in a nominal state (i.e., all systems are functioning correctly). If a fault has not yet occurred, the spacecraft follows the nominal trajectory, which is given by $\mathbf{U}_N$. If a fault occurs during a step that has been guaranteed to be safe in the event of that fault, then the spacecraft begins using the safe input sequence. For the duration of the safe input sequence, the chaser and target spacecraft are guaranteed to not collide. If the invariance constraints in Sec. VI are used, safety can be guaranteed for any time horizon over which the dynamics are valid.

A. Examples

A stochastic analysis of the type performed in Sec. V was conducted using active safety, guaranteeing safety for the last three-fourths of the nominal trajectory ($\mathcal{F} = \{9, \ldots, 19\}$). The results indicated that the average collision probability for failures accounted for by active safety was reduced to 1.96×10^{-5} from 0.0057 for the optimal unsafe case and 4×10^{-4} for the passive safety case ($\mathcal{F} = \{4, \ldots, 19\}$). The differences between the active safety approaches are demonstrated in Figs. 14–17. Figure 14 shows an active safe rendezvous trajectory beginning from a safety ellipse holding orbit. In this case, the safe input sequence $\mathbf{V}$ has been arbitrarily chosen to be an orbit of constant thrusting at 10^{-6} m/s^2 in the $-x$ direction of an LVLH frame centered on target. The last three-quarters of the rendezvous trajectory have been guaranteed through constraints to be actively safe. In the figure, the nominal rendezvous trajectory (line marked with ●) shows the planned rendezvous maneuver which will be followed if no failures occur. Each portion of the trajectory marked with △ shows a possible path followed by the chaser in the event that the safe input sequence is used. Constraints guarantee safe collision avoidance for the entire red portion of the trajectory; however, no safety guarantees exist for the trajectory after the safe input sequence is enacted. The trajectories marked by × show how the path drifts after the end of each safe trajectory. In several cases, the drifting path would result in a collision at some time in the future. To ensure collision avoidance, Fig. 16 shows an active safe trajectory optimized from the same initial conditions, but with the invariance constraint from Eq. (25) imposed. In this case, a failure at any step in the last three-quarters of the nominal trajectory would result in the chaser spacecraft entering a safe, invariant trajectory near the target spacecraft. Figures 16 and 17 show the optimized active safe trajectories using the constraints in Eq. (30) without and with invariance constraints, respectively.

Table 1 compares various approaches for creating rendezvous trajectories with and without safety using the same initial conditions as the examples in Figs. 14–17. The first row refers to the fuel cost (mm/s) of implementing the nominal rendezvous trajectory. The second row gives the cost of implementing a full safe input sequence (mm/s). The last row gives the probability of collision for the trajectory using the method introduced in Sec. V. The columns compare the fuel-optimal path with no safety to the passive safety path and paths using active safety. The active safety columns labeled a priori use the predefined safe input sequence approach in Eq. (28) and the columns labeled optimized use the approach in Eq. (30). The columns marked invariant also use the invariance constraints in Eq. (25). It is notable that for the example in the table, the probability of collision for the fuel-optimal trajectory (i.e., no safety) is 0.012, but the addition of passive or active safety to the problem causes the probability to drop to zero. Note that this probability is predicated on the assumption that a failure is identified within a time step of its

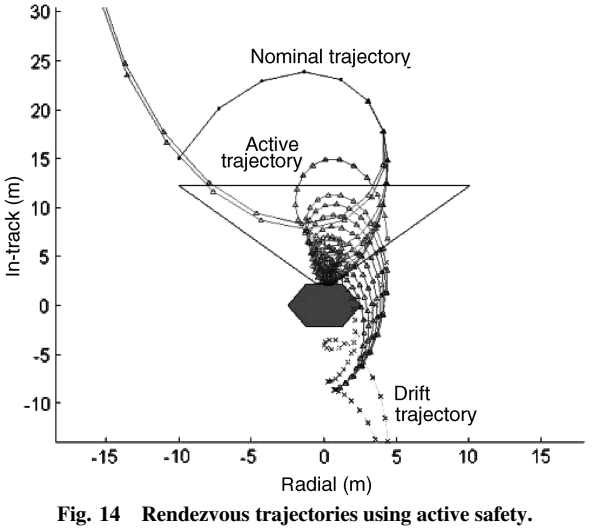

Fig. 14 Rendezvous trajectories using active safety.

