Powered Safe Abort for Autonomous Rendezvous of Spacecraft

Louis Breger* and Jonathan P. How†
MIT Department of Aeronautics and Astronautics

Several recent on-orbit autonomous docking missions have experienced serious failures requiring immediate safing action. The future of autonomous spacecraft rendezvous will depend on the ability of docking algorithms to effectively handle off-nominal situations resulting from anomalous system behaviors. This paper presents a method for online generation of *actively safe* fuel-optimized rendezvous trajectories. These trajectories guarantee the existence of known powered abort trajectories providing collision-free escape, even in the presence of single thruster failures. Numerous examples are presented to demonstrate the overall benefits of incorporating these active safety constraints when compared to nominal trajectory design techniques. A stochastic analysis is used to demonstrate that imposing active safety as a constraint decreases the overall likelihood of collisions occurring.

I. Introduction

On-orbit spacecraft rendezvous is a well-established technology that has been in use since the Apollo program [2]. Autonomous docking of spacecraft is almost as old [12], first dating back to 1967 and used regularly with the Mir space station. However, the degree of autonomy required for future missions is expected to increase [1]. Recently, anomalies in robotic rendezvous missions have occurred on ETS-VII [3] and DART [4, 5]. Multiple anomalies on the ETS-VII mission caused entries into a safe operating mode, at least one of which resulted in a preprogrammed maneuver to move the spacecraft 2.5 km from its target. A navigation failure 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. Previous work introduced an approach for finding efficient, passively safe rendezvous trajectories [32]. This paper builds on that work to develop a method for generating fuel-optimized rendezvous trajectories online that guarantee the existence of known active safe abort trajectories for a large class of possible spacecraft anomalies.

*Research Assistant, MIT Department of Aeronautics and Astronautics, lbreger@mit.edu
†Associate Professor, MIT Department of Aeronautics and Astronautics, jhow@mit.edu

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. For example, the approach in Ref. [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, Refs. [12] and [14] develop the *safety circle* method, in which a nearby orbit with a relative invariant trajectory 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 Ref. [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. Ref. [11] plans passively safe trajectories using potential functions, but the approach is computationally intensive and limited to static obstacles. Various types of safety have been considered in the design of UAV 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. Previous work [32] introduced a method generating fuel optimized *passive safe trajectories*, which guarantee collision avoidance with no thrusting required for safety. This paper extends the concept to include *active safety*, in which a 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. Active safety 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 actively safe. Several examples of active safe trajectories generated for docking with and without invariance constraints establish that adding safety constraints do not result in significantly increased fuel use. Next, a stochastic analysis is conducted to verify that safe trajectories reduce the likelihood of collision in the event of a failure. A method for adding guaranteed robustness to the safety guarantees is also demonstrated.

II. Online Trajectory Optimization for Autonomous Rendezvous and Docking

This section reviews and introduces notation for optimization-based trajectory generation using the approaches presented in Refs [8, 19]. 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 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, 30], but GVE-based approaches [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

$$\mathbf{x} = \begin{bmatrix} x & y & z & v_x & v_y & v_z \end{bmatrix}^T \tag{2}$$

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 an LVLH frame positioned on the center of gravity of a passive target vehicle. The input is defined as

$$\mathbf{u} = \begin{bmatrix} u_x & u_y & u_z \end{bmatrix}^T \tag{3}$$

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]

$$\mathbf{x}_k = A_d^k\mathbf{x}_0 + \begin{bmatrix} A_d^{k-1}B_d & A_d^{k-2}B_d & \dots & A_dB_d & B_d \end{bmatrix} \begin{bmatrix} \mathbf{u}_0 \\ \vdots \\ \mathbf{u}_{k-1} \end{bmatrix} \tag{4}$$

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

where Γ_k is the discrete convolution matrix. Since 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 Ref. [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 N is the total number of possible input steps and 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 [33]

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

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

$$A_k \mathbf{x}_k \leq b_k \tag{8}$$

where A_k is a matrix and 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]

$$A_k \mathbf{x}_k \leq b_k + M\mathbf{y}_k \tag{9}$$

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

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. Since 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

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

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 Refs. [19] and [8].

This section has 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. Active Safety

The trajectories generated by the constraints in Section 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. Refs. [24] and [23] describe computationally feasible methods of generating trajectories online that are robust to process and sensing noise expected under nominal operating conditions, a consideration revisited in Section A. 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 actively safe with respect to a class of system failures. While 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.

Reference [32] considers *passive abort safety*, in which thrusters are turned off in the event of an anomaly. Passive abort provides safe guarantees for a large subset of all possible failures is used, including guidance system shutdowns, which encompasses thruster failures, computer anomalies, and loss of sensing. However, because passive abort requires that all safe characteristics arise from the nominal abort trajectory, it is generally necessary for the safe trajectory to be different from the optimal trajectory, resulting in increased fuel use.

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.

