MITSUBISHI ELECTRIC RESEARCH LABORATORIES
https://www.merl.com

Abort-Safe Spacecraft Rendezvous on Elliptic Orbits

Aguilar Marsillach, Daniel; Di Cairano, Stefano; Weiss, Avishai

TR2022-142 November 10, 2022

Abstract

We develop a spacecraft rendezvous policy that ensures safe, collision-free trajectories under various thrust failure scenarios. We use backward reachable sets to characterize the unsafe region where, if a failure occurs, a collision between a chaser and a target spacecraft cannot be avoided with the remaining available thrust. The chaser spacecraft is guided towards the target via model predictive control that ensures abort-safety by avoiding the unsafe region, which is locally convexified with half-spaces. Simulations of the rendezvous policy on various orbits demonstrate that the approach ensures safe aborts in the event of multiple thruster failures, passive abort safety under total thruster failure, and achieves some robustness to unmodeled orbital perturbations.

IEEE Transactions on Control Systems Technology 2022

Mitsubishi Electric Research Laboratories, Inc.
201 Broadway, Cambridge, Massachusetts 02139

Abort-Safe Spacecraft Rendezvous on Elliptic Orbits

Daniel Aguilar-Marsillach, Stefano Di Cairano, Avishai Weiss

***Abstract*—We develop a spacecraft rendezvous policy that ensures safe, collision-free trajectories under various thrust failure scenarios. We use backward reachable sets to characterize the unsafe region where, if a failure occurs, a collision between a chaser and a target spacecraft cannot be avoided with the remaining available thrust. The chaser spacecraft is guided towards the target via model predictive control that ensures abort-safety by avoiding the unsafe region, which is locally convexified with half-spaces. Simulations of the rendezvous policy on various orbits demonstrate that the approach ensures safe aborts in the event of multiple thruster failures, passive abort safety under total thruster failure, and achieves some robustness to unmodeled orbital perturbations.**

***Index Terms*—Spacecraft rendezvous, model predictive control, reachability, safety.**

I. Introduction

SPACECRAFT guidance, navigation, and control methods are amongst the highest-priority technologies for future autonomous spacecraft missions [1], and have to meet strict criteria prior to flight due to mission cost and lack of repair opportunities [2]. Thus, they must demonstrate robust operation in various conditions, including propulsion failures [3], [4]. Thruster failures are particularly perilous during spacecraft rendezvous, a key maneuver for almost all advanced space operations [5]–[7], because they may lead to collisions. Spacecraft collision avoidance using constrained trajectory optimization techniques, model predictive control (MPC), robotic motion planning algorithms, and artificial potential functions have been developed under nominal thrust conditions [8]–[14]. However, spacecraft collision avoidance must also be ensured in the presence of propulsion failures, which has yet to be studied extensively.

Spacecraft rendezvous approaches must guarantee several layers of safety [3], [4], [15]. Initially, the approaching spacecraft, the chaser, must remain *passively safe* with respect to the target body, the target, for a pre-specified amount of time. That is, instantaneous free-drift trajectories emanating from the trajectory must stay away from an exclusion region around the target. Thus, following a passively safe approach trajectory, in the event of a total loss of propulsion, the chaser will *naturally drift clear* of the target. On closer proximity to the target, *active safety* is required, where, in the event of a partial loss of propulsion, the chaser must be able to perform a *powered-abort maneuver* with its remaining thrust to avoid colliding with the target. Active abort relaxes the safety requirements compared to the passive case, permitting final approach rendezvous trajectories for which an entirely passive approach may not be feasible.

Conventional rendezvous is guaranteed to be passively safe by exploiting orbital mechanics and constraining the chaser's trajectory via ground-computed open-loop guidance. In recent years, autonomous online-generated passive safety techniques have been explored, e.g., by constraining the relative motion using orbital elements [16], or by receding-horizon optimization with collision avoidance constraints based on the free-drift transition matrix [8], [17], [18]. The work in [8] also proposed active safety via online trajectory generation, in which the spacecraft could switch to a safe input sequence to avoid collision in the event of partial thrust failure. The trajectory is computed by solving a problem that includes both nominal and abort sequences, simultaneously. Because [8] does not characterize the region in which feasible abort maneuvers exist, the feasibility of the initial condition at any point of the trajectory is simply assumed.

In this paper, we construct active and passive abort-safe regions of the state space using reachability methods, which allows us to characterize safe initial conditions and compute safe approach trajectories. Given a system, an initial state region, a time-horizon, and admissible inputs, a (forward) reachable set is the set of states that can be attained. Reachable sets have previously been suggested for spacecraft proximity operations. In [19], a benchmark for verification of passively safe rendezvous is proposed, where the rendezvous trajectories are computed by a given continuous-time LQR. The verification problem aims at checking whether the given LQR leads to safe spacecraft operation for the entire set of given initial conditions. While simplified with respect to an actual rendezvous specification, the benchmark has been relevant for validating linear and nonlinear reachability tools [20], [21] and for proposing the use of reachability for safe rendezvous, albeit for verification. Under nominal thrust conditions, [22] determines successful initial conditions for docking by computing backward reachable sets for the linear time-invariant (LTI) Clohessey-Wiltshire (CW) relative motion equations, and [23]–[25] compute sets of states that can be reached while avoiding obstacle regions. While linear and nonlinear techniques have been developed [26]–[28], because proximity operations occur relatively close to the target, linear approaches are often sufficiently accurate. Additionally, with an appropriate choice of sets, linear techniques offer computational advantages in memory usage and algorithm

D. Aguilar-Marsillach is with General Motors Research & Development, Warren, MI 48092, USA. Email: daniel.aguilarmarsillach@gm.com.

A. Weiss and S. Di Cairano are with Mitsubishi Electric Research Laboratories, Cambridge, MA 02139, USA. Emails: {weiss,dicairano}@merl.com

convergence. These advantages are due to these sets being closed under linear transformations, each backwards iteration only generates one new set, and the computations at most involve convex optimization, often only requiring the solution of linear or quadratic programs [29], [30]. Such computational advantages are especially relevant when aiming for on-board implementation, due to the limited memory and computational capabilities of the on-board embedded platforms [31].

In this work we synthesize, as opposed to verify, control policies that guarantee existence of both free-drift and powered-abort maneuvers and hence guarantee abort-safe rendezvous by construction. We characterize the unsafe state space in which passive or active aborts are infeasible by constructing backward reachable sets (RSs) of the linear time-varying (LTV) dynamics modeling the relative equations of motion. Such RSs are the union of convex sets for different initial and final times along the target's periodic orbit, and hence are usually non-convex [32]. As RS-avoidance is a non-convex problem, to obtain a problem that can be solved in real-time, and possibly on-board, we convexify the problem by constructing linear constraints that locally separate the RSs from the spacecraft. While MPC has been proposed for spacecraft rendezvous under nominal propulsion conditions (see, e.g., [9], [33]–[37] and references therein), here we use MPC to enforce the constraints that separate the state from the RSs, resulting in abort-safe rendezvous trajectories that evolve in the region in which safe passive or active aborts exist.

Our earlier works [38], [39] outlined the ideas of using RSs for abort-safe rendezvous in the passive and active cases. In this work, we leverage our early results, suitably extended, for the complete characterization of the method so that it can execute realistic scenarios. The extensions include refined algorithms, such as the construction of separating hyperplanes for ellipsoidal sets, formal discussions of the properties and of the impact of the failures on reachable sets, and on the computational trade-offs between polytopic and ellipsoidal sets. To demonstrate that the method can handle realistic scenarios, we validate it in a rendezvous mission to the International Space Station (ISS) where different safety approaches are used for the different mission phases. In addition, we discuss the robustness of the approach to unmodeled perturbations, and show how different levels of robustness can be achieved by inflating the unsafe sets by a factor determined via simulation. Even if simulation-based, such an approach avoids computing backward set iterations with both controls and disturbances, which tends to be computationally intractable, given the safety horizon and time-scale of rendezvous missions.

The rest of the paper is structured as follows. Section II describes the safe rendezvous problem, the spacecraft model, and the admissible control sets. Section III introduces backward reachability and its use for abort safety. Section IV discusses the prediction model, cost function, and the convexification of the safety constraints for designing a model predictive control for safe rendezvous. Section V presents algorithmic and computational details related to the offline and online formulation of the problem. Section VI presents a variety of simulations and results for both active and passive abort safety. Discussion of benefits and limitations, future work, and concluding remarks are provided in Section VII.

Notation: $\mathbb{R}$, $\mathbb{R}^n$, $\mathbb{Z}$, and $\mathbb{Z}_{0+}$ are the sets of real numbers, the Euclidean space, integers, and non-negative integers, respectively. For intervals, we use notations such as $\mathbb{Z}_{[a,b)} = \{z \in \mathbb{Z} : a \leq z < b\}$. Given a matrix H, $[H]_i$ is the i^{th} row and for H symmetric positive semidefinite, $H^{\frac{1}{2}}$ is a matrix such that $H = {H^{\frac{1}{2}}}^{\mathsf{T}} H^{\frac{1}{2}}$. I_n denotes the n-dimensional identity matrix. Vectors are shown in boldface. A reference frame, $\mathrm{F_x}$, is defined at an origin and consists of three orthonormal dextral basis vectors $\{\hat{\boldsymbol{\imath}}, \hat{\boldsymbol{\jmath}}, \hat{\boldsymbol{k}}\}$. The angular velocity vector of frame $\mathrm{F_x}$ with respect to $\mathrm{F_y}$ is denoted by $\boldsymbol{\omega}_{\mathrm{x/y}}$. A derivative with respect to the inertial frame is denoted by $(\cdot)'$ whereas a derivative with respect to another frame is denoted by $\dot{(\cdot)}$. A vector resolved in frame $\mathrm{F_x}$ is denoted ${}^{\mathrm{x}}(\cdot)$, a unit vector by $\hat{(\cdot)}$, and the Euclidean norm of a vector by $||\cdot||$. Given a continuous time signal $x(t)$ sampled with period ΔT, we denote the value at time instant $k\Delta T$, $k \in \mathbb{Z}_{0+}$, by $\boldsymbol{x}_k = \boldsymbol{x}(k\Delta T)$, and $\boldsymbol{x}_{j|k}$ denotes the value of $\boldsymbol{x}$ predicted j steps ahead from k. The notation $\boldsymbol{u}_k(\boldsymbol{x})$ denotes the computed input at k from the initial state $\boldsymbol{x}$. Given the set $\mathcal{X}$, the complement is denoted by $\mathcal{X}^{\mathrm{c}}$, the set of subsets by $2^{\mathcal{X}}$, and the cardinality by $|\mathcal{X}|$. The image of $\mathcal{C} \subseteq \mathbb{R}^n$ through matrix $A \in \mathbb{R}^{m\times n}$ is $A\mathcal{C} = \{A\boldsymbol{x} \in \mathbb{R}^m : \boldsymbol{x} \in \mathcal{C}\}$. The hyperplane representation (H-representation) of the polyhedron $\mathcal{P} \subseteq \mathbb{R}^n$ is $\mathcal{P}(H, \boldsymbol{l}) = \{\boldsymbol{x} \in \mathbb{R}^n : H\boldsymbol{x} \leq \boldsymbol{l}\}$ with $H \in \mathbb{R}^{p\times n}$, $\boldsymbol{l} \in \mathbb{R}^p$. An ellipsoid centered at $\boldsymbol{d} \in \mathbb{R}^n$ with shape matrix D is $\mathcal{E}(\boldsymbol{d}, D) = \{\boldsymbol{x} \in \mathbb{R}^n : (\boldsymbol{x} - \boldsymbol{d})^\top D^{-1}(\boldsymbol{x} - \boldsymbol{d}) \leq 1\}$ or equivalently, $\{D^{\frac{1}{2}}\boldsymbol{v} + \boldsymbol{d} \in \mathbb{R}^n : \|\boldsymbol{v}\|_2 \leq 1\}$.

II. Abort-Safe Rendezvous

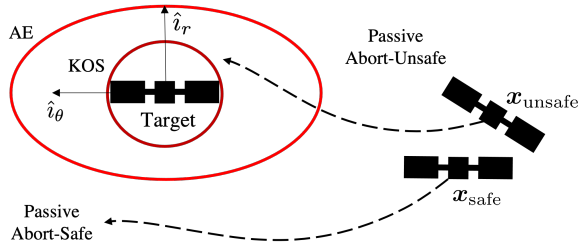
In *abort safe rendezvous*, or simply *safe rendezvous*, a chaser spacecraft must approach a target in a manner such that it can perform an active or passive abort maneuver that avoids collision with the target in the event of partial or total loss of propulsion.

Adopting NASA's convention for safety regions around the ISS [15], the chaser must first maintain passive abort-safety with respect to two exclusion regions centered at the target, referred to as the approach ellipsoid (AE) and the keep-out-sphere (KOS), resulting in two phases of passive safety requirements. Figure 1a shows the AE and KOS, noting that the KOS is a subset of the AE. During a passive abort-safe approach, if the chaser suffers a catastrophic loss of propulsion or another anomaly that requires powering off all thrusters, the chaser is guaranteed to not enter the exclusion region. During rendezvous, passive safety is first maintained with respect to the AE, and, as the chaser nears the AE, with respect to the KOS. A *passively unsafe state* is one from which the natural unforced dynamics enter the AE, or in the second phase the KOS, while a *passively safe state* results in a natural trajectory that does not enter the AE/KOS region.

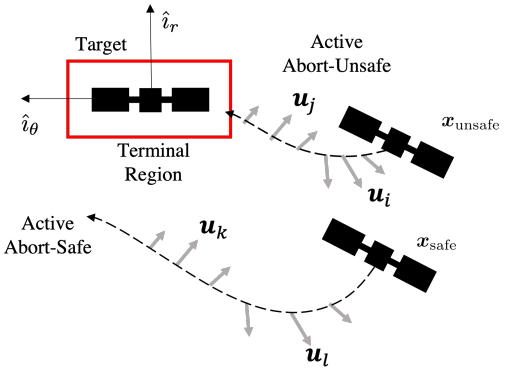
If no failures or anomalies occur along the chaser's passively safe approach, the final approach phase of the mission is initiated. For the chaser to operate in very close proximity to the target for docking or berthing, passive aborts may not be feasible, and active abort-safety with respect to a terminal exclusion region approximating the target physical shape must

be maintained, as shown in Figure 1b. An *active abort-unsafe state* is such that, after partial loss of thrust, all trajectories enter the terminal region regardless of the control actions applied with the remaining thrust. Conversely, from an *active abort-safe state* there exists at least one control sequence that avoids entering the terminal region, using the remaining thrust. Thus, on an active abort-safe approach, if the chaser suffers a partial thrust failure, it will be able to avoid collision with the target using its remaining thrust.

Conventionally, passive abort-safety is guaranteed by designing offline mission-specific passively safe trajectories and then tracking them online. Often, in the event of thruster anomalies in the proximity of the target, redundant thrusters for active abort-safety are engaged in a predetermined active collision avoidance maneuver (CAM) [15]. Here, we do not exploit mission-specific passively safe trajectories or precomputed CAMs. Instead, we characterize offline the region of the state space that is abort-unsafe, which enables online planning of rendezvous trajectories that remain in the safe region. Characterizing safe and unsafe regions is a necessary step towards automating rendezvous, and enables the online computation of fuel optimized, and often non-intuitive from an orbital dynamics perspective, safe trajectories.



(a) For a passive abort-unsafe state $\boldsymbol{x}_{\text{unsafe}}$, the natural dynamics takes the chaser into the AE and KOS, as opposed to a passive abort-safe state $\boldsymbol{x}_{\text{safe}}$.