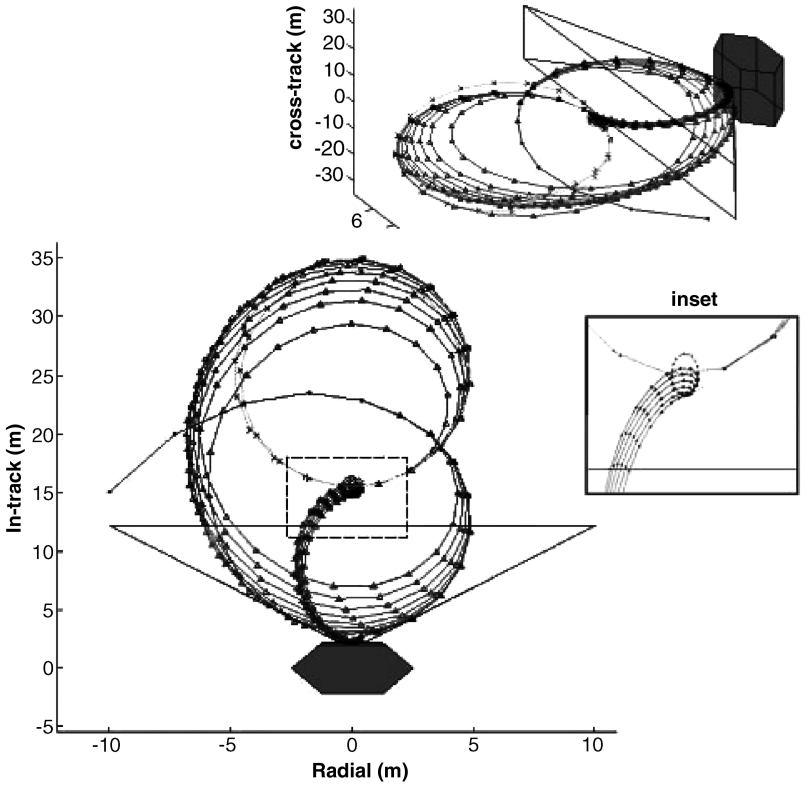

Fig. 15 Rendezvous trajectories using active safety with invariance constraints.

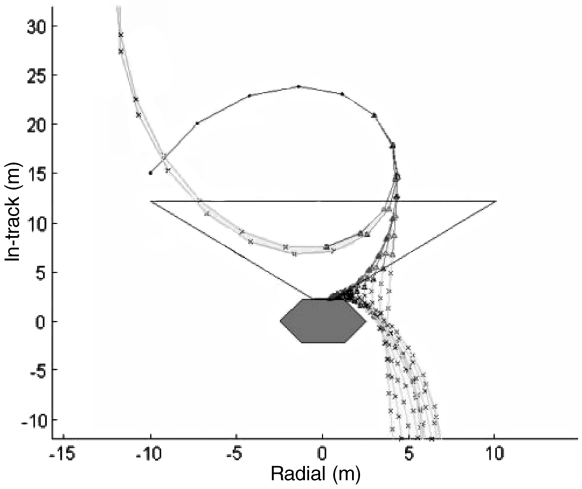

Fig. 16 Rendezvous trajectories using optimized active safety.

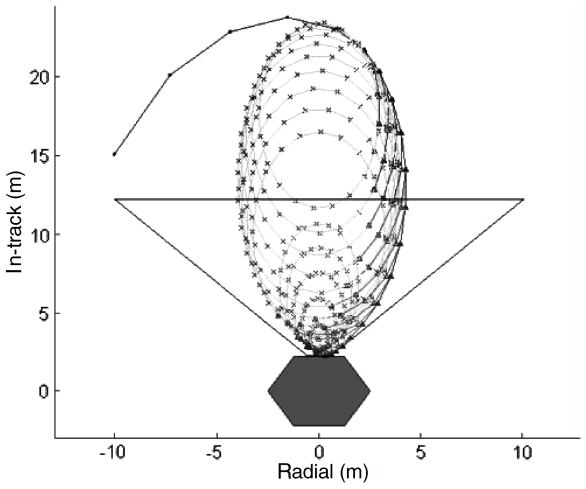

Fig. 17 Rendezvous trajectories using optimized active safety with invariance constraints.

occurrence and that the thrusters can be turned off (for passive safety) or used nominally (for active safety).

