Reachability Calculations for Vehicle Safety during Manned/Unmanned Vehicle Interaction

Jerry Ding*

University of California, Berkeley, CA, 94720-1770

Jonathan Sprinkle†

University of Arizona, Tucson, AZ, 85721-0104

Claire J. Tomlin‡ and S. Shankar Sastry§

University of California, Berkeley, CA, 94720-1770

James L. Paunicka¶

Boeing Research & Technology, St. Louis, MO, 63166-0516

This paper describes an approach based on reachability calculations for ensuring robust operation guarantees in flight maneuver sequences performed by unmanned aerial vehicles (UAVs) under supervision of human operators, with applications to safety-critical scenarios. Using a hybrid system formalism to model the maneuver sequence, the paper devises systematic procedures for designing switching conditions to ensure the properties of safety, target attainability and invariance, using Hamilton-Jacobi reachability calculations. These calculations lay the foundations for refining or designing protocols for multi-UAV and/or manned vehicle interaction. The mathematical foundations necessary are described in order to formulate verification problems on reachability and safety of flight maneuvers, including issues of command latency, and disturbance. An example of this formalism is given in the context of Automated Aerial Refueling, to inform UAV decisions that avoid unsafe scenarios while achieving mission objectives.

*Graduate Student Researcher, Department of Electrical Engineering and Computer Sciences, Student Member AIAA. jding@eecs.berkeley.edu

†Assistant Professor, Department of Electrical and Computer Engineering, Member AIAA. sprinkle@ECE.Arizona.Edu

‡Professor, Electrical Engineering and Computer Sciences, Fellow AIAA. tomlin@eecs.berkeley.edu

§Dean of the College of Engineering, and NEC Distinguished Professor of Electrical Engineering and Computer Sciences, and Professor of Bioengineering. sastry@eecs.berkeley.edu

¶Technical Fellow, Senior Member AIAA. james.l.paunicka@boeing.com

Nomenclature

q_i	transition maneuver
$\hat{q}_i$	stationary maneuver
$\tilde{q}_i$	escape maneuver
f	vector field defining continuous dynamics
x	continuous state vector
u	control input vector
d	disturbance input vector
$\mathbb{U}$	control input space
$\mathbb{D}$	disturbance input space
K_i	feedback control law designed for maneuver q_i
$\sigma_{i(i+1)}$	transition command between maneuver q_i and q_{i+1}
$\gamma_{i(i+1)}$	guard condition specifying set of states for which transition is enabled between q_i and q_{i+1}
Dom	domain of flight maneuvers
X_0	set of permissible initial continuous states
H	Hamiltonian for capture and collision set calculation
p	costate vector
ϕ	solution to a Hamilton-Jacobi equation
t	time, s
τ	time interval, s
R_i	target set for maneuver q_i
$\mathscr{R}_{f_i}(R,K_i,\tau_i)$	capture set for target R , in mode q_i, using controller K_i, over time interval $[0,\tau_i]$
A	avoid set for all maneuvers
$\mathscr{A}_{f_i}(A,K_i,\tau_i)$	collision set for mode q_i, using controller K_i, over time interval $[0,\tau_i]$
W_0	subset of $\mathbb{R}^n$ used to initialize an invariant set calculation
W_f^∞	invariant set under vector field f over infinite time horizon $[0,\infty)$
L	communication latency, s
B	disc in the plane
a_0	unsafe radius, m
V	neighborhood of states around the fuel boom
x_1	longitudinal distance from the tanker to the UAV, m
x_{1_f}	desired longitudinal distance from the tanker to the UAV, m
x_2	lateral distance from the tanker to the UAV, m
x_{2_f}	desired lateral distance from the tanker to the UAV, m
x_3	heading of the tanker relative to the UAV, rad
u_1	control input, translational velocity of UAV, m/s
u_2	control input, angular velocity of UAV, rad/s
d_1	disturbance input, translational velocity of tanker, m/s
v_0	nominal translational velocity of tanker, m/s

Subscript	
i, j	index of a discrete state
Superscript	
C	complement of a set
T	transpose of a vector or matrix

I. Introduction

In modern autonomous flight systems, the tasks of management and control of aircraft are frequently distributed between an onboard autonomous controller and external human operators or supervisors. In safety-critical scenarios, the decision authority to perform a given flight maneuver usually rests exclusively with the human operators, while proper design of the flight control system can be used to ensure that the aircraft remains within safe operational limits during the maneuver.[1] However, if a scenario involves simultaneous control of one or more vehicles over communication delay, then it can become difficult for a human operator to foresee all safety issues, and unsafe situations may arise.[2,3] Thus, an important consideration is how an Unmanned Aerial Vehicle (UAV) would detect and respond to situations in which a human operator command would place the UAV in imminent danger. For cases in which the goals of the vehicle are known at design time, and this vehicle may be the only vehicle in operation, many issues can be accounted for with design choices, specialized operator consoles, and training. However, in so-called *mixed-initiative* scenarios, where many vehicles operate in the same airspace and/or a vehicle is simultaneously operating on several goal sets, run-time decisions regarding safety of commands may prevent unintended behaviors that are mathematically foreseeable, but are not obvious to a trained operator.

This paper considers, in particular, mixed-initiative scenarios composed of a finite sequence of pre-defined flight maneuvers, where the transitions between maneuvers can be controlled by human operators or initiated autonomously by the UAV. The overall system can be modeled formally as a *hybrid system*–a system whose dynamics evolve both in the discrete and continuous domain. In this case, the discrete dynamics are the transitions between flight maneuvers, while the continuous dynamics are comprised of the evolution of aircraft states when executing individual maneuvers.

Under this setting, a systematic approach is proposed, based upon previous work on hybrid system verification and controller synthesis,[4,5,6,7,8,9] for designing maneuver control laws and switching conditions so as to satisfy the following objectives: 1) *target attainability* – each flight maneuver is initiated from a configuration that can be driven into a desired target configuration in finite time; 2) *safety* – each flight maneuver satisfies a pre-defined safety condition through the entire course of the maneuver; and 3) *robustness* – the previous conditions are satisfied even under command latency and environment disturbance.

To discuss this design approach in a concrete setting, consider the particular scenario of Automated (or Autonomous) Aerial Refueling (AAR).[10,11,12,13,14] During a refueling operation, a UAV detaches from its formation, and approaches the rear of a tanker aircraft for refueling. The boom operator onboard the tanker then lowers a fuel boom to refuel the UAV; once the refueling is complete, the operator disconnects the boom and the UAV rejoins its formation.

This description naturally decomposes AAR into several distinct phases, namely an "approach tanker" phase, a "refueling" phase, and a "rejoin formation" phase. To introduce further structure into the refueling operation, the approach and rejoin phases could consist of a sequence of flight maneuvers. Thus, the entire scenario can be modeled by a sequential mode transition system, where each discrete mode represents a particular flight maneuver. In the execution of each flight maneuver, the state evolution of the UAV (position and heading changes) can be described by continuous time kinematic models.

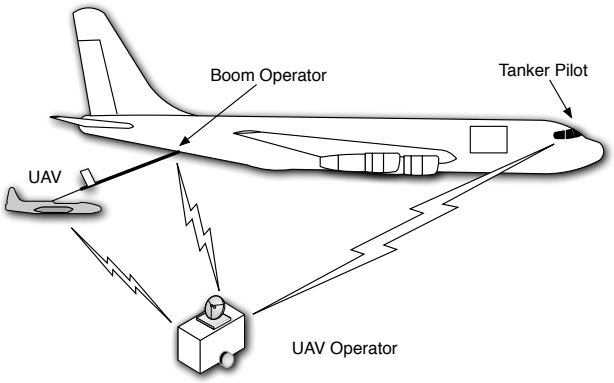


Figure 1. Communications in automated aerial refueling are subject to latency, as commands intended for the unmanned vehicle originate from or are relayed through a UAV Operator.

To ensure the correct and safe operation of AAR, a computational reachability analysis can be performed for each flight maneuver in the refueling sequence to determine 1) the *capture set*: the set of aircraft states from which a maneuver can be completed within a finite time horizon; and 2) the *collision set*: the set of aircraft states from which the trajectory of a flight maneuver passes through a collision zone centered on the tanker aircraft. For nonlinear aircraft dynamics, these sets can be computed using numerical solutions of Hamilton-Jacobi partial differential equations (PDEs).[9]

At design time, the capture sets and collision sets computed for the various maneuvers in the AAR sequence can be used to guide the choice of maneuver control laws and switching conditions so as to ensure that each maneuver terminates in an aircraft state which satisfies the target attainability and safety objective of the next maneuver (thus allowing the next maneuver to be feasibly initiated). Furthermore, through appropriate modifications of the reachability analysis, the effects of bounded disturbances and communication latency can also be taken into account. However, in such cases, the resulting design of maneuver control laws and switching conditions is in general

more conservative than the case in which the robustness factors are not considered.

The methodology and results described in this paper extend the work previously presented at the IEEE Conference on Decision and Control[15] in several important directions. First, a formal description is given of the procedure for applying reachability analysis to general sequential mode transition systems. Second, a framework is included to account for deterministic communication latency when issuing mode transition commands. Finally, the reachability analysis performed in this paper uses distances, velocities, and physical constraints that more accurately reflect the aerial refueling example, including appropriately modified controller parameters.

The organization of this paper is as follows. Section II provides an overview of related work in the domain of formal verification and flight maneuver design. Section III provides a formal statement of the maneuver sequence design problem. Section IV briefly reviews the method of Hamilton-Jacobi reachability for nonlinear continuous systems. Section V introduces a reachability-based procedure for performing the maneuver sequence design. Section VI discusses extensions of this design procedure to account for non-ideal operating conditions such as communication latency and improper initialization. These methods are then specialized to the particular case of automated aerial refueling in Section VII, and the results of the reachability analysis along with simulated scenarios are presented in Section VIII. Finally, some conclusions and directions for future work are discussed in Section IX.

II. Related Work

II.A. Hamilton-Jacobi Reachability

The method of Hamilton-Jacobi (H-J) reachability[9] is developed for computing the set of initial conditions reachable, under continuous time dynamics, to a pre-specified subset of the continuous state space. In the work by Tomlin et al.,[8] one can find a comprehensive overview of the computational techniques underlying the H-J reachability, its use in analyzing and verifying continuous time nonlinear systems as well as hybrid systems.

This method has seen successes in numerous aeronautical applications. In the work by Mitchell et al.[9] and Bayen,[16] the authors present a method for detecting possible "loss of separation" between pairs of aircraft over a given airspace, based upon backward reachable sets computed using H-J PDEs. Using this formulation of the collision avoidance problem, the reachable set method has been used to verify safety of conflict resolution aircraft maneuvers,[17] and closely spaced parallel approaches for airport runways.[18] The results of the reachability calculations were validated in extensive simulations as well as UAV flight experiments.[19,20] While the focus of these previous applications lies largely in safety verification, this paper proposes a method for using reachability analysis as a design tool for choosing the transition conditions and continuous control laws of a maneuver sequence so as to satisfy the desired specifications.

In systems that involve human-automation interactions, H-J reachability has also been successfully demonstrated as a method for informing human decisions. In the work by Oishi et al.,[21] the authors use reachability analysis to determine whether the pilot display of a civil jet aircraft contained enough information for the pilot to safely perform a Take-off/Go-Around (TO/GA) maneuver from a Flare landing maneuver. In another example,[22] reachable sets computed using H-J methods are used to inform decisions on the re-initiation of a landing maneuver during TO/GA, and the results were demonstrated on a fixed-wing UAV (T-33). Building upon these previous works, this paper also proposes methods for using reachable sets as a visual tool for guiding human operator decisions in scenarios where there is latency in the communication channel or when a maneuver sequence is improperly initialized.

II.B. Alternative Reachability Approaches

Aside from H-J reachability, there is a myriad of alternative approaches in the domain of reachable set based system verification for hybrid systems. The work considering timed automata and linear hybrid automata includes seminal papers by Alur[23] and Henzinger.[24] Results have been generalized to linear and nonlinear continuous dynamics, with supporting computational tools.[25,6,7,26,27,28,29,30] Methods that operate on system abstractions can reduce computational complexity, including simulation and bisimulation relations,[31,32,33] which construct discrete abstractions of hybrid system dynamics. In comparison, the H-J method has the advantage of being able to handle nonlinear continuous dynamics perturbed by bounded disturbances, albeit at the cost of higher computational complexity.

In reachability work relating to stochastic systems, Prandini et al.[34] discuss the use of Markov chains to determine the reachability of some stochastic system in some lookahead time (potentially infinite). Air traffic management as a driving example for distributed control and stochastic analysis of safety-critical real-time systems is demonstrated in the HYBRIDGE report.[35] In many of these applications, events that jeopardize the safety of the system are rare, and using probabilistic methods such as Monte Carlo simulations,[36] it is possible to estimate the probability of these events through stochastic reachability and obtain some measure of confidence in the safety of a system design.[37] On the other hand, for systems with persistent environment disturbances that are known to lie within certain bounds, deterministic reachability can be used to provide stronger performance guarantees for relevant disturbances such as perturbations in velocity or heading.

