Abort-Safe Spacecraft Rendezvous in case of Partial Thrust Failure

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

TR2020-175 December 16, 2020

Abstract

In this paper a spacecraft rendezvous policy is developed that yields safe rendezvous trajectories under various thruster failure scenarios. The policy makes use of polytopic robust backwards reachable sets to characterize the state-space that under a given thruster failure scenario would lead to collision between a deputy and a chief spacecraft no matter the remaining available thrust. That is, this region of state-space is such that no feasible evasive abort maneuver exists for the given failure scenario. Abort-safety constraints are formulated as local hyperplanes separating the deputy spacecraft and the unsafe state-space. These constraints are incorporated in a model predictive control-based online trajectory generation scheme in order to guide the deputy to rendezvous with its chief through an inherently safe approach. Simulations demonstrate the effectiveness of the safety constraints in altering a nominally unsafe rendezvous to one that is abort-safe.

IEEE Conference on Decision and Control (CDC)

Abort-Safe Spacecraft Rendezvous in case of Partial Thrust Failure

Daniel Aguilar Marsillach[1], Stefano Di Cairano[2], Avishai Weiss[3]

***Abstract*— In this paper a spacecraft rendezvous policy is developed that yields safe rendezvous trajectories under various thruster failure scenarios. The policy makes use of polytopic robust backwards reachable sets to characterize the state-space that under a given thruster failure scenario would lead to collision between a deputy and a chief spacecraft no matter the remaining available thrust. That is, this region of state-space is such that no feasible evasive abort maneuver exists for the given failure scenario. Abort-safety constraints are formulated as local hyperplanes separating the deputy spacecraft and the unsafe state-space. These constraints are incorporated in a model predictive control-based online trajectory generation scheme in order to guide the deputy to rendezvous with its chief through an inherently safe approach. Simulations demonstrate the effectiveness of the safety constraints in altering a nominally unsafe rendezvous to one that is abort-safe.**

I. INTRODUCTION

Spacecraft rendezvous approaches must often guarantee passive safety for a pre-specified amount of time [1], wherein a spacecraft, called the deputy, avoids collision with a target spacecraft, called the chief, in the event of a complete loss of control. This paper expands upon prior work on passive safety [2] to consider the scenario of partial loss of control, in which the deputy's remaining functional thrusters may be engaged to safely avoid collision. Allowing for active abort maneuvers relaxes the safety requirements as compared to the passive case, permitting trajectories pertinent to the final phase of rendezvous.

Classically, when a deputy spacecraft deviates significantly from its nominal approach in proximity to the chief and its current trajectory is not passively safe, a predetermined active collision avoidance maneuver (CAM) must be engaged [1]. However, depending on approach trajectory and extent of partial thruster failure, a CAM may not be possible. To address this, in [3] a method is proposed for online generation of nominal trajectories that, in the event of partial thruster failure, can switch to a safe input sequence to avoid collision. To guarantee the existence of such a sequence, the method expands the size of the optimization problem by solving for both nominal and abort sequences concurrently given an initial condition for which the method is feasible.

In this work, we formally characterize the region of state-space in which feasible abort maneuvers exist by using robust backwards reachable sets. The concept of reachability has previously been used for spacecraft relative proximity operations and docking. While spacecraft relative motion dynamics are nonlinear and various reachability techniques have been developed for nonlinear systems [4]–[6], spacecraft relative proximity operations generally occur in the linear regime and as such most spacecraft applications do not make use of nonlinear reachability. In [7], backwards reachable sets using the linear time-invariant (LTI) Clohessey-Wiltshire (CW) equations of relative motion are used to determine successful docking initial conditions. The work in [8] computes reach-avoid sets to obtain trajectories that reach the chief while avoiding a line-of-sight set, whereas [9] focuses on using Lagrangian methods to compute stochastic reach-avoid sets. Under-approximated reach-avoid sets are also computed in [10] to ensure a satellite maneuvers to a new location while avoiding debris. Finally, in our prior work [2], we generate passively safe rendezvous trajectories on elliptic orbits by avoiding backwards reachable sets that characterize the unsafe regions of state-space that, in the event of total thruster failure, would lead to a collision between a deputy spacecraft and its chief.

We now expand upon [2] to generate rendezvous trajectories with a guarantee that, in the event of various thrust failure scenarios along these trajectories, safe abort maneuvers exist. In order to achieve this guarantee, offline we compute polytopic robust backwards reachable sets over a time interval (RBRSI) from the chief that, for a given thrust failure scenario, characterize the unsafe state-space that would lead to collision no matter the remaining available thrust. Failure scenarios are encoded in admissible control sets and are treated as if the control was a disturbance, that is, the RBRSI are computed for all possible controls in the admissible set. Thus, these sets determine the regions of state-space for which no feasible evasive abort maneuvers exist. The union represents the unsafe state-space that is to be avoided in order for there to exist a feasible abort maneuver under the thrust failure scenario. As avoiding a union of polytopes results in nonconvex constraints, we convexify by computing a halfspace that covers a local region of unsafe sets, which we use as a safety constraint for the online trajectory generation process.

We develop a model predictive control (MPC) policy that enforces the constraints, thus ensuring that the spacecraft remains outside of the union of RBRSI , and hence guaranteeing the existence of abort maneuvers for the given thrust failure scenario. MPC has previously been applied for spacecraft rendezvous under nominal propulsion conditions, see [11]–[15] and references therein.

[1] D. Aguilar Marsillach is with the Department of Aerospace Engineering Sciences at the University of Colorado - Boulder, Boulder, CO 80303, USA. Email: d.aguilar@colorado.edu. He interned at MERL during the development of this work.

