An optimal control framework for estimating autopilot safety margins

N. Govindarajan*, C.C. de Visser † E. van Kampen‡

Delft University of Technology, Delft, The Netherlands

K. Krishnakumar§, J. Barlow¶, V. Stepanyan‖

NASA Ames Research Center, Moffett Field, CA 94035

This paper presents an optimal control framework to determine a collection of open-loop command signals that mathematically guarantees operation of an aircraft within certain prescribed state constraints. The framework is specifically applied to estimate margins for the reference command inputs of aircraft autopilot systems, so that safe operation within a given flight envelope can be assured under appropriate control action. Flight envelope excursions are generally considered as precursors to Loss-Of-Control incidents, and hence, these margins contain safety critical information that can help improve the situational awareness on-board the aircraft. In off-nominal conditions, the computed safety margins provide indications of a degraded aircraft with reduced flying and handling qualities. These indications appear in the form of increasingly more strict limits on the autopilot reference command input. The entire framework is illustrated on an example problem involving a pitch dynamics model with state constraints on the pitch attitude. Simulations are conducted wherein margins are computed for the reference pitch command of the pitch hold system, while the aircraft enters an off-nominal condition with severely degraded system dynamics and reduced elevator effectiveness.

Acronyms

DP	Dynamic Programming
FEP	Flight Envelope Protection
FSA	Flight Safety Assurance
GTM	Generic Transport Model
HJB PDE	Hamilton-Jacobi-Bellman Partial Differential Equation
LOC	Loss-Of-Control
QLC	Quantitative Loss-of-control Criteria

[*]Visiting researcher, Delft Center for Systems and Control, Faculty of Mechanical, Maritime and Materials Engineering. nithin.govindarajan@gmail.com

[†]Assistant professor, Control and Simulation, Faculty of Aerospace Engineering. C.C.deVisser@tudelft.nl

[‡]Assistant professor, Control and Simulation, Faculty of Aerospace Engineering. E.vankampen@tudelft.nl

[§]Technical Area Lead, Automation Systems and Robotics, Intelligent Systems Division. kalmanje.krishnakumar@nasa.gov

[¶]Research Scientist, Stinger Ghaffarian Technologies Inc. jonathan.s.Barlow@nasa.gov

[‖]Senior Scientist, Mission Critical Technologies Inc. vahram.stepanyan@nasa.gov

Nomenclature

A_0, B_0	=	nominal LTI system matrices
A, B	=	off-nominal LTI system matrices
$\boldsymbol{f}$	=	system dynamics
$\boldsymbol{h}$	=	output equation
H	=	Hamiltonian
J_i	=	cost functional
k_θ, k_q, k_s	=	control system gains [-,1/sec,-]
l_i	=	state constraint
q	=	pitch rate [rad/sec]
t_0	=	current/initial time [sec]
T	=	prediction horizon [sec]
V_i	=	value function
$\boldsymbol{x}$	=	state
$\boldsymbol{x}_0$	=	current or initial state
$\boldsymbol{y}_{ref}$	=	ref. command input
$\boldsymbol{y}$	=	output
Y_{ref}	=	command input space
$\boldsymbol{\mathcal{Y}_{ref}}$	=	set of admissible ref. command signals
δ_e	=	elevator input [deg]
$\delta_{e,\min}, \delta_{e,\max}$	=	min. and max. elevator input [deg,deg]
$\boldsymbol{\zeta}$	=	system state trajectory
$(\boldsymbol{y}_{ref_{\min}}, \boldsymbol{y}_{ref_{\max}})$	=	command margins
θ	=	pitch attitude [deg]
θ_{ref}	=	pitch attitude ref. command [deg]
$(\theta_{ref,\min}, \theta_{ref,\max})$	=	pitch attitude ref. command margins [deg]
$\boldsymbol{\Theta_{ref}}$	=	set of admissible pitch ref. signals

I. Introduction

Loss-of-Control (LOC) is a major contributor to accidents and fatalities across all aircraft, operational categories, and phases of flight. In the commercial jet category alone, LOC was the cause of 22 accidents resulting in 1,991 fatalities [1] for the period between 1999 and 2008. Aircraft LOC accidents are complex, and as stated in Kwatny et al. [2], are often associated with flight outside of the normal operating envelope, with non-linear influences, and with an inability of the pilot to control the aircraft. In an attempt to quantify LOC, Wilborn and Foster [3] defined metrics and criteria that can be used to identify LOC events from flight data. These metrics are collectively known as the Quantitative Loss-of-control Criteria (QLC) and consist of five envelopes related to the airplane flight dynamics, aerodynamics, structural integrity and flight control use.

Due to the complexity and multidisciplinary nature of LOC, there is no single intervention strategy to these incidents. Rather, a holistic approach must be employed which systematically breaks-down the chain of events that precede a LOC incident. Analysis of accident data have shown that LOC is often preceded by an adverse on-board condition (e.g. contaminated airfoil, improper vehicle loading, vehicle damage) or external hazard condition (e.g. poor visibility, wake vortices, wind shear, turbulence, and icing conditions), that eventually lead to an upset condition (e.g. abnormal attitude, abnormal airspeed, uncontrolled descent, or departure into a stall) because of an inability of the crew to deal with the situation [1]. This observation suggests that current flight-crew decision making and supporting flight-deck software for safe vehicle operation are inadequate in dealing with these so-called off-nominal conditions. That is, unawareness on the impact of in-flight failures and hazardous flight conditions often result in situations where inappropriate command signals lead to dangerous flight conditions from which recovery to normal flight is difficult to obtain.

In this regard, Flight Envelope Protection (FEP) is seen as a useful tool to prevent such dangerous excursions, which many times are caused by inappropriate piloting action. The task of FEP is to monitor and maintain vehicle operation within prescribed limits under all circumstances. FEP has been the subject of study in the recent past under various contexts. Yavrucuk et al. [4] have studied automatic envelope protection systems tailored specifically for unmanned aerial vehicles,

Falkena et al. [5] has investigated FEP strategies for small aircraft from the general aviation category perspective, and Sharma et al. [6] have looked into practical FEP schemes for commercial aircraft under icing conditions. For the commercial aircraft category, the industry dictates two philosophies in FEP; in the first philosophy, the responsibility of maintaining the aircraft within prescribed limits is given to the flight control system. This philosophy mandates an active role to the flight control system, as pilot control actions can be overridden to prevent aircraft from leaving certain envelope bounds. In the second philosophy, a more passive approach is taken wherein the flight control system takes a more advisory role, and where the pilot has the final authority over the aircraft [5]. Regardless of which philosophy is being followed, current FEP systems have not always helped in preventing LOC incidents and are not sophisticated enough to adapt to off-nominal conditions that alter the flight dynamical characteristics of the aircraft significantly. To overcome this shortcoming, more advanced Flight Safety Assurance (FSA) systems [1] have to be developed that can help assess and predict the impact of off-nominal conditions on vehicle flight safety.