II.C. Flight Maneuver Design Approaches

State feedback is a common approach to the design and implementation of flight maneuvers. In general, a trajectory is generated (or designed) and the vehicle tracks this trajectory based on an on-board guidance and navigation system. Depending on the maneuver, this trajectory may be

globally fixed (for example, a glideslope for landing) or defined from a location decided at flight time (for example, a waypoint). For certain maneuvers, additional scrutiny is given due to their proximity to regions of stall or other vehicles. Details for optimal Go-Around and Flare maneuvers are given in the work of Buell.[38] Interestingly, transitions between these maneuvers can also be discussed in the framework of reachability, as in the previously mentioned work by Oishi et al.[21]

Alternatively, maneuver sequence synthesis may be performed at runtime using path-planning algorithms. Bottasso et al.[39] demonstrate smooth path planning using motion primitives to pass through a series of waypoints constituting a track. This approach is related to that applied by Frazzoli et al.[40] and Koo et al.,[41] both of which are focused on rotorcraft. Although these algorithms are computationally efficient, providing robust performance guarantees are often complicated by the presence of model uncertainty and environment disturbances at runtime.

To address safety concerns, safe maneuvers with real-time trajectory generation were shown by Waydo et al.[42] for the case of formation flight with an autonomous vehicle, where several control modes are used depending on loss of communication with a manned vehicle. This approach was proved safe using runtime predictive control, requiring a solution to the stationary Riccati equation over (essentially) infinite time, and is interesting to compare to backward reachability, in that this is essentially a forward reachability solution to validate a specific trajectory (rather than validate all potential trajectories using backward reachability).

As an alternative, Lyapunov functions can be also used to provide robust guarantees on the closed-loop performance of the system under a given controller design. Relevant to the work in this paper is a Lyapunov-based method proposed by Burridge et al.,[43] in the context of motion planning applications, for composing sequences of local feedback controllers to achieve a desired final configuration. Under this method, the authors construct local controllers whose domains of attraction are estimated from the level sets of Lyapunov functions. Sequential composition is then performed by ensuring that the goal set of a given controller is contained within the domain of attraction of the next controller in the sequence.

For applications with nonlinear continuous dynamics, constructing appropriate Lyapunov functions satisfying the desired stability objectives can be a non-trivial task. Depending on the choice of Lyapunov functions, estimates of the domain of attraction can be also quite conservative, especially when system dynamics are perturbed by disturbances. By using H-J methods to generate the relevant reachable sets, the methodology proposed in this paper avoids the need for selecting Lyapunov functions, while reducing the conservatism in estimating the domain of attraction. Also, it is worth noting that local controllers produced through Lyapunov methods can be evaluated using Hamilton-Jacobi reachability for satisfaction of target attainability and safety objectives. Thus, the presented approach is not meant to supplant existing methods for robust nonlinear controller design, but to augment them.

II.D. Automated Aerial Refueling

The coordination of high-level mode switches described in this paper depends on external solutions to capturing the boom, and maintaining relative distance while refueling. A vision-based sensing and navigation system for AAR is proposed by Valasek et al.,[12] and Williamson's work[44] discusses a sensor fusion approach for state estimation in AAR. Demonstrations of AAR have been made, notably Boeing's successful demonstration using a UAV surrogate Lear Jet[45] to show proof of concept, and a separate demonstration by DARPA and NASA's Dryden Test Flight Center over Edwards Air Force Base, using a specially configured F/A-18: the first hands-off AAR demonstration.[11]

III. Maneuver Sequence Design Problem

III.A. System Dynamics

Consider a maneuver sequence consisting of flight maneuvers $q_1, q_2, ..., q_N$, where maneuver q_i is followed by maneuver q_{i+1}. In the context of the AAR application, this corresponds to the maneuvers performed by a UAV in the various phases of the refueling procedure.

While performing a given maneuver q_i, the aircraft motion is assumed to be described by an ordinary differential equation (ODE) model $\dot{x} = f_i(x, u_i, d_i)$, $x(0) = x_0$, where $x \in \mathbb{R}^n$ is the state of the aircraft, $u_i \in \mathbb{R}^{n_{c,i}}$ are the control inputs, and $d_i \in \mathbb{R}^{n_{d,i}}$ are the disturbance parameters. The control inputs are subject to the constraint $u_i \in \mathbb{U}_i$, where $\mathbb{U}_i$ is a compact subset of $\mathbb{R}^{n_{c,i}}$. The disturbance parameters are used to capture the effects of modeling uncertainties and environment disturbances. It is assumed that some conservative bounds are available for these parameters in the form of $d_i \in \mathbb{D}_i$, where $\mathbb{D}_i$ is a compact subset of $\mathbb{R}^{n_{d,i}}$.

More concisely, the system dynamics over the course of the maneuver sequence is described by the equation

$$\dot{x} = f_q(x, u, d),\ x(0) = x_0, \tag{1}$$

where $q \in \{1, ..., N\}$, $x \in \mathbb{R}^n$, $u \in \mathbb{U}_q$, and $d \in \mathbb{D}_q$.

In a mixed-initiative scenario, transition from one maneuver to the next is allowed to be either commanded by a human operator or initiated autonomously by the aircraft control system. To model a human commanded transition, the transition between maneuver q_i and q_{i+1} is enabled by an external operator command $\sigma_{i(i+1)}$, when a guard condition $\gamma_{i(i+1)} \subset \mathbb{R}^n$ on the continuous state x is satisfied. To model an autonomous transition, each maneuver q_i is also associated with a domain $Dom(q_i) \subset \mathbb{R}^n$, so that $x \notin Dom(q_i)$ results in an autonomous transition to the next mode q_{i+1} in the maneuver sequence, regardless of whether an external transition command is received. The maneuver sequence model described here is a special class of hybrid systems, thus allowing formal analysis under previously developed tools in this domain.[46,47]

III.B. Maneuver Sequence Design with Target Attainability Objectives

First, consider a problem specification where the objective of each maneuver q_i is to drive the continuous state x into a desired target set $R_i \subset \mathbb{R}^n$, while avoiding a set $A \subset \mathbb{R}^n$. Note that A is the same for each maneuver. Here the sets $R_i \subset \mathbb{R}^n$ could represent a sequence of waypoints, while the set A could represent unsafe operating conditions of the vehicle, or proximity to another vehicle. The control design problem then becomes one of choosing the continuous input in each maneuver as a feedback policy $u_i = K_i(x)$, as well as the switching conditions, defined by the guards and the maneuver domains, so as to achieve the desired objectives. More specifically, the problem statement is as follows.

Problem 1: Given target sets $R_i \subset \mathbb{R}^n$, $i = 1,...,N$, and avoid set $A \subset \mathbb{R}^n$, choose feedback laws K_i, guard conditions $\gamma_{i(i+1)}$, and maneuver domains $Dom(q_i)$ such that regardless of the realization of the disturbances d_i, the system trajectory satisfies $(q(t_i), x(t_i)) \in q_i \times R_i$ and $x(t) \notin A$, $\forall t \leq t_N$, for some sequence of times $t_0 = 0 < t_1 < \cdots < t_N < \infty$.

III.C. Maneuver Sequence Design with Target Attainability and Invariance Objectives

The problem described previously is well-suited for scenarios in which a sequence of maneuvers is to be performed consecutively, without dwelling in any particular maneuver. For cases in which the vehicle is to be held in a certain configuration over an indefinite period of time, for example when the UAV is being refueled during AAR, it is necessary for the maneuver sequence to include flight maneuvers in which the goal is not to reach a target set, but rather to keep the system state within a certain set of desired configurations.

To distinguish the various maneuvers, those with target attainability objectives (as described in Section III.B will be referred to as *transition maneuvers*, while those with invariance objectives (as described in the preceding paragraph) will be referred to as *stationary maneuvers*.

In terms of the system model, the set of transition maneuvers q_i can be augmented with a set of stationary maneuvers $\hat{q}_i$, inserted into the maneuver sequence in between q_i and q_{i+1}, with a possible final stationary maneuver $\hat{q}_N$ following q_N. Similarly, as for the transition maneuvers, the system dynamics in a stationary maneuver $\hat{q}_i$ is described by an ODE model $\dot{x} = \hat{f}_i(x, \hat{u}_i, \hat{d}_i)$, $x(0) = x_0$. A transition from q_i to $\hat{q}_i$ is enabled by a command $\hat{\sigma}_i$ with an associated guard condition $\hat{\gamma}_i$, while a transition $\hat{q}_i$ to q_{i+1} is enabled by $\sigma_{i(i+1)}$ with the guard condition $\gamma_{i(i+1)}$.

The objective of each stationary maneuver $\hat{q}_i$ is to keep the system state within a set $W_i \subset \mathbb{R}^n$ satisfying $R_i \subset W_i \subset \mathbb{R}^n \backslash A$, using an admissible feedback control law $\hat{u}_i = \hat{K}_i(x)$. Namely, following each transition maneuver, it is desired to keep the system state within a neighborhood of the target set while awaiting command for the next transition maneuver. The augmented maneuver design problem is then as follows.

Problem 2: Given $R_i \subset \mathbb{R}^n$, $i = 1,...,N$, and avoid set $A \subset \mathbb{R}^n$, choose feedback laws K_i, $\hat{K}_i$,

guard conditions $\gamma_{i(i+1)}$, $\hat{\gamma}_i$, and maneuver domains $Dom(q_i)$ such that regardless of the realization of the disturbances d_i, the system trajectory satisfies

1. $(q(t_i), x(t_i)) \in q_i \times R_i$ and $x(t) \notin A$, $\forall t \leq t_N$, for some sequence of times $t_0 = 0 < t_1 < \cdots < t_N < \infty$;

2. $(q(t), x(t)) \in \hat{q}_i \times W_i$, $\forall t \in [t_i, \hat{t}_i]$, where $R_i \subset W_i \subset \mathbb{R}^n \backslash A$, and $\hat{t}_i < \infty$ are the time instants at which the system transitions to maneuver q_{i+1} from $\hat{q}_i$.

IV. Overview of Hamilton-Jacobi Reachability

From the descriptions given in the previous section, the maneuver design problems can be viewed as reachability problems where the goal is to design control laws so as to either reach some target set while avoiding some undesired set, or to remain within some invariant set. In this section, some previous work on reachability analysis for nonlinear continuous systems will be reviewed. This will become useful in formulating systematic design procedures for Problems 1 and 2. For the rest of this section, the following continuous system dynamics will be considered.

$$\dot{x} = f(x, u, d),\ x(0) = x_0, \tag{2}$$

where $x \in \mathbb{R}^n$, $u \in \mathbb{U}$, and $d \in \mathbb{D}$.

IV.A. Capture Set

Definition 1: Given a target set R, the *capture* set $\mathscr{R}_f(R, \tau)$ over time horizon τ for system (2) is the set of initial conditions x_0, for which there exists a feedback control policy $u = K(x,t)$ on $[0, \tau]$, such that for any disturbance d satisfying $d(t) \in \mathbb{D}$, $\forall t \in [0, \tau]$, the state trajectory under (2) satisfies $x(t) \in R$, for some $t \in [0, \tau]$.

As shown in previous work by Mitchell et al.,[9] this set can be computed using a Hamilton-Jacobi PDE. Specifically, suppose the target set can be represented by a function ϕ_R such that $x \in R$ if and only if $\phi_R(x) \leq 0$ (referred to as a level set function for R), then consider the following Hamilton-Jacobi (H-J) equation:

$$\frac{\partial \phi}{\partial t} + \min\left[0, H\left(x, \frac{\partial \phi}{\partial x}\right)\right] = 0,\ \phi(x,0) = \phi_R(x) \tag{3}$$

where the optimal Hamiltonian H is given by

$$H(x,p) = \min_{u \in \mathbb{U}} \max_{d \in \mathbb{D}} p^T f(x,u,d). \tag{4}$$

Then by the argument presented in the work of Mitchell et al.,[9] $\mathscr{R}_f(R,\tau) = \{x \in X, \phi(x,-\tau) \leq 0\}$, where ϕ is the unique viscosity solution[48] to (3). Furthermore, as discussed in previous work by Tomlin et al.,[47] a control policy for reaching the target set R can be synthesized, at least in principle, according to

$$u^*(x,t) \in \arg\min_{u\in\mathbb{U}} \max_{d\in\mathbb{D}} p(x,-t)^T f(x,u,d),\ t \in [0,T], \tag{5}$$

where $p = \frac{\partial \phi}{\partial x}$ (typically referred to as the costate vector) can be evaluated by taking spatial derivatives of the solution ϕ to (3).

For cases in which one is interested in finding the capture set with respect to a particular choice of control law $u = K(x)$, namely the set of initial conditions x_0 such that $x(t) \in R$ under K, for some $t \in [0,\tau]$, regardless of the disturbance, then the Hamiltonian reduces to $H(x,p) = \max_{d\in D} p^T f(x,K(x),d)$. The set of such states will be denoted by $\mathscr{R}_f(R,K,\tau)$.

On a computational note, numerical solutions of H-J equations can be calculated on a grid of the continuous state space $\mathbb{R}^n$ using the MATLAB Toolbox for Level Set Methods developed by Mitchell,[49] implemented based upon the level set theory and computational methodologies described extensively in the texts by Osher and Fedkiw[50] and Sethian.[51] The numerical solutions provide convergent approximations of the true solutions of (3) as the grid size is refined. However, due to computational complexity, the continuous models are required to be low order ($n \leq 5$).

IV.B. Unsafe Sets

Two kinds of unsafe sets are introduced in this work: those in which there is no safe behavior within that set if the disturbance plays optimally, and those in which an unsafe situation (e.g. a collision between two aircraft) may result if a specific controller is used while in that set. The latter (called the *collision set* in this work) is of primary importance in this paper.