[2,3] A. Weiss and S. Di Cairano are with Mitsubishi Electric Research Laboratories, Cambridge, MA 02139, USA. Emails: {weiss,dicairano}@merl.com

A. *Preliminaries and Notation*

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 $\boldsymbol{\omega}_{\mathrm{x/y}}$. $\mathbb{R}^n$ denotes the n-dimensional Euclidean space. Given a matrix $A \in \mathbb{R}^{n\times n}$, $\det(A)$ denotes its determinant. I_n denotes the n-dimensional identity matrix. The special orthogonal group $\mathrm{SO}(3) = \{R \in \mathbb{R}^{3\times 3} : \det(R) = +1, R^\top R = I_3\}$. The matrix $C_{\mathrm{x}}^{\mathrm{y}} \in \mathrm{SO}(3)$ denotes the direction cosine matrix (DCM) that transforms vectors in $\mathrm{F_x}$ to $\mathrm{F_y}$. 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 ${}^{\mathrm{x}}(\cdot)$, any unit vector is denoted by $\hat{(\cdot)}$, and the euclidean norm of a vector is given by $||\cdot||$. We denote the value of a signal at a discrete time t as $\boldsymbol{x}_t$, and $\boldsymbol{x}_{k|t}$ denotes the value of $\boldsymbol{x}$ predicted k steps ahead from t. For two sets, $\mathcal{X}$, $\mathcal{Y}$, the Minkowski sum is denoted by $\mathcal{X} \bigoplus \mathcal{Y}$, the complement by $\mathcal{X}^{\mathrm{c}}$, the set of subsets as $2^{\mathcal{X}}$, and the cardinality as $|\mathcal{X}|$. The hyperplane representation (H-representation) of the polyhedron $\mathcal{P} \subseteq \mathbb{R}^n$ is $\mathcal{P}(H, \boldsymbol{k}) = \{\boldsymbol{x} \in \mathbb{R}^n : H\boldsymbol{x} \leq \boldsymbol{k}\}$ with $H \in \mathbb{R}^{p\times n}$, $\boldsymbol{k} \in \mathbb{R}^p$. Given a matrix H, $[H]_i$ denotes the i^{th} row of the matrix.

II. Model and Problem Statement

Consider a chief and a deputy in orbit around a central body, e.g., Earth. The frame $\mathrm{F_e}$ is the Earth-Centered Inertial (ECI) frame, e is an unforced particle, and it is assumed that e is collocated with the center of the Earth. The deputy's center of mass is denoted by d and has a deputy-fixed frame $\mathrm{F_d}$. The chief's center of mass is denoted by c and has a chief-fixed frame $\mathrm{F_c}$. The chief's orbit frame $\mathrm{F_o} = \{\hat{\boldsymbol{\imath}}_r, \hat{\boldsymbol{\imath}}_\theta, \hat{\boldsymbol{\imath}}_h\}$ is Hill's frame with radial, along-track, and cross-track basis vectors [16]. The deputy is controlled and assumed to be aligned with the chief's orbital frame $\mathrm{F_o}$, i.e. $\boldsymbol{\omega}_{\mathrm{d/o}} = \mathbf{0}$.

We denote $\boldsymbol{r}_{\mathrm{c}}, \boldsymbol{r}_{\mathrm{d}}$ as the position vectors of the chief and deputy centers of mass relative to the center of Earth, $m_{\mathrm{c}}, m_{\mathrm{d}}$ are the chief and deputy masses, and $\boldsymbol{f}_{\mathrm{c}}$, $\boldsymbol{f}_{\mathrm{d}}$ represent perturbing forces acting on the chief and deputy, respectively. In this study, the chief is assumed to follow Keplerian motion, i.e. $\boldsymbol{f}_{\mathrm{c}} = \mathbf{0}$, and we neglect orbital perturbations on the deputy i.e. $\boldsymbol{f}_{\mathrm{d}} = \boldsymbol{u}$. Given a chief and deputy spacecraft, the position of the deputy relative to the chief is given by $\boldsymbol{\rho} = \boldsymbol{r}_{\mathrm{d}} - \boldsymbol{r}_{\mathrm{c}}$. The nonlinear equations of relative motion can be linearized about the chief's trajectory and resolved in the chief's orbital frame $\mathrm{F_o}$, yielding [16], [17]

$$\begin{aligned}
\delta\ddot{x} - \left(\frac{2\mu}{r_{\mathrm{c}}^3} + \frac{h^2}{r_{\mathrm{c}}^4}\right)\delta x + \left(\frac{2\boldsymbol{r}_{\mathrm{c}}'\cdot\boldsymbol{r}_{\mathrm{c}}}{r_{\mathrm{c}}^4}h\right)\delta y - \left(\frac{2h}{r_{\mathrm{c}}^2}\right)\delta\dot{y} &= \frac{u_x}{m_{\mathrm{c}}}, \\
\delta\ddot{y} + \left(\frac{\mu}{r_{\mathrm{c}}^3} - \frac{h^2}{r_{\mathrm{c}}^4}\right)\delta y - \left(\frac{2\boldsymbol{r}_{\mathrm{c}}'\cdot\boldsymbol{r}_{\mathrm{c}}}{r_{\mathrm{c}}^4}h\right)\delta x + \left(\frac{2h}{r_{\mathrm{c}}^2}\right)\delta\dot{x} &= \frac{u_y}{m_{\mathrm{c}}}, \\
\delta\ddot{z} + \left(\frac{\mu}{r_{\mathrm{c}}^3}\right)\delta z &= \frac{u_z}{m_{\mathrm{c}}},
\end{aligned} \tag{1}$$

where ${}^{\mathrm{o}}\boldsymbol{\rho} = \begin{bmatrix}\delta x & \delta y & \delta z\end{bmatrix}^\mathsf{T}$ is the relative position resolved in $\mathrm{F_o}$, $r_{\mathrm{c}} = \|\boldsymbol{r}_{\mathrm{c}}\|$, $h = \|\boldsymbol{r}_{\mathrm{c}} \times \boldsymbol{r}_{\mathrm{c}}'\|$ is the inertial specific angular momentum of the chief's orbit, and $\boldsymbol{u} = \begin{bmatrix}u_x & u_y & u_z\end{bmatrix}^\mathsf{T}$ is the control input applied to the deputy resolved in $\mathrm{F_o}$. As r_{c} and h vary along the orbit, the equations of motion (1) result in the linear-time varying system

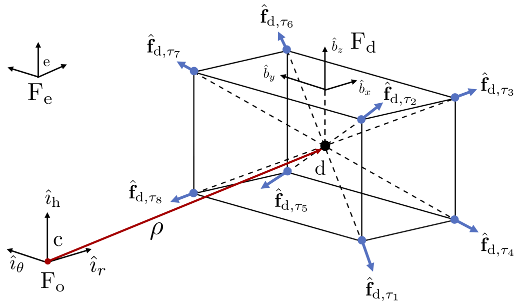

$\hat{\mathbf{f}}_{\mathrm{d},\tau_6}$
$\hat{\mathbf{f}}_{\mathrm{d},\tau_7}$
$\hat{b}_z$
$\mathrm{F_d}$
e
$\mathrm{F_e}$
$\hat{b}_y$
$\hat{b}_x$
$\hat{\mathbf{f}}_{\mathrm{d},\tau_2}$
$\hat{\mathbf{f}}_{\mathrm{d},\tau_3}$
d
$\hat{\mathbf{f}}_{\mathrm{d},\tau_8}$
$\hat{\mathbf{f}}_{\mathrm{d},\tau_5}$
$\hat{\imath}_{\mathrm{h}}$
c
ρ
$\hat{\imath}_\theta$
$\hat{\imath}_r$
$\mathrm{F_o}$
$\hat{\mathbf{f}}_{\mathrm{d},\tau_4}$
$\hat{\mathbf{f}}_{\mathrm{d},\tau_1}$