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 with a predetermined safe input

sequence $\mathbf{v}$ yields

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

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 12 can be written more generally as

$$\mathbf{x}_{FT_k} = \begin{cases} \Gamma_k S(T,k)\mathbf{U}_k + A_d^k\mathbf{x}_0 + \Gamma_{k-T}S(k-T,N_s)\mathbf{V}_k, & T < k \leq N,\ T < k-T \leq N_s \\ A_d^{k-N}\Gamma_N S(T,N)\mathbf{U}_N + A_d^k\mathbf{x}_0 + \Gamma_{k-T}S(k-T,N_s)\mathbf{V}_k, & k > N,\ k-T \leq N_s \\ \Gamma_k S(T,k)\mathbf{U}_k + A_d^k\mathbf{x}_0 + A_d^{k-N_s}\Gamma_{N_s}\mathbf{V}_{N_s}, & k \leq N,\ k-T > N_s \\ A_d^{k-N}\Gamma_N S(T,N)\mathbf{U}_N + A_d^k\mathbf{x}_0 + A_d^{k-N_s}\Gamma_{N_s}\mathbf{V}_{N_s}, & k > N,\ k-T > N_s \end{cases} \tag{13}$$

where k is the time step that the failure trajectory is propagated forward to, $S(q,N_q) = \text{diag}(\mathbf{I}_{3(q)}, \mathbf{0}_{3(N_q-q)})$, $\mathbf{I}_n$ 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 $\mathbf{U}_k^T = [\ \mathbf{u}_0^T \ \dots \ \mathbf{u}_{k-1}^T\ ]$, and the predetermined safe input sequence $\mathbf{V}_k^T = [\ \mathbf{v}_0^T \ \dots \ \mathbf{v}_{k-1}^T\ ]$. The possible ranges in Equation 13 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 in order to allow for safe input sequences that are longer or shorter than the nominal plan length.

Active 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

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

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 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 Sections IV.

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. 13

$$\mathbf{x}_{FT_k} = \begin{cases} \begin{bmatrix} \Gamma_k S(T,k) & \Gamma_{k-T} S(k-T,N_s) \end{bmatrix} \begin{bmatrix} \mathbf{U}_k \\ \mathbf{V}_k \end{bmatrix} + A_d^k \mathbf{x}_0, & T < k \leq N,\ T < k-T \leq N_s \\ \begin{bmatrix} A_d^{k-N}\Gamma_N S(T,N) & \Gamma_{k-T} S(k-T,N_s) \end{bmatrix} \begin{bmatrix} \mathbf{U}_N \\ \mathbf{V}_{N_s} \end{bmatrix} + A_d^k \mathbf{x}_0, & k > N,\ k-T \leq N_s \\ \begin{bmatrix} \Gamma_k S(T,k) & A_d^{k-N_s}\Gamma_{N_s} \end{bmatrix} \begin{bmatrix} \mathbf{U}_N \\ \mathbf{V}_{N_s} \end{bmatrix} + A_d^k \mathbf{x}_0, & k \leq N,\ k-T > N_s \\ \begin{bmatrix} A_d^{k-N}\Gamma_N S(T,N) & A_d^{k-N_s}\Gamma_{N_s} \end{bmatrix} \begin{bmatrix} \mathbf{U}_N \\ \mathbf{V}_{N_s} \end{bmatrix} + A_d^k \mathbf{x}_0, & k > N,\ k-T > N_s \end{cases} \tag{15}$$

such that the safe input sequence $\mathbf{V}_{N_s}$ is optimized at the same time as the nominal rendezvous trajectory.

The implementation of an active safe trajectory is similar to that of the safe trajectory approach in Ref. [32]. 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. Reference [32] introduced the *invariance* constraint

$$\mathbf{x}_{FT_k} = A_d^{N_o} \mathbf{x}_{FT_k} \quad \text{for } k \geq T \tag{16}$$

where N_o is the number of steps in an orbit. If $S \geq N_o$ and the open loop dynamics given by A_d admit invariant solutions then Eq. 16 is sufficient to guarantee safety for any time horizon over which the dynamics are valid.

IV. Rendezvous Scenario

The rendezvous and docking scenario to be examined in this paper involves a target spacecraft being docked with and a chaser spacecraft maneuvering to achieve that docking. Figure 1 shows a target spacecraft that lies at the center of an local frame. A line-of-sight (LOS) cone protrudes

from the target spacecraft and it is required that rendezvous remain within this line-of-sight cone for vision-based sensing. At the interface between the LOS cone and the target is a docking port (rectangular platform). The LOS requirements are

$$A_{\mathrm{LOS}_k}\mathbf{x}_k \leq b_{\mathrm{LOS}_k} \forall k = 1 \ldots N \tag{17}$$

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

$$A_{\mathrm{Term}_N}\mathbf{x}_N \leq b_{\mathrm{Term}_N} \tag{18}$$

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 in order to ensure large thrusts are not planned for the period immediately before docking. The safety constraints in Eq. 14 are imposed for the three quarters 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 $T \in \{4 \ldots 19\}$. The planning horizon is a full orbit. The chaser spacecraft, modeled after the mission in Ref. [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 3 steps to prevent trajectory solutions with large terminal 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 each axial direction. In summary, the safety algorithm used in this section is

$$\begin{aligned} \min_{\mathbf{u}_0,\ldots,\mathbf{u}_{N-1}} \quad & \text{Eq. (6)} \\ \text{s.t.} \quad & \text{Eq. (11)} \quad \forall\, k \in \{0,\ldots,N-1\}, \\ & \text{Eq. (17)}, \\ & \text{Eq. (18)}, \\ & \text{Eq. (14)} \quad \forall\, T \in \mathcal{F} \end{aligned} \tag{19}$$

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. Probability of Collision

To judge the effectiveness of the active safety algorithm introduced in Section III, define a probability of 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