(b) For an active abort-unsafe state $\boldsymbol{x}_{\text{unsafe}}$, no control exists that keeps the chaser away of the terminal polytope, as opposed to an active abort–safe state $\boldsymbol{x}_{\text{safe}}$

Figure 1: Illustrations of passive and active abort-safety

A. Spacecraft Model

Consider a target and a chaser in orbit around a central body such as Earth. The frame $\mathrm{F_e}$ is the Earth-Centered Inertial (ECI) frame. The chaser-fixed frame $\mathrm{F_c}$ is centered at the chaser center of mass c. The target-fixed frame $\mathrm{F_t}$ is centered at the target center of mass t. The target orbit frame $\mathrm{F_o} = \{\hat{\boldsymbol{\imath}}_r, \hat{\boldsymbol{\imath}}_\theta, \hat{\boldsymbol{\imath}}_h\}$ is Hill's frame [40] with radial, along-track, and cross-track basis vectors. The vector $\hat{\boldsymbol{\imath}}_r$ is parallel to the target position vector, $\hat{\boldsymbol{\imath}}_h$ points in the direction of the orbit's angular momentum, and $\hat{\boldsymbol{\imath}}_\theta$ completes the right-hand rule. The chaser is assumed to be rigid and all external forces acting on the target and chaser are modeled as acting on their corresponding centers of mass. In active abort-safety, we assume that the chaser frame $\mathrm{F_c}$ is maintained to align with the target's orbital frame $\mathrm{F_o}$ by the attitude control system, $\boldsymbol{\omega}_{\mathrm{c/o}} = \mathbf{0}$.

The translational equations of motion of the target and the chaser relative to the inertial frame $\mathrm{F_e}$ are

$$\boldsymbol{r}_{\mathrm{t}}'' = -\mu \frac{\boldsymbol{r}_{\mathrm{t}}}{\|\boldsymbol{r}_{\mathrm{t}}\|^3} + \frac{\boldsymbol{f}_{\mathrm{t}}}{m_{\mathrm{t}}}, \tag{1a}$$

$$\boldsymbol{r}_{\mathrm{c}}'' = -\mu \frac{\boldsymbol{r}_{\mathrm{c}}}{\|\boldsymbol{r}_{\mathrm{c}}\|^3} + \frac{\boldsymbol{f}_{\mathrm{c}}}{m_{\mathrm{c}}}, \tag{1b}$$

where $\boldsymbol{r}_{\mathrm{t}}, \boldsymbol{r}_{\mathrm{c}}$ are the position vectors of the target and chaser center of mass relative to the center of the Earth, $m_{\mathrm{t}}, m_{\mathrm{c}}$ are the target and chaser masses, μ is Earth's gravitational constant, and $\boldsymbol{f}_{\mathrm{t}}$, $\boldsymbol{f}_{\mathrm{c}}$ are the external forces acting on the target and chaser, respectively. The external forces include orbital perturbations as well as control actions. For design purposes, the target is assumed to follow periodic Keplerian motion, $\boldsymbol{f}_{\mathrm{t}} = \mathbf{0}$, and we neglect orbital perturbations on the chaser.

Given a target and chaser spacecraft, the position of the chaser relative to the target is given by

$$\boldsymbol{\rho} = \boldsymbol{r}_{\mathrm{c}} - \boldsymbol{r}_{\mathrm{t}}. \tag{2}$$

Taking the derivative of the relative position (2) with respect to the target's orbital frame $\mathrm{F_o}$ yields the relative velocity

$$\dot{\boldsymbol{\rho}} = \boldsymbol{r}_{\mathrm{c}}' - \boldsymbol{r}_{\mathrm{t}}' - \boldsymbol{\omega}_{\mathrm{o/e}} \times \boldsymbol{\rho}, \tag{3}$$

and the derivative of (3) with respect to the target's orbital frame $\mathrm{F_o}$ yields [40]

$$\ddot{\boldsymbol{\rho}} = \boldsymbol{r}_{\mathrm{c}}'' - \boldsymbol{r}_{\mathrm{t}}'' - \dot{\boldsymbol{\omega}}_{\mathrm{o/e}} \times \boldsymbol{\rho} - \boldsymbol{\omega}_{\mathrm{o/e}} \times (\boldsymbol{\omega}_{\mathrm{o/e}} \times \boldsymbol{\rho}) - 2\boldsymbol{\omega}_{\mathrm{o/e}} \times \dot{\boldsymbol{\rho}}. \tag{4}$$

Substituting (1) into (4) yields the relative equations of motion, which can be linearized about the target's trajectory when $\|\boldsymbol{\rho}\| \ll \|\boldsymbol{r}_{\mathrm{t}}\|$, and resolved in the target's orbital frame $\mathrm{F_o}$, resulting in [41]

$$\begin{aligned} \delta\ddot{x} - \left(\tfrac{2\mu}{r_{\mathrm{t}}^3} + \tfrac{h^2}{r_{\mathrm{t}}^4}\right)\delta x + \left(\tfrac{2\boldsymbol{r}_{\mathrm{t}}'\cdot\boldsymbol{r}_{\mathrm{t}}}{r_{\mathrm{t}}^4}h\right)\delta y - \left(\tfrac{2h}{r_{\mathrm{t}}^2}\right)\delta\dot{y} &= \tfrac{u_x}{m_{\mathrm{c}}}, \\ \delta\ddot{y} + \left(\tfrac{\mu}{r_{\mathrm{t}}^3} - \tfrac{h^2}{r_{\mathrm{t}}^4}\right)\delta y - \left(\tfrac{2\boldsymbol{r}_{\mathrm{t}}'\cdot\boldsymbol{r}_{\mathrm{t}}}{r_{\mathrm{t}}^4}h\right)\delta x + \left(\tfrac{2h}{r_{\mathrm{t}}^2}\right)\delta\dot{x} &= \tfrac{u_y}{m_{\mathrm{c}}}, \\ \delta\ddot{z} + \left(\tfrac{\mu}{r_{\mathrm{t}}^3}\right)\delta z &= \tfrac{u_z}{m_{\mathrm{c}}}, \end{aligned} \tag{5}$$

where ${}^{\mathrm{o}}\boldsymbol{\rho} = \begin{bmatrix}\delta x & \delta y & \delta z\end{bmatrix}^{\mathsf{T}} \in \mathbb{R}^3$ is the relative position resolved in $\mathrm{F_o}$, $r_{\mathrm{t}} = \|\boldsymbol{r}_{\mathrm{t}}\|$, $h = \|\boldsymbol{r}_{\mathrm{t}} \times \boldsymbol{r}_{\mathrm{t}}'\|$ is the (constant) inertial specific angular momentum of the target's orbit, and $\boldsymbol{u} = {}^{\mathrm{o}}\boldsymbol{f}_{\mathrm{c}} = \begin{bmatrix}u_x & u_y & u_z\end{bmatrix}^{\mathsf{T}} \in \mathbb{R}^3$ is the control input applied to the chaser resolved in $\mathrm{F_o}$.

Because for general orbits r_{t} varies along the orbit, (5) results in the LTV system

$$\dot{\boldsymbol{x}}(t) = \tilde{A}(t)\boldsymbol{x}(t) + \tilde{B}\boldsymbol{u}(t), \tag{6}$$

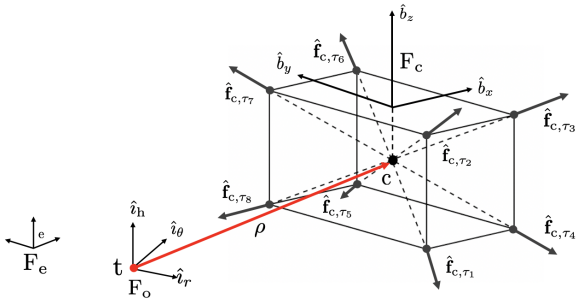


Figure 2: Chaser and thruster configuration schematics. The inertial, target orbital (Hill), and chaser frames, $\mathrm{F_e}, \mathrm{F_o}, \mathrm{F_c}$ are also shown.

where $\boldsymbol{x} = \begin{bmatrix}\delta x & \delta y & \delta z & \delta\dot{x} & \delta\dot{y} & \delta\dot{z}\end{bmatrix}^{\mathsf{T}} \in \mathbb{R}^6$. For reachability calculations and control design, we sample (6) with period ΔT, assumed to be a divisor of the orbital period[1] $t_{\mathrm{p}} = k_{\mathrm{p}}\Delta T$, $k_{\mathrm{p}} \in \mathbb{Z}_+$, and small enough not to lose relevant inter-sampling behavior, obtaining

$$\boldsymbol{x}_{k+1} = \boldsymbol{f}(k, \boldsymbol{x}_k, \boldsymbol{u}_k) = A_k\boldsymbol{x}_k + B_k\boldsymbol{u}_k. \tag{7}$$

Because the target is in a periodic orbit, when ΔT is a fraction of the orbital period, $A_k = A_{k+k_{\mathrm{p}}}$ and $B_k = B_{k+k_{\mathrm{p}}}$.

Remark 1. *While* (7) *is obtained by linearization, for proximity operations where $\|\boldsymbol{\rho}\| \ll \|\boldsymbol{r}_{\mathrm{t}}\|$, the linearization errors are sufficiently small for control design. For validation purposes, the control design based on the simplified model* (7) *is simulated in closed-loop with the nonlinear model of the spacecraft orbital motion that includes orbital perturbations.*

B. Thrusters and Failure Modes

As shown in Figure 2, the chaser spacecraft has eight thrusters rigidly fixed with respect to $\mathrm{F_c}$ and aligned with the center of mass such that no torque is generated. The total force applied to the chaser resolved in $\mathrm{F_o}$ is

$$\boldsymbol{u} = {}^{\mathrm{o}}\boldsymbol{f}_{\mathrm{c}} = \sum_{j=1}^{8} \gamma_j \, {}^{\mathrm{o}}\hat{\boldsymbol{f}}_{\mathrm{c},\tau_j}, \tag{8}$$

where, for thruster j, $\gamma_j \in [0, u_{\mathrm{m},j}]$ is the thrust magnitude, $u_{\mathrm{m},j}$ is the maximum thrust, and ${}^{\mathrm{o}}\hat{\boldsymbol{f}}_{\mathrm{c},\tau_j}$ is the chaser-fixed thrust direction resolved in $\mathrm{F_o}$.

During the execution of a rendezvous maneuver, any number of thrusters may fail. Given the set of thruster indices $\mathcal{I} = \mathbb{Z}_{[1,8]}$, the set of working thruster combinations is $\mathcal{M} = 2^{\mathcal{I}}$, and $n_{\mathrm{F}} = |\mathcal{M}|$. The set $\mathcal{M}_i \in \mathcal{M}$ is a specific set of functional thrusters, also called a thrust mode, where $\mathcal{M}_i = \mathcal{I}$ is the nominal operation, i.e., all thrusters working, and $\mathcal{M}_i = \emptyset$ is the total loss of propulsion. The set of all possible failure modes is $\mathcal{F} = \mathcal{M} \setminus \mathcal{I}$. The admissible control set $\mathcal{U}_i \subset \mathbb{R}^3$ associated with thrust mode $\mathcal{M}_i \in \mathcal{M}$ is

$$\mathcal{U}_i = \bigoplus_{j\in\mathcal{M}_i} \{\gamma_j \, {}^{\mathrm{o}}\hat{\boldsymbol{f}}_{\mathrm{c},\tau_j} : \gamma_j \in [0, u_{\mathrm{m},j}]\}. \tag{9}$$

[1]In practice, if this assumption does not hold exactly, a simple re-synchronization of the control cycle with the orbital period can be easily achieved after every/every few orbits.

Based on the model considered here, the sets $\mathcal{U}_i$ are polytopes, four examples of which are shown in Figure 3.

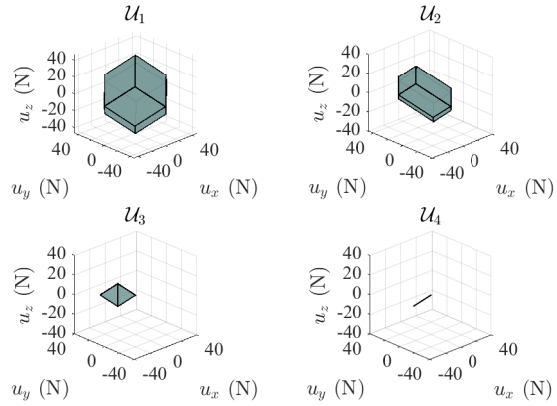


Figure 3: Admissible control sets for different thrust modes. Top left: $\mathcal{M}_i = \mathcal{I}$, all thrusters functional. Top right: $\mathcal{M}_i = \{1, 2, 3\}$, thrusters 1, 2, 3 working. Bottom left: $\mathcal{M}_i = \{7, 8\}$. Bottom right: $\mathcal{M}_i = \{8\}$.

C. Problem Statement

The general objective of spacecraft rendezvous is for the chaser to maneuver to the target in a propellant efficient manner. In addition, given an exclusion region $\tilde{\mathcal{S}} \subset \mathbb{R}^3$, such as the AE, KOS, or a terminal set over-approximating the target's physical geometry, safe rendezvous controls the chaser to approach the target while being passively safe with respect to the AE when far, with respect to the KOS when near, and actively safe with respect to the target just before docking. Thus, in the event of a total or partial thruster failure $\mathcal{M}_i \in \mathcal{F}$ at $t_{\mathrm{fail}} = k_{\mathrm{fail}}\Delta T$, there exists, respectively, an uncontrolled (passive) or controlled (active) N-step abort sequence such that the chaser trajectory does not enter $\tilde{\mathcal{S}}$ at least for N steps in the future. Lifting $\tilde{\mathcal{S}}$ to $\mathcal{S} \subset \mathbb{R}^6$ with the admissible operational chaser velocities, there exists $\boldsymbol{u}_{k_{\mathrm{fail}}}, \ldots, \boldsymbol{u}_{k_{\mathrm{fail}}+N-1} \in \mathcal{U}_i$ such that $\boldsymbol{x}_k \notin \mathcal{S}$ for $k \in \mathbb{Z}_{[k_{\mathrm{fail}}, k_{\mathrm{fail}}+N]}$. In realistic specifications, N is significantly longer than the prediction horizon in practical predictive control designs.

III. Reachable Sets and Abort Safety

Reachability methods for dynamical systems [29] are widely used for analysis and synthesis. Forward reachability determines the set of states that can be attained from a given set of initial conditions and is often used for safety verification [19], e.g., determining whether for some initial states the trajectories collide with an obstacle. Backward reachability determines the set of initial states that achieve a certain objective set, e.g., a goal set. When exogenous signals are considered, the robust backward reachable set [29], [30], determines the set of initial states that enter an objective set irrespective of the applied exogenous signal. In this paper, for reachable sets of dynamical systems with exogenous signals we always implicitly refer to robust backward reachable sets.

In the rendezvous problem, we can use backward reachability to determine the conditions from which the spacecraft

necessarily reaches the exclusion region regardless of the controls applied with the available thrust, and hence the initial states in the unsafe region from which collision cannot be avoided. By maintaining the chaser state outside of the unsafe region, there is always a control sequence that avoids collision in the presence of faults. Hence, we construct the abort-unsafe region for rendezvous from the backward reachable set (RS, for simplicity) of the exclusion region with respect to the after-failure input set, that is, the set of states that will enter the exclusion region regardless of the applied inputs available after the failure.