Fig. 1: Deputy model and thruster configuration.

$$\dot{\boldsymbol{x}}(t) = A(t)\boldsymbol{x}(t) + B\boldsymbol{u}(t), \tag{2}$$

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 this work we consider a discrete time formulation of (2)

$$\boldsymbol{x}_{t+1} = \boldsymbol{f}(t, \boldsymbol{x}_t, \boldsymbol{u}_t) = A_\Delta(t)\boldsymbol{x}_t + B_\Delta(t)\boldsymbol{u}_t, \tag{3}$$

with sampling period Δt, which is assumed to be small enough not to lose significant behavior between samples.

A. *Thrusters and Failure Modes*

The deputy, depicted in Figure 1, has eight thrusters rigidly fixed with respect to $\mathrm{F_d}$ that provide thrust in lines coincident with their positions and the center of mass of the spacecraft such that they do not impart any torque. The total force applied to the deputy resolved in $\mathrm{F_o}$ is

$$\boldsymbol{u} = {}^{\mathrm{o}}\boldsymbol{f}_{\mathrm{d}} = \sum_{j=1}^{8} \gamma_j {}^{\mathrm{o}}\hat{\boldsymbol{f}}_{\mathrm{d},\tau_j}, \tag{4}$$

where $\gamma_j \in [0, u_{\mathrm{m},j}]$ is the magnitude of thruster j, $u_{\mathrm{m},j}$ is the maximum thrust of thruster j, ${}^{\mathrm{o}}\hat{\boldsymbol{f}}_{\mathrm{d},\tau_j} = C_{\mathrm{d}}^{\mathrm{o}}\, {}^{\mathrm{d}}\hat{\boldsymbol{f}}_{\mathrm{d},\tau_j}$ is the fixed thrust direction of thruster j resolved in $\mathrm{F_o}$, and $C_{\mathrm{d}}^{\mathrm{o}} = I_3$ is the DCM that transforms a vector in $\mathrm{F_d}$ to $\mathrm{F_o}$, where we recall the assumption that the deputy is aligned with the chief's orbital frame.

In the course of executing a rendezvous maneuver, any number of thrusters may fail. Given the set of thruster indices $\mathcal{I} = \{1, 2, \ldots, 8\}$, the set of working thruster combinations is $\mathcal{M} = 2^{\mathcal{I}}$, $n_F = |\mathcal{M}|$. The set $\mathcal{M}_i \in \mathcal{M}$, $i \in \{1, \ldots, n_F\}$, denotes a specific set of functional thrusters, also called a thrust mode. $\mathcal{M}_i = \mathcal{I}$ indicates nominal operation of all thrusters, and $\mathcal{M}_i = \emptyset$ indicates total loss of control. The set of all possible failure modes is $\mathcal{FM} = \mathcal{M} \setminus \mathcal{I}$. The admissible control set $\mathcal{U}_i$ associated with thrust mode $\mathcal{M}_i \in \mathcal{M}$ is given by

$$\mathcal{U}_i = \bigoplus_{j\in\mathcal{M}_i}^{|\mathcal{M}_i|} \{\gamma_j {}^{\mathrm{o}}\hat{\boldsymbol{f}}_{\mathrm{d},\tau_j} : \gamma_j \in [0, u_{\mathrm{m},j}]\}. \tag{5}$$

B. Problem Statement

A compact target set $\mathcal{S}_f$ fixed in the orbital frame F_o is given, that includes the origin and where the extension along the position dimensions over-approximates the chief's physical geometry, and the extension along the velocity dimensions spans the deputy's admissible operational velocities. The set $\mathcal{S}_f$ defines a region in state-space that the deputy must avoid in the event of partial thruster failure. The objective of the abort-safe spacecraft rendezvous problem is for the deputy to approach the chief in a manner that, in the event of a thruster failure $\mathcal{M}_i \in \mathcal{FM}$ at a generic discrete time instant t_{fail}, there exists an N step abort sequence such that the deputy does not enter $\mathcal{S}_f$ for $t \in [t_{\text{fail}}, t_{\text{fail+N}}]$, i.e. there exists $\boldsymbol{u}_{t_{\text{fail}}}, \ldots, u_{t_{\text{fail}}+N-1} \in \mathcal{U}_i$ such that $\boldsymbol{x}_t \notin \mathcal{S}_f$ for all discrete times $t \in [t_{\text{fail}}, t_{\text{fail+N}}]$.

III. Robust Reachable Sets and Abort Safety

We enforce abort safety by maintaining the deputy vehicle outside of the unsafe region of state-space, that is, the region where if a failure occurs, a safe abort does not exist ie. a collision cannot be avoided. We determine such region by the robust backwards reachable sets (RBRS) of the target set with respect to the input set, that is the set of states that will enter the target set regardless of the inputs. Thus, when the failure occurs and the state is in the RBRS, no admissible control exists to avoid collision.

Definition 1: Given $\boldsymbol{x}_{t+1} = \boldsymbol{f}(t, \boldsymbol{x}_t, \boldsymbol{u}_t)$, where $\boldsymbol{u} \in \mathcal{U}$, and final time t_f, the N-step robust backward reachable set $\mathcal{R}_b(N; \mathcal{S}_f, \mathcal{U}, t_f)$ of target region $\mathcal{S}_f \subseteq \mathbb{R}^n$ is

$$\begin{aligned} &\mathcal{R}_b(0; \mathcal{S}_f, \mathcal{U}, t_f) = \mathcal{S}_f, \\ &\mathcal{R}_b(j; \mathcal{S}_f, \mathcal{U}, t_f) = \{\boldsymbol{x} \in \mathbb{R}^n : \\ &\qquad \boldsymbol{f}(t_f - j, \boldsymbol{x}, \boldsymbol{u}) \in \mathcal{R}_b(j-1; \mathcal{S}_f, \mathcal{U}, t_f), \forall \boldsymbol{u} \in \mathcal{U}\}. \end{aligned} \tag{6}$$

Here the RBRS is the set of initial conditions at time $t_0 = t_f - N$ from which the deputy will not be able to avoid collision at time t_f, regardless of the admissible control sequence applied.