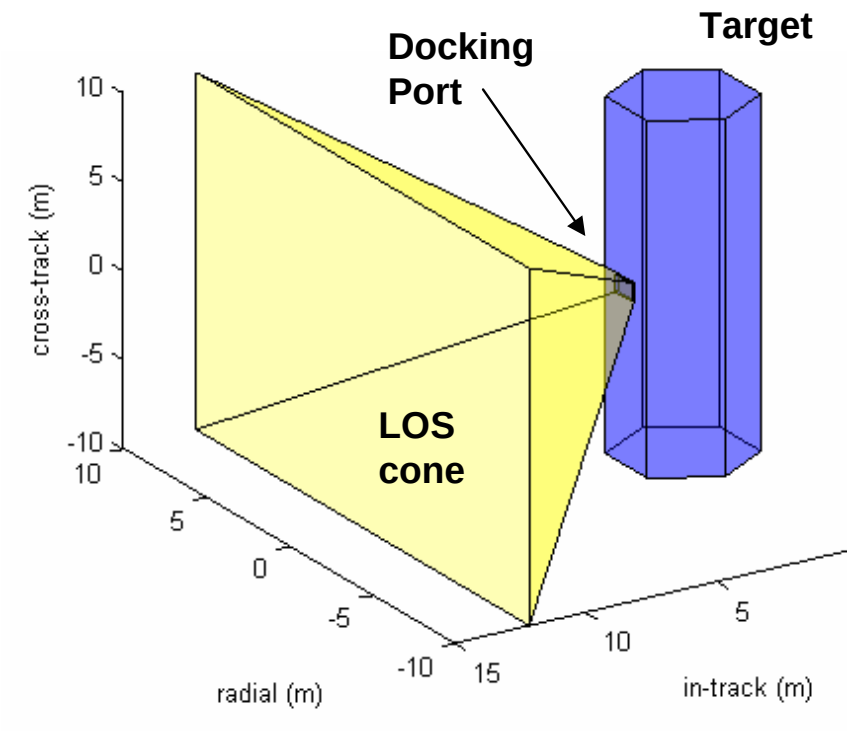

Fig. 1: Target spacecraft and docking configuration

given by

$$P_{col} = \sum_{i=1}^{N} P(\text{failure at i} \mid \text{no failure before i}) \cdot P(\text{collision occurs} \mid \text{failure at i}) \tag{20}$$

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

$$P(\text{failure at i} \mid \text{no failure before i}) = (1-f)^{i-1} f \tag{21}$$

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 Ref. [14] to create a *safety circle*. This creates a situation where each rendezvous trajectory begins from a safe, invariant orbit within range of a final approach rendezvous trajectory.

Figures 2 and 3 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 probably 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 Figure 4. The dashed line indicates an overbound, $\bar{P}_{col}$, 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

$$\sum_{\{0,\ldots,N-1\}\setminus\mathcal{F}} P(\text{failure at i} \mid \text{no failure before i}) \tag{22}$$

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 Figure 3 for each different set $\mathcal{F}$ used to create Figure 4. The minimum (line marked by •) shows that in each case, there were 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 Figure 3, 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.

Eq. 22 indicates that the overbound $\bar{P}_{col}$ 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.

B. Examples

Figure 5 shows the fuel-minimizing rendezvous trajectory beginning from a safety circle holding orbit. The nominal trajectory is marked by • and the trajectories followed in the event failures occur in the last 3/4 of the nominal trajectory are marked by ×. Several of the failure trajectories pass through the target spacecraft and would result in a collision, indicating that the nominal rendezvous trajectory is not safe. Several active safety approaches to optimizing the same initial conditions as in Fig. 5 are demonstrated in Figures 6-9. Figure 6 shows an active safe rendezvous trajectory beginning from a safety circle 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 in no failures

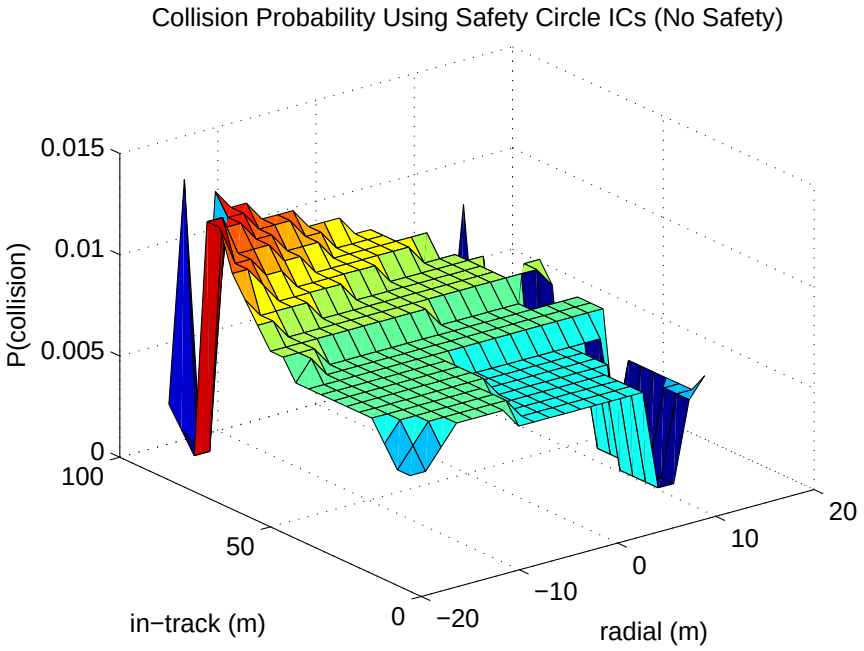

Fig. 2: Probability of a collision occurring for a range of initial conditions with $\mathcal{F} = \emptyset$ (No safety guarantees).