Passive safety requires more fuel for rendezvous than the case without safety; however, active safety with an optimized safe input sequence has the same cost as the fuel-optimal case. In the cases where invariance is imposed as a constraint, the fuel cost using active optimized safety is lower than the passive invariance case, but not as low as the optimal trajectory. Thus, for these initial conditions, both the nominal trajectory and the safe abort trajectory must be shaped to achieve active invariance. The cost of safety for the nominal and passive safety trajectories is zero, because those cases do not consider safety and do not require thrusting for failures, respectively. In each active safety case, the safety cost is very small compared to the cost of the nominal trajectory, indicating that it should be possible to implement active safety on a space mission without significantly increasing the ΔV budget.

B. Active Safety for Thruster Failures

The active safety approach in Eq. (30) can be modified to guarantee safety for cases of individual thruster failure by optimizing multiple safe input sequences. Each safe input sequence is constrained to only use a single thruster direction, or alternately, a single thruster assuming that thrusters act through the center of gravity. This guarantees that if only one thruster fails, another safe trajectory which does not use the failed thruster still exists. Thus, in a system with at least two thrusters, any single thruster failure to the off state will be in the set of possible system failures covered by active safety. Likewise, if thrusters in the system can be used to cancel each other (e.g., a system with axial thrusters), then this active safety extension can also be used in the presence of thruster-on failures. In that case, the thruster opposite that which failed can be used to cancel erroneous thrusting, while a thruster in another direction can be used to enact a preplanned safe input sequence.

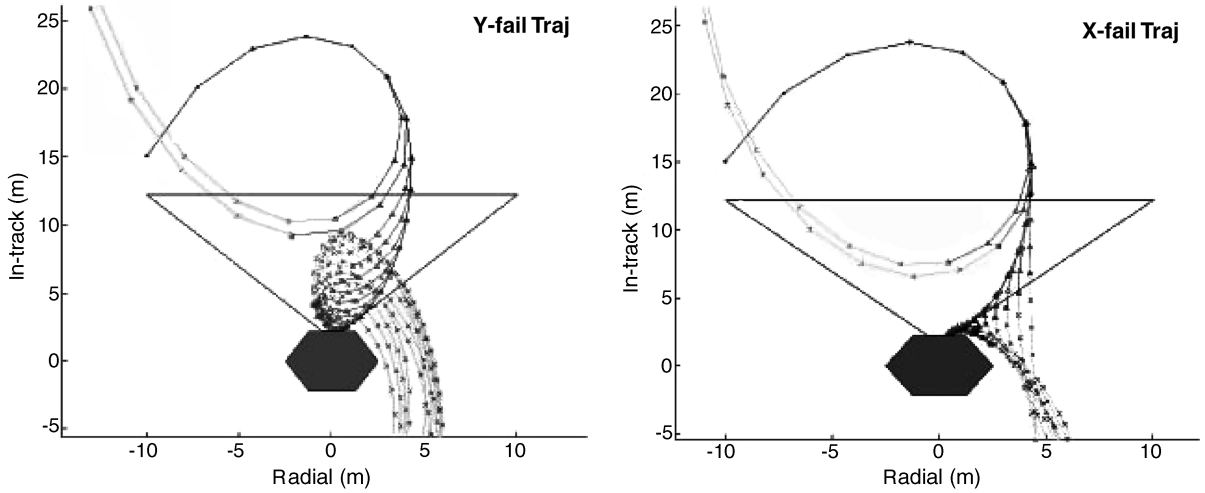

Fig. 18 Rendezvous trajectories using active safety optimized for two possible thruster failure directions.