Definition 2: Given a set A to be avoided, the *unsafe* set $\mathscr{A}_f(A,\tau)$ over time horizon τ for system (2) is the set of initial conditions x_0, for which regardless of the choice of feedback control policy $u = K(x,t)$ on $[0,\tau]$, there exists a realization of the disturbance d satisfying $d(t) \in \mathbb{D}$, $\forall t \in [0,\tau]$, such that the state trajectory under (2) satisfies $x(t) \in A$, for some $t \in [0,\tau]$.

From this definition, it can be observed that the main difference between a capture set and an unsafe set lies in the objective of the control. Namely, in the former case, the control tries to reach some terminal set R, while in the latter case, it tries to avoid some terminal set A. Correspondingly, an unsafe set can be computed similarly as in (3) by setting $\phi(x,0) = \phi_A(x)$ for some level set representation of A and defining the Hamiltonian as

$$H(x,p) = \max_{u\in\mathbb{U}} \min_{d\in\mathbb{D}} p^T f(x,u,d). \tag{6}$$

It is important to note that the complement of the unsafe set, denoted by $\mathscr{A}_f^C(A,\tau) = \mathbb{R}^n \backslash \mathscr{A}_f(A,\tau)$, is the set of initial conditions x_0 for which there exists some choice of policy $u = K(x,t)$ such that regardless of the disturbance d, the system trajectory satisfies $x(t) \notin A$, $\forall t \in [0,\tau]$ and hence the safety constraint.

Definition 3: Given a set A to be avoided, and a choice of control law $K : \mathbb{R}^n \to \mathbb{R}^n$, the *collision* set $\mathscr{A}_f(A,K,\tau)$ over time horizon τ for system (2) is the set of initial conditions x_0 for which there exists a disturbance realization d satisfying $d(t) \in \mathbb{D}$, $\forall t \in [0,\tau]$, such that $x(t) \in A$ for some $t \in [0,\tau]$, if $u = K(x)$ on $[0,\tau]$.

In other words, a collision set is the set of states for which the system trajectory under a particular choice of control law may be rendered unsafe by run-time disturbances. This set can be found by setting the Hamiltonian to $H(x,p) = \min_{d \in D} p^T f(x,K(x),d)$. By inverting the above definition, it can be seen that the complement of a collision set $\mathscr{A}_f^C(A,K,\tau) = \mathbb{R}^n \backslash \mathscr{A}_f(A,K,\tau)$ is the set of initial conditions x_0 for which regardless of the disturbance realization d, the system trajectory satisfies $x(t) \notin A$, $\forall t \in [0,\tau]$, if $u = K(x)$ on $[0,\tau]$.

IV.C. Invariant Set

Definition 4: An *invariant* set W_f^∞ for system (2) is a set of initial conditions x_0, for which there exists a choice of control policy $u = K(x,t)$, such that regardless of any disturbance d satisfying $d(t) \in \mathbb{D}$, $\forall t \in [0,\tau]$, the state trajectory under (2) satisfies $x(t) \in W_f^\infty$, $\forall t \geq 0$.

In fact, this set can be computed by a modification of the unsafe set calculation. Specifically, observe that for a given set $W_0 \subset \mathbb{R}^n$, the set of initial conditions $x_0 \in W_0$ for which there exists a policy $u = K(x,t)$ such that the system trajectory satisfies $x(t) \in W_0$, $\forall t \in [0,\tau]$, regardless of the disturbance d is given by $W_f(\tau) = \mathscr{A}_f^C(W_0^C,\tau)$. Thus, by letting $\tau \to \infty$, an invariant subset of W_0 can be computed over arbitrarily long time horizons. If the solution of the corresponding H-J equation for $W_f(\tau)$ converges, namely suppose $W_f(\tau) \to \bar{W}_f \subset \mathbb{R}^n$, then the infinite horizon invariant set is simply given by $W_f^\infty = \bar{W}_f$. For further details, the interested reader is referred to previous work by Tomlin et al.[47]

V. Maneuver Sequence Design Using Reachability Analysis

From the discussions in Section III, the main difficulties associated with the maneuver sequence design problems posed in Problem 1 and 2 include 1) nondeterminism in system dynamics, and 2) proper composition of the maneuver sequence through the switching conditions.

The nondeterminism in the system dynamics arises from both the realization of the disturbances, which is unknown at design time, and the timings of the external switching commands given by human operators, which could vary from one execution of the maneuver sequence to another. For a robust controller design, the design procedure needs to take into account the set of all

admissible system trajectories under these uncertainties. On the other hand, proper composition of maneuvers is necessary to ensure that any given maneuver in the sequence will terminate in a condition for which the objectives of the next maneuver is feasible.

In the following, some procedures are proposed for performing controller design for Problems 1 and 2 in a systematic manner, through the use of reachability analysis as described in Section IV to guide the design of continuous feedback laws and switching conditions.

V.A. Target Attainability Objectives

Suppose that the target set sequence R_i and the avoid set A are given. Consider the following procedure to satisfy the objectives of Problem 1, starting with $q_i = q_N$.

1. Design a control law K_i that regulates the continuous state x from R_{i-1} to R_i.
2. Compute the capture set for q_i to the first time instant τ_i, such that $R_{i-1} \subset \mathscr{R}_{f_i}(R_i, K_i, \tau_i)$.
3. Compute (over the same period $[0, \tau_i]$) the corresponding collision set $\mathscr{A}_{f_i}(A, K_i, \tau_i)$.
4. Verify the safety condition $R_{i-1} \subset \mathscr{A}^C_{f_i}(A, K_i, \tau_i)$. If this condition does not hold, modify the design of the control law K_i. Otherwise, go on to the following step.
5. Repeat steps 1-3 for q_{i-1} until q_1. For q_1, set $R_0 = X_0$, where X_0 is the set of permissible initial conditions.
6. Choose guard conditions as

$$\gamma_{i(i+1)} = \mathscr{R}_{f_{i+1}}(R_{i+1}, K_{i+1}, \tau_{i+1}) \cap \mathscr{A}^C_{f_{i+1}}(A, K_{i+1}, \tau_{i+1}),\ i = 0, ..., N-1.$$

7. Choose domain of each maneuver as $Dom(q_i) = R_i^C$, $i = 1, ..., N-1$ and $Dom(q_N) = \mathbb{R}^n$.

It can be verified that the resulting feedback laws and switching conditions from this procedure will satisfy the specifications of Problem 1. First, by steps 1-4 of the design procedure, the feedback law K_i satisfies $R_{i-1} \subset \mathscr{R}_{f_i}(R_i, K_i, \tau_i) \cap \mathscr{A}^C_{f_i}(A, K_i, \tau_i)$, thus ensuring that, under the dynamics of maneuver q_{i-1}, any system trajectory initialized from within R_{i-1} will reach R_i within τ_i time units under K_i, regardless of the realization of the disturbance d_i. Second, by the choice of the guard condition in step 6, a commanded transition from maneuver q_{i-1} to q_i is only enabled when the continuous state x is in a configuration for which the objectives of q_i is feasible under control law K_i. Finally, the choice of the maneuver domain in step 7 specifies an autonomous transition to the next maneuver when the target set of a given maneuver q_i is reached, so as to prevent scenarios where the system trajectory enters and leaves the feasible set of maneuver q_{i+1}, before an operator command to transition is received by the UAV.

Remark 1: It is assumed that the maneuvers q_i and the target sets R_i are chosen in such a manner so as to enable the design of a family of control laws K_i driving the system state from R_{i-1} to R_i according to standard techniques for either linear or nonlinear continuous time systems, for example according to previous work on motion primitive design for autonomous aerial vehicles.[40,41]

For the AAR application, it is sufficient to consider simple proportional controllers for driving the vehicle states from one waypoint to the next under standard kinematic models for the motion of the UAV and the tanker aircraft.

Remark 2: The safety verification step 4 in the above procedure is important due to the fact that there may be nonempty intersection between the capture set $\mathscr{R}_{f_i}(R_i, K_i, \tau_i)$ and the collision set $\mathscr{A}^C_{f_i}(A, K_i, \tau_i)$. This corresponds to the set of initial conditions x_0 for which there may exist some realization of the disturbance d_i on $[0, \tau_i]$ such that, under control law K_i, the system trajectory satisfies $x(t) \in R_i$, for some $t \in [0, \tau_i]$, but $x(t') \in A$ for some $t' \in [0, t)$. In such a case, K_i is a choice of control law which achieves the target attainability, but not necessarily the safety objective.

Remark 3: The choice of guard condition in step 6 is somewhat conservative due to the fact it may preclude certain system states from which the system trajectory can enter the desired target set of a maneuver before entering an unsafe configuration. To reduce this conservatism, a modified reachability calculation combining target attainability and safety objectives can be performed, by solving a *constrained* H-J PDE.[52] This would then replace the capture sets and collision sets in the maneuver sequence design procedure. The method given here is chosen for simplicity of presentation and ease of computation.

V.B. Invariance Objectives

For Problem 2, it can be observed that the target attainability objectives for the transition maneuvers q_i can still be satisfied by performing the design procedures given in the preceding section. However, some additional design steps are necessary in order to ensure that the invariance objectives are met, and that the stationary maneuvers are properly composed with the transition maneuvers. For this, consider the following design procedure for the stationary maneuvers $\hat{q}_i$.

1. Design a stabilizing control law $\hat{K}_i$ for R_i.
2. Choose a set $\tilde{W}_i$ satisfying $R_i \subset \tilde{W}_i \subset \gamma_{i(i+1)}$, where the guard condition $\gamma_{i(i+1)}$ is as chosen in step 6 of the design procedure for Problem 1 (note that $\gamma_{i(i+1)} \subset \mathbb{R}^n \backslash A$).
3. Compute an invariant subset $W^{\infty}_{\hat{f}_i} \subset \tilde{W}_i$ as per the procedures described in Section IV.C.
4. Check the condition $R_i \subset W^{\infty}_{\hat{f}_i}$. If this condition does not hold, then modify either the control law $\hat{K}_i$ or the choice of $\tilde{W}_i$.
5. Choose guard conditions $\hat{\gamma}_i = W^{\infty}_{\hat{f}_i}$, $i = 1, \ldots, N$.

6. Repeat steps 1-5 for each stationary maneuver $\hat{q}_i$. For $i = N$, set $\gamma_{N(N+1)} = \mathbb{R}^n \backslash A$.

For a control law $\hat{K}_i$ designed according to steps 1-4 of this procedure, the resulting system trajectory initiated from any state $x_0 \in W^{\infty}_{\hat{f}_i}$ will satisfy $x(t) \in W^{\infty}_{\hat{f}_i}$, $\forall t \geq 0$, by definition of the invariant set given in Section IV.C. Furthermore by ensuring the condition $R_i \subset W^{\infty}_{\hat{f}_i}$ in step 4 and by choosing the guard condition as in step 5, it is assured that a transition from maneuver q_i into $\hat{q}_i$ is only taken when x lies in the invariant set $W^{\infty}_{\hat{f}_i}$. Finally, by choosing $\tilde{W}_i$ as in step 2, the invariant subset $W^{\infty}_{\hat{f}_i}$ is assured to lie within the feasible set of the next transition maneuver q_{i+1}. As in the case of Problem 1, it is assumed that a stabilizing control laws $\hat{K}_i$ can be designed for maneuver $\hat{q}_i$ in a feasible manner, for example through appropriate choices of motion primitives.[40,41]

VI. Extensions for Non-ideal Operating Conditions

VI.A. Command Latency

In scenarios where a human operator is situated at a large geographical distance away from the UAV, communication latency could cause large delays in the reception of operator commands by the UAV, as well as in the transmission of state data to the operator. Without some mitigating control or supervision, this could result in significant difficulties for the UAV operator in awareness of dangerous approaches, awareness of collision, etc.[2]

The design of guard conditions as described in Section V will guard against unsafe commands made under delayed information, by checking feasibility conditions defined in terms of capture sets and collision sets. However, to minimize operator mistakes, appropriate modifications of the capture sets and collision sets can be presented as visual aids, taking into account the effects of latency. In the following discussion, it is assumed that there is a deterministic, symmetric latency of L time units in the communication channel, known at design time. For simplicity of presentation, these modifications will be described only for the case of Problem 1.

First, it is remarked that the capture set calculation given in Section IV.A can be appropriately modified to compute the set of initial conditions controllable to a target set R *at the end* of some time interval $[0,\tau]$, rather than *within* $[0,\tau]$, by simply replacing the $\min(0,H)$ term in (3) by H.[48] This modified capture set will be denoted by $\bar{\mathscr{R}}_f(R,K,\tau)$.

To ensure the target attainability condition, first consider a modification of the capture set for maneuver q_i under latency as follows.

$$\mathscr{R}^{Lat}_{q_i}(R_i,K_i,\tau_i,L) = \bar{\mathscr{R}}_{f_{i-1}}(\mathscr{R}_{f_i}(R_i,K_i,\tau_i),K_{i-1},2L)$$

In other words, this is the set of states that can be driven inside the capture set of q_i at the end of the time interval $[0,2L]$ by the control law K_{i-1}.