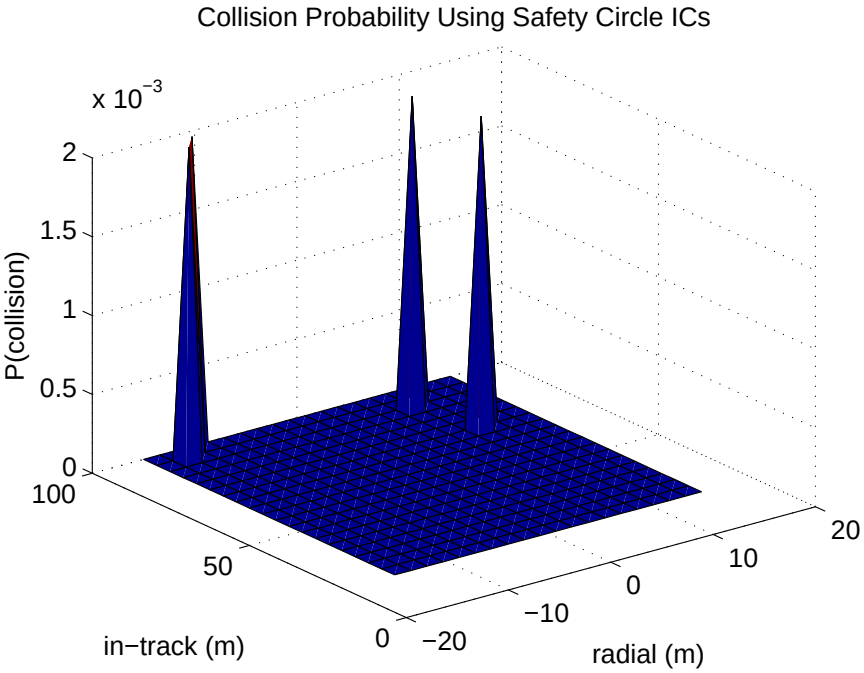

Fig. 3: Probability of a collision occurring for a range of initial conditions with $\mathcal{F} = \{4, \ldots, 19\}$ (latter 3/4 of trajectory guaranteed safe)

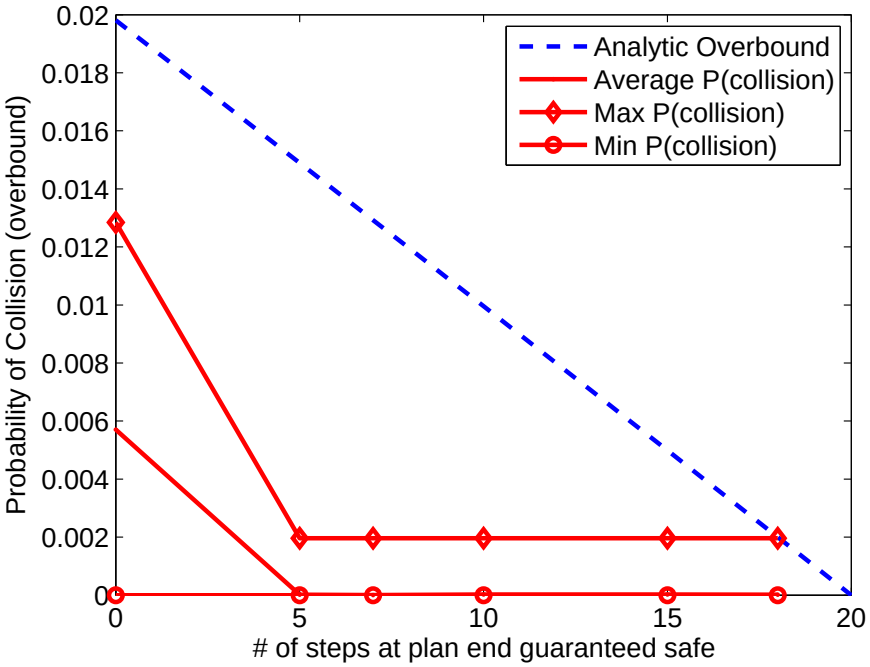

Fig. 4: Probability of collision occurring for various values of $\mathcal{F}$

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

occur. Each portion of the trajectory marked with $\triangle$ 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 $\times$ show the 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, Figure 8 shows an active safe trajectory optimized from the same initial conditions, but with the invariance constraint from Eq. 16 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 8 and 9 show the optimized active safe trajectories using the constraints in Eq. 15 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 Figures 6-9. 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 Section A. 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. 13 and the columns labeled *optimized* use the approach in Eq. 15. The columns marked invariant also use the invariance constraints in Eq. 16. 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 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.

V. Active Safety for Thruster Failures

The active safety approach in Eq. 15 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. 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.

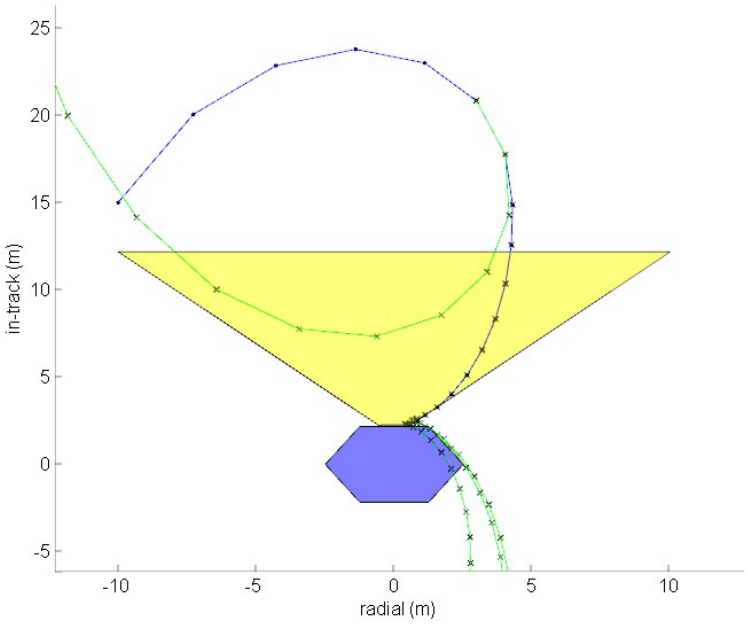

Fig. 5: Rendezvous trajectory optimized without safety. Nominal trajectory is marked by • and trajectories followed in the event of failures in last 3/4 of nominal trajectory are marked by ×.