In line with this goal, this paper presents a novel framework to determine *"safety margins"* for the reference command signals of an aircraft autopilot system. These safety margins ensure that an aircraft will never violate certain state constraints which define the boundaries of a safe maneuvering envelope. Hence, provided that off-nominal dynamics are detected and identified almost immediately, the computed margins provide important information concerning the operational freedom of the aircraft. The proposed framework to compute the margins involves optimizing a set of cost functionals over a space of admissible command signals. The sign of these cost functionals signify whether a state trajectory of the system can violate a state constraint within a certain predefined time-window. The information extracted by the optimization of the cost functionals subsequently allows us to use an iterative procedure to find suitable margins for the system. The extrema of the cost functionals are computed using Dynamic Programming (DP) principles. This involves solving a time-dependent Hamilton-Jacobi-Bellman Partial Differential Equation (HJB PDE) which often arises in optimal control problems (see Kirk [7, Ch. 3] or Bardi and Capuzzo-Dolcetta [8, Ch. 3] for more background).

In comparison to other related work [9–12] that aims to compute certain safety metrics for

inputs signals of aircraft systems, the significance of the optimal control formulation presented in this paper is that the computed margins *mathematically* guarantee operation of the system within the state envelope for a *specified prediction horizon*. Furthermore, the method is directly applicable to a large class of nonlinear systems, since no stringent assumptions are made concerning the structure of the system. The practical application of the proposed methodology is illustrated on a simplified aircraft system with state constraints on the pitch attitude. Simulations are conducted to study the dynamic behavior of the margins in response to abrupt changes in the system dynamical properties and control behavior. In line with expectations and theory, simulation results verify that envelope excursions only occur under prolonged neglect of the margins. These excursions are preceded by a rapid shrinkage of the margins, indicating that the aircraft is rapidly approaching the edge of the envelope. On the other hand, if the command inputs continuously satisfy the margins, an envelope excursion never seems to occur.

The remainder of this paper is organized as follows. Section II elaborates on the details of the problem addressed in this paper. Section III then casts this problem in an optimal control framework, which is subsequently solved using DP principles. Section IV applies the proposed method on an example involving a pitch dynamics approximation of a Generic Transport Model [13]. Section V presents simulation results where margins are computed for the pitch reference command along the simulated flight trajectory. Section VI states the conclusions of the work.

II. Problem formulation

Many physical systems operate safely only when they are confined to certain operating conditions. In order to maintain a system within certain prescribed state constraints, one needs to be cautious on how the system gets excited. For the case of an aircraft, this would relate to the type of command signals provided to the autopilot system. The objective in this paper is to classify a collection of feasible command signals that meet the requirement of keeping the aircraft within flight envelope constraints. The goal in this section is to describe how the problem is approached quantitatively. The aim is to clarify the overall setting of the problem by stating the assumptions, and also pointing out to some additional considerations which go beyond the present scope of this paper.

A. Modeling the aircraft as a command-driven system

In modern aircraft, it is often the case that a specific reference command signal is provided to the autopilot system, after which an existing controller *steers* the aircraft towards that reference. Hence, from the viewpoint of the cockpit, the aircraft can be viewed as a command-driven control system. In addition, command limiting an autopilot is an easier retrofit option than the replacement of a certified flight control system. This command-driven control system is modeled by

$$\dot{\boldsymbol{x}} = \boldsymbol{f}\left(\boldsymbol{x}, \boldsymbol{y}_{ref}\right) \tag{1a}$$

$$\boldsymbol{y} = \boldsymbol{h}(\boldsymbol{x}) \tag{1b}$$

where $\boldsymbol{f}$ and $\boldsymbol{h}$ are Lipschitz continuous functions, and where $\boldsymbol{x} \in \mathbb{R}^n$ denotes the state, $\boldsymbol{y} \in \mathbb{R}^m$ denotes the output, and $\boldsymbol{y}_{ref} \in \mathrm{Y}_{ref} \subset \mathbb{R}^m$ denotes the reference command input. In (1a), the symbol $\boldsymbol{y}_{ref}$ is deliberately used to emphasize that the input to the system is a *reference command*. Thus for the application in consideration, $\boldsymbol{y}_{ref}$ denotes typical inputs to an autopilot system such as: the reference pitch attitude, reference flight path angle, reference bank angle, reference velocity, etc. In FEP, the goal is to determine how the reference command signals, denoted by $\boldsymbol{y}_{ref}(\cdot)$, have to be limited, in order to ensure that certain state constraints are never violated by the state trajectories of (1).

For the scope of this paper, we assume complete knowledge of the system (1). In practice, an accurate model of the system will not always be present. This holds especially true when the aircraft is flying in an off-nominal condition. Therefore, given this uncertainty on the system, an important requirement is to develop in-flight system identification procedures that are capable of estimating the anomalies in the flight dynamical characteristics. The challenging part of this requirement is that the detection and identification of off-nominal conditions has to be done with minimum time delays. LOC incidents can develop in a matter of seconds, and given the unforgiving and unpredictable nature of LOC, deliberate excitation of the controls in order to meet persistence of excitation requirements is unacceptable during a failure condition. Despite all of this, note here that many LOC incidents also occur when the aircraft appears to be in a nominal state, hence

making the work discussed in this paper relevant even without the existence of on-line system identification procedures. In addition, some recent research [14] has shown that pilot inputs during a normal task can be effective at near real-time system identification and this may be an approach that is relevant to this task.