Modifying Eq. (30) to include multiple safe input sequences yields

$$\mathbf{x}_{FT_k} = \begin{cases} \begin{bmatrix} \Gamma_k S(T) & \Gamma_k S(T-k) H_x & \mathbf{0} \\ \Gamma_k S(T) & \mathbf{0} & \Gamma_k S(T-k) H_y \end{bmatrix} \begin{bmatrix} \mathbf{U}_k \\ \mathbf{V}_k^x \\ \mathbf{V}_k^y \end{bmatrix} + A_d^k \mathbf{x}_0, & k \le N, k-T \le N_s \\ \begin{bmatrix} A_d^{k-N}\Gamma_N S(T) & \Gamma_k S(T-k) H_x & \mathbf{0} \\ A_d^{k-N}\Gamma_N S(T) & \mathbf{0} & \Gamma_k S(T-k) H_y \end{bmatrix} \begin{bmatrix} \mathbf{U}_k \\ \mathbf{V}_k^x \\ \mathbf{V}_k^y \end{bmatrix} + A_d^k \mathbf{x}_0, & k > N, k-T \le N_s \\ \begin{bmatrix} \Gamma_k S(T) & A_d^{k-N}\Gamma_{N_s} H_x & \mathbf{0} \\ \Gamma_k S(T) & \mathbf{0} & A_d^{k-N}\Gamma_{N_s} H_y \end{bmatrix} \begin{bmatrix} \mathbf{U}_k \\ \mathbf{V}_k^x \\ \mathbf{V}_k^y \end{bmatrix} + A_d^k \mathbf{x}_0, & k \le N, k-T > N_s \\ \begin{bmatrix} A_d^{k-N}\Gamma_N S(T) & A_d^{k-N}\Gamma_{N_s} H_x & \mathbf{0} \\ A_d^{k-N}\Gamma_N S(T) & \mathbf{0} & A_d^{k-N}\Gamma_{N_s} H_y \end{bmatrix} \begin{bmatrix} \mathbf{U}_N \\ \mathbf{V}_{N_s}^x \\ \mathbf{V}_{N_s}^y \end{bmatrix} + A_d^k \mathbf{x}_0, & k > N, k-T > N_s \end{cases} \tag{31}$$

where $\mathbf{V}_{N_s}^x$ is the safe input sequence of only x-direction inputs, $\mathbf{V}_{N_s}^y$ is the safe input sequence of only y-direction inputs, and H_x and H_y are matrices that extract only elements of Γ pertaining to u_x and u_y inputs, respectively. The active safety algorithm remains the same, but the failure trajectory used in formulating Eq. (29) must be propagated using Eq. (30) instead of Eqs. (28) and (30).

Figure 18 shows an example trajectory using the multisolution active safety form in Eq. (31) to solve the safe rendezvous problem for the initial conditions used in Table 1. The left side of the figure shows the nominal rendezvous trajectory and the safe trajectories that would be used in the event of a failure in the $\pm y$ direction thruster (resulting from using $\mathbf{V}_{N_s}^x$). The right side shows the same nominal trajectory, but the safe trajectories shown correspond to $\mathbf{V}_{N_s}^y$. In this case, a single optimization has produced two sets of safe input sequences, either valid at any time step with guaranteed safety. The safe input sequence solutions are

$$\mathbf{V}_{N_s}^x = \begin{bmatrix} -4.56 \times 10^{-6} \\ 0 \\ 0 \\ 0 \end{bmatrix} \qquad \mathbf{V}_{N_s}^y = \begin{bmatrix} -3.06 \times 10^{-6} \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{32}$$

The nominal trajectory in this case requires 13.67 mm/s of fuel, equivalent to the fuel-optimal, "unsafe" trajectory. The cost of safety for implementing $\mathbf{V}_{N_s}^x$ is 1.43 mm/s and for $\mathbf{V}_{N_s}^y$ is 0.96 mm/s, which follows the trend of low safety trajectory costs observed in Table 1.

The algorithm for using passive safety only requires that thrusters be disabled in the event of a failure and active safety only requires that a predetermined safe input sequence be used. The implementation algorithm for the modified active safety formulation in this section requires an additional input from the spacecraft fault detection and isolation system which indicates the type of fault. In the case of thruster failure, this would also need to include which thruster failed and the nature of the failure. This additional information enables the active safety implementation to choose the appropriate safe input sequence to use.

IX. Conclusions

Safety in autonomous spacecraft rendezvous trajectory design allows abort with guaranteed collision avoidance for a class of anomalous system behaviors. This paper introduced several online optimization formulations that guarantee passive and active safety and demonstrated in numerous simulations that the additional fuel costs are comparatively small, particularly relative to commonly considered suboptimal trajectories. Additional restrictions to guarantee failure trajectories that minimize drift and guarantee long-horizon passive collision avoidance were shown to require fuel use on the same order of magnitude as optimized solutions that do not include safety guarantees. Approximate analytic methods for creating upper and lower bounds on the expected fuel use for several mission types yielded accurate estimates compared to optimized fuel costs. A convex formulation of the safety problem was introduced

Table 1 Comparison of various types of safe rendezvous trajectories. Fuel costs in mm/s

	No safety, nominal	Passive safety	Passive safety, invariant	Active safety, a priori	Active safety, a priori invariant	Active safety, optimized	Active safety, optimized, invariant
Nominal cost	13.67	14.21	19.32	13.84	18.17	13.67	17.58
Safety cost	0	0	0	6.28	6.28	0.76	2.14
P (collision)	0.012	0	0	0	0	0	0

which uses approximately twice as much fuel, but more than 150 times less computation time than the nonconvex formulation. An active safety approach was developed and shown to be capable of achieving the same fuel costs as trajectories without safety while still guaranteeing collision-free escape trajectories for a large class of potential anomalies, including single thruster failures. The safety algorithms presented provide a fuel-efficient, computationally feasible framework for designing safe-mode procedures for multispacecraft missions.