Definition III.1 (Backwards Reachable Set)**.** *For $\boldsymbol{x}_{k+1} = \boldsymbol{f}(k, \boldsymbol{x}_k, \boldsymbol{u}_k)$, where $\boldsymbol{u} \in \mathcal{U}$, and $\mathcal{U}$ is the admissible input set, given a set $\mathcal{S} \subset \mathbb{R}^n$ and a time step k_f, the N-step backward reachable set from k_f, $\mathcal{R}_b(N; \mathcal{S}, \mathcal{U}, k_\mathrm{f})$, is the set of states $\boldsymbol{x}_{k_\mathrm{f}-N}$ for which $\boldsymbol{x}_{k_\mathrm{f}} \in \mathcal{S}$, for all input sequences $U_N \in \mathcal{U}^N$.*

The RS can be constructed iteratively as

$$\mathcal{R}_b(j; \mathcal{S}, \mathcal{U}, k_\mathrm{f}) = \mathcal{S}, \ j = 0, \tag{10a}$$

$$\mathcal{R}_b(j; \mathcal{S}, \mathcal{U}, k_\mathrm{f}) = \{\boldsymbol{x} \in \mathbb{R}^n : \forall \boldsymbol{u} \in \mathcal{U} \ \boldsymbol{f}(k_\mathrm{f} - j, \boldsymbol{x}, \boldsymbol{u}) \in \mathcal{R}_b(j-1; \mathcal{S}, \mathcal{U}, k_\mathrm{f})\}, \ j \in \mathbb{Z}_{[1,N]}. \tag{10b}$$

For rendezvous, the N-step RS describes the initial conditions at $k_0 = k_\mathrm{f} - N$ from which the chaser cannot avoid being in $\mathcal{S}$ at time k_f, for any admissible input sequence.

Definition III.2 (RS over interval)**.** *Given an interval of time steps, $\mathbb{Z}_{[k_0,k_\mathrm{f}]}$, where $k_0 = k_\mathrm{f} - N$, the backward reachable set over the interval $\mathbb{Z}_{[k_0,k_\mathrm{f}]}$ (RSi) is*

$$\mathcal{R}_N(\mathcal{S}, \mathcal{U}, k_\mathrm{f}) = \bigcup_{j=0}^{N} \mathcal{R}_b(j; \mathcal{S}, \mathcal{U}, k_\mathrm{f}). \tag{11}$$

For rendezvous, the RSi describes the initial conditions such that there exists a time step $k \in \mathbb{Z}_{[k_0,k_\mathrm{f}]}$ from which the chaser cannot avoid being in $\mathcal{S}$ at time k_f, for any admissible input sequence[2].

For a periodic orbit, the orbit RSi is the union of RSi over $\mathbb{Z}_{[k_0,k_\mathrm{f}]}$, for k_f that varies along the orbit,

$$\bar{\mathcal{R}}_N(\mathcal{S}, \mathcal{U}) = \bigcup_{k_\mathrm{f}=M_\mathrm{p}k_\mathrm{p}+1}^{(M_\mathrm{p}+1)k_\mathrm{p}} \mathcal{R}_N(\mathcal{S}, \mathcal{U}, k_\mathrm{f}), \tag{12}$$

where M_p is any integer such that $M_\mathrm{p}k_\mathrm{p} + 1 \geq N$. For rendezvous, (12) describes the states for which there exists an instant in the orbit such that the chaser cannot avoid being in $\mathcal{S}$ after at most N steps, for any admissible input sequence. In (12), the time steps k_f can be associated to the orbit true anomaly $\theta \in [0, 2\pi]$, since $k\Delta T_s \propto \theta$.

Remark 2. *Typically, the robust backward reachable set, RS in our notation, is the set of states that enter the objective set for all disturbances. By De Morgan's laws, we obtain the RS as used here, that is, the set of states where an abort maneuver that avoids the objective set does not exist. Thus, in the RS computation we use the control set $\mathcal{U}$ as the disturbance set is used in other works.*

[2]The discrete time RS and RSi are approximations of their continuous-time descriptions. However, these approximations can be made sufficiently accurate by an appropriate choice of the sampling period ΔT.

A. Abort-Safe Sets

For a discrete-time interval $\mathbb{Z}_{[k_0,k_\mathrm{f}]}$, given the state $\boldsymbol{x}_0$ at k_0, the state at $k > k_0$ is

$$\boldsymbol{x}_k = \Phi(k, k_0)\boldsymbol{x}_0 + \mathcal{C}(k, k_0)\tilde{\boldsymbol{u}}, \tag{13}$$

where $\mathcal{C}(k, k_0)$ is the input sequence to state sequence matrix of (7), akin to the controllability matrix of an LTI system, $\tilde{\boldsymbol{u}}^\mathsf{T} = \begin{bmatrix}\boldsymbol{u}_{k-1}^\mathsf{T} & \dots & \boldsymbol{u}_{k_0}^\mathsf{T}\end{bmatrix}$, and $\Phi(k, k_0) = A_{k-1} \cdots A_{k_0}$ is the k_0-to-k transition matrix. For the sake of notation let

$$\boldsymbol{x}_k = \boldsymbol{\phi}(k; \boldsymbol{x}_0, \tilde{\boldsymbol{u}}, k_0), \tag{14}$$

where $\tilde{\boldsymbol{u}} \in \mathcal{U}^h$, and, with a little abuse of notation, $h \geq k - k_0$, i.e., $\tilde{\boldsymbol{u}}$ may include u_j, $j > k-1$ that have no impact on $\boldsymbol{x}_k$.

Let $\mathcal{S}$ be the objective set that, for rendezvous, is the avoidance set that the spacecraft must not enter, even after a propulsion failure.

Definition III.3 (Safe Set)**.** *Given an avoidance set $\mathcal{S}$, for any interval $\mathbb{Z}_{[k_0,k_\mathrm{f}]}$, where $N = k_\mathrm{f} - k_0$, a safe set for input set $\mathcal{U}$ is $\mathcal{X}_N^{\mathrm{safe}}(\mathcal{S}, \mathcal{U}) = \{\boldsymbol{x} \in \mathbb{R}^n : \ \exists \tilde{\boldsymbol{u}} \in \mathcal{U}^N, \ \boldsymbol{\phi}(k; \boldsymbol{x}_0, \tilde{\boldsymbol{u}}, k_0) \notin \mathcal{S}, \ \forall k \in \mathbb{Z}_{[k_0,k_\mathrm{f}]}\}$.*

According to Definition III.3, $\mathcal{X}_N^{\mathrm{safe}}(\mathcal{S}, \mathcal{U})$ is the set of initial conditions from which $\mathcal{S}$ can be avoided during the entire interval with the available control authority.

Proposition III.1. *Let $\bar{\mathcal{R}}_N(\mathcal{S}, \mathcal{U})$ be constructed according to* (12)*. Then,*

$$\mathcal{X}_N^{\mathrm{safe}}(\mathcal{S}, \mathcal{U}) = \bar{\mathcal{R}}_N(\mathcal{S}, \mathcal{U})^c, \tag{15}$$

is a safe set according to Definition III.3.

Proof. By construction of (11) and (12), $\bar{\mathcal{R}}_N(\mathcal{S}, \mathcal{U})$ contains all the initial conditions $\boldsymbol{x}_0$ such that for all $\tilde{\boldsymbol{u}} \in \mathcal{U}^N$ there exists $k \in \mathbb{Z}_{[k_0,k_\mathrm{f}]}$ such that $\boldsymbol{\phi}(k; \boldsymbol{x}_0, \tilde{\boldsymbol{u}}, k_0) \in \mathcal{S}$. Thus, the complement $\bar{\mathcal{R}}_N(\mathcal{S}, \mathcal{U})^c$ contains the initial conditions $\boldsymbol{x}_0$ for which there exists $\tilde{\boldsymbol{u}} \in \mathcal{U}^N$ such that for all $k \in \mathbb{Z}_{[k_0,k_\mathrm{f}]}$, $\boldsymbol{\phi}(k; \boldsymbol{x}_0, \tilde{\boldsymbol{u}}, k_0) \notin \mathcal{S}$, which is the safety condition of Definition III.3. The validity for any $k_0 \in \mathbb{Z}_{0+}$ is due to including in (12) the RSi for all $k_\mathrm{f} \in \mathbb{Z}_{[M_\mathrm{p}k_\mathrm{p}+1,(M_\mathrm{p}+1)k_\mathrm{p}]}$, which covers all the time instants by considering that the LTV system is periodic with period k_p. □

Due to the definition of $\mathcal{X}_N^{\mathrm{safe}}(\mathcal{S}, \mathcal{U})$, if the state is kept inside it, the existence of a control sequence that avoids $\mathcal{S}$ in any interval $\mathbb{Z}_{[k_0,k_\mathrm{f}]}$ is guaranteed. Given a safe set $\mathcal{X}_N^{\mathrm{safe}}(\mathcal{S}, \mathcal{U})$, any subset $\mathcal{X} \subseteq \mathcal{X}_N^{\mathrm{safe}}(\mathcal{S}, \mathcal{U})$ is also a safe set.

Since (12) is constructed from a discrete-time model, $\mathcal{X}_N^{\mathrm{safe}}(\mathcal{S}, \mathcal{U})$ ensures safety pointwise in time, at the discrete time samples. Thus, ΔT must be chosen small enough, or the set to be avoided must be enlarged, to avoid significant constraint violations in intersampling, as is commonly done for discrete-time constrained control methods.

Leveraging the reachable sets, we determine the abort safe sets for rendezvous in which safety is ensured in the pres-

ence of propulsion failures as follows. First, we consider the admissible control sets (9) for the failure modes of interests,

$$\bar{\mathcal{U}} = \bigcup_{i=1}^{q} \mathcal{U}_i, \tag{16}$$

where $q \leq n_{\mathrm{F}}$ is the number of the failure modes of interest, which will, in general, be smaller than the total number of failure modes since, for instance, the spacecraft may be re-oriented to change the configuration of the faulty thrusters. To ensure safety across all the failure modes of interest,

$$\mathcal{X}^{\mathrm{unsafe}}_{N,q}(\mathcal{S},\bar{\mathcal{U}}) = \bigcup_{\mathcal{U}_i \in \bar{\mathcal{U}}} \bar{\mathcal{R}}_N(\mathcal{S},\mathcal{U}_i), \tag{17}$$

which is the set of unsafe states from which $\mathcal{S}$ cannot be avoided for at least one fault. Once again, the safe set with respect to q failure modes of interest is

$$\mathcal{X}^{\mathrm{safe}}_{N,q}(\mathcal{S},\bar{\mathcal{U}}) = \mathcal{X}^{\mathrm{unsafe}}_{N,q}(\mathcal{S},\bar{\mathcal{U}})^{\mathrm{c}}. \tag{18}$$

Remark 3. *The sets in $\bar{\mathcal{U}}$ are constructed under the assumption that $\mathrm{F_c}$ is aligned with $\mathrm{F_o}$. If this were not the case, the chaser may be reoriented by the attitude control system to align itself with the orientation used to compute $\mathcal{X}^{\mathrm{unsafe}}_{N,q}(\mathcal{S},\bar{\mathcal{U}})$ by maneuvers that are, in general, much faster than orbital maneuvers. For passive abort-safety, reorientation is not necessary since $\bar{\mathcal{U}} = \mathbf{0}$.*

The unsafe set depends explicitly on the admissible control sets $\mathcal{U}$. The more $\mathcal{U}$ grows, i.e., the more abort maneuvers can be executed, the fewer states are unsafe, as formalized next.

Proposition III.2. *Given a time step k_{f} and two control sets $\mathcal{U}_v$, $\mathcal{U}_y$, such that $\mathcal{U}_y \subseteq \mathcal{U}_v$, for all $j \in \mathbb{Z}_{0+}$,*

$$\mathcal{R}_b(j;\mathcal{P}_{\mathrm{f}},\mathcal{U}_v,k_{\mathrm{f}}) \subseteq \mathcal{R}_b(j;\mathcal{P}_{\mathrm{f}},\mathcal{U}_y,k_{\mathrm{f}}). \tag{19}$$

Proof. We prove the statement by induction, assuming $\mathcal{R}_b(j-1;\mathcal{S},\mathcal{U}_v,k_{\mathrm{f}}) \subseteq \mathcal{R}_b(j-1;\mathcal{S},\mathcal{U}_y,k_{\mathrm{f}})$. Let $\bar{\boldsymbol{x}} \in \mathcal{R}_b(j;\mathcal{S},\mathcal{U}_v,k_{\mathrm{f}})$, then $f(k_{\mathrm{f}}-j,\bar{\boldsymbol{x}},\boldsymbol{u}) \in \mathcal{R}_b(j-1;\mathcal{S},\mathcal{U}_v,k_{\mathrm{f}})$, for all $\boldsymbol{u} \in \mathcal{U}_v$. Then, $f(k_{\mathrm{f}}-j,\bar{\boldsymbol{x}},\boldsymbol{u}) \in \mathcal{R}_b(j-1;\mathcal{S},\mathcal{U}_y,k_{\mathrm{f}})$ for all $\boldsymbol{u} \in \mathcal{U}_y$ since $\mathcal{U}_y \subseteq \mathcal{U}_v$ and $\mathcal{R}_b(j-1;\mathcal{S},\mathcal{U}_y,k_{\mathrm{f}}) \supseteq \mathcal{R}_b(j-1;\mathcal{S},\mathcal{U}_v,k_{\mathrm{f}})$, by the inductive assumption. Thus, $\mathcal{R}_b(j;\mathcal{S},\mathcal{U}_v,k_{\mathrm{f}}) \subseteq \mathcal{R}_b(j;\mathcal{S},\mathcal{U}_y,k_{\mathrm{f}})$. The initial step for the inductive assumption is provided by $\mathcal{R}_b(0;\mathcal{P}_{\mathrm{f}},\mathcal{U}_v,k_{\mathrm{f}}) = \mathcal{R}_b(0;\mathcal{P}_{\mathrm{f}},\mathcal{U}_y,k_{\mathrm{f}}) = \mathcal{S}$. □

Aligned with Proposition III.2, passive safety is the most stringent requirement. Because of this, spacecraft rendezvous missions are often staged to maintain passive safety first, as a chaser approaches but is still far from the target, and active safety later, as the chaser comes into close proximity to the target where passive safety is impossible to achieve.

While (17) provides a general expression for the unsafe set, the actual computations depend on the system dynamics and avoidance sets. Next, we consider the LTV spacecraft relative motion (7) in the cases where the avoidance sets are polytopes or ellipsoids. For LTV dynamics (7), such sets are closed under reachability operations, which also means that only one new set is constructed at every iteration, thus limiting the memory requirements. Furthermore, as it will be clear later, the offline and online computations require at most solving convex problems, for which convergence is guaranteed. These features are advantageous when seeking to implement the approach in on-board embedded platforms, which have memory and computing power limitations [31].

B. Safety based on Polytopes

For linear dynamics (7), when the avoidance set $\mathcal{S}$ is a polytope, the RS is also a polytope constructed by solving linear programs (LPs) [29]. Let $\mathcal{S} = \mathcal{P}_{\mathrm{f}} = \mathcal{P}(H_{\mathrm{f}},\boldsymbol{l}_{\mathrm{f}})$, and the j-step RS $\mathcal{R}_b(j;\mathcal{P}_{\mathrm{f}},\mathcal{U},k_{\mathrm{f}}) = \mathcal{P}(H_j,\boldsymbol{l}_j)$, the $j+1$-step RS is $\mathcal{R}_b(j+1;\mathcal{P}_{\mathrm{f}},\mathcal{U},k_{\mathrm{f}}) = \mathcal{P}(H_{j+1},\boldsymbol{l}_{j+1}) = \{\boldsymbol{x}:\ A_{k_{\mathrm{f}}-(j+1)}\boldsymbol{x} + B_{k_{\mathrm{f}}-(j+1)}\boldsymbol{u} \in \mathcal{P}(H_j,\boldsymbol{l}_j),\ \forall u \in \mathcal{U}\}$, where

$$H_{j+1} = H_j A_{k_{\mathrm{f}}-(j+1)}, \tag{20a}$$

$$[\boldsymbol{l}_{j+1}]_i = \min_{\boldsymbol{u}\in\mathcal{U}} \quad [\boldsymbol{l}_j]_i - [H_j]_i B_{k_{\mathrm{f}}-(j+1)}\boldsymbol{u}. \tag{20b}$$

The minimal representation of $\mathcal{P}(H_j,\boldsymbol{l}_j)$ is obtained by removing redundant constraints with LPs. The RSi (12) and the unsafe set (17) are, in general, non-convex because they are the union of polytopes that account for avoidance in a time interval, different target orbital positions, and different failures. For illustration, Figure 4 shows the projections of the active abort-unsafe sets onto the $\delta x - \delta y$ plane for a simplified spacecraft that can thrust independently in the radial (δx) and along-track (δy) directions, when the example spacecraft loses propulsion capabilities on the along-track and radial directions.