Definition 2: The robust backwards reachable set over the time interval $[t_0, t_f]$ (RBRSI), where $t_0 = t_f - N$, is the union of the j-steps RBRS,

$$\mathcal{R}_N(\mathcal{S}_f, \mathcal{U}, t_f) = \bigcup_{j=0}^{N} \mathcal{R}_b(j; \mathcal{S}_f, \mathcal{U}, t_f). \tag{7}$$

The RBRSI denotes the set of states $\bar{\boldsymbol{x}}$ for which there exists $t \in [t_0, t_f]$, such that from $\boldsymbol{x}(t) = \bar{\boldsymbol{x}}$, the deputy will not be able to avoid collision at time t_f, regardless of the admissible control sequence applied.

Next, we account for changing final time, considering that the orbit, and hence the time-varying system, is periodic. To this end the orbit-RBRSI is the union of the RBRSI (7) for t_f that varies along one orbit

$$\bar{\mathcal{R}}_N(\mathcal{S}_f, \mathcal{U}) = \bigcup_{t_f = t_p + 1}^{2t_p} \mathcal{R}_N(\mathcal{S}_f, \mathcal{U}, t_f), \tag{8}$$

where t_p is the orbital period, and we assumed $N < t_p$ due to the type of spacecraft maneuver we target.

By taking the union of the RBRSI for changing final time around one orbit, (8) contains sets of states for which there exists a time in the chief's periodic orbit such that a collision will necessarily occur after at most N steps, $\bigcup_{j=0}^{N} \mathcal{R}_b(j; \mathcal{S}_f, \mathcal{U}, t_0 + j)$.

Remark 1: We arrive at the construction of $\bar{\mathcal{R}}_N(\mathcal{S}_f, \mathcal{U})$ "backwards," by fixing first the final time and considering all initial times within N-steps in (7), and then considering all final times within the orbit in (8). We did that to stay closer to the definition and computation of RBRS, which are backwards in time.

A. Case of Polytopic Target Set and LTV Dynamics

When the dynamics are linear as in (2) and the target set $\mathcal{S}_f$ is a polytope, the RBRS is also a polytope and is computed by solving linear programs [18]. Consider the target set $\mathcal{S}_f = \mathcal{P}(H_f, \boldsymbol{k}_f)$. Let the j-steps RBRS from final time t_f be $\mathcal{R}_b(j; \mathcal{S}_f, \mathcal{U}, t_f) = \mathcal{P}(H_j, \boldsymbol{k}_j)$, the $j+1$-steps RBRS is $\mathcal{R}_b(j+1; \mathcal{S}_f, \mathcal{U}, t_f) = \{\boldsymbol{x} \in \mathbb{R}^n : \ H_{j+1}\boldsymbol{x} \leq \boldsymbol{k}_{j+1}\}$, where

$$H_{j+1} = H_j A_\Delta(t_f - (j+1)), \tag{9a}$$

$$[\boldsymbol{k}_{j+1}]_i = \min_{\boldsymbol{u} \in \mathcal{U}} \ [\boldsymbol{k}_j]_i - [H_j]_i B_\Delta(t_f - (j+1))\boldsymbol{u}. \tag{9b}$$

In practice, additional linear programs to the ones in (9b) are solved to remove redundant hyperplanes for obtaining a minimal representation of $\mathcal{P}(H_j, \boldsymbol{k}_j)$.

When the RBRS is computed for all thrusters failed, i.e, $\mathcal{M}_i = \emptyset$, it becomes the set of passively unsafe states, i.e. initial conditions for which free-drift trajectories enter $\mathcal{S}_f$. This is similar to [2] where, however, ellipsoids are used instead of polyhedra.

B. Abort-Safe Sets

Consider a time interval $[t_0, t_f]$, and a target set $\mathcal{S}_f$ constant in such interval. Given the state at an initial time t_0, the state at any time $t > t_0$ is found using

$$\boldsymbol{x}_t = \Phi(t, t_0)\boldsymbol{x}_0 + \mathcal{C}\tilde{\boldsymbol{u}}, \tag{10}$$

where $\mathcal{C}$ is the controllability matrix of the LTV system, $\tilde{\boldsymbol{u}}^\mathsf{T} = \begin{bmatrix} \boldsymbol{u}_{t-1}^\mathsf{T} & \ldots & \boldsymbol{u}_{t_0}^\mathsf{T} \end{bmatrix}$, and $\Phi(t, t_0) = A_\Delta(t)A_\Delta(t-1)\cdots A_\Delta(t_0)$ is the t_0-to-t transition matrix. For the sake of notation let

$$\boldsymbol{x}_t = \boldsymbol{\phi}(t; \boldsymbol{x}_0, \tilde{\boldsymbol{u}}, t_0), \tag{11}$$

where $\tilde{\boldsymbol{u}} \in \mathcal{U}^h$, and, with a little abuse of notation, $h \geq t - t_0$, i.e., we may include more inputs in $\tilde{\boldsymbol{u}}$ even though the ones with indexes $j > t-1$ have no impact on $\boldsymbol{x}_t$. Letting $t_f - t_0 = N$, we define the safe set $\mathcal{X}_N^{\text{safe}}$ as the set of initial conditions that can be made to not collide with $\mathcal{S}_f$ within the desired interval $\mathcal{X}_N^{\text{safe}} = \{\boldsymbol{x} \in \mathbb{R}^n : \ \exists \tilde{\boldsymbol{u}} \in \mathcal{U}^N, \ \boldsymbol{\phi}(t; \boldsymbol{x}_0, \tilde{\boldsymbol{u}}, t_0) \notin \mathcal{S}_f, \ \forall t \in [t_0, t_f]\}$.