Acknowledgments

This work was funded under Cooperative Agreement NCC5-729 through the Goddard Space Flight Center Formation Flying NASA Research Announcement. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Aeronautics and Space Administration.

References

[1] Zimpfer, D. J., Spehar, P. S., Clark, F., D' Souza, C., and Jackson, M., "Autonomous Rendezvous and Capture Guidance, Navigation and Control," *Flight Mechanics Symposium*, Goddard Space Flight Center, Greenbelt, MD [CD-ROM], Session 3, Paper 7, 18–20 Oct. 2005.

[2] Polites, M. E., "Technology of Automated Rendezvous and Capture in Space," *Journal of Spacecraft and Rockets*, Vol. 36, No. 2, March–April 1999, pp. 280–291.

[3] Kawano, I., Mokuno, M., Kasai, T., and Suzuki, T., "Result and Evaluation of Autonomous Rendezvous Docking Experiments of ETS-VII," AIAA Paper 1999-4073, Aug. 1999.

[4] Rumford, T. E., "Demonstration of Autonomous Rendezvous Technology (DART) Project Summary," *Proceedings of SPIE: The International Society for Optical Engineering*, Vol. 5088, 2003, pp. 10–19. doi:10.1117/12.498811

[5] "Overview of the DART Mishap Investigation Results," NASA.gov [online database], http://www.nasa.gov/mission_pages/dart/main/ [retrieved May 2006].

[6] Young, K., "Autonomous Rendezvous in Space Becomes Hit and Run," *New Scientist Space* [online journal], http://www.newscientistspace.com/article/dn7303, 25 April 2005 [retrieved Jan. 2006].

[7] Berger, B., "Fender Bender: NASA's DART Spacecraft Bumped Into Target Satellite," Space.com [online] http://www.space.com/missionlaunches/050422_dart_update.html [retrieved Jan. 2006].

[8] Richards, A. G., Schouwenaars, T., How, J. P., and Feron, E., "Spacecraft Trajectory Planning with Collision and Plume Avoidance Using Mixed Integer Linear Programming," *Journal of Guidance, Control, and Dynamics*, Vol. 25, Aug. 2002, pp. 755–764.

[9] Garcia, I., and How, J. P., "Trajectory Optimization for Satellite Reconfiguration Maneuvers with Position and Attitude Constraints," *Proceedings of the American Control Conference*, IEEE, Piscataway, NJ, June 2005, pp. 889–895.

[10] Wang, P. K. C., Mokuno, M., and Hadaegh, F. Y., "Formation Flying of Multiple Spacecraft with Automatic Rendezvous and Docking Capability," *AIAA Guidance, Navigation, and Control Confrence*, AIAA, Reston, VA, 11–14 Aug. 2003.

[11] Roger, A. B., and McInnes, C. R., "Safety Constrained Free Flyer Path Planning at the International Space Station," *Journal of Guidance, Control, and Dynamics*, Vol. 23, No. 6, Nov.–Dec. 2000, pp. 971–979.

[12] Fehse, W., *Automated Rendezvous and Docking of Spacecraft*, Cambridge Univ. Press, Cambridge, England, U.K., 2003, pp. 76–111.

[13] Geller, D. K., "Linear Covariance Techniques for Orbital Rendezvous Analysis and Autonomous Onboard Mission Planning," *Journal of Guidance, Control, and Dynamics*, Vol. 29, No. 6, Nov.–Dec. 2006, pp. 1404–1414.

[14] Naasz, B., "Safety Ellipse Motion with Coarse Sun Angle Optimization," *2nd International Symposium on Formation Flying Missions and Technologies*, NASA CP-2005-212781, 14–16 Sept. 2004.