Now suppose that the human operator uses the set $\mathscr{R}^{Lat}_{q_i}(R_i,K_i,\tau_i,L)$ as a visual aid for the

decision whether to transition from q_{i-1} to q_i. Consider a scenario during run-time where the state vector of the UAV at time t satisfies $x(t) \in \mathscr{R}^{Lat}_{q_i}(R_i, K_i, \tau_i, L)$. This information is received by the human operator at time $t+L$, when the actual state of the UAV has translated to some new value $x(t+L)$ under control law K_{i-1}. If the operator decides, based upon this information, to issue a maneuver transition command, then the command will be received by the UAV at time $t+2L$. Then by definition of the modified capture set calculation, $x(t+2L) \in \mathscr{R}_{f_i}(R_i, K_i, \tau_i)$. This ensures that the target attainability objective will be satisfied for maneuver q_i.

To also ensure the safety condition, consider a modified collision set calculation for maneuver q_i under latency as follows.

$$\mathscr{A}^{Lat}_{q_i}(A, K_i, \tau_i, L) = \mathscr{A}_{f_{i-1}}(\mathscr{A}_{f_i}(A, K_i, \tau_i), K_{i-1}, 2L)$$

In other words, this is the set of states that can arrive inside the collision set of q_i within the time interval $[0, 2L]$ under the control law K_{i-1}.

Now suppose that the human operator also has access to the set $\mathscr{A}^{Lat}_{q_i}(A, K_i, \tau_i, L)$ when making the decision on transitioning from q_{i-1} to q_i. Consider a scenario during run-time where the state vector of the UAV at time t satisfies $x(t) \notin \mathscr{A}^{Lat}_{q_i}(A, K_i, \tau_i, L)$. This information is received by the human operator at time $t+L$, when the actual state of the UAV has translated to some new value $x(t+L)$ under control law K_{i-1}. If the operator decides, based upon this information, to issue a maneuver transition command, then the command will be received by the UAV at time $t+2L$. Then by definition of the collision set, the system trajectory satisfies $x(t') \notin \mathscr{A}_{f_i}(A, K_i, \tau_i), \forall t' \in [t, t+2L]$. This ensures that the transition to maneuver q_i will be safe.

It is important to note that in the case where L is only an upper bound rather than the exact communication latency, then the use of $\mathscr{A}^{Lat}_{q_i}(A, K_i, \tau_i, L)$ as described above will still ensure that the safety condition is not violated when the transition command is received by the UAV.

VI.B. Improper Initialization

In scenarios where a fault condition occurring during run-time causes the assumptions of the hybrid system model to be violated, the guarantees provided by the reachability analysis will no longer be valid. However, some appropriate design choices can be made at design time to enable recovery from certain classes of fault condition. In this work, the fault condition of improper initialization will be considered. Specifically, this is the case where the overall maneuver sequence is initialized in an initial condition $x_0 \notin \gamma_{01} = \mathscr{R}_{f_1}(R_1, K_1, \tau_1) \cap \mathscr{A}^C_{f_1}(A, K_1, \tau_1)$, for example due to difficulties in resolving multiple collision constraints in mixed-initiative scenarios. In such cases, there is no guarantee that the system trajectory will satisfy the target attainability and safety objectives of maneuver q_1, under the control law K_1. However, there may nonetheless exist alternative choices of control laws which will recover the system within the guard condition $\gamma_{i-1(i)}$ of some maneuver

q_i, possibly with $i \neq 1$, so that the maneuver sequence can be performed from q_i onwards.

To address this fault condition, the designer can consider adding a finite number of general purpose maneuvers $\{\tilde{q}_1, \tilde{q}_2, ..., \tilde{q}_M\}$, for example "turn left", "turn right", "move forward", etc., each equipped with system dynamics $\dot{x} = \tilde{f}_i(x, \tilde{u}_i, \tilde{d}_i)$ and control law $\tilde{K}_i$. Throughout the rest of this paper, these maneuvers will be referred to as *escape maneuvers*. The problem of recovering from the fault condition could then be formulated as one of constructing a maneuver sequence from the library of escape maneuvers at run-time, which drives the continuous state of the system into the feasible set $\gamma_{i-1(i)}$ of a maneuver q_i in the nominal maneuver sequence.

In this case, the ordering of escape maneuvers may not be anticipated at design time. Thus, in scenarios with large latency L, an autonomous solution to this problem is preferred. In separate work by the authors,[53] an algorithm for automatically synthesizing a maneuver sequence that drives the state of the system into some desired target set while evading some undesirable avoid set is discussed. In this paper, to take full advantage of the insight provided by trained human operators, the focus will be on scenarios with small latency, where reachable set information can be used at run-time to guide the construction of the maneuver sequence under human supervision.

First, for each escape maneuver $\tilde{q}_i$, a collision set computation can be performed at design time to determine the set of states $\mathscr{A}_{\tilde{f}_i}(A, \tilde{K}_i, \tilde{\tau}_i)$ that can be driven into A by some realization of the disturbance $\tilde{d}_i$, over some appropriate choice of time horizon $\tilde{\tau}_i$. The time horizon should be long enough so that the collision set does not provide misleading information to the human operator, but also not so long that the resulting decisions are rendered excessively conservative, and appropriate time horizons will differ for each application and system dynamics.

At run-time, a human operator can consult these sets to determine appropriate choices of escape maneuvers. As long as the system is initialized at a state outside the intersection of collision sets for the escape maneuvers, namely $x_0 \notin \bigcap_{\tilde{q}_i} \mathscr{A}_{\tilde{f}_i}(A, \tilde{K}_i, \tilde{\tau}_i)$, at least one safe escape maneuver $\tilde{q}_i$ is available. A safe maneuver can then be selected so as to make progress towards the feasible set $\gamma_{i-1(i)}$ of q_i, while avoiding the set A. During the execution of this maneuver over time interval $[0, \tilde{\tau}_i]$, the operator can consult the computed collision sets and plan the next escape maneuver $\tilde{q}_j$ in the fault recovery sequence. Then when it is safe to perform maneuver $\tilde{q}_j$, a command can be issued to transition, and the procedure would repeat until the system state enters $\gamma_{i-1(i)}$.

VII. Example

VII.A. Automatic Aerial Refueling (AAR) Process

In a typical aerial refueling process, a formation of unmanned aerial vehicles (UAVs) approaches a human piloted tanker aircraft. One by one, the UAVs perform a sequence of maneuvers to dock with a human operated fuel boom and then return to formation. A graphical top down view of the refueling process is shown in Fig. 2.

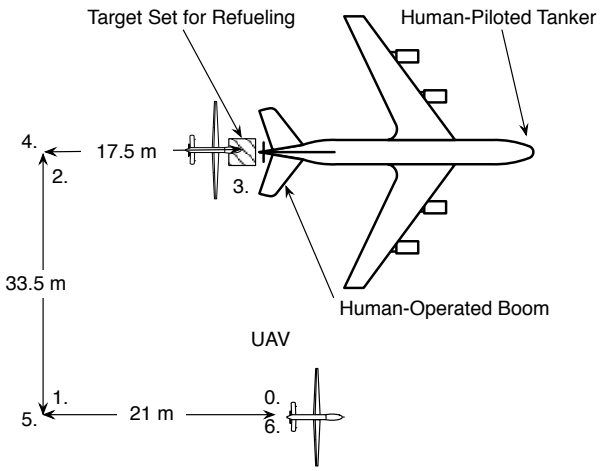


Figure 2. Aerial Refueling Process. Maneuvers between each waypoint are described in Table 1.

The tanker aircraft is shown in the center, with the refueling UAV flying in formation to be refueled. In the actual refueling process, the UAV would always approach from a fixed position in the formation. For modeling purposes, the aircraft to be refueled is assumed to approach from a position behind and to the right of the tanker aircraft. From this position, the UAV will initiate a sequence of maneuvers through the numbered waypoints, under a combination of human operator commands and autonomous decisions. The possible maneuvers in the process are shown in Table 1. The calculations in this paper utilize the separation of these waypoints found in the work of Ross et al.[10]

Event	**Maneuver**	**Man.#**	**Description**
σ_{12}	Detach 1	1	a single UAV detaches from a formation of UAVs in flight to a position slightly behind and to the right of a tanker aircraft.
σ_{23}	Precontact	2	the UAV banks left towards a position directly behind the tanker aircraft.
σ_{34}	Contact	3	the UAV approaches the tanker aircraft from behind to allow the boom operator on board the tanker to lower the fuel boom and catch the UAV.
σ_{45}	Postcontact	4	the UAV slows down and moves away from the tanker aircraft after the boom operator detaches the fuel boom.
σ_{56}	Detach 2	5	the UAV banks right towards a position directly behind the UAV formation.
σ_{67}	Rejoin	6	the UAV speeds up and rejoins the formation to complete the refuel sequence.

Table 1. Default maneuvers in the aerial refueling process (see Fig. 2).

VII.B. Aircraft Model

Note that in a formation of UAVs, refueling occurs one vehicle at a time. Thus the rest of this paper examines the interaction between a single UAV and the tanker aircraft. This approach leverages previous work[8,17] by modeling the continuous behavior of the two aircraft in relative coordinates. The model assumes that the two aircraft do not change altitude significantly in performing the aerial refueling maneuvers, and this is justified in the state of the practice for human-piloted maneuvers of this kind. In fact, using a change in altitude might jeopardize the success of the mission, as a Boom Operator might suspend the mission if loss of line of sight occurs; thus, there is motivation to preserve a 2D solution. Recent work by Williamson et al.[44] provides promise that autonomous vehicles will be capable of sufficiently accurate onboard sensing to utilize the selected coordinate system. Placing the two aircraft in a 2D plane, the relative motion of the two aircraft in the UAV reference frame can be modeled as:

$$\dot{x} = f(x,u,d) = \frac{d}{dt}\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} -u_1 + d_1\cos x_3 + u_2 x_2 \\ d_1 \sin x_3 - u_2 x_1 \\ -u_2 \end{bmatrix} \tag{7}$$

where x_1, x_2, x_3 are the longitudinal, lateral, and heading coordinates of the tanker aircraft in the UAV reference frame, u_1, u_2 are the translational and angular velocities of the UAV as indicated in Fig. 3, and d_1 is the translational velocity of the tanker aircraft. In this model, the tanker is assumed to hold a constant heading, namely it is in straight and level flight.

Capture sets and collision sets will be computed for each maneuver in Table 1 using the above dynamics. The computations will initially assume the velocity of the tanker aircraft to be deterministic, namely the range $\mathbb{D}$ is the single element v_0 representing the nominal forward velocity of the tanker aircraft. However, as discussed in Section IV, the computation can be modified in a straightforward manner to account for fluctuations in the tanker velocity within a bounded range, and this case is covered in Section VIII.E which demonstrates the corresponding changes to the capture sets and collision sets.

For completeness, it should be noted that the relative coordinates in the UAV reference frame and the tanker reference frame are related by a nonlinear coordinate transformation. Specifically, suppose $x = (x_1, x_2, x_3)$ is the coordinates of the tanker in the UAV reference frame, and $\tilde{x} = (\tilde{x}_1, \tilde{x}_2, \tilde{x}_3)$ is the coordinates of the UAV in the tanker reference frame, then $\tilde{x} = T(x)$, where $T : \mathbb{R}^3 \to \mathbb{R}^3$ is given by

$$T\left(\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}\right) = \begin{bmatrix} -x_1\cos x_3 - x_2 \sin x_3 \\ x_1 \sin x_3 - x_2 \cos x_3 \\ -x_3 \end{bmatrix} \tag{8}$$

This transformation will become useful in transforming target sets and avoid sets specified in tanker coordinates into UAV coordinates. Specifically, suppose a set $\tilde{S}$ is represented by a function $\tilde{\phi}$ in the tanker reference frame (namely $\tilde{\phi}(\tilde{x}) \leq 0$, $\forall \tilde{x} \in \tilde{S}$), then the corresponding set S in the UAV reference frame is represented by the function $\phi = \tilde{\phi} \circ T$.

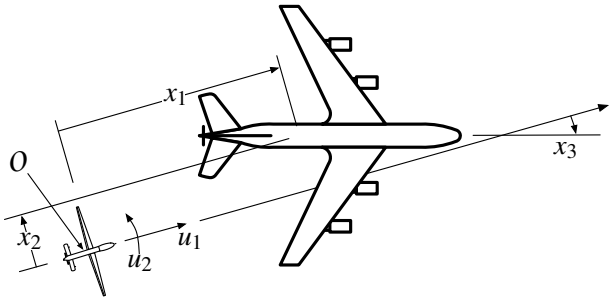


Figure 3. Relative-coordinate system, kinematic model. The origin of the coordinate system is centered on the UAV.

VII.C. Hybrid System Model

In the specific case of aerial refueling, consider the hybrid automaton shown in Fig. 4. In this model, the maneuver sequence consists of the set of flight maneuvers listed in Table 1, labeled q_1 to q_6, along with six stationary modes $\hat{q}_1$ to $\hat{q}_6$. In addition, there are four general purpose escape maneuvers, labeled $\tilde{q}_1$ to $\tilde{q}_4$ to handle fault conditions as discussed in Section VI. The system dynamics within each flight maneuver is identical and given by (7). The various maneuvers differ only by the choice of control laws K_i, $\tilde{K}_i$, and $\hat{K}_i$, corresponding to transition maneuvers, stationary maneuvers, and escape maneuvers, respectively.

As discussed in Section III, the design parameters include the maneuver control laws, guard conditions for the command transitions, along with the domain of each flight maneuver. In order to proceed with the design procedure given in Section V, the form of the control laws chosen for each flight maneuver, along with the target sets and avoid sets will be defined.