Since for total thruster failure $\mathcal{U} = \{\mathbf{0}\}$, the computation of the RS for passive safety is simplified, as (20b) no longer involve optimization, and

$$\mathcal{R}_b(j;\mathcal{P}_{\mathrm{f}},\mathbf{0},k_{\mathrm{f}}) = \{\boldsymbol{x} \in \mathbb{R}^n:\ H_{\mathrm{f}}\Phi(k_{\mathrm{f}},k_{\mathrm{f}}-j)\boldsymbol{x} \leq \boldsymbol{l}_{\mathrm{f}}\}. \tag{21}$$

C. Passive Safety based on Ellipsoids

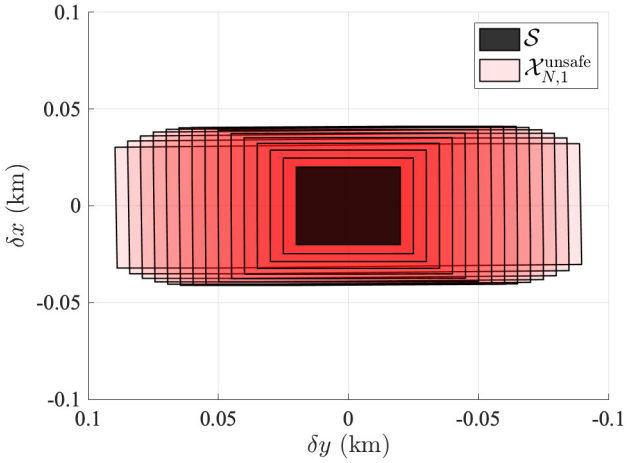
For passive safety, an alternative is to consider an ellipsoidal avoidance set $\mathcal{S} = \mathcal{E}_{\mathrm{f}} = \mathcal{E}(\mathbf{0},P_{\mathrm{f}})$ centered at the origin with shape matrix P. The set $\mathcal{E}_{\mathrm{f}}$ can characterize both AE and KOS, and hence, $\mathcal{E}_{\mathrm{f}} = \mathcal{E}_{\mathrm{AE}}$ during the initial approach and $\mathcal{E}_{\mathrm{f}} = \mathcal{E}_{\mathrm{KOS}}$ when in closer proximity to the target. For $\mathcal{E}_{\mathrm{f}}$ and dynamics (7) with $\boldsymbol{u} = 0$, i.e., passive abort, the j-step RS is

$$\mathcal{R}_b(j;\mathcal{E}_{\mathrm{f}},\mathbf{0},k_{\mathrm{f}}) = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{x}^\top \Phi(k_{\mathrm{f}},k_{\mathrm{f}}-j)^\top\ P^{-1}\ \Phi(k_{\mathrm{f}},k_{\mathrm{f}}-j)\ \mathbf{x} \leq 1\}. \tag{22}$$

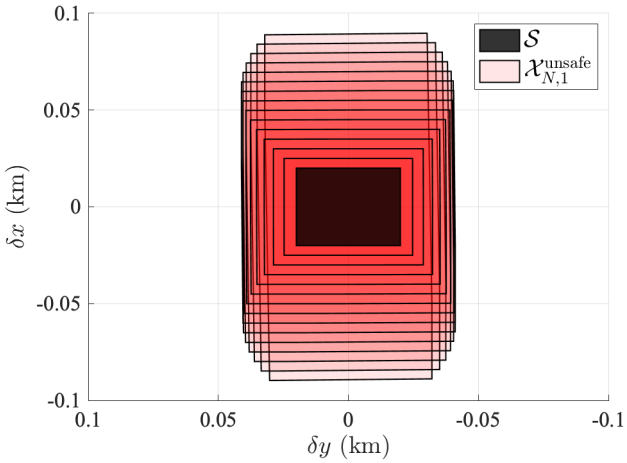
The N-step RSi $\mathcal{R}_N(\mathcal{E}_{\mathrm{f}},\mathbf{0},k_{\mathrm{f}})$ and orbit RSi $\bar{\mathcal{R}}_N(\mathcal{E}_{\mathrm{f}},\mathbf{0})$ are unions of finite sets of ellipsoids.

IV. Abort-Safe Rendezvous Control Design

To obtain an abort-safe rendezvous we use the safe set (18) in the design of the rendezvous policy. Specifically, we develop a model predictive control [42] that minimizes a cost function that encodes the performance metrics for rendezvous, while enforcing that the trajectory remains within the safe region. Thus, if a failure occurs, there exists a maneuver that maintains the spacecraft outside the avoidance set, hence avoiding collisions for at least the given time interval.



(a) Projections of the unsafe sets $\mathcal{X}_{N,1}^{\text{unsafe}} \subset \mathbb{R}^6$ onto the δx-δy plane for $u_y = 0$, i.e., the failure mode results in loss of along-track control. Because $u_y = 0$ more states along δy are unsafe.



(b) Projections of the unsafe sets $\mathcal{X}_{N,1}^{\text{unsafe}} \subset \mathbb{R}^6$ onto the δx-δy plane for $u_x = 0$, i.e., the failure mode results in loss of radial control. Because $u_x = 0$ more states along δx are unsafe.

Figure 4: Illustration of the unsafe sets for sample failure modes.

At every time step k, the MPC policy solves the finite horizon optimal control problem

$$\min_{\boldsymbol{U}_k} \quad \boldsymbol{x}_{N_\text{p}|k}^\mathsf{T} M \boldsymbol{x}_{N_\text{p}|k} + \sum_{j=0}^{N_\text{p}-1} \boldsymbol{x}_{j|k}^\mathsf{T} L \boldsymbol{x}_{j|k} + \boldsymbol{u}_{j|k}^\mathsf{T} R \boldsymbol{u}_{j|k} \quad (23a)$$

$$\text{s.t.} \quad \boldsymbol{x}_{j+1|k} = A_{j+k}\boldsymbol{x}_{j|k} + B_{j+k}\boldsymbol{u}_{j|k} \quad (23b)$$

$$\boldsymbol{g}_{h|k}(\boldsymbol{x}_{j|k}) \leq 0, h \in \mathbb{Z}_{[0,N_p-1]} \quad (23c)$$

$$u_{j|k} \in \mathcal{U}(k) \quad (23d)$$

$$\boldsymbol{x}_{0|k} = \boldsymbol{x}_k \quad (23e)$$

where $L = L^\top \geq 0$, $R = R^\top > 0$, $M = M^\top > 0$ are weight matrices defining the desired performance, $N_\text{p} \ll N$ is the prediction horizon length, (23b) is the prediction model based on (7), and (23d) is the input constraint, where $\mathcal{U}(k) \in \mathcal{U}_i$ is the admissible input set at step k based on the propulsion system condition (9). The safety constraint (23c) enforces that $x_{j|k} \in \mathcal{X}_{N,q}^{\text{safe}}(\mathcal{S}, \bar{\mathcal{U}})$ so that abort maneuvers exist in the presence of propulsion system failures. In (23a), L affects the primary objective, reaching the target, and R affects the secondary objective, minimizing the propellant use. The terminal weight M is usually chosen to obtain stability properties, although here these are not a major focus. The resulting MPC control law is

$$\boldsymbol{u}_k = \kappa_\text{mpc}(\boldsymbol{x}_k) = \boldsymbol{u}_{0|k}^*, \quad (24)$$

where $\boldsymbol{U}_k^* = (\boldsymbol{u}_{0|k}^* \dots \boldsymbol{u}_{N_\text{p}-1|k}^*)$ is the optimizer of (23).

Implementing (23c) directly as

$$x_{j|k} \in \mathcal{X}_{N,q}^{\text{safe}} = \mathcal{X}_{N,q}^{\text{unsafe}}(\mathcal{P}_\text{f}, \bar{\mathcal{U}})^c, \quad (25)$$

renders (23) non-convex and hence hard to solve in real-time. Next we propose methods for convexifying (23c) in the polytopic and ellipsoidal cases.

A. Convexification of Polytopic Safe Set

When the avoidance set is a polytope, we convexify (25) by implementing (23c) as convex constraints that exclude (17) from the feasible set of (23) based on the following result.

Result 1. *([29, Prop.3.31]) Given polytopes $\mathcal{P}_1(H_1, \boldsymbol{l}_1)$, $\mathcal{P}_2(H_2, \boldsymbol{l}_2)$, $\mathcal{P}_2(H_2, \boldsymbol{l}_2) \supset \mathcal{P}_1(H_1, \boldsymbol{l}_1)$ if and only if there exists a non-negative matrix Λ such that*

$$\begin{aligned} \Lambda H_1 &= H_2 \\ \Lambda \boldsymbol{l}_1 &\leq \boldsymbol{l}_2. \end{aligned} \quad (26)$$

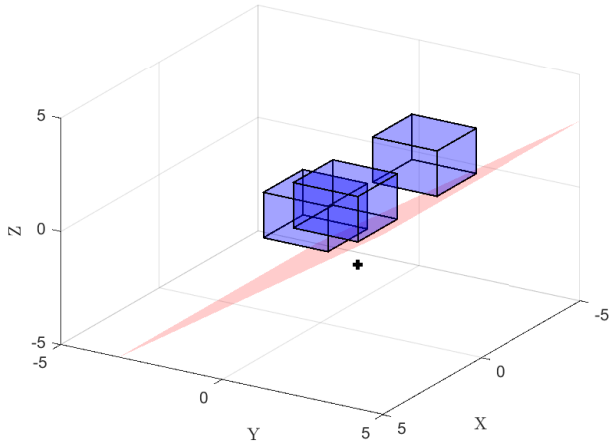


Figure 5: Example of Result 1 in $\mathbb{R}^3$. The blue polytopes represent sets to be avoided, while the red hyperplane separates the state marked by the black cross from the polytopes.

At time k, we construct (23c) from Result 1 and the optimal trajectory at time $k-1$, $(\boldsymbol{x}_{0|k-1}^* \dots \boldsymbol{x}_{N_\text{p}|k-1}^*)$. Given $\boldsymbol{x}_{j+1k-1}^*$, $j \in \mathbb{Z}_{1,N_\text{p}}$, we compute the distance from the polytopes $\mathcal{P} \in \mathcal{X}_{N,q}^{\text{unsafe}}(\mathcal{P}_\text{f}, \bar{\mathcal{U}})$,

$$\begin{aligned} \text{d}(\boldsymbol{x}_{j+1|k-1}^*, \mathcal{P}) = \min_{\boldsymbol{y}} \quad & \|\boldsymbol{x}_{j+1|k-1}^* - \boldsymbol{y}\|_2 \\ \text{s.t.} \quad & \boldsymbol{y} \in \mathcal{P} \end{aligned} \quad (27)$$

and select the ℓ closest ones, $\{\mathcal{P}(H_{j|k}^i, l_{j|k}^i)\}_{i=1}^\ell$, where $H_{j|k}^i \in \mathbb{R}^{n_{c_i} \times n}$, and where ℓ is a design choice, possibly including all polytopes in $\mathcal{X}_{N,q}^{\text{unsafe}}(\mathcal{P}_\text{f}, \bar{\mathcal{U}})$. Then, we construct

a halfspace $\mathcal{P}(\boldsymbol{h}_{j|k},1)=\{\boldsymbol{x}\in\mathbb{R}^n:\ \boldsymbol{h}_{j|k}\boldsymbol{x}\leq 1\}$ such that $\mathcal{P}(\boldsymbol{h}_{j|k},1)\supset\mathcal{P}(H^i_{j|k},\ \boldsymbol{l}^i_{j|k})$, for all $i\in\mathbb{Z}_{[1,\ell]}$, as

$$
\begin{aligned}
&(\boldsymbol{h}_{j|k},s^*,\{\boldsymbol{\lambda}_i^*\}_{i=1}^{\ell})=\\
&\quad\arg\max_{\boldsymbol{h},s,\{\boldsymbol{\lambda}_i\}_{i=1}^{\ell}} \quad s && \text{(28a)}\\
&\qquad\text{s.t.}\quad s\geq 0 && \text{(28b)}\\
&\qquad\quad \boldsymbol{h}\boldsymbol{x}^*_{j+1|k-1}\geq 1+s && \text{(28c)}\\
&\qquad\quad [\boldsymbol{\lambda}_i]_j\geq 0,\quad j\in\mathbb{Z}_{[1,n_{ci}]} && \text{(28d)}\\
&\qquad\quad \boldsymbol{\lambda}_i H^i_{j|k}=\boldsymbol{h} && \text{(28e)}\\
&\qquad\quad \boldsymbol{\lambda}_i\boldsymbol{l}^i_{j|k}\leq 1,\quad i\in\mathbb{Z}_{[1,\ell]} && \text{(28f)}
\end{aligned}
$$

where $\boldsymbol{\lambda}_i\in\mathbb{R}^{1\times n_{ci}}$, for all $i=\mathbb{Z}_{[1,\ell]}$. For an arbitrary small $\rho>0$, we implement (23c) as

$$-\boldsymbol{h}_{j|k}\boldsymbol{x}_{j|k}\leq -1-\rho. \tag{29}$$

Any feasible solution of the LP (28) is such that $\mathcal{P}(\boldsymbol{h}_{j|k},1)\supset\mathcal{P}(H^i_{j|k},\boldsymbol{l}^i_{j|k})$, for all $i\in\mathbb{Z}_{[1,\ell]}$, and $\boldsymbol{x}_{j|k}\notin\mathcal{P}(\boldsymbol{h}_{j|k},1)$. Hence (29) does not intersect any $\mathcal{P}(H^i_{j|k},\boldsymbol{l}^i_{j|k})$ $i\in\mathbb{Z}_{[1,\ell]}$. Cost function (28a) selects a halfspace that leaves the spacecraft more clearance to maneuver and possibly to optimize the rendezvous trajectory.

Remark 4. *If ℓ is chosen to include all polytopes of $\mathcal{X}^{\text{unsafe}}_{N,q}(\mathcal{P}_{\text{f}},\bar{\mathcal{U}})$, the feasible set of (29) is contained in $\mathcal{X}^{\text{safe}}_{N}(\mathcal{P}_{\text{f}},\bar{\mathcal{U}})$. Including only the closest polytopes reduces the computational burden of (23), (28), and avoids being excessively conservative, leveraging the receding horizon nature of (24), since $\mathcal{X}^{\text{unsafe}}_{N,q}(\mathcal{P}_{\text{f}},\bar{\mathcal{U}})$ considers all the orbit, while the phases of the rendezvous maneuver considered here terminate in a small fraction of the orbital period.*

B. Convexification of Ellipsoidal Safe Set

For the case where (17) contains ellipsoids, we convexify (23c) using the following result.

Result 2. *([43, Section 2.5]) Given $j+e$ ellipsoids*

$$\mathcal{E}_i=\{Q_i^{\frac{1}{2}}\boldsymbol{v}+\boldsymbol{q}_i\in\mathbb{R}^n\ :\|\boldsymbol{v}\|_2\leq 1\}, \tag{30}$$

where $Q_i=Q_i^{\mathsf{T}}\succ 0$, a hyperplane $\boldsymbol{a}^\top\boldsymbol{x}=b$ such that

$$
\begin{aligned}
-\|Q_i^\top\boldsymbol{a}\|_2+\boldsymbol{a}^\top\boldsymbol{q}_i-b>0,\quad i\in\mathbb{Z}_{[1,j]} && \text{(31a)}\\
\|Q_i^\top\boldsymbol{a}\|_2+\boldsymbol{a}^\top\boldsymbol{q}_i-b<0,\quad i\in\mathbb{Z}_{[j+1,j+e]} && \text{(31b)}
\end{aligned}
$$

strictly separates $\bigcup_{i=1}^{j}\mathcal{E}_i$ from $\bigcup_{i=j+1}^{j+e}\mathcal{E}_i$.