B. The safe maneuvering envelope

The state domain in which the aircraft must be operated denotes the safe maneuvering envelope. This envelope is described in terms of inequality constraints on the state of the system, i.e.

$$l_i(\boldsymbol{x}) \leq 0, \qquad i = 1, \ldots, r \tag{2}$$

A trivial example of an inequality constraint that helps define the contours of the envelope is the limitation imposed on the angle-of-attack. Moreover, the five envelopes defined in [3]: the adverse aerodynamics envelope, unusual Attitude envelope, structural integrity envelope, dynamic pitch control envelope, and dynamic roll control envelope, may also be represented in terms of inequality constraints (2).

Although not the focus in this paper, note that the actual safe maneuvering envelope may shrink under adverse on-board conditions. To estimate changes in the flight envelope is a non-trivial matter, and currently is an active area of research within the aeronautical community. The survey paper of Tang et al. [15] summarizes some of the developments in adaptive flight envelope estimation. In general, the literature describes two different approaches for estimating the safe maneuvering envelope. The first approach aims to represent the envelope as the collection of all achievable aircraft trim conditions along with their local stability maps. For example, in Tang et al. [16] the stable and controllable trim conditions were determined off-line for a Generic Transport Model (GTM) with left wing damage. The authors saw this as a comprehensive and consistent way of representing the maneuvering envelope, so that it can be used to determine feasible trajectories for safe vehicle landing during emergency conditions. The other approach that can be found in the literature is the reachability formulation for estimating the safe flight envelope (see also [17, 18]). For example,

in Oort et al. [19] and Lombearts et al. [20] the flight envelope was characterized as the intersection between the forward and backward reachable set of the aircraft trim set. In any case, both approaches are computationally intensive and require a fully integrated modeling of aerodynamic, structural and propulsive aspects of the aircraft in order to obtain high fidelity approximations of the maneuvering envelope. In the present study, we assume that the safe maneuvering envelope, or equivalently, the constraints (2) are a given information.

C. The command margins

In order to classify a collection of reference command signals that ensure operation within the constraints (2), the input space Y_{ref} is parameterized in terms of the interval

$$\mathrm{Y}_{ref} := \left[\boldsymbol{y}_{ref_{\min}}, \boldsymbol{y}_{ref_{\max}}\right] \tag{3}$$

where $\boldsymbol{y}_{ref_{\min}}$ and $\boldsymbol{y}_{ref_{\max}}$ denote respectively the lower and upper limit imposed on the reference command. Collectively, the pair: $(\boldsymbol{y}_{ref_{\min}}, \boldsymbol{y}_{ref_{\max}})$ is referred to as the command margins for the system (1). These margins are used to define a function space

$$\boldsymbol{\mathcal{Y}_{ref}} := \left\{\boldsymbol{y}_{ref}(\cdot) : [t_0, t_0 + T] \mapsto [\boldsymbol{y}_{ref_{\min}}, \boldsymbol{y}_{ref_{\max}}] \;\middle|\; \boldsymbol{y}_{ref}(\cdot) \text{ is measurable}\right\} \tag{4}$$

where $\boldsymbol{\mathcal{Y}_{ref}}$ denotes a collection of reference signals $\boldsymbol{y}_{ref}(\cdot)$ for the time period $[t_0, t_0 + T]$. These signals are effectively piecewise continuous functions and satisfy the imposed margins for the time period of consideration. That is, for any $\boldsymbol{y}_{ref}(\cdot) \in \boldsymbol{\mathcal{Y}_{ref}}$, we have that

$$\boldsymbol{y}_{ref_{\min}} \leq \boldsymbol{y}_{ref}(\tau) \leq \boldsymbol{y}_{ref_{\max}}$$

for all $\tau \in [t_0, t_0 + T]$.

The problem we lay out is as follows. Suppose that the aircraft is at some initial condition $\boldsymbol{x}_0$ at time t_0. The goal is to determine the margins: $(\boldsymbol{y}_{ref_{\min}}, \boldsymbol{y}_{ref_{\max}})$, such that, no matter what

admissible command signal satisfying the margins for the next T seconds (i.e. $\boldsymbol{y}_{ref}(\cdot) \in \boldsymbol{\mathcal{Y}_{ref}}$) is provided to the system, the resulting state trajectory, denoted by $\boldsymbol{\zeta}(\tau; \boldsymbol{x}_0, \boldsymbol{y}_{ref}(\cdot))$, will never violate the envelope during that time period. That is, the aim is to have

$$\max_{\tau \in [t_0, t_0+T]} l_i\left(\boldsymbol{\zeta}(\tau; \boldsymbol{x}_0, \boldsymbol{y}_{ref}(\cdot))\right) < 0, \qquad i = 1, \ldots, r \tag{5}$$

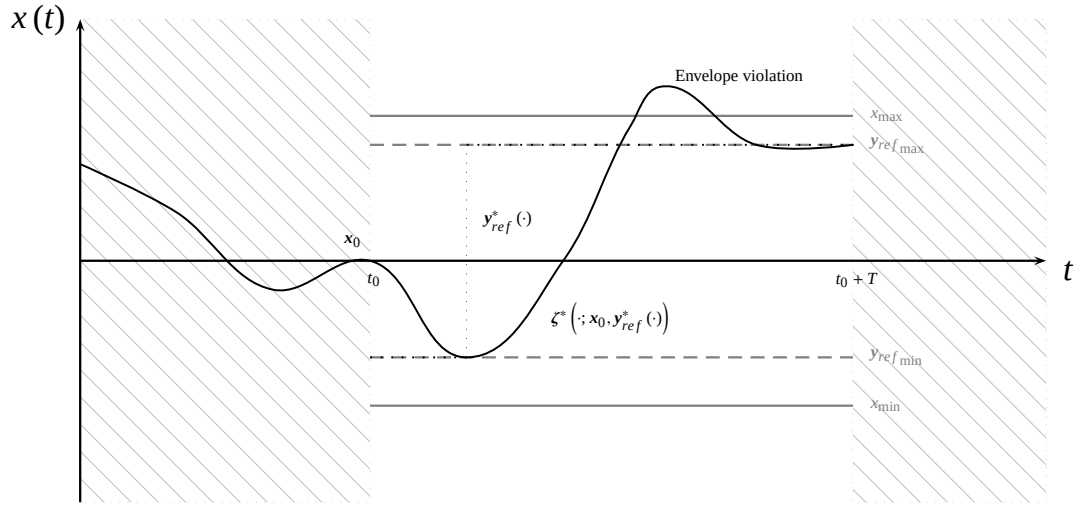
for all $\boldsymbol{y}_{ref}(\cdot) \in \boldsymbol{\mathcal{Y}_{ref}}$.