VII.D. Control Law Design

The feedback control laws to perform the various maneuvers are applied through the inputs u_1 and u_2. To emulate high-level waypoint following algorithms, proportional control laws are used to steer the UAV to the various desired waypoints. For transition maneuvers q_1 to q_6, the equations for the feedback laws are given by

$$u_1 = k_1(x_1 - x_{1f}) + v_0 \tag{9}$$

$$u_2 = k_2(x_2 - x_{2f}) \tag{10}$$

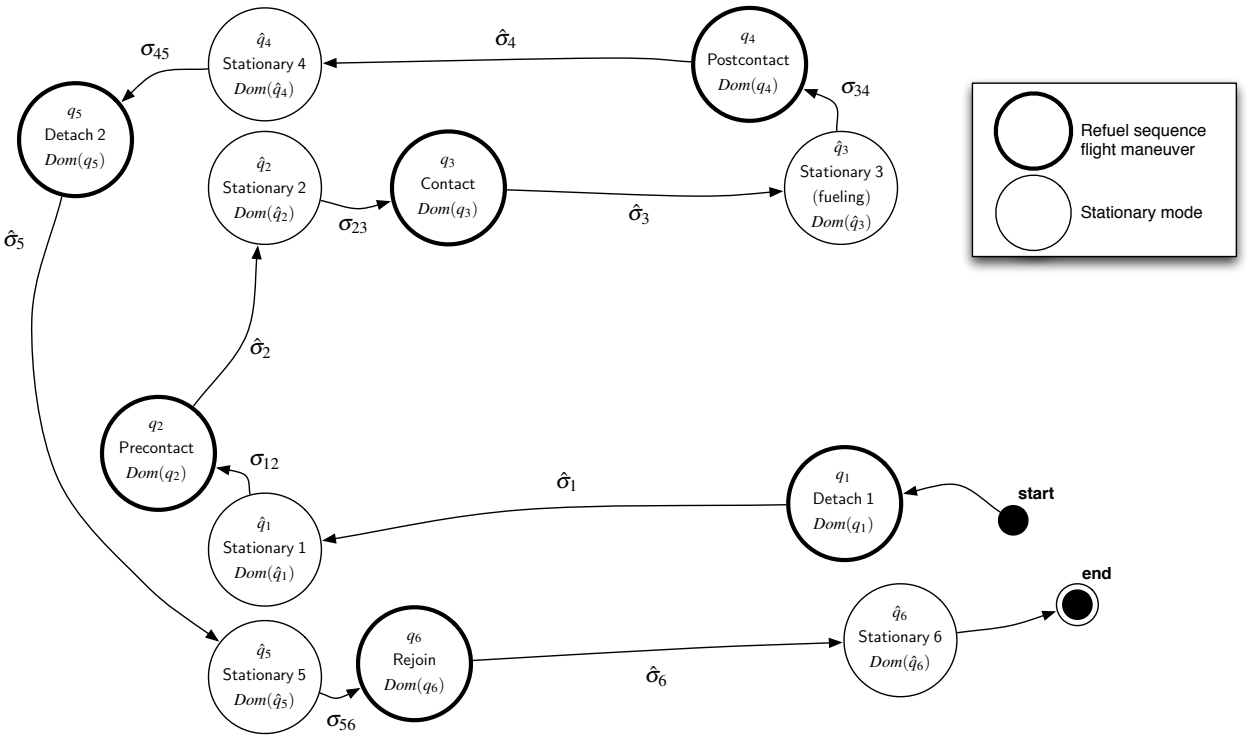


Figure 4. Aerial refueling formation transition model. The layout of the stationary flight modes pictured here roughly corresponds to relative positions of the target sets (compare to Fig. 2).

where k_1 and k_2 are proportional gain constants, and x_{1f}, x_{2f} are the desired waypoint locations in the UAV reference frame. To take into account actuator limitations, the above control law is saturated to be within the input ranges $[u_{1_{\min}}, u_{1_{\max}}]$ and $[-u_{2_{\max}}, u_{2_{\max}}]$, which defines the control input space $\mathbb{U}$. The control law for each stationary maneuver $\hat{q}_i$, $i = 1, ..., 6$ is chosen to be identical as that of the immediately preceding maneuver q_i.

The control laws for the four escape maneuvers $\tilde{q}_i$, $i = 1, ..., 4$ are designed as follows: 1) *Escape 1* (steer left at max speed): $u_1 = u_{1_{\max}}$, $u_2 = u_{2_{\max}}$; 2) *Escape 2* (steer right at max speed): $u_1 = u_{1_{\max}}$, $u_2 = -u_{2_{\max}}$; 3) *Escape 3* (slow down): $u_1 = u_{1_{\min}}$, $u_2 = 0$; 4) *Escape 4* (speed up): $u_1 = u_{1_{\max}}$, $u_2 = 0$.

The desired final locations for the flight maneuvers (except the escape maneuvers) are specified in Table 2. The proportional gain constants will be chosen so as to achieve the safety and reachability objectives in the maneuver sequence design.

VII.E. Target, Avoid Sets

The target set R_i for each maneuver q_i is chosen to be a disc shaped neighborhood around each desired waypoint (see Fig. 5), with bounds on the relative heading error. This selection of a disc shaped target is consistent with the objective of controlling the aircraft to within some Euclidean distance of a given waypoint. For waypoint i, this set can be specified in tanker coordinates as $\tilde{R}_i = B([-x_{1f}(q_i),\ -x_{2f}(q_i)], r_0) \times [-\Delta\theta, \Delta\theta]$ where $B(x_0, r)$ denotes a ball of radius r, centered

Table 2. Target Position Offsets (x_{1f}, x_{2f}, in meters).

Maneuver	Mode Label	x_{1f}	x_{2f}
Detach 1, Stationary 1	$q_1, \hat{q}_1$	25.5	33.5
Precontact, Stationary 2	$q_2, \hat{q}_2$	25.5	0
Contact, Stationary 3	$q_3, \hat{q}_3$	8.0	0
Postcontact, Stationary 4	$q_4, \hat{q}_4$	25.5	0
Detach 2, Stationary 5	$q_5, \hat{q}_5$	25.5	33.5
Rejoin, Stationary 6	$q_6, \hat{q}_6$	4.5	33.5

at x_0 in $\mathbb{R}^2$. In this case, the radius and heading tolerance are chosen to be $r_0 = 4$ m and $\Delta\theta = \pi/16$ rad, respectively. The corresponding set in the UAV coordinate frame is obtained from the transformation T in (8).

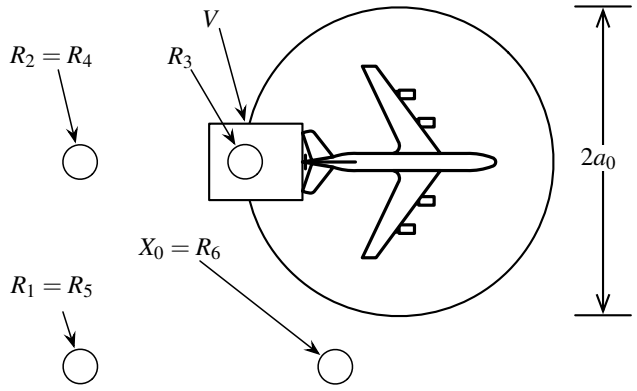


Figure 5. Target sets for each maneuver, the avoid set (with radius a_0), and safe neighborhood around the boom, V.

Each flight maneuver uses an identical avoid set A, namely the set of continuous states corresponding to minimum separation infringement (MSI) violation between the tanker aircraft and UAV. This set consists of a disc in the x_1-x_2 plane, with a small neighborhood of states around the fuel boom removed to allow approach by the UAV. In the tanker reference frame, this is given by $\tilde{A} = (B([15,\ 0], a_0) \times [-\pi, \pi]) \setminus V, \forall q_i \in Q$, where $a_0 = 30\,\text{m}$ is the protected radius (chosen based upon published data of the wingspan of a Boeing KC-135 Stratotanker), the origin of the tanker's coordinate system is 15 m from the centroid of the tanker, and V is a small hyper-rectangle of states around the boom location, defined in the tanker reference frame as $V = \left\{\tilde{x} \in \mathbb{R}^3 : -15\text{m} \leq \tilde{x}_1 \leq 10\text{m}, -8\text{m} \leq \tilde{x}_2 \leq 8\text{m}, -\pi \leq \tilde{x}_3 \leq \pi\right\}$. The corresponding avoid set A in the UAV coordinate frame can be obtained from the coordinate transformation T.

VIII. Production and Analysis of Results

The maneuver sequence design procedures described in Section V is now applied to the aerial refueling example, and a simulation of the complete sequence is performed to validate the safety and reachability conditions. This is followed by an example scenario illustrating the use of escape maneuvers to recover from a faulty initialization of the refueling sequence. Finally, the effects of disturbances on capture and collision sets are shown in the case of varying tanker velocity.

For the reachable set computations and simulation results shown in this section, the nominal velocity of the tanker aircraft is chosen to be $v_0 = 84.8$ m/s (75% of the maximum allowable velocity of the UAV); the velocity input u_1 for the UAV has the saturation limits $[40, 113]$ m/s, and the angular velocity input u_2 has the saturation limits $[-\pi/6, \pi/6]$ s^{-1}. The maximum UAV velocity value is based on published specifications for the MQ-9 Predator B; other values are chosen based on realistic constraints.

VIII.A. Capture Sets and Collision Sets

Following the procedure given in Section V.A, the capture set for each mode q_i is computed with respect to a target set R_i to a time instant τ_i at which $R_{i-1} \subset \mathscr{R}_{f_i}(R_i, K_i, \tau_i)$. A collision set computation is then performed to verify the condition $R_{i-1} \subset \mathscr{A}^C_{f_i}(A, K_i, \tau_i)$. For mode q_1, the set R_0 is specified to be the set of permissible initial states X_0, as shown in Fig. 5. The proportional control law for each flight maneuver is tuned appropriately so as to ensure the target attainability and safety objectives are met at each design step. The set of gain constants and maneuver timings obtained from this design procedure is summarized in Table 3.

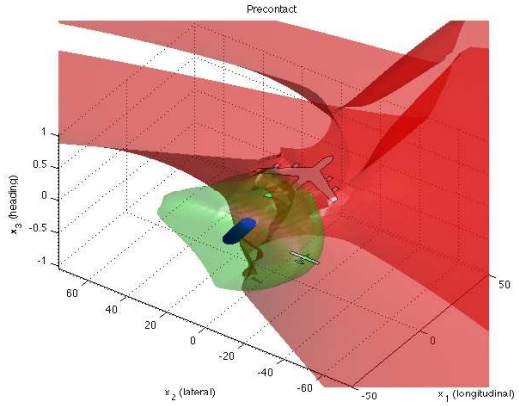
Table 3. Proportional Gain Constants (k_1, k_2) and Maneuver Timings (τ_i in seconds), with elapsed time for an autonomous execution.

Maneuver	k_1	k_2	**Time τ_i (s)**	**Elapsed time (s)**
Detach 1	3	1	1.25	1.25
Precontact	0.5	5	3.00	4.25
Contact	2.5	1	1.00	5.25
Postcontact	2.5	1	1.00	6.25
Detach 2	1	5	3.50	9.75
Rejoin	3	1	1.25	11.0
Escape 1	n/a	n/a	1.5	n/a
Escape 2	n/a	n/a	1.5	n/a
Escape 3	n/a	n/a	1.5	n/a
Escape 4	n/a	n/a	1.5	n/a

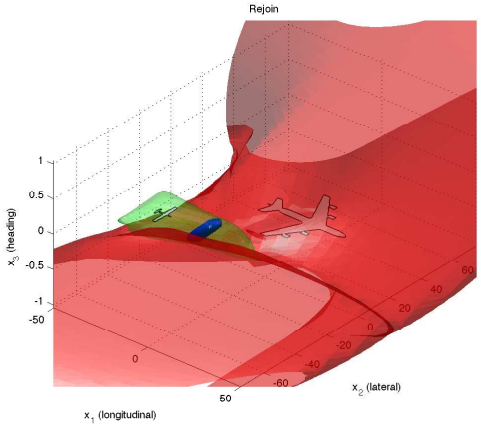
Note that the timings for the escape maneuvers are chosen by the designer, according to the

criterion discussed in Section VI.B. Example capture sets are shown in Fig. 6a and Fig. 6b for the Contact (q_3) and Rejoin (q_6) maneuvers. Using these results, the switching conditions can be synthesized as in Section V.A.

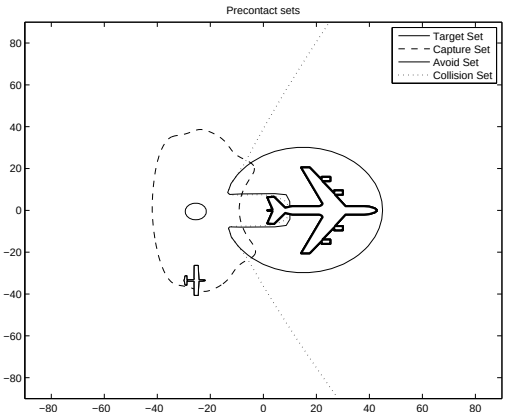
Casual examination of Fig. 6b seems to indicate asymmetric results for a symmetric problem. However, recall that in Fig. 6a, (6b), the vertical axis represents angular heading difference, not altitude difference. In Fig. 6d, a "slice" of the capture and collision sets for Precontact mode at $x_3 = 0$, the asymmetry for the collision set reflects overshoot of the controller that forces the UAV into the avoid set; asymmetry for the capture set is from the granularity of the computational grid. As discussed in Section IV.A, the reachable set surface is an approximation, and if additional grid points exist, the surface more closely approximates a symmetric reach set.