Proposition 1: Let $\boldsymbol{x}_0 \in \bar{\mathcal{R}}_N(\mathcal{S}_f, \mathcal{U})^\mathrm{c}$. Then, for any t_0 and $t_f = t_0 + N$, there exists $\tilde{\boldsymbol{u}} \in \mathcal{U}^N$, such that $\boldsymbol{\phi}(t; \boldsymbol{x}_0, \tilde{\boldsymbol{u}}, t_0) \notin \mathcal{S}_f$, for all $t \in [t_0, t_f]$. Hence,

$$\mathcal{X}_N^{\text{safe}} = \bar{\mathcal{R}}_N(\mathcal{S}_f, \mathcal{U})^\mathrm{c}. \tag{12}$$

Proof: By construction (7), (8), $\bar{\mathcal{R}}_N(\mathcal{S}_f,\mathcal{U})$, contains all the initial conditions $\boldsymbol{x}_0$ such that for all $\tilde{\boldsymbol{u}} \in \mathcal{U}^N$ there exists $t \in [t_0, t_0+N]$ such that $\boldsymbol{\phi}(t;\boldsymbol{x}_0,\tilde{\boldsymbol{u}},t_0) \ \in \mathcal{S}_f$. The properties of the complement $\bar{\mathcal{R}}_N(\mathcal{S}_f,\mathcal{U})^{\mathrm{c}}$ are obtained by negating the properties of $\bar{\mathcal{R}}_N(\mathcal{S}_f,\mathcal{U})$. Thus, $\bar{\mathcal{R}}_N(\mathcal{S}_f,\mathcal{U})^{\mathrm{c}}$ contains the initial conditions $\boldsymbol{x}_0$ such that there exists $\tilde{\boldsymbol{u}} \in \mathcal{U}^N$ such that for all $t \in [t_0, t_f]$, $\boldsymbol{\phi}(t;\boldsymbol{x}_0,\tilde{\boldsymbol{u}},t_0) \ \notin \mathcal{S}_f$, which is the desired safety condition. The validity for any t_0 is due to (6) and to including in (8) the RBRSI for all $t_f \in [t_p+1, 2t_p]$, which covers all the time instants by considering that the LTV system is periodic with period t_p. Thus, $\mathcal{X}_N^{\mathrm{safe}} = \bar{\mathcal{R}}_N(\mathcal{S}_f,\mathcal{U})^{\mathrm{c}}$. ■

Due to the definition of $\mathcal{X}_N^{\mathrm{safe}}$, if the state is kept inside it, the existence of a control sequence that avoids the set $\mathcal{S}_f$ in any interval $[t_0, t_0+N]$ is guaranteed.

IV. Abort-Safe Rendezvous Control

Next, we develop an abort-safe control policy that exploits the safe set (12) and its complement (8). Specifically, we develop a model predictive control (MPC) policy that generates a trajectory constrained to remain within (12), and hence outside its complement (8), while minimizing a cost function designed based on performance metrics.

The MPC policy solves the optimal control problem

$$\min_{\boldsymbol{U}_t} \quad E(\boldsymbol{x}_{N_p|t}) + \sum_{k=0}^{N_p-1} F(\boldsymbol{x}_{k|t}, \boldsymbol{u}_{k|t}) \tag{13a}$$

$$\text{s.t.} \quad \boldsymbol{x}_{k+1|t} = A_\Delta(t+k)\boldsymbol{x}_{k|t} + B_\Delta(t+k)\boldsymbol{u}_{k|t} \tag{13b}$$

$$g_t(\boldsymbol{x}_{k|t}, \boldsymbol{u}_{k|t}) \leq 0 \tag{13c}$$

$$u_{k|t} \in \mathcal{U}(t) \tag{13d}$$

$$\boldsymbol{x}_{0|t} = \boldsymbol{x}_t \tag{13e}$$

where N_p is the prediction horizon length, usually (much) smaller than N in (8), the prediction model (13b) is (3), (13c) is the constraint ensuring that collision can be averted in presence of propulsion system failures, and $\mathcal{U}(t) \in \{\mathcal{U}_i\}_i$ is the input set at time t, which depends on the propulsion system condition according to (5). Since the control sequence over the horizon is $\boldsymbol{U}_t = (\boldsymbol{u}_{0|t} \dots \boldsymbol{u}_{N_p-1|t})$, the following control is applied as an input

$$\boldsymbol{u}_t = \kappa_{mpc}(\boldsymbol{x}_t) = \boldsymbol{u}^*_{0|t}, \tag{14}$$

where $\boldsymbol{U}^*_t = (\boldsymbol{u}^*_{0|t} \dots \boldsymbol{u}^*_{N_p-1|t})$ is the optimizer of (13).

A. Safety Constraints

For (13c) we construct the unsafe set as the union of the orbit-RBRSI in (8) over the input sets (5). Since some failure modes may not need to be considered, e.g., they cannot occur or the spacecraft may be re-oriented to change the location of faulty thrusters, the unsafe set is constructed from given $q \leq n_F$ input sets (5) as

$$\bar{\mathcal{R}}_N^{\mathrm{rdv}}(\mathcal{S}_f) = \bigcup_{i=1}^{q} \bar{\mathcal{R}}_N(\mathcal{S}_f, \mathcal{U}_i). \tag{15}$$

In (15), it is enough to consider all input sets that are not supersets of others, i.e., $\{\mathcal{U}_i : i,j \in \{1,\dots q\}, \nexists j \leq i,\ \mathcal{U}_i \supseteq \mathcal{U}_j\}$, so that we can ignore the input set for nominal conditions. While ideally (13c) could be implemented simply as $x_{k|t} \in \mathcal{X}_N^{\mathrm{safe}} = \bar{\mathcal{R}}_N^{\mathrm{rdv}}(\mathcal{S}_f)^{\mathrm{c}}$, such a constraint is non-convex and will make (13) hard to solve numerically. Instead, we impose constraints on the state to remain outside of (15) by computing a hyperplane that excludes (15) from the feasible space of (13), based on the following well known result.