The objective is to estimate these margins continuously in a real-time setting along the followed state trajectory of the system. The variable T is a design parameter and denotes the *prediction horizon* for which the margins are valid. The goal is to set the prediction horizon T sufficiently large so that all important transients in the dynamics are included in the analysis. Too small a prediction horizon can lead to deceitfully lenient margins which ignore the effects that come into play at a later stage. Very small prediction horizons are misleading and can create the illusion that there is a lot of operational freedom. On the other hand, very large prediction horizons are computationally more challenging, but also do not add much value because of largely unmodeled higher-order effects. Typically, only a local model of the aircraft flight dynamics around the current flight condition is available, hence projecting too much into the future is not possible. As a thumb rule, a suggestion is to fix T equal to two or three times the time-constant of the system.

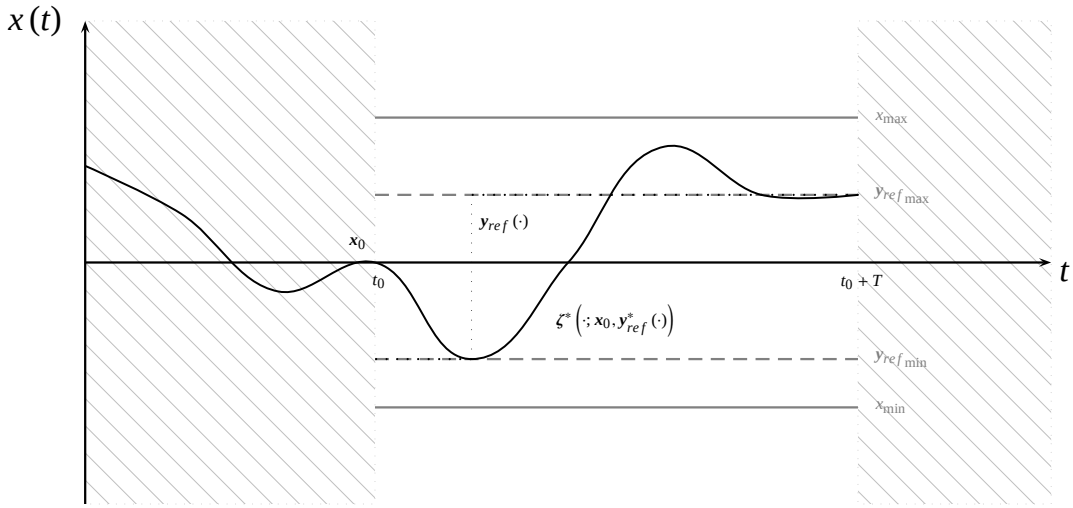
Figure 1 illustrates the receding horizon approach for computing safety margins. In the figure, the past state trajectory of an aircraft system is shown up to time t_0 and state $\boldsymbol{x}_0$. Furthermore, a time-window is depicted from the present time t_0 to some future time $t_0 + T$. Supposing that certain command margins are set for this time-window, for the specified margins in figure 1a, it appears that there exists a reference command signal $\boldsymbol{y}^*_{ref}(\cdot) \in \boldsymbol{\mathcal{Y}_{ref}}$ that can give rise to an extremal trajectory $\boldsymbol{\zeta}^*(\cdot; \boldsymbol{x}_0, \boldsymbol{y}^*_{ref}(\cdot))$ violating the envelope. On the other hand, for the slightly more limited margins in figure 1b, there exists no such command signal that can lead to such a trajectory. The goal is to continuously ensure that the margins exhibit the property depicted in figure 1b. When this is the case, those margins are called “safe”, where safety is interpreted as whether the margins can guarantee flight inside the state envelope for a specified prediction horizon.

Note that the safety margins should be interpreted as advisory information, since violation of

the margins does not imply an inevitable envelope excursion. A reference signal outside of the margins can still be commanded to the aircraft, as long as one constantly monitors the dynamic behavior of the safety margins after such actions. As will be seen later in section V, if a rapid shrinkage of the margins occurs, then this would be an indication of the aircraft getting closer to edge of the envelope.



a) There exists *at-least one* reference command $y_{ref}(\cdot) \in \mathcal{Y}_{ref}$ that can steer the system outside the envelope in T seconds.



b) There exists *no* reference command $y_{ref}(\cdot) \in \mathcal{Y}_{ref}$ that can steer the system outside the envelope in T seconds.

Figure 1. "Safe" (figure 1b) and "unsafe" (figure 1a) command margins for some hypothetical dynamical system

III. The Optimal Control Methodology

The objective formulated in section II C requires one to analyze the properties of a whole class of system state trajectories at once. In this section, a systematic methodology is presented to tackle this problem with the help of optimal control ideas for computing reachable sets of dynamical systems (see [18, 21]).

The details of the proposed methodology are explained in the context of the general problem formulation given in section II. Later in section IV, the methodology is illustrated on a specific example problem which involves computing safety margins for a pitch hold system.

A. The cost functional

The safety margins for the system (1) are found using an iterative approach. This approach involves fixing certain margins for the system, and then, checking whether the corresponding signal space (4) can contain reference signals that lead to state trajectories $\boldsymbol{\zeta}(\tau; \boldsymbol{x}_0, \boldsymbol{y}_{ref}(\cdot))$ which violate the conditions (5).

This verification of the system state trajectories for a specific collection of command signals (4) can be done statistically through the means of simulating many individual state trajectories. However, such a Monte Carlo approach will never provide a guarantee of whether all system state trajectories are checked. That is, there might still exist some reference command signal within $\boldsymbol{\mathcal{Y}}_{\boldsymbol{ref}}$ that can lead to a trajectory crossing the envelope boundaries. Instead of analyzing the properties of certain random state trajectory individually, it suffices that this verification process can be handled analytically by recasting the problem in an optimal control framework. Contrary to Monte Carlo simulations, solving the problem using this framework allows for a systematic check of all state trajectories.