Modifying Eq. 15 to include multiple safe input sequences yields

$$\mathbf{x}_{FT_k} = \begin{cases} \begin{bmatrix} \Gamma_k S(T) & \Gamma_k S(T-k) H_x & \mathbf{0} \\ \Gamma_k S(T) & \mathbf{0} & \Gamma_k S(T-k) H_y \end{bmatrix} \begin{bmatrix} \mathbf{U}_k \\ \mathbf{V}_k^x \\ \mathbf{V}_k^y \end{bmatrix} + A_d^k \mathbf{x}_0, & k \le N,\ k-T \le N_s \\ \begin{bmatrix} A_d^{k-N}\Gamma_N S(T) & \Gamma_k S(T-k) H_x & \mathbf{0} \\ A_d^{k-N}\Gamma_N S(T) & \mathbf{0} & \Gamma_k S(T-k) H_y \end{bmatrix} \begin{bmatrix} \mathbf{U}_k \\ \mathbf{V}_k^x \\ \mathbf{V}_k^y \end{bmatrix} + A_d^k \mathbf{x}_0, & k > N,\ k-T \le N_s \\ \begin{bmatrix} \Gamma_k S(T) & A_d^{k-N}\Gamma_{N_s} H_x & \mathbf{0} \\ \Gamma_k S(T) & \mathbf{0} & A_d^{k-N}\Gamma_{N_s} H_y \end{bmatrix} \begin{bmatrix} \mathbf{U}_k \\ \mathbf{V}_k^x \\ \mathbf{V}_k^y \end{bmatrix} + A_d^k \mathbf{x}_0, & k \le N,\ k-T > N_s \\ \begin{bmatrix} A_d^{k-N}\Gamma_N S(T) & A_d^{k-N}\Gamma_{N_s} H_x & \mathbf{0} \\ A_d^{k-N}\Gamma_N S(T) & \mathbf{0} & A_d^{k-N}\Gamma_{N_s} H_y \end{bmatrix} \begin{bmatrix} \mathbf{U}_N \\ \mathbf{V}_{N_s}^x \\ \mathbf{V}_{N_s}^y \end{bmatrix} + A_d^k \mathbf{x}_0, & k > N,\ k-T > N_s \end{cases} \tag{23}$$

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 inputs and u_y inputs, respectively. The active safety algorithm remains the same, but the failure trajectory used in formulating Eq. 14 must be propagated using Eq. 15 instead of Eqs. 13 or 15.

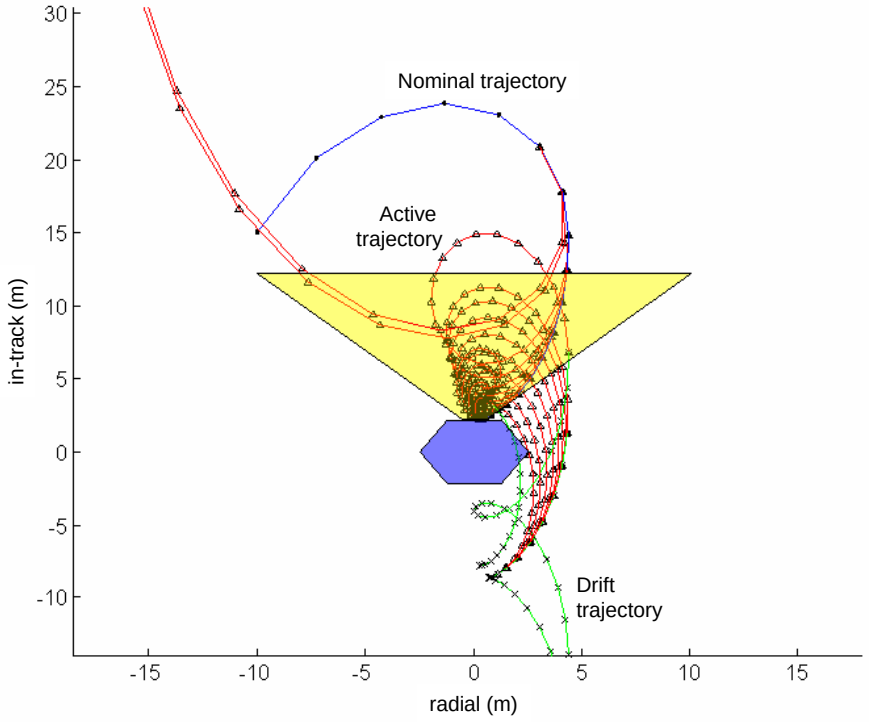

Fig. 6: Rendezvous trajectories using active safety.