When (17) consists of ellipsoids, for an arbitrary small $\rho>0$, constraint (23c) is implemented by (29), where $\boldsymbol{h}_{j|k}$ is now given from the solution of the second-order cone program (SOCP)

$$
\begin{aligned}
&(\boldsymbol{h}_{j|k},s^*)=\\
&\arg\max_{\boldsymbol{a},s}\quad s && \text{(32a)}\\
&\quad\text{s.t.}\quad s\geq 0 && \text{(32b)}\\
&\qquad \boldsymbol{a}^{\mathsf{T}}\boldsymbol{x}^*_{j+1|k-1}\geq 1+s && \text{(32c)}\\
&\qquad \|Q^{i\top}_{j|k}\boldsymbol{a}\|_2+\boldsymbol{a}^\top\boldsymbol{q}^i_{j|k}\leq 1,\quad i\in\mathbb{Z}_{[1,\ell]} && \text{(32d)}
\end{aligned}
$$

where $\{\mathcal{E}(\boldsymbol{q}^i_{j|k},Q^i_{j|k})\}_{i=1}^{\ell}\subseteq\mathcal{X}^{\text{unsafe}}_N(\mathcal{E}_{\text{f}},\boldsymbol{0})$ are the ℓ closest ellipsoids to $\boldsymbol{x}^*_{j+1|k-1}$. Solving (32) results in $\mathcal{P}(\boldsymbol{h}_{j|k},1)\supset\mathcal{E}(\boldsymbol{q}^i_{j|k},Q^i_{j|k})\}_{i=1}^{\ell}$ and hence the complement (29) does not intersect $\mathcal{E}(\boldsymbol{q}^i_{j|k},Q^i_{j|k})\}_{i=1}^{\ell}$.

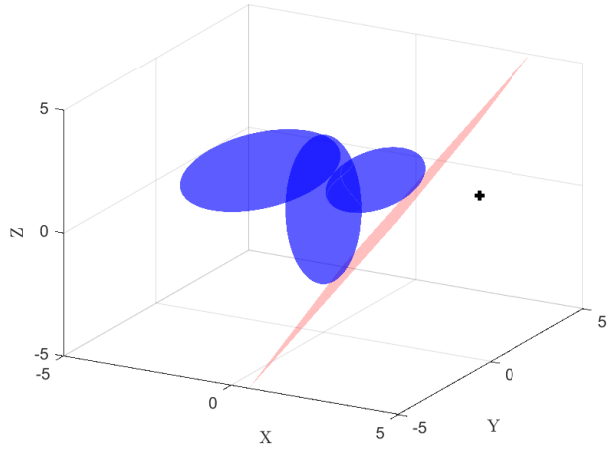


Figure 6: Example of Result 2 in $\mathbb{R}^3$. The blue ellipsoids represent sets to be avoided, while the red hyperplane separates the state marked by the black cross from the ellipsoids.

Remark 5. *If $\ell=1$, only the closest, i.e., more restrictive, ellipsoid is used. The hyperplane may be selected as its tangent $\boldsymbol{h}_{j|k}=2Q_i^{-1}\bar{\boldsymbol{y}}$ at the state radial projection, $\bar{\boldsymbol{y}}=\boldsymbol{x}^*_{j+1|k-1}/(\boldsymbol{x}^{*\top}_{j+1|k-1}Q_i^{-1}\boldsymbol{x}^*_{j+1|k-1})^{1/2}$, which avoids solving the SOCP [38].*

While our problem convexifies constraint boundaries in $\mathbb{R}^n$, Figures 5-6 show illustrative examples of this convexification in $\mathbb{R}^3$. These sample hyperplanes represent the convex (local) safety constraint at a specific instant in time.

V. Implementation and Practical Aspects

Next we provide additional information on the implementation of the approach, discuss the computational burden of the different safety constraints, and discuss how to increase robustness to unmodeled perturbations.

A. Implementation

As introduced in Section II, rendezvous missions have three phases where abort safety is required. In the first two phases, passive safety is maintained with respect to the AE, and the KOS, respectively. For these two phases, it is typical to use ellipsoidal sets (22) as the NASA specifications are ellipsoidal. If the AE and KOS are over-approximated as polytopes, (21) may also be used. In the third phase, active abort safety is maintained with respect to terminal region, based on (20). When the chaser engages the final approach to the target, the safety constraints are removed to allow for berthing or docking. For all mission phases, the unsafe set computations can be performed offline as they do not require real-time data.

Algorithm 1 summarizes the approach for abort-safe rendezvous. The algorithm is initialized by separating $\boldsymbol{x}_0$ from

Algorithm 1 Abort-Safe Rendezvous Control

Offline: Compute the unsafe set $\mathcal{X}^{\text{unsafe}}_{N,q}(\mathcal{S},\bar{\mathcal{U}})$ using polytopes and ellipsoids for the different mission phases
Online:
1: **repeat**
2: **input:** $\boldsymbol{x}_k$, $(\boldsymbol{x}^*_{0|k-1}\dots\boldsymbol{x}^*_{N_\text{p}|k-1})$, $\mathcal{X}^{\text{unsafe}}_{N,q}(\mathcal{S},\bar{\mathcal{U}})$
3: For each $\boldsymbol{x}^*_{j+1|k-1}$, $j\in\mathbb{Z}_{[0,N_\text{p}-1]}$ select the ℓ closest polytopes/ellipsoids in $\mathcal{X}^{\text{unsafe}}_{N,q}(\mathcal{S},\bar{\mathcal{U}})$
4: Convexify safety constraint (25) pointwise along the MPC horizon as (29) for $j\in\mathbb{Z}_{[0,N_\text{p}-1]}$, by (28)/(32)
5: Solve the optimal control problem (23) with (23c) implemented by (29)
6: Apply command (24) to the chaser spacecraft
7: **until** Final approach is activated

the nearest unsafe sets along the entire MPC window, solving (23) to obtain an initial prediction for constructing the initial constraints. After initialization, the constraint sequence is iteratively updated with the new predicted states in receding horizon.

Let the number of sets in $|\mathcal{X}^{\text{unsafe}}_{N,q}(\mathcal{S},\bar{\mathcal{U}})|=n_\text{s}$. The following proposition summarizes how (24) achieves the desired property of abort safe rendezvous when (23) is feasible.

Proposition V.1. *Let the MPC safety constraint* (23c) *be* (29) *implemented by* (28) *or* (32)*, for all polytopes or ellipsoids, respectively. Given the dynamics* (7) *in closed-loop with feedback law* (24)*, at any time step k such that the optimal control problem* (23) *admits a solution, safe abort maneuvers for faults occurring before and after the execution of $\boldsymbol{u}_k$ exist, i.e., for faults at time step k and $k+1$.*

Proof. Because (29) is such that the complement $\mathcal{P}(\boldsymbol{h}_{j|k},1)\supset\{S^i_{j|k}\}_{i=1}^{n_\text{s}}=\mathcal{X}^{\text{unsafe}}_{N,q}(\mathcal{S},\bar{\mathcal{U}})$, where $S^i_{j|k}$ are the polytopic or ellipsoidal sets in $\mathcal{X}^{\text{unsafe}}_{N,q}(\mathcal{S},\bar{\mathcal{U}})$, any feasible solution of (23) ensures $\boldsymbol{x}_{j|k}\in\mathcal{X}^{\text{safe}}_{N,q}$. Then, per Proposition III.1, for every $\boldsymbol{x}_{j|k}$, $j\in\mathbb{Z}_{[0,N_\text{p}]}$, there exists at least one abort sequence $\boldsymbol{u}^\text{a}_{j+v|k}(\boldsymbol{x}^*_{j|k})$, $v\in\mathbb{Z}_{[0,N-1]}$, that results in a trajectory $\boldsymbol{x}^\text{a}_{j+v|k}\notin\mathcal{S}$, for all $v\in\mathbb{Z}_{[0,N]}$.

By feasibility of (23), $\boldsymbol{x}_k=\boldsymbol{x}^*_{0|k}\notin\mathcal{X}^{\text{unsafe}}_{N,q}(\mathcal{S},\bar{\mathcal{U}})$, and if a fault occurs before the execution of $\boldsymbol{u}_k$, then $\boldsymbol{u}^\text{a}_{v|k}(\boldsymbol{x}^*_{0|k})$ is the safe abort maneuver. Similarly, by feasibility of (23), $\boldsymbol{x}_{k+1}=\boldsymbol{x}^*_{1|k}\notin\mathcal{X}^{\text{unsafe}}_{N,q}(\mathcal{S},\bar{\mathcal{U}})$. Thus, if $\boldsymbol{u}_k$ is applied and a fault occurs at $k+1$, the abort safe maneuver is $\boldsymbol{u}^\text{a}_{v+1|k}(\boldsymbol{x}^*_{1|k})$. □

Remark 6. *If the MPC problem* (23) *becomes infeasible at $k+1$, because $\boldsymbol{x}_{0|k+1}=\boldsymbol{x}_{1|k}\in\mathcal{X}^{\text{safe}}_{N,q}$, an abort maneuver exists and can be engaged to ensure the safety of the chaser and target.*

In the passive safety case, $\{\boldsymbol{u}^\text{a}_{j+v|k}(x^*_{j|k})\}_{v=0}^{N-1}=\{\boldsymbol{0}\}_{v=0}^{N-1}$. Moreover, we let $\ell\ll n_\text{s}$ to reduce the computational burden. By choosing ℓ large enough and selecting the sets based on distance (27), we ignore sets that are far away from the spacecraft trajectory, possibly already accounted for by the included ones, and Proposition V.1 still holds, in practice.

B. Comparison of the Different Safety Constraints

We presented three methods to convexify the safety constraints that are obtained for the linear time varying system (7) for polytopic and ellipsoidal avoidance sets. Two methods require solving online convex optimization problems, the LPs (28) or the SOCPs (32), while the tangent method in Remark 5 only requires linear algebra operations. In all cases, using (7), the finite horizon optimal control problem (23) is a quadratic program (QP), for which solvers exist for embedded platform implementation [31]. Thus, while using linear models and polytopes or ellipsoids may be conservative or introduce small approximation errors, such designs result in solver requirements that are possibly suitable for on-board implementation. Table I shows the number and type of optimization problems that each convexification method requires, including the determination of the ℓ closest sets and the construction of the hyperplanes. For passive safety based on ellipsoids, the tangent method may be desirable, since it significantly reduces the computational complexity compared to its SOCP counterpart, albeit suboptimally. If separation from multiple sets is required, the method for polytopes may be more appealing than the method for ellipsoids, since LPs are computationally easier to solve than SOCPs.

Tables II-III report sample times for distance and separating hyperplane computations, executed on 2.5 GHz Dual-Core Intel Core i7 processor a laptop with 16GB RAM, in MATLAB R2020b. The unsafe sets are computed offline using MPT3.0 [44] and complete in the order of minutes, for polytopes. For ellipsoids, the unsafe sets are computed with matrix operations in the order of seconds.

Table I: Online optimization problems solved at each time step for the different convexification approaches.

Variations	LPs	QPs	SOCP
$\mathcal{P}$ Active safety	N_p	$n_\text{s}+1$	0
$\mathcal{P}$ Passive-Safety	N_p	$n_\text{s}+1$	0
$\mathcal{E}$ Passive-Safety	0	1	$N_\text{p}+n_\text{s}$
$\mathcal{E}$ Passive-Safety Heuristic	0	1	0

	Polytopic (QP)	Ellipsoidal (QCQP)	Radial Projection
Time (ms)	0.9421	0.1646	0.0110

Table II: Average time to compute the distances to a polytope and an ellipsoid, and a radial projection.

	Polytopic (LP)	Ellipsoidal (SOCP)	Tangent
Time (ms)	2.6499	12.6514	0.0025

Table III: Average time to compute separating hyperplanes for polytopes, ellipsoids and ellipsoid tangent.

C. Avoidance Set and Admissible Velocities

While avoidance sets $\mathcal{S}$ are normally defined only in terms of spacecraft positions, for using Results 1, 2 we need compact, i.e., bounded, regions of the state space. Hence, we further impose velocity bounds to the avoidance sets. For the polytopic case this results in $\mathcal{P}_\text{f}=\mathcal{P}(H_\text{f},\boldsymbol{l}_\text{f})$, where $H_\text{f}=\begin{bmatrix}I_6 & -I_6\end{bmatrix}^\mathsf{T}$, and $\boldsymbol{l}_\text{f}$ defines the upper and lower position

and velocity bounds, e.g., $\boldsymbol{l}_{\mathrm{f}} = \begin{bmatrix} p_{\mathrm{m}}\mathbf{1} & v_{\mathrm{m}}\mathbf{1} & p_{\mathrm{m}}\mathbf{1} & v_{\mathrm{m}}\mathbf{1} \end{bmatrix}^{\mathsf{T}}$ for symmetric bounds. Similarly, for the ellipsoidal case this results in $\mathcal{E}_{\mathrm{f}} = \mathcal{E}(\mathbf{0}, P)$, where

$$P = \begin{bmatrix} P_{\mathrm{p}} & 0 \\ 0 & P_{\mathrm{v}} \end{bmatrix} \in \mathbb{R}^{6\times 6}, \tag{33}$$

$P_{\mathrm{p}} = P_{\mathrm{p}}^{\mathsf{T}} \succ 0$, and $P_v = P_v^{\mathsf{T}} = v_{\mathrm{m}} I_3 \succeq 0$. For a finite v_{m}, trajectories that enter the avoidance set at high speeds may be classified as safe. Selecting $v_{\mathrm{m}} \gg 0$ to include all the chaser's admissible operational velocities, ensures that any such misclassified trajectory is not physically possible, while retaining compactness of $\mathcal{P}_i$ or $\mathcal{E}_i$.

D. Increasing robustness to unmodeled perturbations

The safety constraints in (23c) and the prediction model (23b) are designed based on (5), which applies to Keplerian orbits. Thus, (23c) and (23b) ignore perturbations such as Earth's non-spherical and unequal mass distribution, air-drag effects in low-Earth orbits, and third-body effects [40]. Using exclusion regions such as the AE or KOS allow for the effects of these perturbations to be ignored at design time, while still ensuring safety of the target in the event of chaser propulsion failures. If the spacecraft nominal dynamics does not enter the exclusion region, when subject to non-Keplerian dynamics for short time-horizons it will not collide with the target, although it may enter the exclusion region. That is, the exclusion region works as a safety margin against unmodeled perturbations.

To achieve robust avoidance of the exclusion region the techniques presented in Section III could be extended to account for a set $\mathcal{W}$ bounding the unmodeled perturbations. This amounts to computing controllable sets, the set of states for which there exists at least one disturbance sequence that causes entering the exclusion region for all the admissible sequences of command inputs, according to the propulsion system condition. Such computation is numerically challenging because it must perform projections [30], which have non-polynomial complexity even for polytopes.

A heuristic suboptimal approach, yet simpler to implement, is to inflate the unsafe sets (17) computed according to the nominal dynamics by a margin $\gamma > 1$. For ellipsoids and polytopes, the inflated sets are $\cup_{i=1}^{n_{\mathrm{s}}}\{\boldsymbol{x} \in \mathbb{R}^6,\ \boldsymbol{x}^\top P_i^{-1}\boldsymbol{x} \leq \gamma\}$ and $\cup_{i=1}^{n_{\mathrm{s}}}\mathcal{P}_i(H_i, \gamma \boldsymbol{l}_i)$, respectively. Such inflation results in tightening constraint (29) that implements (23c), with an effect similar to that of tube-based MPC [42], but without calculating the tightening from the minimum positive invariant set of the LTV system. Rather, the set inflation parameter γ is used here as a calibration variable, or determined numerically via high-precision orbital simulation. While the set inflation is a practical method to robustify the approach to unmodeled disturbances, which account for most of the modeling errors, it also compensates for the small errors introduced by linearizing and time discretizing the dynamics (1).