To further elaborate on this, consider the cost functional

$$J_i\left(\boldsymbol{x}_0, \boldsymbol{y}_{ref}(\cdot)\right) := \max_{\tau \in [t_0, t_0+T]} l_i\left(\boldsymbol{\zeta}(\tau; \boldsymbol{x}_0, \boldsymbol{y}_{ref}(\cdot))\right) \tag{6}$$

where $\boldsymbol{x}_0$ denotes the state condition at time t_0, and $\boldsymbol{y}_{ref}(\cdot)$ denotes a reference command signal over

the time period $[t_0, t_0 + T]$. Suppose that (6) is optimized over the space of admissible command signals (4), i.e.

$$J_i^*(\boldsymbol{x}_0) = \max_{\boldsymbol{y}_{ref}(\cdot) \in \boldsymbol{\mathcal{Y}_{ref}}} J_i\left(\boldsymbol{x}_0, \boldsymbol{y}_{ref}(\cdot)\right) \tag{7}$$

Then the following can be stated for the selected margins $(\boldsymbol{y}_{ref_{\min}}, \boldsymbol{y}_{ref_{\max}})$:

- When $J_i^*(\boldsymbol{x}_0) \leq 0$, the system is guaranteed to not violate i-th state constraint (i.e. $l_i(\boldsymbol{x}) \leq 0$) in the time-window $[t_0, t_0 + T]$ for any admissible command signal.
- On the other hand, when $J_i^*(\boldsymbol{x}_0) > 0$, there exists one or perhaps several command signals $\boldsymbol{y}_{ref}(\cdot) \in \boldsymbol{\mathcal{Y}_{ref}}$ that do result in trajectories violating the i-th state constraint.

Effectively, the optimization in (7) translates into a search within the function space (4) for the worst possible command signal which will steer the system towards the boundaries of flight envelope as much as possible inside the time-window: $[t_0, t_0 + T]$. In other words, the optimization will find the extremal command signal $\boldsymbol{y}_{ref}^*(\cdot) \in \boldsymbol{\mathcal{Y}_{ref}}$, leading to the extremal trajectory $\boldsymbol{\zeta}^*(\cdot; \boldsymbol{x}_0, \boldsymbol{y}_{ref}^*(\cdot))$ shown in figure 1a or 1b. The extremal trajectories violate the envelope when $J_i^*(\boldsymbol{x}_0) \leq 0$ for some $i \in \{1, 2, \ldots, r\}$. Vice versa, the state trajectories of (1) are guaranteed to stay inside the envelope (2), if and only if

$$\max_{i \in \{1,2,\ldots,r\}} J_i^*(\boldsymbol{x}_0) \leq 0 \tag{8}$$

B. The iterative procedure to find safety margins

The properties of the cost functional are exploited to find safe command margins for the system in a systematic way. An iterative procedure is used for that purpose. This iterative procedure involves solving the optimal control problem (7) multiple times for different margin settings. At every iteration step, incremental changes are made to the lower and upper limits of the margins, i.e. to $\boldsymbol{y}_{ref_{\min}}$ and $\boldsymbol{y}_{ref_{\max}}$ respectively, until margins are found that meet the condition in (8). The entire procedure is schematically depicted in figure 2.

The command margins are a function of the system dynamics (1) and the current state $\boldsymbol{x}_0$. To explain this in more detail, consider that a degradation of the system dynamics (i.e. a slightly less stable system) will lead for instance to more strict margins for the reference command inputs.

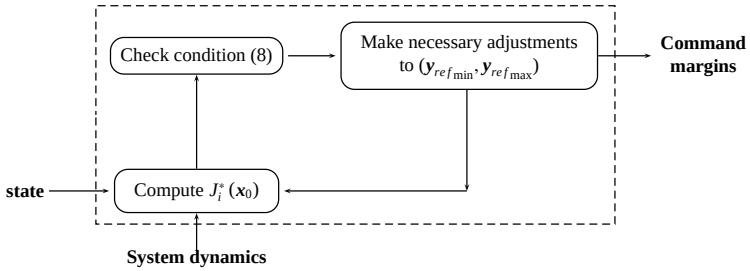


Figure 2. The iterative procedure for finding safe command margins.

Likewise, certain states will be more susceptible to envelope violations than others. For these states, the margins will turn out to be more strict as well. In fact, for some state conditions which are still within the envelope, it may be inevitable to prevent the aircraft from violating the safe maneuvering envelope, no matter what command inputs are provided to the control system. In that case, there will be no more margins left for the system and condition (8) will never be satisfied.

Our goal is to compute safety margins continuously along the actual state trajectory followed by system. The intention is to continuously update the margins in-flight, so that this information can be either: 1) fed-back to the pilot through cockpit displays for improving situational awareness, or 2) used to directly augment command inputs provided to the autopilot system. The overall way in which the information is used in the FEP system depends on the specific philosophy being followed (as discussed in the introduction). Both implementations are illustrated in figure 3 with the dashed lines.

C. Dynamic programming and the Hamilton-Jacobi-Bellman equation

The most challenging part of the procedure depicted in figure 2 is to solve the optimal control problem in (7). In the present implementation, $J_i^*(\boldsymbol{x}_0)$ is found through the dynamic programming principle. In [18] it was shown[a] that J_i^* can be related to the value function of a terminal-cost

[a] See proposition 3 on page 920.

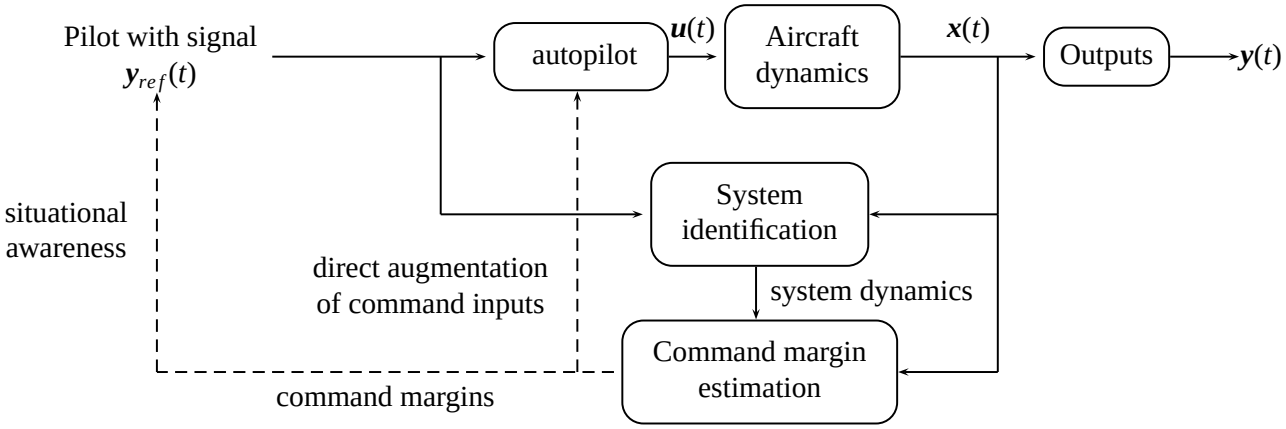


Figure 3. The intended applications for the estimated command margins in the FEP architecture.