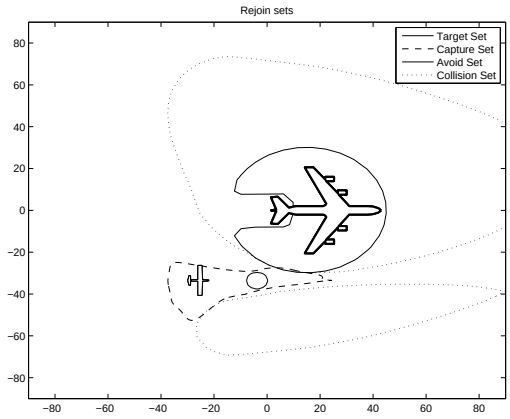
(a) Capture (light, green) and collision (dark, red) sets for Precontact.



(b) Capture (light, green) and collision (dark, red) sets for Rejoin.



(c) Slice of (a) at $x_3 = 0$



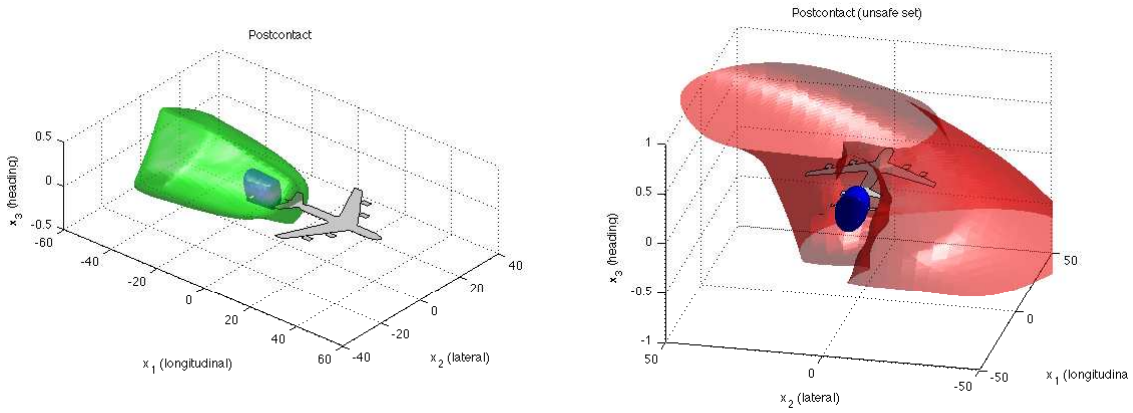
(d) Slice of (b) at $x_3 = 0$

Figure 6. (a) Capture Set for Transition 2 to 3 (Precontact). (b) Capture set for Transition 5 to 6 (Rejoin). Note that the changes in gains and desired waypoint location make this set dramatically different from (a). In each figure, x_1 and x_2 represent longitudinal and lateral offset (respectively), and x_3 represents the offset in heading between the UAV and tanker. (c) A slice of the sets in (a) at $x_3 = 0$ shows that the target set for the Precontact mode is disjoint from the collision set for that maneuver. Likewise, (d) shows the same result for the Rejoin maneuver. Finally, note the disconnected regions of the collision set in (d); the upper region represents the area where executing the control law results in overshoot, putting the UAV in the avoid set (MSI region).

VIII.B. Invariant Sets

For each stationary maneuver $\hat{q}_i$, $i = 1,2,...,6$ in Fig. 4, an invariant set calculation is performed according to the procedure described in Section V.B.

Using the control laws defined in Section VII.D, and with the choice of corresponding gain constants given in Table 3, the invariance criteria are indeed verified for each of the stationary maneuvers. The result of an invariant set calculation is shown in Fig. 7 for Stationary 3 ($\hat{q}_3$), corresponding to when the UAV is expected to be refueling. In these plots, the invariant set $W^{\infty}_{\hat{f}_3}$ satisfies $R_3 \subset W^{\infty}_{\hat{f}_3}$. Additionally, it lies within the feasible set of the next maneuver *Postcontact* (q_4), namely $W^{\infty}_{\hat{f}_3} \subset \mathscr{R}_{f_4}(R_4, K_4, \tau_4) \cap \mathscr{A}^C_{f_4}(A, K_4, \tau_4)$. This condition also implies $W^{\infty}_{\hat{f}_3} \subset A^C$, which means that the trajectory in $\hat{q}_3$ is guaranteed to be safe at all times.



(a) Capture set and invariant set.

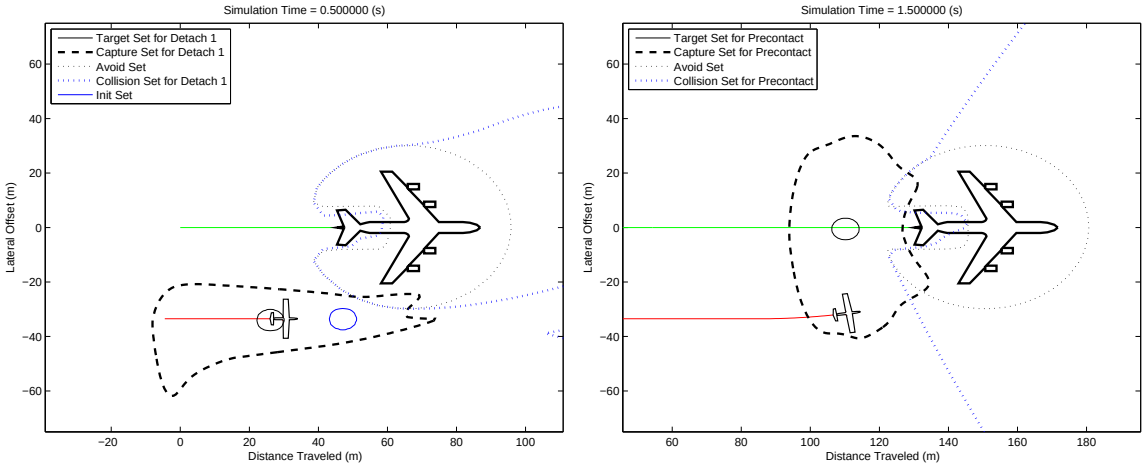
(b) Collision set and invariant set.

Figure 7. Results of the invariance calculation, applied to the Stationary 3 (fueling) maneuver. (a) $W^{\infty}_{\hat{f}_3} \subset \mathscr{R}_{f_4}(R_4, K_4, \tau_4)$, i.e., the inner, blue area shows full containment of the invariant set of maneuver $\hat{q}_3$ within the capture set of maneuver q_4. (b) $W^{\infty}_{\hat{f}_3} \subset \mathscr{A}^C_{f_4}(A, K_4, \tau_4)$, i.e., the collision set of the maneuver q_4 is disjoint from the invariant set of maneuver $\hat{q}_3$.

VIII.C. Refueling Sequence Simulation

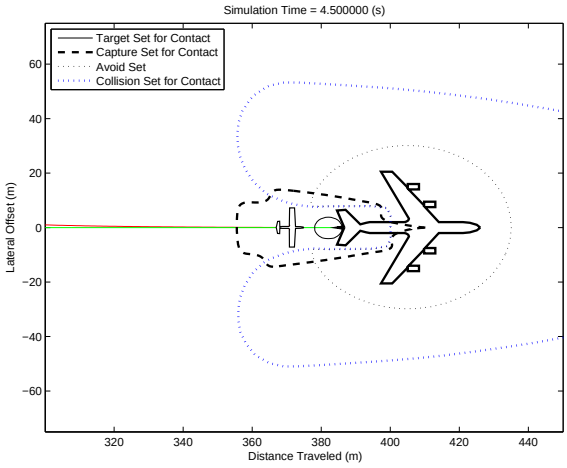
A complete simulation of the refueling sequence is constructed to check the satisfaction of the safety and target attainability objectives. In this simulation, the transitions from maneuver q_i to stationary mode $\hat{q}_i$ are autonomous, namely a forced transition is taken into a stationary mode as the state of the UAV enters the target set of each maneuver.

Some snapshots of the simulation are shown in Fig. 8, where the capture sets and collision sets for each flight maneuver are superimposed on the trajectory of the UAV. As guaranteed by the mode switching conditions, each maneuver is completed within the transition timing given in Table 3, without entering the avoid set A corresponding to MSI. Furthermore, it is verified that with $x \in R_i$ in mode q_i, the conditions $x \in \mathscr{R}_{f_{i+1}}(R_{i+1}, K_{i+1}, \tau_{i+1})$ and $x \notin \mathscr{A}_{f_{i+1}}(A, K_{i+1}, \tau_{i+1})$ are satisfied, allowing the next maneuver in the sequence to be initiated.

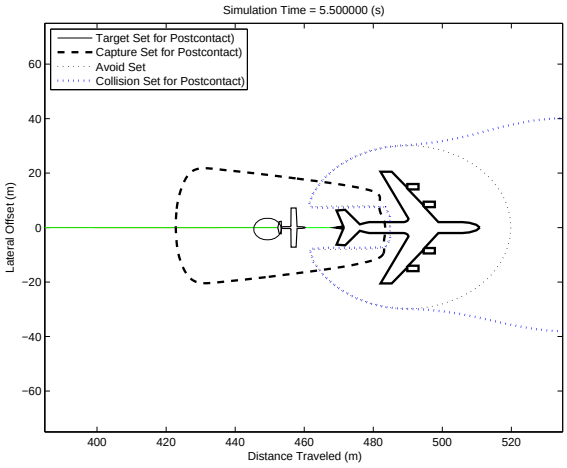


(a) Detach 1

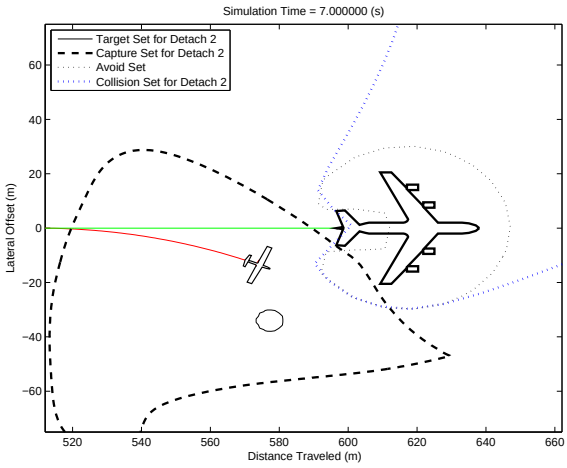
(b) Precontact



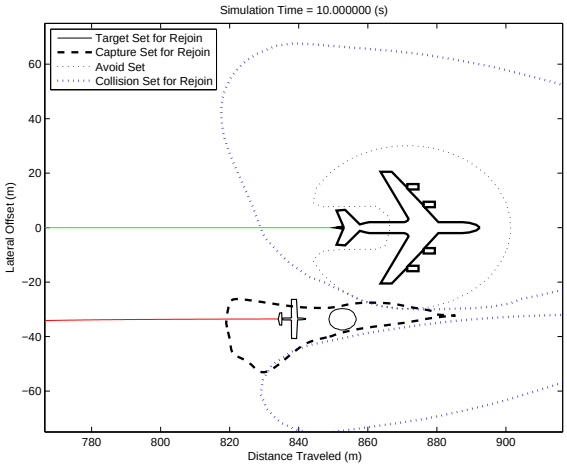
(c) Contact



(d) Postcontact



(e) Detach 2



(f) Rejoin

Figure 8. Refueling sequence simulation with capture sets (dashed lines), avoid and collision sets (dotted lines).

VIII.D. Recovery from Faulty Initialization

In this section, a simulation scenario is formulated with the system state initialized outside the set of feasible initial conditions for *Detach 1* (q_1), as given by γ_{01}. The goal in this case is to construct a sequence of escape maneuvers to arrive at the target set R_2 of the *Precontact* (q_2) maneuver, using the collision sets $\mathscr{A}_{\tilde{f}_i}(A, \tilde{K}_i, \tilde{\tau}_i)$ computed for escape maneuvers 1-4, as well as the capture and collision sets for the *Precontact* maneuver. Human supervision is used to guide the construction of this sequence, the selection of the maneuvers in this simulation is performed using examination of the generated sets by the authors. The results are shown in Fig. 9.