VI. Simulation Results

We first present ellipsoidal passive abort safety results along with a robustness study to determine how Algorithm 1 behaves when subjected to unmodeled perturbations. Then, we report simulations that validate the polytopic active abort safety. Finally, the proposed method is demonstrated on a phased, full mission scenario of abort-safe rendezvous with the ISS. We define an AE around the target of size $\begin{bmatrix} 1 & 2 & 1 \end{bmatrix}$ km in the radial, along-track, and out-of-plane directions, and a KOS of size $\begin{bmatrix} 100 & 100 & 100 \end{bmatrix}$ m. With maximum approach velocities of $v_{\mathrm{m}} = 0.1$km/s, these ellipsoidal sets are given by $\mathcal{E}_{\mathrm{AE}}$ and $\mathcal{E}_{\mathrm{KOS}}$, respectively. A zero-order hold (ZOH) discretization is adopted with sampling period is $\Delta T = 30$s. The mass of the chaser spacecraft is $m_{\mathrm{c}} = 4000$ kg. Each thruster can apply a maximum thrust of $u_{\mathrm{m}} = 0.02$ kN. Where relevant, we discuss the performance trade-off between enforcing safety and not enforcing safety using delta-V, which is the mass-independent propellant consumption of the maneuver $\Delta V = \sum_{k=0}^{N-1} \|\tilde{B}\boldsymbol{u}_k\| \cdot \Delta T$. We run the discrete-time MPC (24) in closed-loop with the continuous-time nonlinear model (4), (1) resolved in $\mathrm{F_o}$ using MPCTools, CasADI [45], and IPOPT [46]. In the subsequent simulations, mission phase changes are triggered when the chaser approaches a particular avoidance set, i.e., when the distance to the set is below designated thresholds $d(\boldsymbol{x}_{0|k}, \mathcal{S}_i) < d_i$. In practical missions, the spacecraft may wait near the exclusion region border for some time, until additional checks are done and the mission can proceed.

A. Passive Abort Safety using Ellipsoids

1) Radial projection vs. SOCP: We compare the radial projection of Remark 5 with the SOCP-based safety constraint for a target in a circular Earth-orbit and an ellipsoidal AE, $\mathcal{E}_{\mathrm{AE}} \subset \mathbb{R}^6$. The target's orbit is defined by the classical orbital elements $\begin{bmatrix} a & e & i & \omega & \Omega & f \end{bmatrix}^\top = \begin{bmatrix} 6726.27\text{km} & 0 & 51.64^\circ & 94.07^\circ & 302.37^\circ & 0^\circ \end{bmatrix}^\top$, see [40] for their relation to inertial states. For circular orbits, (5) simplifies to the well-known CW equations [40]. Because the CW equations are linear time-invariant, the RSi are invariant along the orbit and (11) with $\mathcal{U} = \{\mathbf{0}\}$ ensures passive safety. The safety horizon N is chosen as three orbital periods, $N = \frac{3t_{\mathrm{p}}}{\Delta T}$, where $t_{\mathrm{p}} = 5490$s. Thus, if the chaser state remains in $\mathcal{X}_N^{\mathrm{safe}}(\mathcal{S}, \mathbf{0})$, it will not drift into the AE for at least three subsequent orbital revolutions, even if complete propulsion failure occurs.

The SOCP method separates the chaser spacecraft from $\ell = 3$ ellipsoids at every time step in the MPC horizon, whereas the radial projection separates the chaser from a single $\ell = 1$ ellipsoid. Figure 7 shows that the approaches are similar in this simulation. Although not guaranteed for all initial conditions, the radial-projection may achieve similar approaches to the SOCP technique with lower computational burden.

2) V-bar Approach: Next, we consider an along-track, also called V-bar, approach such that the initial position is purely in the $\hat{\imath}_\theta$ direction (positive δy). We compare a passively safe control policy to a simulation where the passive safety constraints are removed. Passive safety is enforced via the radial projection method in Remark 5. The target is in an eccentric Earth-orbit with orbital elements $\begin{bmatrix} a & e & i & \omega & \Omega & f \end{bmatrix}^\top =$

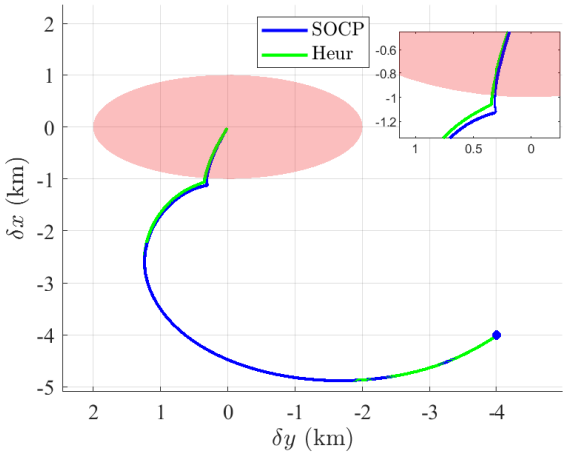


Figure 7: Comparing the rendezvous resulting from SOCP and radial projection ellipsoid-based passive safety constraints.

$\begin{bmatrix}7419.32\text{km} & 0.1 & 0.01° & 0° & 0° & 145°\end{bmatrix}^\top$. The resulting orbital period of the target is $t_\mathrm{p} = 106$ min $= 6360$ s.

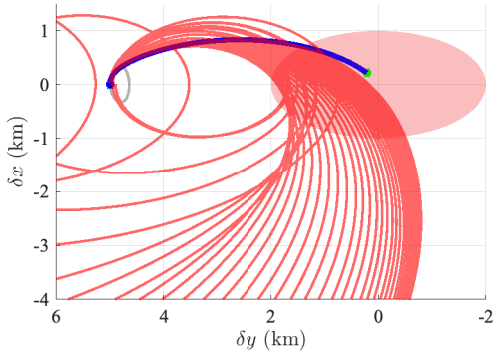


Figure 8: *Passively unsafe rendezvous* with respect to the AE from the along-track direction for a target in an eccentric orbit. States along the trajectory enter the AE under free-drift dynamics.

The MPC cost function weights are $Q = I_6$, $R = 1.3{\cdot}10^4 I_3$, terminal cost $M = 10^2 I_6$, and $N_\mathrm{p} = 30$. The safety horizon N is three orbital periods, which is more than 20 times the length of the prediction horizon. The initial state is $\boldsymbol{x}_0 = \begin{bmatrix}\boldsymbol{p}_0^\mathsf{T} & \boldsymbol{v}_0^\mathsf{T}\end{bmatrix}^\mathsf{T}$, where $\boldsymbol{p}_0^\mathsf{T} = \begin{bmatrix}0 & 5 & 0\end{bmatrix}$ km and $\boldsymbol{v}_0^\mathsf{T} = \begin{bmatrix}0 & 0 & 0\end{bmatrix}$ km/s.

The results are shown in Figures 8–10, where, the initial condition is shown as a blue circle, and the trajectory of the relative position of the chaser with respect to the target as seen in the target's orbital frame F_o is shown in blue. The free-drift trajectories are shown to verify passive safety, in gray when safe and in red when they enter the AE or the KOS.

As a baseline, we apply the MPC policy (24) that does not enforce the passive safety constraints. The resulting maneuver is shown in Figure 8 and requires $\Delta V_\mathrm{unsafe} = 0.0134$ km/s. The free-drift trajectories along the nominal rendezvous maneuver intersect the AE and are unsafe if propulsion failure occurs. The same simulation while enforcing the passive safety constraint yields the maneuver shown in Figure 9, where now the free-drift trajectories do not enter the AE, at the price of an increased propellant consumption, $\Delta V_\mathrm{safe} = 0.0206$ km/s.

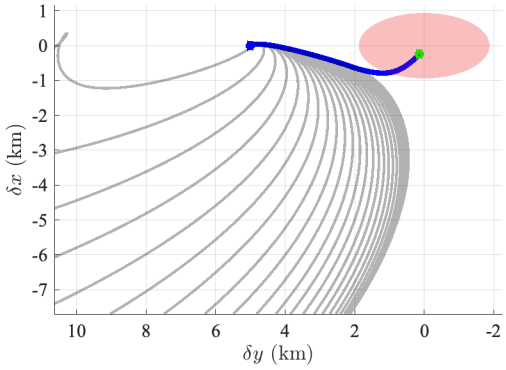


Figure 9: *Passively safe rendezvous* with respect to the AE, in red, from the along-track direction for a target in an eccentric orbit. States do not enter the AE within the safety horizon N under free-drift dynamics.

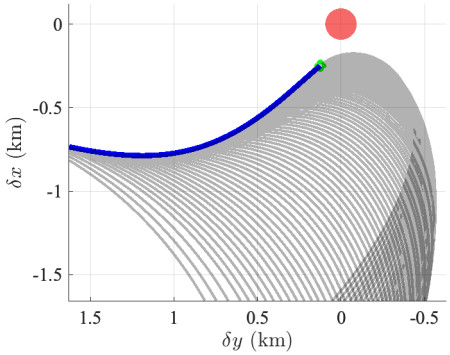


Figure 10: *Passively safe rendezvous* with respect to the KOS, in red, from the along-track direction for a target in an eccentric orbit. States do not enter the KOS within the safety horizon N under free-drift dynamics.

Once the chaser is near the AE, the maneuver proceeds towards the target while maintaining passive safety with respect to the KOS. The resulting maneuver is shown in Figure 10.

3) Robustness to Unmodeled Perturbations: In order to evaluate the proposed control policy in the presence of realistic and unmodeled perturbations, we consider the dynamical models of the target and chaser spacecraft to be perturbed by Earth's oblateness, captured by the J2 zonal harmonic acceleration, and third body gravitational disturbances from the sun and the moon [40]. These perturbations are given by $\boldsymbol{a}_\mathrm{t}^\mathrm{d}$ and $\boldsymbol{a}_\mathrm{c}^\mathrm{d}$ for the target and chaser, respectively. Although other perturbations can be included, these are the dominant ones for most near-Earth orbital regimes. The inertial acceleration model (1) is modified to include the perturbations,

$$\boldsymbol{r}_\mathrm{t}'' = -\mu \frac{\boldsymbol{r}_\mathrm{t}}{\|\boldsymbol{r}_\mathrm{t}\|^3} + \boldsymbol{a}_\mathrm{t}^\mathrm{d}, \tag{34a}$$

$$\boldsymbol{r}_\mathrm{c}'' = -\mu \frac{\boldsymbol{r}_\mathrm{c}}{\|\boldsymbol{r}_\mathrm{c}\|^3} + \frac{\boldsymbol{u}}{m_\mathrm{c}} + \boldsymbol{a}_\mathrm{c}^\mathrm{d}, \tag{34b}$$

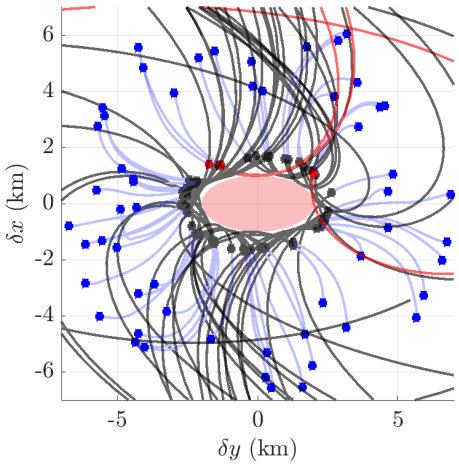
yielding orbits that are no longer Keplerian. While the ground-truth simulation model (34) is perturbed, the reachability analysis and MPC model is not, i.e., we retain (7) for constructing the RS and as the MPC prediction model (23b).

As discussed in Section V-D, under perturbations the proposed safe rendezvous method is no longer guaranteed to provide abort-safe trajectories that avoid the original exclusion zones. Rather, we expect the approach trajectories to cross near the border of the exclusion zone but still far away from the target, because the integration of perturbations for the mission duration results in small deviations.

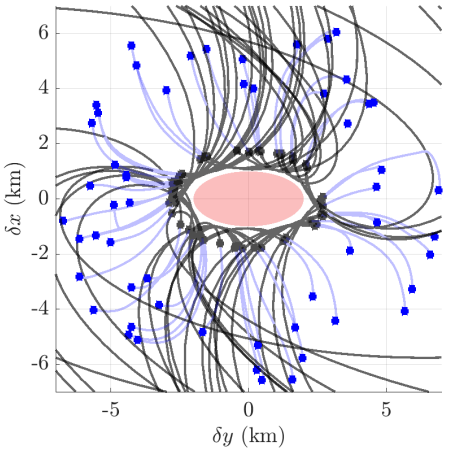
Figure 11 shows $N_{\text{sim}} = 55$ closed-loop simulations of passive safety with respect to the AE, where the total loss of propulsion occurs close to the boundary of the AE. In Figure 11, the portions of the approach where the propulsion system operates nominally are shown in blue, while the free-drift trajectories after the failures are in black. The black marks show the states at which the thrust is fully lost, and the trajectories that enter the AE are shown in red.

Figure 11a shows the results for various random initial conditions when the nominal RSs for the passive case are used, i.e., the inflation parameter of Section V-D is $\gamma = 1$. In this scenario, 3 out of 55 simulations result in trajectories that enter the AE. However, such trajectories cross the AE near the edge, clearing the target by kilometers. As expected, the AE provides a sufficient margin to avoid the target, when used in conjunction with our proposed approach.

As discussed in Section V-D, to ensure that the trajectories remain outside of the exclusion zone even under perturbations, the unsafe sets can be inflated. Figure 11b shows the trajectories for the same initial conditions and failure times as in Figure 11a where the RSs are inflated by a factor $\gamma = 1.1$. In these cases, none of the trajectories enter the AE, showing how a small inflation allows us to retain the same RS computation and nominal controller while obtaining robustness of the entire exclusion zone in the presence of perturbations. The value of γ was determined by simulations, although more formal approaches, similar to those used in tube-based MPC can be explored [37], possibly at the price of a more complex and time consuming design process.



(a) Rendezvous from various initial conditions with nominal prediction model and nominal RS ($\gamma = 1$). Passively safe approaches (blue), free-drift trajectories (black), failure events (black marker); $3/55$ trajectories (red) entered (briefly) the AE.



(b) Rendezvous from various initial conditions with nominal prediction model and inflated RS ($\gamma = 1.1$). Passively safe approaches (blue), free-drift trajectories (black), failure events (black marker). No trajectory (even briefly) enters the AE.

Figure 11: Closed-loop simulations of passively safe rendezvous in presence of perturbations.