optimal control problem. The relationship is given by

$$J_i^*(\boldsymbol{x}_0) = \max_{\tau \in [t_0, t_0+T]} V_i(\tau, \boldsymbol{x}_0) \tag{9}$$

where $V_i : [t_0, t_0 + T] \times \mathbb{R}^n \mapsto \mathbb{R}$ is the value function given by the unique viscosity solution of the time-dependent Hamilton-Jacobi-Bellman PDE

$$\frac{\partial V_i(t, \boldsymbol{x})}{\partial t} + H\left(\boldsymbol{x}, \frac{\partial V_i(t, \boldsymbol{x})}{\partial \boldsymbol{x}}^T\right) = 0 \tag{10a}$$

$$V_i(t_0 + T, \boldsymbol{x}) = l_i(\boldsymbol{x}) \tag{10b}$$

In (10), $H : \mathbb{R}^n \times \mathbb{R}^n \mapsto \mathbb{R}$ denotes the Hamiltonian and consists of the optimization

$$H\left(\boldsymbol{x}, \frac{\partial V_i(t, \boldsymbol{x})}{\partial \boldsymbol{x}}\right) = \max_{y_{ref} \in \boldsymbol{y_{ref}}} \left\langle \frac{\partial V_i(t, \boldsymbol{x})}{\partial \boldsymbol{x}}, \boldsymbol{f}\left(\boldsymbol{x}, \boldsymbol{y}_{ref}\right) \right\rangle \tag{11}$$

with $\langle \cdot, \cdot \rangle$ denoting the standard inner product. Furthermore, notice that the boundary condition (10b) equals l_i from (2).

Analytic solutions are rarely found for (11). Hence, in order to find J_i^* through the relationship

(9), the HJB PDE (11) has to be solved numerically. Well established convergent finite-difference schemes exist (see e.g. Osher and Fedwick [22, Ch. 5]) that solve (11) on a fixed Cartesian grid in the state-space. However, a major drawback of these methods is the exponential growth of the grid-size with respect to the state dimension, limiting their applicability to low-order problems. This computational complexity issue is a common problem in dynamic programming. A common strategy used to overcome these computational challenges is to use Adaptive Dynamic Programming (ADP) techniques [23] to find approximations of the value function with general function approximators. In this paper, we have used the method from Govindarajan et al. [24], that uses multivariate simplex splines [25, 26] to find an approximation of $V_i(t, \boldsymbol{x})$.

The investigation of other methods that solve (7) more effectively is an area of research that requires more attention. In the present study, the focus was largely on solving (7) through the DP principle. However, the literature (see also the survey papers [27, 28]) offers a breadth of other numerical methods to solve optimal control problems, each with their own share of advantages and disadvantages. The aim of this paper is not to present a detailed analysis of numerical methods that can solve (7), but more to illustrate the overall application of the framework presented in this paper. In any case, we briefly hint out to the Gauss-Pseudospectral method [29, 30] as an suitable alternative method which converts (7) into a nonlinear program. For very specific cases, such as when $\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{y}_{ref})$, $\boldsymbol{h}(\boldsymbol{x})$ are linear, and $l_i(\boldsymbol{x})$ are convex functions, the nonlinear program reduces to a convex optimization problem that can be solved effectively with existing algorithms.

IV. Illustrations on a pitch dynamics model

In this section, the working principles of the optimal control approach detailed in section III is illustrated on an example involving the longitudinal pitch dynamics of a Generic Transport Model (GTM) [13]. The methodology is applied on a case where reference pitch attitude commands are provided to the pitch hold mode of the autopilot. More specifically, safety margins are computed for the reference pitch attitude command, so that the aircraft is guaranteed to stay inside a safe maneuvering envelope, defined in terms of limitations on the pitch attitude.

Safety margins are determined for two situations. The first situation represents the *nominal*

case wherein the aircraft is in a healthy state. The second situation represents an *off-nominal case* wherein the aircraft has experienced a failure and is in a degraded state.

A. The pitch dynamics model: the nominal & off-nominal case

The longitudinal pitch dynamics of the GTM is approximated with a second-order linear system. The approximation describes the pitch dynamics motion of the GTM in clean configuration at an altitude 30000 ft, flying at Mach 0.8. In the approximate model, the aircraft is described by two states: the pitch angle θ [deg] and pitch rate q [rad/s]. The input to the system is the elevator deflection δ_e [deg]. The input is bounded by the upper and lower limits: $\delta_{e,\max}$ [deg] and $\delta_{e,\min}$ [deg], respectively.

Let $\boldsymbol{x} = [\theta, q]^T$ denote the state of the system. Under nominal conditions, the pitch dynamics of the GTM [9] are

$$\dot{\boldsymbol{x}} = \mathrm{A}_0\boldsymbol{x} + \mathrm{B}_0\delta_e, \quad \delta_{e,\min} \leq \delta_e \leq \delta_{e,\max} \tag{12}$$

where[b]:

$$\mathrm{A}_0 = \begin{bmatrix} 0 & 1 \\ -2.6923 & -0.7322 \end{bmatrix}, \quad \mathrm{B}_0 = \begin{bmatrix} 0 \\ -3.3552 \end{bmatrix}$$

and

$$\delta_{e,\min} = -30 \text{ deg}, \quad \delta_{e,\max} = 30 \text{ deg}$$

In the nominal case, the natural frequency of the system ω_{n_0} is equal to 1.64 rad/s and the damping ratio ς_0 is 0.223.