Result 1: ([18, Prop.3.31]) Given polyhedra $\mathcal{P}_1(H_1, \boldsymbol{k}_1)$, $\mathcal{P}_2(H_2, \boldsymbol{k}_2)$, it holds that $\mathcal{P}_2(H_2, \boldsymbol{k}_2) \supset \mathcal{P}_1(H_1, \boldsymbol{k}_1)$, if and only if there exists a non-negative matrix Λ such that

$$\begin{aligned} \Lambda H_1 &= H_2 \\ \Lambda \boldsymbol{k}_1 &\leq \boldsymbol{k}_2. \end{aligned} \tag{16}$$

Given a subset of the polyhedra $\{\mathcal{P}(H_i^{\bar{\mathcal{R}}}, k_i^{\bar{\mathcal{R}}})\}_{i=1}^{\ell}$ within $\bar{\mathcal{R}}_N^{\mathrm{rdv}}(\mathcal{S}_f)$, where $H_i^{\bar{\mathcal{R}}} \in \mathbb{R}^{n_{ci} \times n}$, we use Result 1 to construct a halfspace $\mathcal{P}_h(\boldsymbol{h}, 1) = \{\boldsymbol{x} \in \mathbb{R}^n : \ \boldsymbol{h}\boldsymbol{x} \leq 1\}$ such that $\mathcal{P}_h(\boldsymbol{h}, 1) \supset \{\mathcal{P}(H_i^{\bar{\mathcal{R}}}, \boldsymbol{k}_i^{\bar{\mathcal{R}}})\}_{i=1}^{\ell}$. Given $\bar{\boldsymbol{x}} \in \mathbb{R}^n$, let $\boldsymbol{h}^*(\bar{\boldsymbol{x}})$, $\{\boldsymbol{\lambda}_i^*(\bar{\boldsymbol{x}})\}_{i=1}^{\ell}$, $s^*(\bar{\boldsymbol{x}})$ be the solution of

$$\min_{s, \boldsymbol{h}, \{\boldsymbol{\lambda}_i\}_{i=1}^{\ell}} \quad -s \tag{17a}$$

$$\text{s.t.} \quad s \geq 0 \tag{17b}$$

$$\boldsymbol{h}\bar{\boldsymbol{x}} \geq 1 + s \tag{17c}$$

$$[\boldsymbol{\lambda}_i]_j \geq 0, \quad j = 1, \dots, n_{ci} \tag{17d}$$

$$\boldsymbol{\lambda}_i H_i^{\bar{\mathcal{R}}} = \boldsymbol{h} \tag{17e}$$

$$\boldsymbol{\lambda}_i \boldsymbol{k}_i^{\bar{\mathcal{R}}} \leq 1, \quad i = 1, \dots, \ell \tag{17f}$$

where $\boldsymbol{\lambda}_i \in \mathbb{R}^{1 \times n_{ci}}$, for all $i = 1, \dots, \ell$. Any feasible solution of the linear program (17) is such that $\mathcal{P}_h(\boldsymbol{h}, 1) \supset \{\mathcal{P}(H_i^{\bar{\mathcal{R}}}, \boldsymbol{k}_i^{\bar{\mathcal{R}}})\}_{i=1}^{\ell}$. Furthermore, any feasible solution of (17) is such that $\bar{\boldsymbol{x}} \notin \mathcal{P}_h(\boldsymbol{h}, 1)$, and the cost function (17a) maximizes the "distance" of $\bar{\boldsymbol{x}}$ to the half space $\mathcal{P}_h(\boldsymbol{h}^*, 1)$, for reasons that will be clear next.

At any time t, we construct (13c) exploiting the optimal trajectory according to (13) at time $t-1$, $(\boldsymbol{x}^*_{0|t-1} \dots \boldsymbol{x}^*_{N_p|t-1})$. Given $\boldsymbol{x}^*_{k|t-1}$, $k \in \{1, \dots, N_p\}$, we select the ℓ closest polyhedra among those in $\bar{\mathcal{R}}_N^{\mathrm{rdv}}(\mathcal{S}_f)$ based on the distance

$$\begin{aligned} \mathrm{d}(\boldsymbol{x}^*_{k|t-1}, \mathcal{P}_i) = \min_{\boldsymbol{y}} \quad & \|\boldsymbol{x}^*_{k|t-1} - \boldsymbol{y}\|_2 \\ \text{s.t.} \quad & \boldsymbol{y} \in \mathcal{P}_i. \end{aligned} \tag{18}$$

Then, we compute $\boldsymbol{h}_{k|t} = \boldsymbol{h}(\boldsymbol{x}^*_{k+1|t-1})$ from (17) based on the selected $\{\mathcal{P}_i\}_{i=1}^{\ell}$ and implement (13c) as its complement

$$-\boldsymbol{h}_{k|t}\boldsymbol{x}_{k|t} \leq -1 - \rho, \tag{19}$$

where $\rho > 0$ is an arbitrarily small constant, in order for (13c) to be feasible in a closed set, and possibly to add a safety margin. Since $\mathcal{P}_h(\boldsymbol{h}, 1) \supset \{\mathcal{P}_i\}_{i=1}^{\ell}$, its complement (19) does not intersect $\{\mathcal{P}_i\}_{i=1}^{\ell}$.

Remark 2: If ℓ is chosen to include all polyhedra of $\bar{\mathcal{R}}_N^{\mathrm{rdv}}(\mathcal{S}_f)$, the feasible set of (19) is contained in $\mathcal{X}_N^{\mathrm{safe}}$. We consider the possibility of including only the subset of closest polyhedra to take advantage of the receding horizon nature of (14) for reducing the computational burden of (13) and (17), and to avoid possible infeasibility of (17), which are local (over)-approximations of $\bar{\mathcal{R}}_N^{\mathrm{rdv}}(\mathcal{S}_f)$. In fact, $\bar{\mathcal{R}}_N^{\mathrm{rdv}}(\mathcal{S}_f)$ considers all terminal times around the orbit, while the final approach of the rendezvous maneuver considered here terminates in a small, albeit difficult to predict, fraction of the orbital period.

Cost function (17a) is meant to increase the residual of $\boldsymbol{x}^*_{k|t-1}$ in satisfying (19), so that the deputy has more clearance to maneuver and select an optimal trajectory without riding on or near the constraint, if possible.

B. *Cost Function*

In order to obtain in (13) a linear quadratic MPC, we design the stage cost and the terminal cost in (13a) as

$$F(\boldsymbol{x},\boldsymbol{u}) = \boldsymbol{x}^\top Q\boldsymbol{x} + \boldsymbol{u}^\top R\boldsymbol{u}, \tag{20a}$$

$$E(\boldsymbol{x}) = \boldsymbol{x}^\top M\boldsymbol{x}, \tag{20b}$$

where the weight matrices $Q = Q^\top \geq 0$, $R = R^\top > 0$, $M = M^\top > 0$ are selected to achieve the desired performance. The primary objective is to approach the chief, which amounts to reaching zero position and velocity, and can be affected by Q. A secondary objective is to minimize the total required propellant, since this allows for increased payload, which often requires minimizing the thrust, and hence is affected by R.