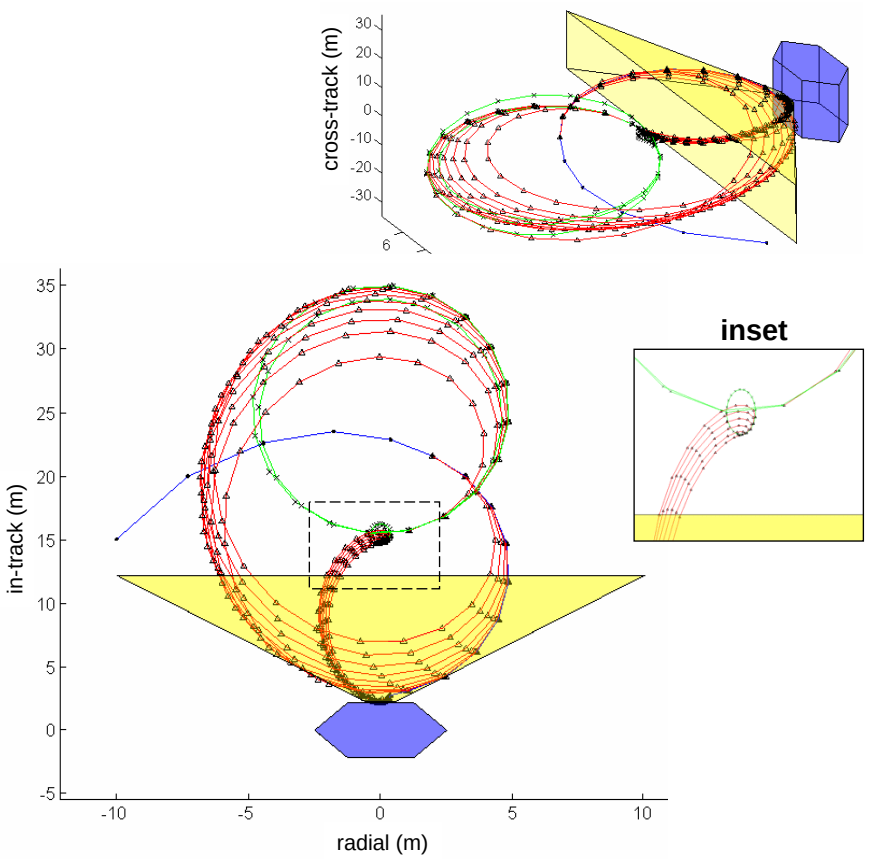

Fig. 7: Rendezvous trajectories using active safety with invariance constraints.

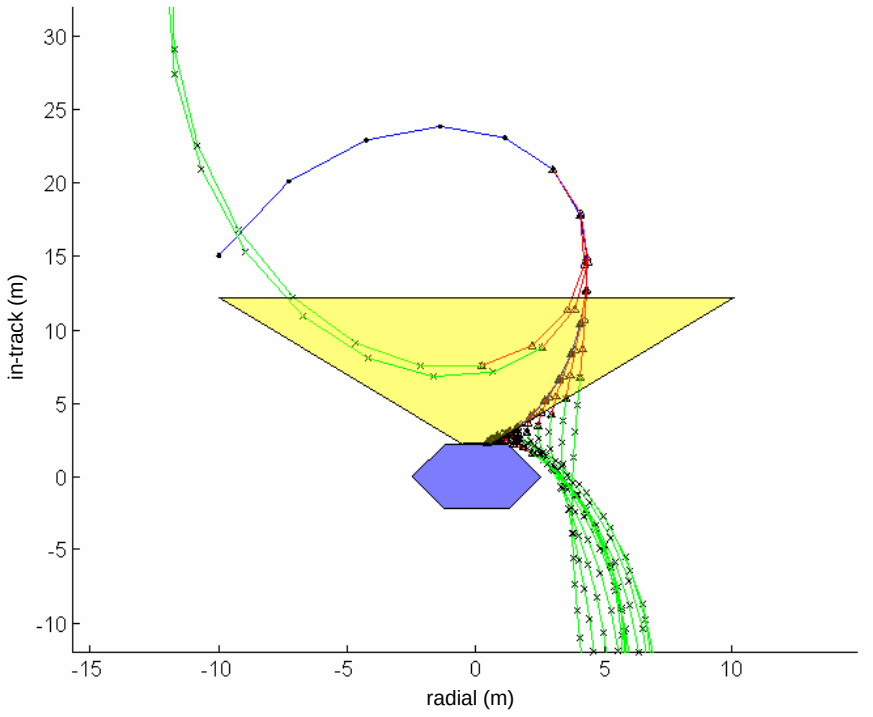

Fig. 8: Rendezvous trajectories using optimized active safety.

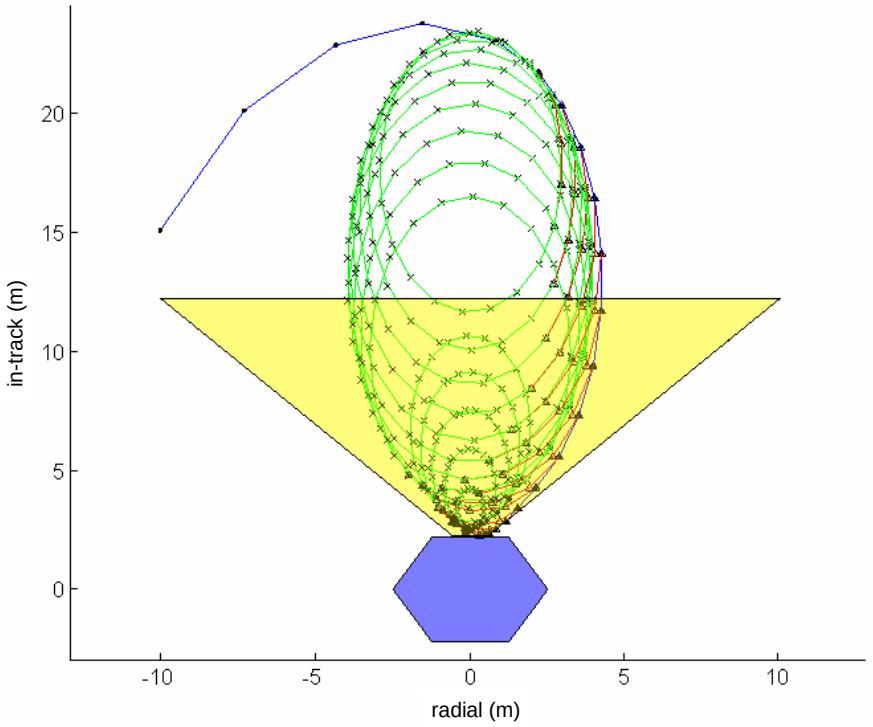

Fig. 9: Rendezvous trajectories using optimized active safety with invariance constraints.