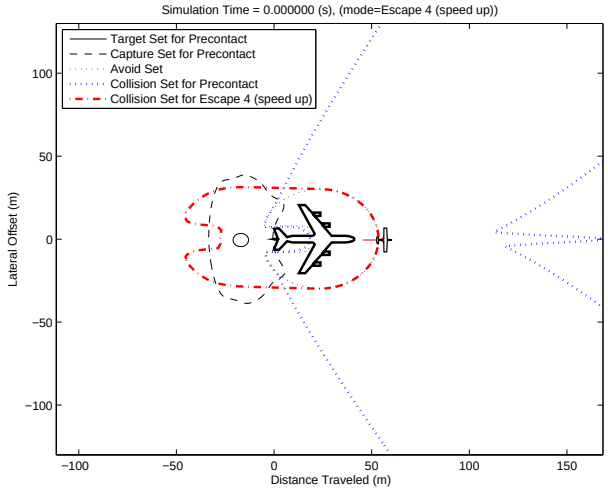
From the first plot, the UAV is initialized with $x \notin \mathscr{R}_{f_2}(R_2, K_2, \tau_2)$ (outside the capture set for Precontact); in fact $x \in \mathscr{A}_{f_2}(A, K_2, \tau_2)$ (the UAV is in the collision set for mode q_2, Precontact). However, being within the collision set for Precontact means only that if the Precontact mode is *selected* that unsafe behavior will occur, not that unsafe behavior is unavoidable. Thus, at this location a safe maneuver is selected—Escape 4 ($\tilde{q}_4$), namely "speed up"—since $x \notin \mathscr{A}_{\tilde{f}_4}(A, \tilde{K}_4, \tilde{\tau}_4)$. After performing this maneuver for some time, while consulting the collision sets, it is found that both $\tilde{q}_2$ (Escape 2) and $\tilde{q}_1$ (Escape 1) become available corresponding to turn right and turn left, respectively. State $\tilde{q}_2$ is chosen first, followed by $\tilde{q}_1$ to return the heading to that of the tanker vehicle, and then $\tilde{q}_3$ (slow down). While reducing speed, the state of the UAV enters the capture set of the *Precontact* maneuver ($x \in \mathscr{R}_{f_2}(R_2, K_2, \tau_2)$), and the UAV mode transitions to the *Precontact* maneuver, and the fault recovery sequence completes.

VIII.E. Effects of Disturbance on Reachable Set Computation

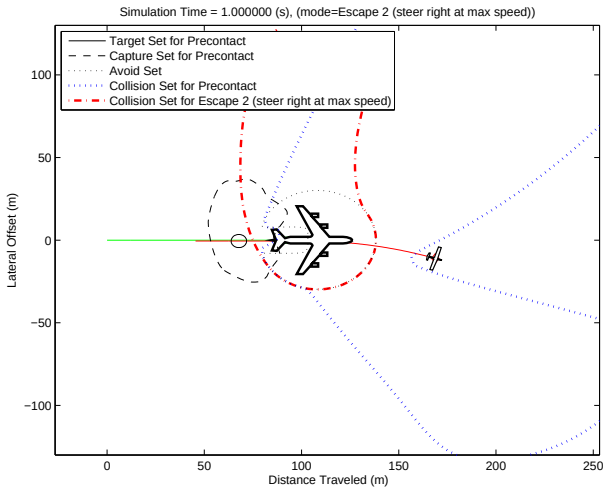
In the preceding simulations, all capture and collision sets are generated assuming the nominal tanker velocity $v_0 = 84.8 m/s$. However, during execution time, there is some degree of uncertainty associated with the velocity of the tanker, due to unmodeled dynamics and various environment disturbances (for example wind effects). This uncertainty may not be significant for maneuvers far enough from the tanker aircraft. However, for the *Contact* maneuver where the UAV needs to come within close proximity of the tanker aircraft, even slight variations in the tanker aircraft speeds may compromise the safety of the maneuver.

As discussed in Section IV, the Hamilton-Jacobi formulation of reachable sets offers the flexibility to account for this uncertainty in the tanker aircraft velocity. In this case, the tanker velocity d_1 is allowed to fluctuate in the bounded range $[79.14, 90.45]$ m/s (70-80% of the maximum allowable velocity of the UAV). The capture and collision sets for the Contact maneuver under the effects of this disturbance are shown in Fig. 10 (a) and (b), along with the same sets calculated under the nominal tanker velocity.

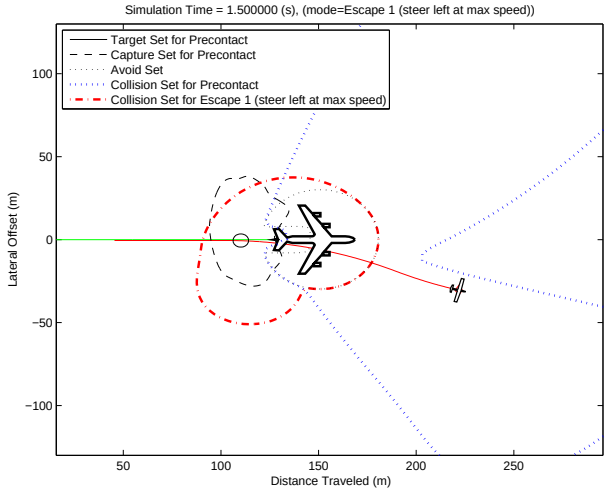
As expected, the capture set with added uncertainty is smaller than that without uncertainty, shown in Fig. 10a. This is due to the fact that under worst case tanker aircraft speed input, the



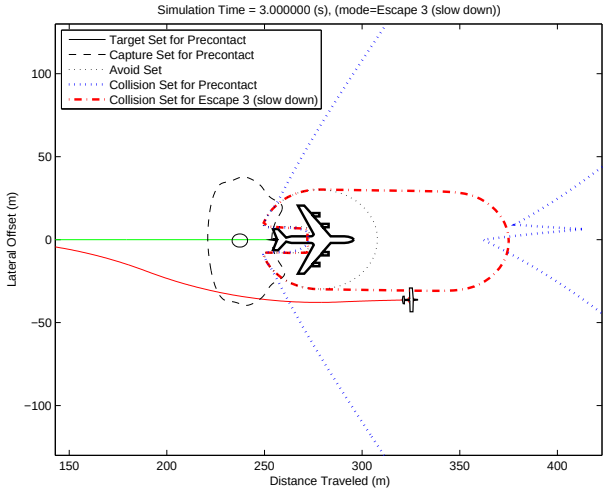
(a) Escape Mode 4 (Speed Up) initiated at $t = 0s$



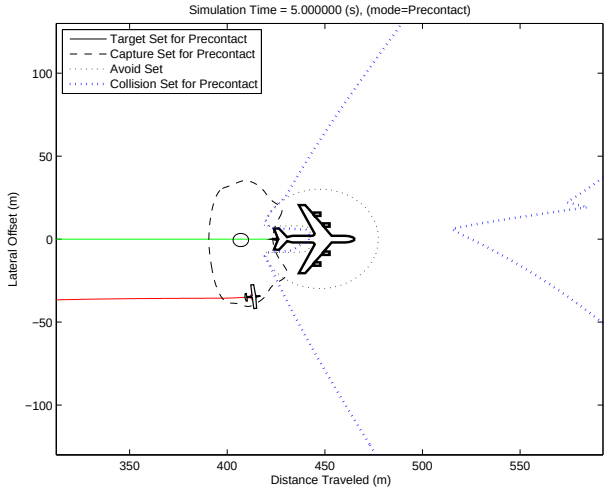
(b) Escape Mode 2 (Steer Right at Max Speed) was initiated at $t = 0.5s$, shown here at $t = 1.0s$



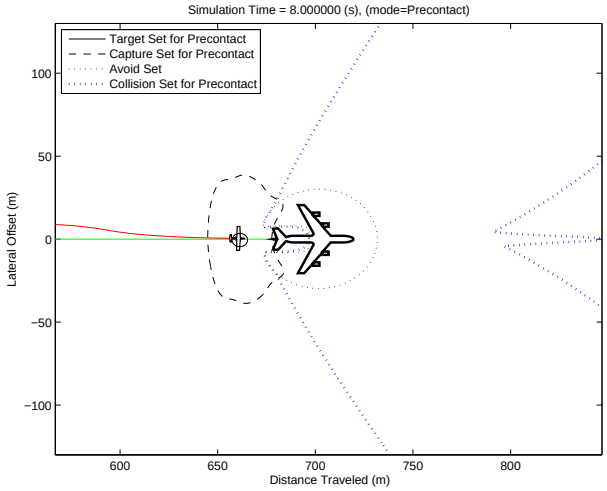
(c) Escape Mode 1 (Steer Left at Max Speed) initiated just before $t = 1.25s$



(d) Escape Mode 3 (Slow down), shown at $t = 3s$

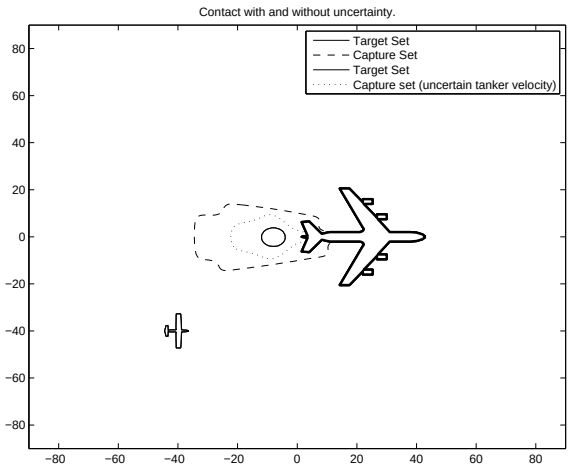


(e) Performing Precontact, shown here at $t = 5s$

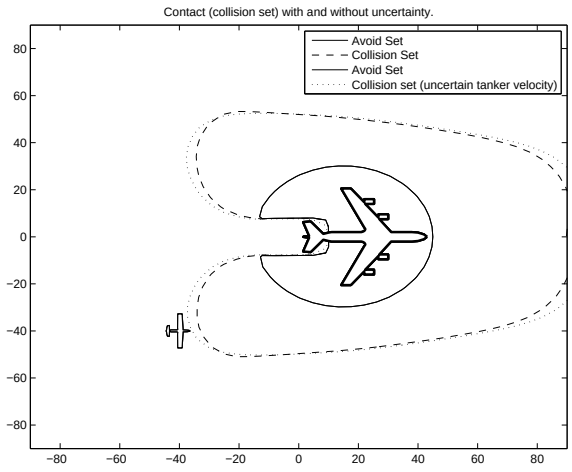


(f) Precontact completed, shown here at $t = 8s$

Figure 9. Maneuvers for fault recovery sequence. The legend shows the capture and collision sets for Precontact, and the collision set for the currently selected escape maneuver. Note that in this design, there is a period where $x \in \mathscr{A}_{f_2}(A, K_2, \tau_2)$, but the controller performs instead a safe escape maneuver $\tilde{q}_i$, for which $x \notin \mathscr{A}_{\tilde{f}_i}(A, \tilde{K}_i, \tilde{\tau}_i)$.



(a) "Contact" capture set without uncertainty (outer line), with uncertainty (inner line).



(b) "Contact" collision set with uncertainty (outer line), collision set without uncertainty (middle line), as well as the MSI (innermost line).

Figure 10. Capture set and collision set for Contact under worst-case tanker speed.

tanker is effectively trying to prevent the UAV from entering the refueling zone. Similarly, the worst case collision set under uncertainty, shown in Fig. 10b, is larger than that without uncertainty. This results from the worst case tanker speed input which effectively tries to force a collision with the UAV.

IX. Conclusions and Future Work

In this paper, a systematic method is presented for designing maneuver control laws and transition conditions to ensure the safe and correct operation of a sequential mode transition system with both human-operated and autonomous transitions. The method is based on a hybrid formalism and Hamilton-Jacobi based reachability analysis, which guarantees robustness of the design to bounded continuous disturbances. Procedures for handling symmetric, deterministic communication latency and for recovering from faulty initial conditions are also provided. This approach is applied to the specific example of automated aerial refueling, with simulation results verifying the satisfaction safety and reachability objectives, and reachability computations demonstrating the influence of tanker velocity disturbances on the size of capture sets and collision sets. It is important to note that the performance guarantees of the proposed design approach are only valid under the assumed bounds on the environment disturbances. Further work needs to be performed to determine whether these bounds in fact apply for a typical aerial refueling scenario.

Ongoing work focuses on constructing a formal algorithm, based upon the design procedures given in this paper, with which the UAV could generate decisions for formation transitions in scenarios involving interactions with human operators. This would be done in conjunction with the vehicle's onboard state as well as reachable set data. Additional work focuses on domain-

specific models of the interaction protocols, in order to automatically synthesize the code that generates the reachable sets, as well as simulators to validate the designs. Further investigation into computationally efficient techniques for calculating the reachable sets would also enable the application of the described techniques to scenarios with high-order continuous dynamics.

Acknowledgments

This work was supported in part by the "Certification Technologies for Flight Critical Systems (CerTA FCS)" project, Air Force Research Labs (AFRL), through a contract with Boeing Research & Technology; and in part by the Center for Hybrid and Embedded Software Systems (CHESS) at UC Berkeley, which receives support from the National Science Foundation (NSF awards #CCR-0225610 (ITR),#0720882 (CSR-EHS: PRET), #0647591 (CSR-SGER), and #0720841 (CSR-CPS)), the U. S. Army Research Office (ARO #W911NF-07-2-0019), U.S. Air Force Office of Scientific Research (AFOSR) awards MURI #FA9550-06-0312 and AF-TRUST #FA9550-06-1-0244, AFRL, the State of California Micro Program, and the following companies: Agilent, Bosch, DGIST, Lockheed Martin, National Instruments, and Toyota. Additional support was provided by AFOSR Award #FA9550-091-0519 titled "Modeling of Embedded Human Systems," and NSF awards CNS-0915010 and CNS-0930919.

The authors gratefully acknowledge the additional contributions of Dr. Doug Stuart and Jim Barhorst of Boeing Research & Technology, who aided in the development of the AAR scenario, and provided valuable feedback with regards to questions of discrete reachability. Also, many of the research ideas that produced this work were conceived in David Homan's yearly meetings on Verification and Validation at Wright-Patterson AFB in Dayton, OH. In those meetings, this work was influenced in the conversation and presentations of many of those participants, and the authors are grateful for their contribution.