[15] Jacobsen, S., Lee, C., Zhu, C., and Dubowsky, S., "Planning of Safe Kinematic Trajectories for Free Flying Robots Approaching an Uncontrolled Spinning Satellite," *Proceedings of the ASME 27th Annual Biennial Mechanisms and Robotics Conference*, American Society of Mechanical Engineers, Fairfield, NJ, Sept. 2002.

[16] Matsumoto, S., Dubowsky, S., Jacobsen, S., and Ohkami, Y., "Fly-By Approach and Guidance for Uncontrolled Rotating Satellite Capture," *AIAA Guidance, Navigation, and Control Confrence*, AIAA, Reston, VA, 11–14 Aug. 2003.

[17] Schouwenaars, T., How, J. P., and Feron, E., "Decentralized Cooperative Trajectory Planning of Multiple Aircraft with Hard Safety Guarantees," AIAA Paper 2004-5141, Aug. 2004.

[18] Tomlin, C., Mitchell, I., and Ghosh, R., "Safety Verification of Conflict Resolution Maneuvers," *IEEE Transactions on Intelligent Transportation Systems*, Vol. 2, No. 2, June 2001, pp. 110–120. doi:10.1109/6979.928722

[19] Tillerson, M., Inalhan, G., and How, J. P., "Co-Ordination and Control of Distributed Spacecraft Systems Using Convex Optimization Techniques," *International Journal of Robust and Nonlinear Control*, Wiley, New York, Vol. 12, 2002, pp. 207–242.

[20] Hill, G. W., "Researches in Lunar Theory," *American Journal of Mathematics*, Vol. 1, No. 3, 1878, pp. 5–26, 129–147, 245–260. doi:10.2307/2369430

[21] Breger, L. S., and How, J. P., "J_2-Modified GVE-Based MPC for Formation Flying Space," *AIAA Guidance, Navigation, and Control Conference Conference*, AIAA, Reston, VA, Aug. 2005, pp. 1–21.

[22] Franklin, G., Powell, J., and Workman, M., *Digital Control of Dynamic Systems*, 3rd ed., Addison–Wesley, Reading, MA, 1998.

[23] Richards, A. G., "Robust Constrained Model Predictive Control," Ph.D. Thesis, Massachusetts Institute of Technology, Cambridge, MA, Nov. 2004.

[24] Tillerson, M., and How, J. P., "Analysis of the Impact of Sensor Noise on Formation Flying Control," *Proceedings of the American Control Conference*, IEEE, Piscataway, NJ, 25–27 June 2001, pp. 1–6.

[25] Breger, L. S., and How, J.P., "Gauss's Variational Equation-Based Dynamics and Control for Formation Flying Spacecraft," *Journal of Guidance, Control, and Dynamics*, 18 April 2006 (to be published).

[26] Breger, L. S., Inalhan, G., Tillerson, M., and How, J. P., "Cooperative Spacecraft Formation Flying: Model Predictive Control with Open- and Closed-Loop Robustnes," *Modern Astrodynamics*, edited by P. Gurfil, Elsevier, Oxford, 2006.

[27] How, J. P., Twiggs, R., Weidow, D., Hartman, K., and Bauer, F., "Orion —A Low-Cost Demonstration of Formation Flying in Space Using GPS," *Proceedings of AIAA/AAS Astrodynamics Specialist Conference and Exhibit*, AIAA, Collection of Technical Papers (A98-37348 10-13), 1998, pp. 276–286.

[28] Richards, A. G., Breger, L. S., and How, J. P., "Analytical Performance Prediction for Robust Constrained Model Predictive Control," *International Journal of Control*, Vol. 79, No. 8, Aug. 2006, pp. 877–894. doi:10.1080/00207170600699740

[29] Kaplan, M., *Modern Spacecraft Dynamics and Control*, Wiley, New York, 1976, pp. 24–122.

[30] Strang, G., *Introduction to Applied Mathematics*, Wellesley–Cambridge Press, Wellesley, MA, 1986, pp. 1–758.

[31] Greenwood, D. T., *Advanced Dynamics*, Cambridge Univ. Press, Cambridge, England, U.K., 2003, pp. 141–150.

[32] Breger, L. S., How, J. P., and Alfriend, K. T., "Partial J_2-Invariance for Spacecraft Formations," *AIAA Guidance, Navigation, and Control Conference Conference*, AIAA, Reston, VA, Aug. 2006.

[33] Bertsimas, D., and Tsitsiklas, J. N., *Introduction to Linear Optimization*, Athena Scientific, Belmont, MA, 1997, pp. 17–19.