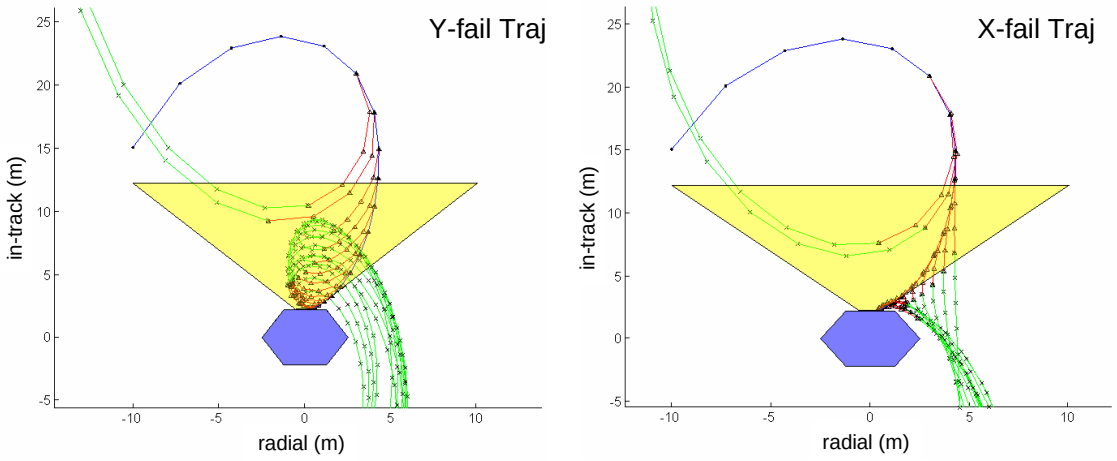

Fig. 10: Rendezvous trajectories for using active safety optimized for two possible thruster failure directions.

Figure 10 shows an example trajectory using the multi-solution active safety form in Eq. 23 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 $\mathbf{V}^x_{N_s}$). The right side shows the same nominal trajectory, but the safe trajectories shown correspond to $\mathbf{V}^y_{N_s}$. 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

$$\mathbf{V}^x_{N_s} = \begin{bmatrix} -4.56 \times 10^{-6} \\ 0 \\ 0 \\ 0 \end{bmatrix} \qquad \mathbf{V}^y_{N_s} = \begin{bmatrix} 3.06 \times 10^{-6} \\ 0 \\ 0 \\ 0 \end{bmatrix} \tag{24}$$

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 $\mathbf{V}^x_{N_s}$ is 1.43 mm/s and for $\mathbf{V}^y_{N_s}$ 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.

A. Mitigating Effects of Process Noise and Navigation Error

The safety formulation in Equations 13 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

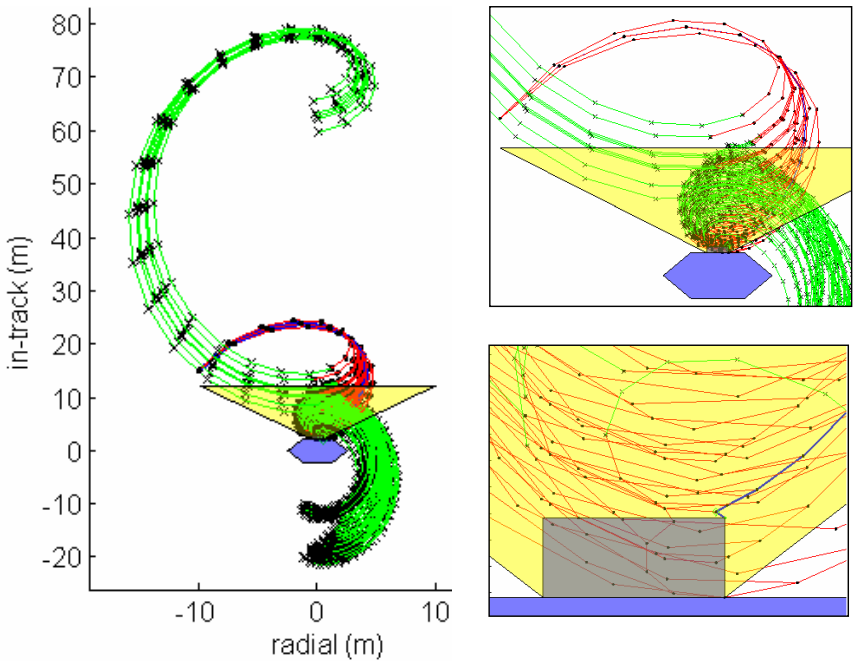

Fig. 11: Safe rendezvous trajectory with robustness to initial condition velocity uncertainty

within the accuracy provided by the navigation system. Likewise, the propagation used in Eq. 13 is only as accurate as the linear dynamics used to formulate that equation, since the actual vehicle would be subject to nonlinear dynamics, and disturbances from effects such as drag, J_2, separation distance, and eccentricity. Equation 13 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 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. Reference [26] introduces such an approach and an algorithm for minimizing the effect of robustness constraints on the size of the resulting optimization. Figure 11 shows a safe trajectory optimized using the same initial conditions as those used to create Table 1. In the figure, active safety with guaranteed collision avoidance for the last 3/4 of the trajectory is used with the addition of robustness to initial condition uncertainty. In this case, the initial velocity of the chaser is only known to within ± 0.75 mm/s in the radial direction and ± 0.0002 mm/s in the in-track direction. The resulting trajectory requires 13.84 mm/s nominally and the safe input sequence requires 2.1 mm/s. The cost of robustness in this case is less then 2% of the cost of the nominal safe trajectory without robustness. However, the problem is particularly sensitive to the amount of uncertainty present in the in-track velocity and can quickly become infeasible for larger uncertainties.