References

[1]Yavrucuk, I., Unnikrishnan, S., and Prasad, J., "Envelope Protection for Autonomous Unmanned Aerial Vehicles," *Journal of Guidance, Control, and Dynamics*, Vol. 32, No. 1, 2009, pp. 262–275.

[2]Lam, T., Mulder, M., and Paassen, M. V., "Haptic Feedback in Uninhabited Aerial Vehicle Teleoperation with Time Delay," *Journal of Guidance, Control, and Dynamics*, Vol. 31, No. 6, 2008, pp. 1728–1739.

[3]Cummings, M. and Mitchell, P., "Predicting Controller Capacity in Supervisory Control of Multiple UAVs," *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*, Vol. 38, No. 2, 2008, pp. 451 – 460., doi:10.1109/TSMCA.2007.914757

[4]Henzinger, T. A., Ho, P. H., and Wong-Toi, H., "HYTECH: a Model Checker for Hybrid Systems," *Journal International Journal on Software Tools for Technology Transfer (STTT)*, Vol. 1, No. 1-2, Dec. 1997, pp. 110–122.

[5]Asarin, E., Dang, T., and Maler, O., "d/dt: A Verification Tool for Hybrid Systems," *Decision and Control,*

Proceedings of the 40th IEEE Conference on, Vol. 3, 2001, pp. 2893–2898., doi:10.1109/.2001.980715

[6]Chutinan, A. and Krogh, B. H., "Computational Techniques for Hybrid System Verification," *Automatic Control, IEEE Transactions on*, Vol. 48, No. 1, Jan 2003, pp. 64–75., doi:10.1109/TAC.2002.806655

[7]Botchkarev, O. and Tripakis, S., "Verification of Hybrid Systems with Linear Differential Inclusions Using Ellipsoidal Approximations," *Hybrid Systems: Computation and Control*, edited by N. Lynch and B. Krogh, Vol. 1790 of *Lecture Notes in Computer Science*, Springer Berlin / Heidelberg, 2000, pp. 73–88., doi:10.1007/3-540-46430-1_10

[8]Tomlin, C., Mitchell, I., Bayen, A., and Oishi, M., "Computational Techniques for the Verification of Hybrid Systems," *Proceedings of the IEEE*, Vol. 91, No. 7, July 2003, pp. 986–1001., doi:10.1109/JPROC.2003.814621

[9]Mitchell, I., Bayen, A., and Tomlin, C., "A Time-Dependent Hamilton-Jacobi Formulation of Reachable Sets for Continuous Dynamic Games," *IEEE Transactions on Automatic Control*, Vol. 50, No. 7, July 2005, pp. 947–957., doi:10.1109/TAC.2005.851439

[10]Ross, S., Pachter, M., Jacques, D., Kish, B., and Millman, D., "Autonomous Aerial Refueling Based on the Tanker Reference Frame," *2006 IEEE Aerospace Conference*, July 2006, pp. 22., doi:10.1109/AERO.2006.1656016

[11]"DARPA Completes Autonomous Airborne Refueling Demonstration," DARPA Press Release, Aug. 9, 2007.

[12]Valasek, J., Kimmett, J., Hughes, D., Gunnam, K., and Junkin, J. L., "Vision Based Sensor and Navigation System for Autonomous Aerial Refueling," *AIAA 1st UAV Conference*, AIAA, 2002, AIAA 2002-3441.

[13]Jin, Z., Shima, T., and Schumacher, C., "Scheduling and Sequence Reshuffle for Autonomous Aerial Refueling of Multiple UAVs," *American Control Conference*, June 2006, pp. 2177–2182., doi:10.1109/ACC.2006.1656542

[14]Nalepka, J. P. and Hinchman, J. L., "Automated Aerial Refueling: Extending the Effectiveness of Unmanned Air Vehicles," *AIAA Modeling and Simulation Technologies Conference and Exhibit*, 15-18 August 2005, AIAA 2005-6005.

[15]Ding, J., Sprinkle, J., Sastry, S. S., and Tomlin, C. J., "Reachability Calculations for Automated Aerial Refueling," *Decision and Control, 47th IEEE Conference on*, Dec. 2008, pp. 3706–3712., doi:10.1109/CDC.2008.4738998

[16]Bayen, A. M., *Computational Control of Networks of Dynamical Systems: Application to the National Airspace System*, Ph.D. thesis, Stanford University, Stanford, CA, 2003.

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

[18]Teo, R. and Tomlin, C. J., "Computing Danger Zones for Provably Safe Closely Spaced Parallel Approaches," *Journal of Guidance, Control, and Dynamics*, Vol. 26, No. 3, May-June 2003, pp. 434–443.

[19]Jang, J. and Tomlin, C. J., "Control Strategies in Multi-Player Pursuit and Evasion Game," *Proceedings of the AIAA Conference on Guidance, Navigation and Control*, 15-18 August 2005, AIAA 2005-6239.

[20]Teo, R., *Computing Danger Zones for Provably Safe Closely Spaced Parallel Approaches: Theory and Experiment*, Ph.D. thesis, 2005.

[21]Oishi, M., Mitchell, I., Bayen, A., Tomlin, C., and Degani, A., "Hybrid Verification of an Interface for an Automatic Landing," *Proceedings of the 41st IEEE Conference on Decision and Control*, Vol. 2, 10-13 Dec. 2002, pp. 1607–1613.

[22]Sprinkle, J., Ames, A. D., Eklund, J. M., Mitchell, I., and Sastry, S. S., "Online Safety Calculations for Glideslope Recapture," *Innovations in Systems and Software Engineering*, Vol. 1, No. 2, September 2005, pp. 157–175., doi:10.1007/s11334-005-0017-x

[23]Alur, R. and Dill, D. L., "A theory of timed automata," *Theoretical Computer Science*, Vol. 126, No. 2, 1994, pp. 183 – 235.

[24]Henzinger, T., "The theory of hybrid automata," *Logic in Computer Science, 1996. LICS '96. Proceedings., Eleventh Annual IEEE Symposium on*, July 1996, pp. 278 –292.

[25]Asarin, E., Olivier, B., Dang, T., and Maler, O., "Approximate Reachability Analysis of Piecewise-Linear Dynamical Systems," *Lecture Notes in Computer Science, Hybrid Systems: Computation and Control*, Vol. 1790, Springer-Verlag, Berlin, Germany, 2000, pp. 20–31.

[26]Kurzhanski, A. B. and Varaiya, P., "Ellipsoidal Techniques for Reachability Analysis," *Lecture Notes in Computer Science, Hybrid Systems: Computation and Control*, Vol. 1790, Springer-Verlag, Berlin, Germany, 2000, pp. 202–214.

[27]Bemporad, A., Torrisi, D., and Morari, M., "Optimization-Based Verification and Stability Characterization of Piecewise Affine and Hybrid Systems," *Lecture Notes in Computer Science, Hybrid Systems: Computation and Control*, Vol. 1790, Springer-Verlag, Berlin, Germany, 2000, pp. 45–59.

[28]Aubin, J.-P., Lygeros, J., Quincampoix, M., Sastry, S., and Seube, N., "Impulse differential inclusions: a viability approach to hybrid systems," *Automatic Control, IEEE Transactions on*, Vol. 47, No. 1, Jan 2002, pp. 2 –20.

[29]Girard, A., "Reachability of Uncertain Linear Systems Using Zonotopes," *Lecture Notes in Computer Science, Hybrid Systems: Computation and Control*, Vol. 3414, Springer-Verlag, Berlin, Germany, 2005, pp. 291–305.

[30]Han, Z. and Krogh, B., "Reachability analysis of nonlinear systems using trajectory piecewise linearized models," *American Control Conference, 2006*, June 2006, pp. 1505–1510.

[31]Alur, R., Henzinger, T., Lafferriere, G., and Pappas, G., "Discrete abstractions of hybrid systems," *Proceedings of the IEEE*, Vol. 88, No. 7, July 2000, pp. 971 –984.

[32]Haghverdi, E., Tabuada, P., and Pappas, G. J., "Bisimulation relations for dynamical, control, and hybrid systems," *Theoretical Computer Science*, Vol. 342, No. 2-3, 2005, pp. 229 – 261.

[33]Girard, A., Julius, A. A., and Pappas, G. J., "Approximate simulation relations for hybrid systems," *Discrete event dynamic systems*, Vol. 18, No. 2, June 2008, pp. 163–179.

[34]Prandini, M. and Hu, J., "A Stochastic Approximation Method for Reachability Computations," *Stochastic Hybrid Systems*, Vol. 337/2006, Springer Berlin/Heidelberg, 2006, pp. 107–139.

[35]Blom, H. and Lygeros, J., editors, *HYBRIDGE Final Project Report*, 2005.

[36]Blom, H. A., Obbink, B. K., and Bakker, G. B., "Safety Risk Simulation of an Airborne Self Separation Concept of Operation," *7th AIAA-ATIO Conference*, AIAA, September 18–20 2007, AIAA 2007-7729.

[37]Blom, H., Bakker, G., and Krystul, J., "Rare Event Estimation for a Large-Scale Stochastic Hybrid System with Air Traffic Application," *Rare event simulation using Monte Carlo methods*, edited by G. Rubino and B. Tuffin, chap. 9, John Wiley & Sons, 2009, pp. 193–214.

[38]Buell, G. and Leondes, C., "Optimal Aircraft Go - Around and Flare Maneuvers," *Aerospace and Electronic Systems, IEEE Transactions on*, Vol. AES-9, No. 2, march 1973, pp. 280 –289., doi:10.1109/TAES.1973.309796

[39]Bottasso, C., Leonello, D., and Savini, B., "Path Planning for Autonomous Vehicles by Trajectory Smoothing Using Motion Primitives," *Control Systems Technology, IEEE Transactions on*, Vol. 16, No. 6, nov. 2008, pp. 1152 –1168., doi:10.1109/TCST.2008.917870

[40]Frazzoli, E., Dahleh, M., and Feron, E., "Maneuver-based motion planning for nonlinear systems with symmetries," *Robotics, IEEE Transactions on*, Vol. 21, No. 6, 2005, pp. 1077 – 1091.

[41]Koo, T. J., Pappas, G. J., and Sastry, S., "Mode Switching Synthesis for Reachability Specifications," *Lecture Notes in Computer Science, Hybrid Systems: Computation and Control*, Vol. 2034, Springer-Verlag, Berlin, Germany, 2001, pp. 333–346.

[42]Waydo, S., Hauser, J., Bailey, R., Klavins, E., and Murray, R., "UAV as a Reliable Wingman: A Flight Demonstration," *Control Systems Technology, IEEE Transactions on*, Vol. 15, No. 4, july 2007, pp. 680 –688., doi:10.1109/TCST.2007.899172

[43]Burridge, R. R., Rizzi, A. A., and Koditschek, D. E., "Sequential Composition of Dynamically Dexterous Robot Behaviors," *The International Journal of Robotics Research*, Vol. 18, No. 6, 1999, pp. 534–555., doi:10.1177/02783649922066385

[44]Williamson, W. R., Glenn, G. J., Dang, V. T., Speyer, J. L., Stecko, S. M., and Takacs, J. M., "Sensor Fusion Applied to Autonomous Aerial Refueling," *Journal of Guidance, Control, and Dynamics*, Vol. 32, No. 1, 2009, pp. 262–275.

[45]Warwick, G., "Boeing To Lead UAV Aerial Refueling Demo," *Aviation Week*, Nov. 21, 2008.

[46]Lygeros, J., Tomlin, C., and Sastry, S., "Controllers for reachability specifications for hybrid systems," *Automatica*, Vol. 35, No. 3, 1999, pp. 349 – 370., doi:10.1016/S0005-1098(98)00193-9

[47]Tomlin, C., Lygeros, J., and Sastry, S. S., "A Game Theoretic Approach to Controller Design for Hybrid Systems," *Proceedings of the IEEE*, Vol. 88, No. 7, Jul 2000, pp. 949–970., doi:10.1109/5.871303

[48]Evans, L. C. and Souganidis, P. E., "Differential games and representation formulas for solutions of Hamilton-Jacobi-Isaacs equations," *Indiana Univ. Math. J.*, Vol. 33, No. 5, 1984, pp. 773–797.

[49]Mitchell, I. M., "The Flexible, Extensible and Efficient Toolbox of Level Set Methods," *Journal of Scientific Computing*, Vol. 35, No. 2-3, June 2008., doi:10.1007/s10915-007-9174-4

[50]Osher, S. and Fedkiw, R., *Level Set Methods and Dynamic Implicit Surfaces*, Springer-Verlag, 2002, ISBN: 978-0-387-95482-0.

[51]Sethian, J. A., *Level Set Methods and Fast Marching Methods*, Cambridge University Press, 1999, ISBN: 9780521645577.

[52]Mitchell, I., *Application of Level Set Methods to Control and Reachability Problems in Continuous and Hybrid Systems*, Ph.D. thesis, 2002.

[53]Ding, J. and Tomlin, C., "Robust reach-avoid controller synthesis for switched nonlinear systems," *Decision and Control (CDC), 2010 49th IEEE Conference on*, dec. 2010, pp. 6481 –6486., doi:10.1109/CDC.2010.5717115