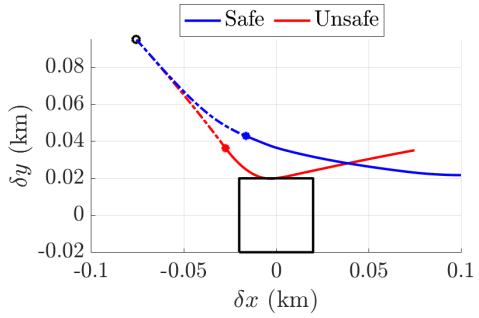
B. Active Abort-Safety using Polytopes

For active abort-safety, the weight matrices in the cost function (23a) are $Q = 10^3 \cdot I_6$, $R = I_3$, $M = Q$. The avoidance set is defined by a polytope $\mathcal{P}(H_{\text{f}}, \boldsymbol{l}_{\text{f}})$ where $H_{\text{f}} = \begin{bmatrix} I_6 & -I_6 \end{bmatrix}^{\mathsf{T}}$ and $\boldsymbol{l}_{\text{f}} = \begin{bmatrix} p_{\text{m}} \mathbb{1}_{1\times 3} & v_{\text{m}} \mathbf{1} & p_{\text{m}} \mathbf{1} & v_{\text{m}} \mathbf{1} \end{bmatrix}^{\mathsf{T}}$, $p_{\text{m}} = 0.02$ km, and $v_{\text{m}} = 6.0 \times 10^{-3}$ km/s. The target initial conditions are defined by the classical orbit elements $\begin{bmatrix} a & e & i & \omega & \Omega & f \end{bmatrix}^{\mathsf{T}} = \begin{bmatrix} 7419.32\text{km} & 0.1 & 0.01^\circ & 0^\circ & 0^\circ & 140^\circ \end{bmatrix}^{\mathsf{T}}$, which yields an orbital period of 6360s. The number of steps in the MPC horizon is $N_{\text{p}} = 8$. The safety horizon is a quarter of the orbital period, $N = \lceil \frac{t_{\text{p}}}{4\Delta T} \rceil + 1 = 54$, almost 8 times larger than N_{p}. The failure occurs at $t_{\text{fail}} = 240$s, when the state is $x_{k_{\text{fail}}}$, so that for $k < k_{\text{fail}}$, $\boldsymbol{u}_k \in \mathcal{U}_1$, where $\mathcal{M}_1 = \mathcal{I}$, is nominal control. For $k \geq k_{\text{fail}}$, $\boldsymbol{u}_k \in \mathcal{U}_i$ where $\mathcal{M}_i \in \mathcal{F}$, i.e., some thrusters have failed, where we recall the thruster layout in Figure 2. For $k \geq k_{\text{fail}}$ we set $Q, M = 0$, so that the cost function does not aim at approaching the target.

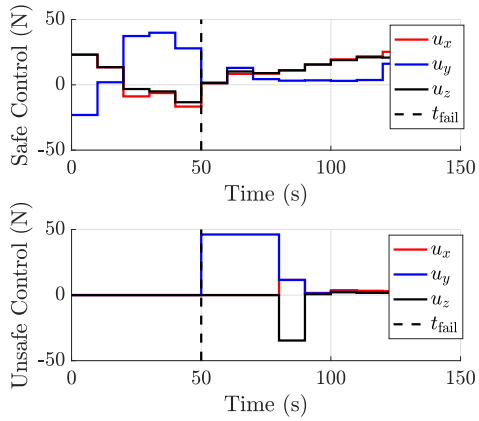
We compare the behavior of the *safe controller* (24) that enforces $\boldsymbol{x} \in \mathcal{X}_N^{\text{safe}}(\mathcal{P}_{\text{f}}, \mathcal{U})$ to a standard design, called the *unsafe controller*, that only enforces $\boldsymbol{x} \notin \mathcal{P}_{\text{f}}$. We consider two cases with different thruster failures, where in both cases $q = 1$, so that only one failure mode may occur.

In the first simulation, thruster τ_1 fails and $\mathcal{M}_2 = \mathcal{I} \setminus \{1\} \in \mathcal{F}$. Initially, $\boldsymbol{u}_k \in \mathcal{U}_1$, where $\mathcal{U}_1$ is the nominal control set. After the failure occurs, $\boldsymbol{u}_k \in \mathcal{U}_2$ for the rest of the simulation. The initial state in the target's Hill frame is $\boldsymbol{x}_0 = \begin{bmatrix} \boldsymbol{p}_0^{\mathsf{T}} & \boldsymbol{v}_0^{\mathsf{T}} \end{bmatrix}^{\mathsf{T}}$ where $\boldsymbol{p}_0^{\mathsf{T}} = \begin{bmatrix} -75.7 & 95.1 & -54.7 \end{bmatrix} \times 10^{-3}$ km and $\boldsymbol{v}_0^{\mathsf{T}} = \begin{bmatrix} 1.0 & -1.1 & 0.7 \end{bmatrix} \times 10^{-3}$ kms^{-1} for the simulations of both controllers. Figures 12a, 12b show the trajectories for the safe and unsafe controllers, and the corresponding control histories, respectively. The unsafe controller cannot avoid entering the exclusion zone, despite saturating the controls, while an avoidance maneuver is possible for the safe controller. The safe trajectory is more expensive in terms of delta-V, $\Delta V_{\text{safe}} = 5.8 \times 10^{-3}$ km/s, then the unsafe trajectory,

$\Delta V_{\text{unsafe}} = 2.8 \times 10^{-3}$ km/s.



(a) Rendezvous towards the terminal region (black) for safe (blue) and unsafe (red) controllers. The black circle and marks show the initial and failure states, respectively. Dashed and solid lines are states before and after propulsion failure, respectively.



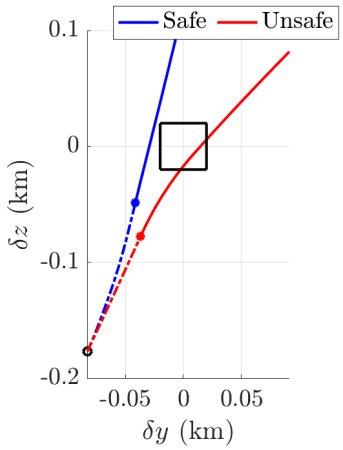
(b) Control histories for safe and unsafe controllers. Vertical dash line shows t_{fail}.

Figure 12: *Actively safe rendezvous*, comparison of the safe and unsafe controllers when only thruster τ_1 fails, i.e., $\mathcal{M}_2 = \mathcal{I} \setminus \{1\}$.

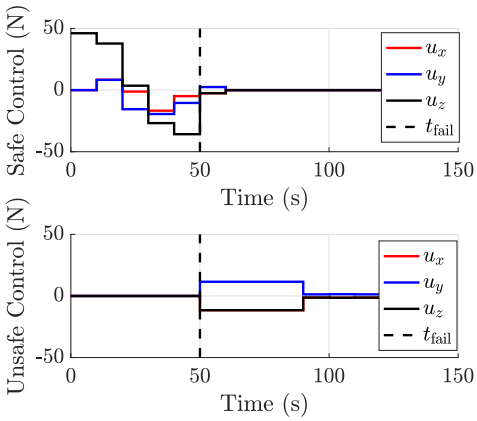
The second simulation shows the case when only thruster τ_8 remains functional after failure, i.e., $\mathcal{M}_3 = \{8\} \in \mathcal{F}$. After the failure occurs, $\boldsymbol{u}_k \in \mathcal{U}_3$, which is a line segment. The initial condition for both controllers is $\boldsymbol{x}_0 = \begin{bmatrix}\boldsymbol{p}_0^{\mathsf{T}} & \boldsymbol{v}_0^{\mathsf{T}}\end{bmatrix}^{\mathsf{T}}$ where $\boldsymbol{p}_0^{\mathsf{T}} = \begin{bmatrix}-32.8 & -83.0 & -177.1\end{bmatrix} \times 10^{-3}$ km and $\boldsymbol{v}_0^{\mathsf{T}} = \begin{bmatrix}0.3 & 0.9 & 2\end{bmatrix} \times 10^{-3}$ km/s. Figures 13a, 13b show the trajectories for the safe and unsafe controllers, and the corresponding control histories, respectively. Again, the unsafe controller cannot avoid entering the exclusion region, which the safe controller can. As previously noted, the price is increased propellant consumption, as for the safe controller, $\Delta V_{\text{safe}} = 1.8 \times 10^{-3}$ km/s, while for the unsafe controller, $\Delta V_{\text{unsafe}} = 1.0 \times 10^{-3}$ km/s.

C. Varying Initial Conditions

We show that initial conditions in the safe set admit abort maneuvers, while initial conditions outside do not. For simplicity and clarity, we consider a planar rendezvous, $\delta z, \delta \dot{z} = 0$, where the failure mode considered is $\mathcal{M}_3 = \{8\} \in \mathcal{F}$, that is, thrusters τ_1 through τ_7 simultaneously fail, at $k_{\text{fail}} = 0$, and as a consequence $\boldsymbol{u}_k \in \mathcal{U}_3$, for all $k \geq 0$. We generate random initial conditions $\boldsymbol{x}_0^{\text{safe,i}} \in \mathcal{X}_{N,1}^{\text{safe}}(\mathcal{P}_{\text{f}}, \mathcal{U}_3)$ and



(a) Rendezvous to the terminal set (black) for the safe (blue) and unsafe (red) controllers. The black circle and marks are the initial and failure states, respectively. Dashed and solid lines are states before and after propulsion failure, respectively.



(b) Control histories for the safe and unsafe controllers. Vertical dash line shows t_{fail}.

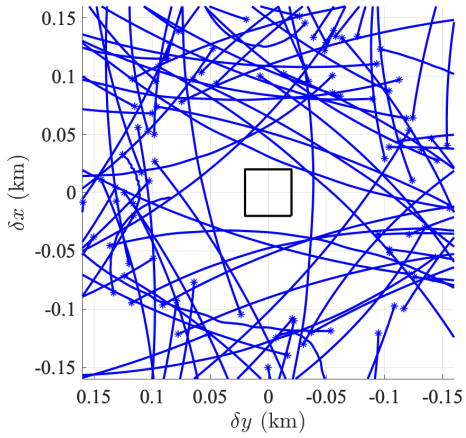
Figure 13: *Actively safe rendezvous*, comparison of the safe and unsafe controllers when thrusters τ_1–τ_7 fail, i.e., $\mathcal{M}_3 = \{8\}$.

$\boldsymbol{x}_0^{\text{unsafe,i}} \in \tilde{\mathcal{R}}_N(\mathcal{P}_{\text{f}}, \mathcal{U}_3, k_{\text{f}}) = \mathcal{X}_{N,1}^{\text{unsafe}}$ in a region around the target.

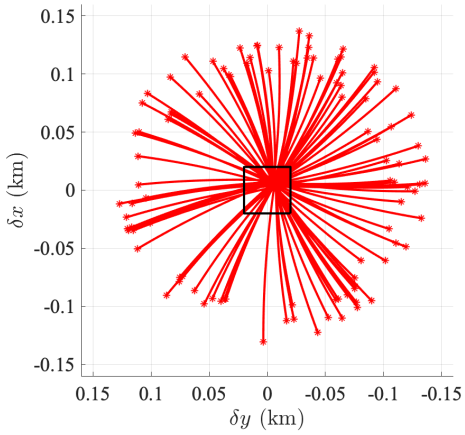
Figure 14a shows that for all of the initial conditions within the safe set an abort maneuver that avoids the terminal region can be found. Figure 14b shows that from initial conditions in the unsafe set $\tilde{\mathcal{R}}_N(\mathcal{P}_{\text{f}}, \mathcal{U}_3, k_{\text{f}})$, the unsafe controller that only aims at avoiding the terminal region, i.e., $\boldsymbol{x}_{j|k} \notin \mathcal{P}_{\text{f}}$, for all $j \in \mathbb{Z}_{[1,N_{\text{p}}]}$, cannot avoid the terminal region.

D. Full Mission Simulation: ISS Rendezvous

We consider a realistic mission scenario where the chaser has to rendezvous with a target in a circular low Earth orbit. In this scenario, the mission incorporates both passive and active safety in a sequence of phases. Initially, passive safety is required with respect to the AE. As the chaser gets closer to the AE, the next phase starts, where passive safety is maintained with respect to the KOS. Upon close proximity, the active safety phase starts. We consider a target representing the international space station (ISS) in a circular orbit with



(a) Trajectories from safe initial conditions, $\boldsymbol{x}_0 \in \mathcal{X}_{N,1}^{\text{safe}}(\mathcal{P}_\text{f}, \mathcal{U}_3)$. The terminal region $\mathcal{P}_\text{f}$ is avoided.



(b) Trajectories from multiple unsafe initial conditions $\boldsymbol{x}_0 \in \mathcal{X}_{N,1}^{\text{unsafe}}(\mathcal{P}_\text{f}, \mathcal{U}_3)$. The terminal region $\mathcal{P}_\text{f}$ cannot be avoided.

Figure 14: *Actively safe rendezvous*, trajectories from several initial conditions for the case when thrusters τ_1–τ_7 fail, i.e., $\mathcal{M}_3 = \{8\}$, highlighting unsafe set correctness.

orbital elements given in Section VI-A1. Active safety is maintained with respect to all thruster failure combinations, yielding $n_\text{F} = 255$ failure modes. Because the dynamics is LTI, $n_\text{s} = 2527$, which permits consideration of all the sets, while for the LTV case n_s would be much larger.

We consider the initial state for the relative equations of motion, $\boldsymbol{x}_0 = \begin{bmatrix}\boldsymbol{p}_0^\mathsf{T} & \boldsymbol{v}_0^\mathsf{T}\end{bmatrix}^\mathsf{T}$, where $\boldsymbol{p}_0^\mathsf{T} = \begin{bmatrix}0 & 5 & 0\end{bmatrix}$ km and $\boldsymbol{v}_0^\mathsf{T} = \begin{bmatrix}0 & 0 & 0\end{bmatrix}$ km/s. Figure 15 shows the rendezvous and highlights the mission phases. The leftmost green circle shows the initial state at the start of the trajectory segment, where passive safety is maintained with respect to $\mathcal{E}_\text{AE}$. Next, at $\delta y \approx 2$ km, the mission progresses to the next phase and passive safety is maintained with respect to $\mathcal{E}_\text{KOS}$. Then, the active abort-safety phase begins. Finally, the green circle closest to the origin shows the start of the final approach, i.e., where the chaser reaches the target.

Figure 16 shows that safety is maintained in the various phases because the chaser only enters the unsafe set of each phase after the next phase is initiated, i.e., after it has

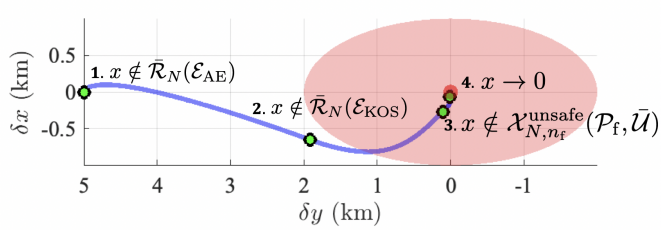


Figure 15: *Full rendezvous mission*, safe trajectory with annotated phases and corresponding safety specifications. Each phase begins at a green circle.

permission to advance to the next part of the mission. The transition times are shown by the black dashed vertical lines. Figure 17 shows the reaction of the controller to the phase changes as a consequence of the changing constraints.

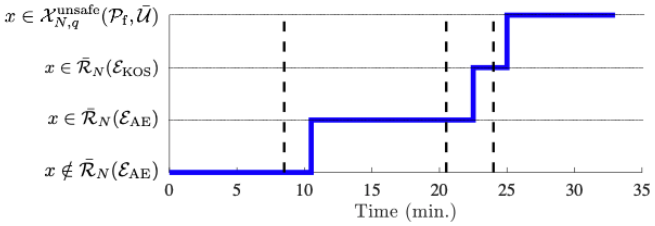


Figure 16: *Full rendezvous mission*. The trajectory enters the unsafe set of each phase only after the next phase has started.

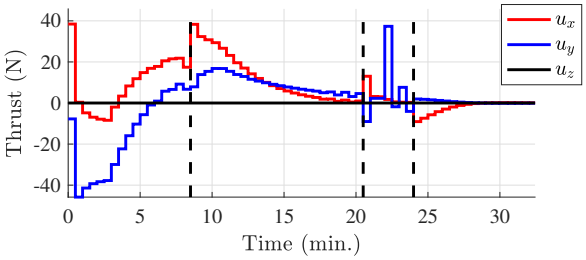


Figure 17: *Full rendezvous mission*, reaction of the control signal to the changing constraints due to the changing phases.