VI. Conclusion

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 active safety and demonstrated in numerous simulations that the additional fuel costs are comparatively small, particularly relative to commonly considered suboptimal trajectories. The active safety approach achieved 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 multi-spacecraft missions.

Acknowledgments

This work was funded under Cooperative Agreement NCC5-729 through the NASA GSFC 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] D. J. Zimpfer, P. S. Spehar, F. Clark, C. D' Souza, and M. Jackson, "Autonomous rendezvous and capture guidance, navigation and control," *Flight Mechanics Symposium*, (Goddard Space Flight Center, Greenbelt, Maryland), Session 3, Paper 7, October 18–20, 2005.

[2] M. E. Polites, "Technology of Automated Rendezvous and Capture in Space," AIAA *Journal of Spacecraft and Rockets,* vol. 36, no. 2, March-April 1999, p. 280-291.

[3] I. Kawano, M. Mokuno, T. Kasai, T. Suzuki, "Result and evaluation of autonomous rendezvous docking experiments of ETS-VII," Proceedings of the AIAA *Guidance, Navigation and Control Conference,* Aug 1999. AIAA-1999-4073.

[4] T. E. Rumford, "Demonstration of Autonomous Rendezvous Technology (DART) Project Summary," *Proceedings of SPIE*, Volume 5088, pp.10–19, 2003.

[5] "Overview of the DART Mishap Investigation Results," *NASA.gov*, online at `http://www.nasa.gov/mission_pages/dart/main/index.html`, last accessed May 2006.

[6] K. Young, "Autonomous rendezvous in space becomes hit and run," *New Scientist Space*, online at `http://www.newscientistspace.com/article/dn7303`, last accessed Jan. 2006.

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

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

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

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

[11] A. B. Roger and C. R. McInnes, "Safety Constrained FreeFlyer Path Planning at the International Space Station," *Journal of Guidance, Control, and Dynamics*, 23(6):971979, NovemberDecember 2000.

[12] W. Fehse. *Automated Rendezvous and Docking of Spacecraft.* Cambridge University Press, 2003.

[13] D. K. Geller, "Linear Covariance Techniques for Orbital Rendezvous Analysis and Autonomous Onboard Mission Planning," *Journal of Guidance, Control, and Dynamics*, 29(6):1404-1414, NovemberDecember 2006.

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

[15] S. Jacobsen, C. Lee, C. Zhu, and S. Dubowsky, "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, Montreal, Canada, September 2002.

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

[17] T. Schouwenaars, J. P. How, and E. Feron, "Decentralized Cooperative Trajectory Planning of Multiple Aircraft with Hard Safety Guarantees," Proceedings of the AIAA *Guidance, Navigation and Control Conference,* Aug 2004. AIAA-2004-5141.

[18] C. Tomlin, I. Mitchell, R. Ghosh, "Safety Verification of Conflict Resolution Maneuvers," *IEEE Transactions on Intelligent Transportation Systems*, vol 2., no 2., June 2001, p.110.

[19] M. Tillerson, G. Inalhan, and J. P. How, "Co-ordination and control of distributed spacecraft systems using convex optimization techniques," *International Journal of Robust and Nonlinear Control*, Vol.12, John Wiley & Sons, 2002, p. 207-242.

[20] G. W. Hill, "Researches in Lunar Theory," *A*merican Journal of Mathematics, Vol. 1, 1878, pp. 5–26,129–147,24–260.

[21] L. S. Breger and J. P. How, "J_2-Modified GVE-Based MPC for Formation Flying Space," *AIAA Guidance, Navigation, and Control Conference Conf.*, August 2005.

[22] G. Franklin, J. Powell, and M. Workman, "Digital Control of Dynamic Systems," Third Edition,Addison-Wesley, 1998.

[23] A. G. Richards, "Robust Constrained Model Predictive Control," PhD Thesis, Massachusetts Institute of Technology, November 2004.

[24] M. Tillerson and J. P. How, "Analysis of the Impact of Sensor Noise on Formation Flying Control," Proceedings of the *American Control Conference*, Arlington, VA, June 25-27, 2001.

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

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

[27] J. P. How, R. Twiggs, D. Weidow, K. Hartman, F. Bauer, "Orion - A low-cost demonstration of formation flying in space using GPS," *Proceedings of AIAA/AAS Astrodynamics Specialist Conference and Exhibit*, Boston, MA, Aug. 10-12, 1998, Collection of Technical Papers (A98-37348 10-13), Reston, VA, American Institute of Aeronautics and Astronautics, 1998, p. 276-286.

[28] A. G. Richards, L. S. Breger and J. P. How, "Analytical Performance Prediction for Robust Constrained Model Predictive Control," *International Journal of Control*, Vol. 79, No. 6, August 2006, pp. 877-894.

[29] Y. Kuwata, *Real-time Trajectory Design for Unmanned Aerial Vehicles using Receding Horizon Control,* S.M. Thesis, Dept. of Aeronautics and Astronautics, MIT, Jun. 2003.

[30] M. Kaplan. *Modern Spacecraft Dynamics and Control*. Wiley, 1976.

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

[32] L. S. Breger and J. P. How, "Safe Trajectories for Autonomous Rendezvous of Spacecraft," *AIAA Guidance, Navigation, and Control Conference Conf.*, August 2006.

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