Many different failure scenarios can be considered for the GTM. In this paper, the analysis is restricted to one hypothetical off-nominal condition which is representative of a case wherein the open-loop dynamics become marginally stable. Additionally, a 50% loss of elevator effectivenes is assumed in the failure condition. The dynamics of the off-nominal condition are

$$\dot{\boldsymbol{x}} = \mathrm{A}\boldsymbol{x} + \mathrm{B}\delta_e, \quad \delta_{e,\min} \leq \delta_e \leq \delta_{e,\max} \tag{13}$$

[b]The matrices A_0 and B_0 are given for θ, and δ_e expressed in radians.

where

$$\mathrm{A} = \begin{bmatrix} 0 & 1 \\ -2.3388 & -0.0252 \end{bmatrix}, \quad \mathrm{B} = \begin{bmatrix} 0 \\ -1.7676 \end{bmatrix}$$

In (13), notice that the loss of elevator effectiveness can be recognized in the change of magnitude in the second *B*-matrix entry from −3.3552 to −1.7676. In comparison to the nominal system (12), the off-nominal system has indeed become marginally stable, since the damping ratio ς is now only 0.0083. The natural frequency ω_n has remained more or less constant which is now equal to 1.53 rad/s.

B. The pitch hold system

A pitch hold system is designed for the nominal case of the pitch dynamics model (12). The pitch hold system takes a reference pitch attitude as a command input, and aims to bring the aircraft state to that reference pitch attitude. The pitch hold system is a PD controller and takes the form[c]

$$\delta_e = k_\theta \left(k_s \theta_{ref} - \theta \right) - k_q q \tag{14}$$

with θ_{ref} denoting reference pitch attitude and q_{ref} set to 0 rad/s. Let $K_1 = [k_\theta, k_q]$ and $K_2 = k_\theta k_s$, so that (14) can be rewritten as

$$\delta_e = -K_1 \boldsymbol{x} + K_2 \theta_{ref} \tag{15}$$

Stability requirements demand the natural frequency ω_{n_r} to be 2.5 rad/s and the damping ratio ς_r to be 0.707. Pole-placement yields

$$K_1 = \begin{bmatrix} -1.0604 & -0.8354 \end{bmatrix}$$

The gain K_2 is used to eliminate the steady-state error for a step reference command. For the nominal system, this gain would be set to −1.8628. Note that the saturation of the elevator introduces non-linear effects. Within the saturation bounds however, the closed-loop system is completely

[c]The gains k_θ, k_s, and k_q are given for θ, θ_{ref}, and δ_e expressed in radians.

linear and given by

$$\dot{\boldsymbol{x}} = (\mathrm{A}_0 - \mathrm{B}_0 K_1)\,\boldsymbol{x} + \mathrm{B}_0 K_2 \theta_{ref}$$

For the off-nominal case (13), the closed-loop dynamics are

$$\dot{\boldsymbol{x}} = (\mathrm{A} - \mathrm{B} K_1)\,\boldsymbol{x} + \mathrm{B} K_2 \theta_{ref}$$

Note that the gains K_1 and K_2 remain the same in the off-nominal case. Consequently, the closed-loop dynamics is degraded during the off-nominal condition. That is, apart from a sluggish response (i.e. high overshoot, large settling time, etc), a steady-state error is expected when a certain reference pitch attitude is commanded. Also, larger elevator deflections are required to obtain the same reference pitch attitude because of the loss in elevator effectiveness.

C. The safe maneuvering envelope and the reference pitch attitude margins

Our aim is to maintain the aircraft within an envelope constrained by limitations on the pitch attitude. The constraints on the pitch attitude are

$$l_1(\boldsymbol{x}) := \quad -\theta - 10^\circ \quad \leq 0 \tag{16a}$$

$$l_2(\boldsymbol{x}) := \quad \theta - 25^\circ \quad \leq 0 \tag{16b}$$

Given that the aircraft is at some state $\boldsymbol{x}_0 = [\theta_0, q_0]^T$ at time t_0, the computed reference pitch attitude margins $(\theta_{ref,\min}, \theta_{ref,\max})$ ensure that the state trajectory will not violate the constraints (16) for the next T seconds, as long as

$$\theta_{ref,\min} \leq \theta_{ref}(\tau) \leq \theta_{ref,\max}$$

for all $\tau \in [t_0, t_0 + T]$.

D. Implementation of the optimal control framework

In order to compute the margins for the reference pitch attitude, the framework outlined in section III is followed. Define the following cost functionals

$$J_i\left(\boldsymbol{x}_0, \boldsymbol{y}_{ref}(\cdot)\right) := \max_{\tau\in[t_0,t_0+T]} l_i\left(\boldsymbol{\zeta}(\tau; \boldsymbol{x}_0, \theta_{ref}(\cdot))\right), \quad i = 1, 2 \tag{17}$$

In (17), the cost functional J_1 refers to the lower bound set on the pitch attitude (16a). The cost functional J_2 on the other hand refers to upper bound set on the pitch attitude (16b). For a given set of margins $(\theta_{ref,\min}, \theta_{ref,\max})$, the cost functionals (17) are optimized over the space of admissible reference signals

$$\boldsymbol{\Theta_{ref}} := \left\{\theta_{ref}(\cdot) : [t_0, t_0 + T] \mapsto [\theta_{ref,\min}, \theta_{ref,\max}] \;\middle|\; \theta_{ref}(\cdot) \text{ is measurable}\right\} \tag{18}$$

That is, the following are computed

$$J_i^*(\boldsymbol{x}_0) = \max_{\theta_{ref}(\cdot)\in\boldsymbol{\Theta_{ref}}} J_i\left(\boldsymbol{x}_0, \theta_{ref}(\cdot)\right), \quad i = 1, 2 \tag{19}$$

$J_i^*(\boldsymbol{x}_0)$ can be found from the relationship (9), which subsequently requires solving PDE (10). In the present study, (10) is solved using the method presented in [24].