V. Simulation Results

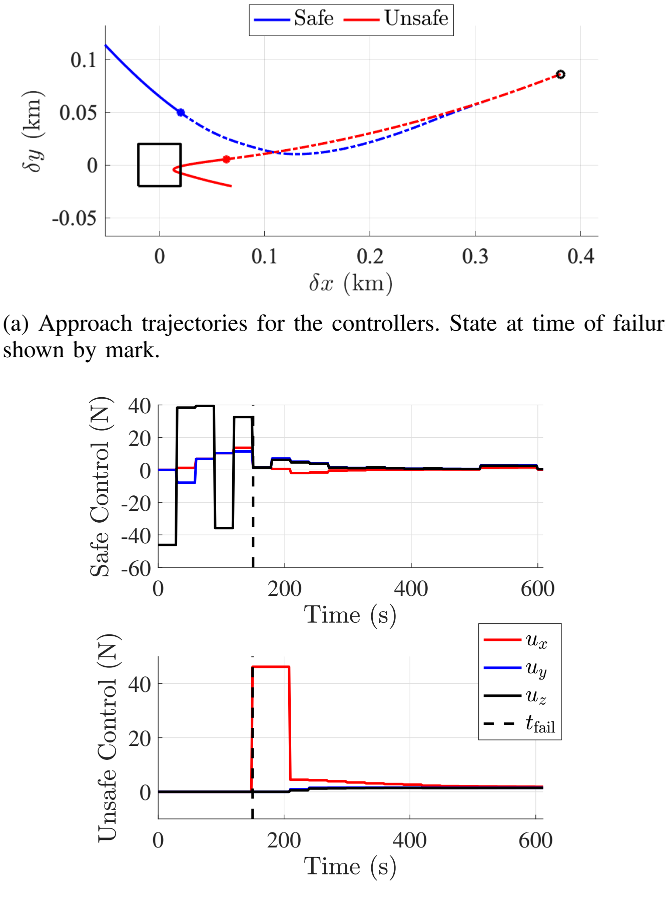
We run the discrete-time MPC (13), (14) in closed-loop with the continuous-time model of the nonlinear equations of relative motion resolved in $\mathrm{F_o}$. The number of steps in the MPC horizon and the MPC sampling period are $N_p = 8$, $\Delta t_{\mathrm{MPC}} = 30$s. Each thruster can apply a maximum thrust of $u_{\mathrm{m}} = 20$ N. The terminal set is defined by a polytope with position bounds $p_{\mathrm{m}} = 20$ m and velocity bounds $v_{\mathrm{m}} = 6$ m/s. The LTV RBRSI sets are computed for a quarter of the orbital period, such that the safety horizon is $N = \lceil \frac{t_p}{4\Delta t} \rceil + 1 = 54$ and the RBRS sampling period is chosen such that $\Delta t_{\mathrm{RBRS}} < \Delta t_{\mathrm{MPC}}$.

The failure occurs at t_{fail}, when the state is $x(t_{\mathrm{fail}})$, so that for $t < t_{\mathrm{fail}}$, $\boldsymbol{u}_t \in \mathcal{U}_1$, which corresponds to $\mathcal{M}_1 \triangleq \mathcal{I}$, i.e., nominal control. For $t \geq t_{\mathrm{fail}}$, $\boldsymbol{u}_t \in \mathcal{U}_i$ where $\mathcal{M}_i \in \mathcal{FM}$, i.e., some thrusters have failed. For $t \geq t_{\mathrm{fail}}$ we set $Q, M = 0$ so that the only objective is to avoid the constraints, i.e., safety. Next we show the behavior of the *safe controller*, that is designed as described in Section IV to be safe in case of partial thruster failure by enforcing $\boldsymbol{x} \in \mathcal{X}_N^{\mathrm{safe}}$, so that safe abort maneuvers exist, as per Proposition 1. We compare it with a standard design, called *unsafe controller*, that only aims at avoiding $\mathcal{S}_f$ using that itself as a constraint, yet has no formal guarantees.

A. *Safe Controller vs. Unsafe Controller*

In this section, a simulation is presented to compare the trajectories of the unsafe and safe controllers. In Figure 2a, the dashed lines represent the part of the trajectory before the failure time $t \in [t_0, t_{\mathrm{fail}}]$, where in these simulations $t_{\mathrm{fail}} = 240$s, while the solid lines represent the part after the failure time and within the safety horizon, $t \in [t_{\mathrm{fail}}, t_{\mathrm{fail}}{+}N]$. The mark on the trajectory indicates the position at which the failure occurs, $\boldsymbol{x}(t_{\mathrm{fail}})$. The unsafe approach is shown in red while the safe approach is shown in blue. The positions within the target set $\mathcal{S}_f$ are shown as a transparent cube. For these simulations, $q = 1$ so safety is only maintained with respect to one failure mode in each trajectory.

The case when only thruster 1 has failed is shown in Figure 2a, where $\mathcal{M}_2 \triangleq \mathcal{I} \setminus \{1\} \in \mathcal{FM}$, so that, after the failure occurs, $\boldsymbol{u}_t \in \mathcal{U}_2$ for the remainder of the simulation. The initial state in the chief's Hill frame is $\mathbf{x}(t_0) = \begin{bmatrix}-0.3178 & 0.7149 & -0.1200 & 0.0017 & -0.0021 & 0.0004\end{bmatrix}^\mathsf{T}$ for both controllers. The trajectories for the safe and unsafe controllers are shown in Figure 2a, while the control histories are shown in Figure 2b. Indeed, while the unsafe controller cannot avoid colliding with the chief, when the safe controller is used, an avoidance maneuver is possible.



(a) Approach trajectories for the controllers. State at time of failure shown by mark.

(b) Control histories for the controllers. Vertical dash line marks t_{fail}.

Fig. 2: Comparison of the safe and unsafe controllers when only thruster, τ_1, fails i.e. $\mathcal{M}_2 = \mathcal{I} \setminus \{1\}$.