VII. Discussion and Future Work

In this paper we have developed a control policy for safe spacecraft rendezvous that guarantees the existence of passive or active abort trajectories that avoid the rendezvous target in the event of thruster failures. We used reachable sets to characterize the abort-safe region, and model predictive control to generate rendezvous trajectories that remain in such region. Our work shows how reachability methods, suggested for verifications in [19], may also be used to synthesize abort-safe controllers, including in the challenging case of active abort with post-failure residual thrust. A slightly counterintuitive step towards this is the use of control inputs as disturbances in the reachable set computations. The simulation results show effective spacecraft operation in a significant number of relevant scenarios, and show the trade-off between guarantees and required computational effort that may make the method

effective for on-board implementation on realistic spacecraft computing platforms [31].

Within the general approach proposed here, certain design choices related to set computations and control implementations were made due to the simplicity of exposition and due to practical implementation considerations for spacecraft with realistic specifications and limited computational capabilities. Indeed, the proposed approach can be extended to support more sophisticated techniques. The modeling error limitations of pointwise-in-time constraints, and sensitivity to perturbations could possibly be reduced by applying continuous-time nonlinear techniques for reachability [21], including Hamilton-Jacobi methods [27], perhaps at the price of larger computational burden or solver complexity in the MPC optimal control problem. The switching among the different mission phases, that here is externally controlled, may be addressed by means of state-triggered constraints [47]. Further extensions may involve handling practical implementation issues, such as the specifications of thrusters commonly deployed on spacecraft, which are often on-off in nature and have minimum impulse bit, and reducing the propellant consumption of safe rendezvous, see, [48] for an initial investigation.

Robustness guarantees of safe rendezvous with respect to realistic disturbances is also an important area of future investigation. While we showed that with the proposed method, even in the presence of orbital perturbations, the safety margin provided by the exclusion zones is usually enough to ensure avoidance of collision after failure, and that avoiding the exclusion zone is possible by inflating the unsafe sets, formal methods for guaranteeing robustness are of key importance. Beyond robustness to orbital perturbations, dynamics linearization, and time discretization, additional sources of errors include actuation errors and navigational uncertainty. Initial work on formalizing the set inflation and constraint tightening presented in Section V-D in the presence of such disturbances was recently introduced in [49] and is currently being evaluated in realistic simulation scenarios.

REFERENCES

[1] National Academies of Sciences, Engineering, and Medicine, *NASA Space Technology Roadmaps and Priorities Revisited*. Washington, DC: The National Academies Press, 2016.

[2] U. Eren, A. Prach, B. B. Koçer, S. V. Raković, E. Kayacan, and B. Açıkmeşe, "Model predictive control in aerospace systems: Current state and opportunities," *J. Guidance, Control, and Dynamics*, vol. 40, no. 7, pp. 1541–1566, 2017.

[3] E. D. Pasquale, "ATV Jules Verne: a step by step approach for in-orbit demonstration of new rendezvous technologies," in *SpaceOps Conference*, 2012.

[4] P. Miotto, "Designing and validating proximity operations rendezvous and approach trajectories for the cygnus mission," in *AIAA Guidance, Navigation, and Control Conference*, 2010.

[5] A. Flores-Abad, O. Ma, K. Pham, and S. Ulrich, "A review of space robotics technologies for on-orbit servicing," *Progress in Aerospace Sciences*, vol. 68, pp. 1–26, 2014.

[6] N. Murakami, S. Ueda, T. Ikenaga, M. Maeda, T. Yamamoto, H. Ikeda *et al.*, "Practical rendezvous scenario for transportation missions to cis-lunar station in earth-moon L2 Halo orbit," in *Int. Symp. Space Flight Dynamics*, 2015.

[7] N. T. Redd, "Bringing satellites back from the dead: Mission extension vehicles give defunct spacecraft a new lease on life - [news]," *IEEE Spectrum*, vol. 57, no. 8, pp. 6–7, 2020.

[8] L. S. Breger and J. P. How, "Safe trajectories for autonomous rendezvous of spacecraft," *J. Guidance, Control, and Dynamics*, vol. 31, no. 5, pp. 1478–1489, 2008.

[9] S. Di Cairano, H. Park, and I. Kolmanovsky, "Model predictive control approach for guidance of spacecraft rendezvous and proximity maneuvering," *Int. J. Robust and Nonlinear Control*, vol. 22, no. 12, pp. 1398–1427, 2012.

[10] E. Denenberg and P. Gurfil, "Debris avoidance maneuvers for spacecraft in a cluster," *J. Guidance, Control, and Dynamics*, vol. 40, no. 6, pp. 1428–1440, 2017.

[11] A. Richards, T. Schouwenaars, J. P. How, and E. Feron, "Spacecraft trajectory planning with avoidance constraints using mixed-integer linear programming," *J. Guidance, Control, and Dynamics*, vol. 25, no. 4, pp. 755–764, 2002.

[12] L. Palacios, M. Ceriotti, and G. Radice, "Close proximity formation flying via linear quadratic tracking controller and artificial potential function," *Adv. in Space Research*, vol. 56, no. 10, pp. 2167–2176, 2015.

[13] J. A. Starek, E. Schmerling, G. D. Maher, B. W. Barbee, and M. Pavone, "Fast, safe, propellant-efficient spacecraft motion planning under clohessy–wiltshire–hill dynamics," *J. Guidance, Control, and Dynamics*, vol. 40, no. 2, pp. 418–438, 2016.

[14] A. Weiss, C. Petersen, M. Baldwin, R. S. Erwin, and I. Kolmanovsky, "Safe positively invariant sets for spacecraft obstacle avoidance," *J. Guidance, Control, and Dynamics*, vol. 38, no. 4, pp. 720–732, 2015.

[15] W. Fehse, *Automated Rendezvous and Docking of Spacecraft*, ser. Cambridge Aerospace Series. Cambridge University Press, 2003.

[16] A. W. Koenig and S. D'Amico, "Robust and safe n-spacecraft swarming in perturbed near-circular orbits," *J. Guidance, Control, and Dynamics*, vol. 41, no. 8, pp. 1643–1662, 2018.

[17] M. Holzinger, J. DiMatteo, J. Schwartz, and M. Milam, "Passively safe receding horizon control for satellite proximity operations," in *IEEE Conf. Decision and Control*, 2008, pp. 3433–3440.

[18] M. Saponara, V. Barrena, A. Bemporad, E. Hartley, J. M. Maciejowski, A. Richards, A. Tramutola, and P. Trodden, "Model predictive control application to spacecraft rendezvous in mars sample return scenario," in *Progress in Flight Dynamics, GNC, and Avionics*. EDP Sciences, 2013, vol. 6, pp. 137–158.

[19] N. Chan and S. Mitra, "Verifying safety of an autonomous spacecraft rendezvous mission," in *Int. Work. of Applied Verification of Continuous and Hybrid Systems*, G. Frehse and M. Althoff, Eds., vol. 48, 2017, pp. 20–32.

[20] M. Althoff, S. Bak, Z. Bao, M. Forets, G. Frehse, D. Freire, N. Kochdumper, Y. Li, S. Mitra, R. Ray, C. Schilling, S. Schupp, and M. Wetzlinger, "Continuous and hybrid systems with linear continuous dynamics," in *Int. Work. of Applied Verification of Continuous and Hybrid Systems*, vol. 74, 2020, pp. 16–48.

[21] L. Geretti, J. A. D. Sandretto, M. Althoff, L. Benet, A. Chapoutot, X. Chen, P. Collins, M. Forets, D. Freire, F. Immler, N. Kochdumper, D. P. Sanders, and C. Schilling, "Continuous and hybrid systems with nonlinear dynamics," in *Int. Work. of Applied Verification of Continuous and Hybrid Systems*, vol. 74, 2020, pp. 49–75.

[22] C. Zagaris and M. Romano, "Reachability analysis of planar spacecraft docking with rotating body in close proximity," *J. Guidance, Control, and Dynamics*, vol. 41, no. 6, pp. 1416–1422, 2018.

[23] B. HomChaudhuri, M. Oishi, M. Shubert, M. Baldwin, and R. S. Erwin, "Computing reach-avoid sets for space vehicle docking under continuous thrust," in *IEEE Conf. Decision and Control*, 2016, pp. 3312–3318.

[24] J. D. Gleason, A. P. Vinod, and M. M. Oishi, "Lagrangian approximations for stochastic reachability of a target tube," *Automatica*, vol. 128, p. 109546, 2021.

[25] M. Shubert, M. Oishi, M. Baldwin, and R. S. Erwin, "Under-approximating reach-avoid sets for space vehicle maneuvering in the presence of debris," *IFAC*, vol. 51, no. 12, pp. 142–147, 2018.

[26] M. Althoff, O. Stursberg, and M. Buss, "Reachability analysis of nonlinear systems with uncertain parameters using conservative linearization," in *IEEE Conf. Decision and Control*, 2008, pp. 4042–4048.

[27] S. Bansal, M. Chen, S. Herbert, and C. J. Tomlin, "Hamilton-Jacobi reachability: A brief overview and recent advances," in *IEEE Conf. Decision and Control*, 2017, pp. 2242–2253.

[28] M. J. Holzinger and D. J. Scheeres, "Reachability results for nonlinear systems with ellipsoidal initial sets," *IEEE Trans. on Aerospace and Electronic Systems*, vol. 48, no. 2, pp. 1583–1600, 2012.

[29] F. Blanchini and S. Miani, *Set-Theoretic Methods in Control*, 1st ed., 2007.

[30] F. Borrelli, A. Bemporad, and M. Morari, *Predictive Control for Linear and Hybrid Systems*. Cambridge University Press, 2017.

[31] S. Di Cairano and I. V. Kolmanovsky, "Real-time optimization and model predictive control for aerospace and automotive applications," in *American Control Conf.*, 2018, pp. 2392–2409.

[32] M. Althoff, C. Le Guernic, and B. H. Krogh, "Reachable set computation for uncertain time-varying linear systems," in *Int. Conf. on Hybrid Systems: Computation and Control*, 2011, pp. 93–102.

[33] A. Weiss, M. Baldwin, R. S. Erwin, and I. Kolmanovsky, "Model predictive control for spacecraft rendezvous and docking: Strategies for handling constraints and case studies," *Trans. Control Systems Technology*, vol. 23, no. 4, pp. 1638–1647, 2015.

[34] B. P. Malladi, S. Di Cairano, and A. Weiss, "Nonlinear model predictive control of coupled rotational-translational spacecraft relative motion," in *American Control Conf.*, 2019, pp. 3581–3586.

[35] F. Gavilan, R. Vazquez, and E. F. Camacho, "Chance-constrained model predictive control for spacecraft rendezvous with disturbance estimation," *Control Eng. Practice*, vol. 20, no. 2, pp. 111–122, 2012.

[36] M. Mammarella, M. Lorenzen, E. Capello, H. Park, F. Dabbene, G. Guglieri, M. Romano, and F. Allgöwer, "An offline-sampling smpc framework with application to autonomous space maneuvers," *IEEE Trans. on Control Systems Technology*, vol. 28, no. 2, pp. 388–402, 2020.

[37] M. Mammarella, E. Capello, H. Park, G. Guglieri, and M. Romano, "Tube-based robust model predictive control for spacecraft proximity operations in the presence of persistent disturbance," *Aerospace Science and Technology*, vol. 77, pp. 585–594, 2018.

[38] D. Aguilar Marsillach, S. Di Cairano, and A. Weiss, "Fail-safe rendezvous control on elliptic orbits using reachable sets," in *American Control Conf.*, 2020, pp. 4920–4925.

[39] ——, "Abort-safe spacecraft rendezvous in case of partial thrust failure," in *IEEE Conf. Decision and Control*, 2020, pp. 1490–1495.

[40] J. L. Junkins and H. Schaub, *Analytical mechanics of space systems*. American Institute of Aeronautics and Astronautics, 2009.

[41] H. Curtis, *Chapter 7 - Relative Motion and Rendezvous, Orbital Mechanics for Engineering Students*, 3rd ed. Butterworth-Heinemann, 2013.

[42] J. B. Rawlings and D. Q. Mayne, *Model Predictive Control: Theory and Design*. Nob Hill Pub., 2009.

[43] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

[44] M. Herceg, M. Kvasnica, C. Jones, and M. Morari, "Multi-Parametric Toolbox 3.0," in *European Control Conference*, 2013, pp. 502–510.

[45] J. A. Andersson, J. Gillis, G. Horn, J. B. Rawlings, and M. Diehl, "CasADi – A software framework for nonlinear optimization and optimal control," *Mathematical Programming Computation*, vol. 11, pp. 1–36, 2019.

[46] L. T. Biegler and V. M. Zavala, "Large-scale nonlinear programming using ipopt: An integrating framework for enterprise-wide dynamic optimization," *Computers & Chemical Eng.*, vol. 33, no. 3, pp. 575–582, 2009.

[47] M. Szmuk, T. P. Reynolds, and B. Açıkmeşe, "Successive convexification for real-time six-degree-of-freedom powered descent guidance with state-triggered constraints," *J. Guidance, Control, and Dynamics*, vol. 43, no. 8, pp. 1399–1413, 2020.

[48] D. A. Marsillach, S. Di Cairano, U. Kalabić, and A. Weiss, "Fail-safe spacecraft rendezvous on near-rectilinear halo orbits," in *American Control Conf.*, 2021, pp. 2980–2985.

[49] A. P. Vinod, S. Di Cairano, and A. Weiss, "Abort-safe spacecraft rendezvous under stochastic actuation and navigation uncertainty," in *IEEE Conf. Decision and Control*, 2021.

Daniel Aguilar-Marsillach received the B.Eng. (first-class) degree in mechanical engineering at the University of Manchester, UK, in 2015, the M.S. degree in aerospace engineering at the Georgia Institute of Technology, Atlanta, GA, USA, in 2017, and the Ph.D. at the University of Colorado Boulder, CO, USA, in 2021. He is currently a researcher with the Perception, Planning, and Decision Systems Group at General Motors Research & Development in Warren, MI, USA. The work herein was completed while interning with Mitsubishi Electric Research Laboratories and during his Ph.D.

Stefano Di Cairano received the master's (Laurea) and the Ph.D. degrees in information engineering from the University of Siena, Siena, Italy, in 2004 and 2008, respectively. From 2008 to 2011, he was with Powertrain Control R&A, Ford Research, and Advanced Engineering, Dearborn, MI, USA. Since 2011, he has been with Mitsubishi Electric Research Laboratories, Cambridge, MA, USA, where he is currently a Distinguished Research Scientist, and a Senior Team Leader. He has authored/coauthored more than 200 peer reviewed papers in journals and conference proceedings and 60 patents. His research is on optimization-based control strategies for complex mechatronic systems, in automotive, factory automation, transportation, and aerospace. His research interests include model predictive control, constrained control, particle filtering, hybrid systems, optimization. Dr. Di Cairano was the Chair of the IEEE CSS Technical Committee on Automotive Controls and of the IEEE CSS Standing Committee on Standards. He was an Associate Editor of the IEEE Transactions on Control Systems Technology, and is the inaugural Chair of the IEEE CSS Technology Conferences Editorial Board.

Avishai Weiss received the B.S. degree in electrical engineering and the M.S. degree in aeronautics and astronautics from Stanford University, Stanford, CA, USA, in 2008 and 2009, respectively, and the Ph.D. degree in aerospace engineering from the University of Michigan, Ann Arbor, MI, USA, in 2013. He is currently a Principal Research Scientist at Mitsubishi Electric Research Laboratories (MERL), Cambridge, MA, USA. His main research interests and contributions are in the areas of spacecraft orbital and attitude control, constrained control, model predictive control, motion planning, and time-varying systems, in which he has authored more than 75 peer-reviewed papers and patents.