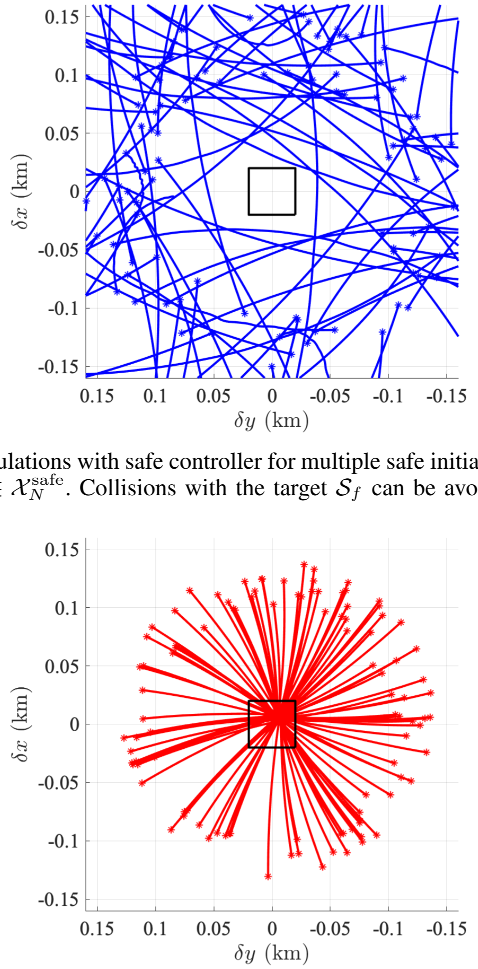
B. *Varying Initial Conditions*

We demonstrate that within the orbit-RBRSI safe-abort is impossible, while outside it is guaranteed. This is shown by using the safe controller for various safe initial states, $\boldsymbol{x}(t_0) \in \mathcal{X}_N^{\mathrm{safe}}$, and unsafe, $\boldsymbol{x}(t_0) \notin \mathcal{X}_N^{\mathrm{safe}}$, where for the unsafe initial conditions, (13c) is softened by slack variables. For simplicity and clarity, we consider a scenario of a planar rendezvous, $\delta z, \delta \dot{z} = 0$. Here, a more significant failure mode is considered defined by $\mathcal{M}_3 \triangleq \{8\} \in \mathcal{FM}$, such that thrusters τ_1 through τ_7 simultaneously fail. In these simulations, the failure occurs at $t_0 = t_{\text{fail}} = 0$, and as a consequence $\boldsymbol{u}_t \in \mathcal{U}_3$, for all $t \geq 0$. We generate random initial conditions in $\boldsymbol{x}_0^{\text{safe,i}} \in \mathcal{X}_N^{\text{safe}}$ and $\boldsymbol{x}_0^{\text{unsafe,i}} \in \tilde{\mathcal{R}}_N(\mathcal{S}_f, \mathcal{U}, t_f) \subset \mathcal{X}_N^{\text{unsafe}}$. Additionally, the following position and velocity norm constraints are imposed on the samples: $\|\boldsymbol{x}_p(t_0)\|_2 \in [r_1, r_2]$ and $\|\boldsymbol{x}_v(t_0)\|_2 \in [v_1, v_2]$, where $\begin{bmatrix} r_1 & r_2 & v_1 & v_2 \end{bmatrix} = \begin{bmatrix} 0.1\text{km} & 0.16\text{km} & -1.5\text{ms}^{-1} & 1.5\text{ms}^{-1} \end{bmatrix}$.

All of the initial conditions that start in the safe set remain so for the remainder of the simulation as shown in Figure 3a. For comparison, Figure 3b shows the resulting trajectories when the safe controller is used on initial conditions in $\tilde{\mathcal{R}}_N(\mathcal{S}_f, \mathcal{U}, t_f)$. In this case, the safe controller is incapable of avoiding a collision with the chief, despite safety being enforced, which is true by construction of (6). This highlights the importance of the proposed method, which formally allows the deputy to avoid the chief by remaining in $\tilde{\mathcal{R}}_N(\mathcal{S}_f, \mathcal{U}, t_f)^{\text{c}}$ at all discrete times.

VI. CONCLUSIONS

We developed an abort-safe control policy against partial thruster failures for spacecraft rendezvous on generic elliptic orbits using robust backwards reachable sets and model predictive control. The proposed control policy generates rendezvous trajectories such that if a fault occurs in the propulsion system, it is always possible to maneuver the deputy spacecraft to avoid colliding with the chief.



(a) Simulations with safe controller for multiple safe initial conditions, $\boldsymbol{x}(t_0) \in \mathcal{X}_N^{\text{safe}}$. Collisions with the target $\mathcal{S}_f$ can be avoided.

(b) Simulations with the safe controller for multiple unsafe initial conditions $\boldsymbol{x}(t_0) \in \mathcal{X}_N^{\text{unsafe}}$. Collisions with the target $\mathcal{S}_f$ cannot be avoided.

Fig. 3: Various initial conditions for the case when only 1 thruster remains functional after the failure, i.e., $\mathcal{M}_3 = \{8\}$.

REFERENCES

[1] W. Fehse, *Automated rendezvous and docking of spacecraft*. Cambridge university press, 2003, vol. 16.

[2] D. Aguilar Marsillach, S. Di Cairano, and A. Weiss, “Fail-safe rendezvous control on elliptic orbits using reachable sets,” in *2020 American Control Conference (ACC)*. IEEE, 2020, pp. 4920–4925.

[3] 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.

[4] M. Althoff, “An introduction to CORA 2015,” in *Proc. Work. Applied Verification for Continuous and Hybrid Systems*, 2015.

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

[6] M. J. Holzinger and D. J. Scheeres, “Reachability results for nonlinear systems with ellipsoidal initial sets,” *IEEE trans. aerospace and electronic systems*, vol. 48, no. 2, pp. 1583–1600, 2012.

[7] 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.

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

[9] J. D. Gleason, A. P. Vinod, and M. M. Oishi, “Underapproximation of reach-avoid sets for discrete-time stochastic systems via lagrangian methods,” in *Conf. Decision and Control*, 2017, pp. 4283–4290.

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

[11] 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.

[12] 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,” *IEEE Trans. Control Systems Technology*, vol. 23, no. 4, pp. 1638–1647, 2015.

[13] 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.

[14] E. N. Hartley, M. Gallieri, and J. M. Maciejowski, “Terminal spacecraft rendezvous and capture with lasso model predictive control,” *International Journal of Control*, vol. 86, no. 11, pp. 2104–2113, 2013.

[15] 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,” *Journal of Guidance, Control, and Dynamics*, vol. 40, no. 7, pp. 1541–1566, 2017.

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

[17] H. D. Curtis, *Orbital mechanics for engineering students*. Butterworth-Heinemann, 2013.

[18] F. Blanchini and S. Miani, *Set-theoretic methods in control*. Springer, 2008.