The PDEs in (10) are coupled with an optimization problem. This optimization consist of evaluating the Hamiltonian in (11). What follows next is an elaboration on how this evaluation is performed. Let

$$\boldsymbol{f}_0\left(\boldsymbol{x}, \theta_{ref}\right) = \begin{cases} \mathrm{A}_0\boldsymbol{x} + \mathrm{B}_0\delta_{e,\min} & \text{if } -K_1\boldsymbol{x} + K_2\theta_{ref} < \delta_{e,\min} \\ \mathrm{A}_0\boldsymbol{x} + \mathrm{B}_0\delta_{e,\max} & \text{if } -K_1\boldsymbol{x} + K_2\theta_{ref} > \delta_{e,\max} \\ (\mathrm{A}_0 - \mathrm{B}_0K_1)\,\boldsymbol{x} + \mathrm{B}K_2\theta_{ref} & \text{otherwise} \end{cases} \tag{20}$$

denote the dynamics of the nominal system. Similarly, let

$$\boldsymbol{f}\left(\boldsymbol{x},\theta_{ref}\right)=\begin{cases}\mathrm{A}\boldsymbol{x}+\mathrm{B}\delta_{e,\min} & \text{if } -K_1\boldsymbol{x}+K_2\theta_{ref}<\delta_{e,\min}\\ \mathrm{A}\boldsymbol{x}+\mathrm{B}\delta_{e,\max} & \text{if } -K_1\boldsymbol{x}+K_2\theta_{ref}>\delta_{e,\max}\\ (\mathrm{A}-\mathrm{B}K_1)\,\boldsymbol{x}+\mathrm{B}K_2\theta_{ref} & \text{otherwise}\end{cases} \tag{21}$$

denote the dynamics of the off-nominal system. Hence, the Hamiltonians that need to be evaluated are respectively

$$H_0\left(\boldsymbol{x},\frac{\partial V_i(t,\boldsymbol{x})}{\partial \boldsymbol{x}}\right)=\max_{\theta_{ref}\in\left[\theta_{ref,\min},\theta_{ref,\max}\right]}\frac{\partial V_i(t,\boldsymbol{x})}{\partial \boldsymbol{x}}^{T}\boldsymbol{f}_0\left(\boldsymbol{x},\theta_{ref}\right) \tag{22}$$

for the nominal case, and

$$H\left(\boldsymbol{x},\frac{\partial V_i(t,\boldsymbol{x})}{\partial \boldsymbol{x}}\right)=\max_{\theta_{ref}\in\left[\theta_{ref,\min},\theta_{ref,\max}\right]}\frac{\partial V_i(t,\boldsymbol{x})}{\partial \boldsymbol{x}}^{T}\boldsymbol{f}\left(\boldsymbol{x},\theta_{ref}\right) \tag{23}$$

for the off-nominal case. From (20) and (21) it follows that the optimization variable θ_{ref} in (22) and (23) is affine to both $\boldsymbol{x}$ and $\frac{\partial V_i(t,\boldsymbol{x})}{\partial \boldsymbol{x}}$. Because of this fact, the optimization in (22) and (23) becomes very straightforward as it can be expressed analytically with the feedback laws

$$\boldsymbol{g}^*_0(t,\boldsymbol{x})=\begin{cases}\theta_{ref,min} & \text{if } \frac{\partial V_i(t,\boldsymbol{x})}{\partial \boldsymbol{x}}^{T}\mathrm{B}_0K_2\le 0\\ \theta_{ref,max} & \text{if } \frac{\partial V_i(t,\boldsymbol{x})}{\partial \boldsymbol{x}}^{T}\mathrm{B}_0K_2>0\end{cases} \tag{24}$$

for the nominal case, and

$$\boldsymbol{g}^*(t,\boldsymbol{x})=\begin{cases}\theta_{ref,min} & \text{if } \frac{\partial V_i(t,\boldsymbol{x})}{\partial \boldsymbol{x}}^{T}\mathrm{B}K_2\le 0\\ \theta_{ref,max} & \text{if } \frac{\partial V_i(t,\boldsymbol{x})}{\partial \boldsymbol{x}}^{T}\mathrm{B}K_2>0\end{cases} \tag{25}$$

for the off-nominal case. Subsequently, (22) and (23) can be reduced to

$$H\left(\boldsymbol{x},\frac{\partial V_i(t,\boldsymbol{x})}{\partial \boldsymbol{x}}\right)=\frac{\partial V_i(t,\boldsymbol{x})}{\partial \boldsymbol{x}}^{T}\boldsymbol{f}\left(\boldsymbol{x},\boldsymbol{g}^*_0(t,\boldsymbol{x})\right)$$

and

$$H\left(\boldsymbol{x},\frac{\partial V_i(t,\boldsymbol{x})}{\partial \boldsymbol{x}}\right)=\frac{\partial V_i(t,\boldsymbol{x})}{\partial \boldsymbol{x}}^{T}\boldsymbol{f}\left(\boldsymbol{x},\boldsymbol{g}^*(t,\boldsymbol{x})\right)$$

respectively.

E. The algorithm to compute safety margins for the pitch dynamics model

The margins on the pitch command reference are determined by using the procedure depicted in figure 2. Simple heuristics are used to iteratively adjust the margins of the pitch command reference. This involves making incremental changes to the upper and lower limits of the pitch command reference.

Given the dependency of J_i^* on the margins: $(\theta_{ref,\min}, \theta_{ref,\max})$, we may express

$$J_i^* = J_i^*\left(\boldsymbol{x}_0; \theta_{ref,\min}, \theta_{ref,\max}\right), \quad i = 1, 2$$

The following algorithm finds the least restrictive margins for the considered example problem. The margins are found by making incremental changes of *one degree* to $\theta_{ref,\min}$ and $\theta_{ref,\max}$.

Algorithm

Let $\boldsymbol{x}_0$ denote the current state. Furthermore, let $\theta_{ref,\min_0}$ and $\theta_{ref,\max_0}$ denote the margin limits computed in the previous time-step. For the next time-step, initialize $\theta^{(0)}_{ref,\min} = \theta_{ref,\min_0}$ and $\theta^{(0)}_{ref,\max} = \theta_{ref,\max_0}$, and perform the following iteration at least k_{min} times.

1. Compute $J_i^*(\boldsymbol{x}_0; \theta^{(k)}_{ref,\min}, \theta^{(k)}_{ref,\max})$ for $i = 1, 2$.
2. If $k > k_{min}$, break the iteration at this point and return the safety margins $(\theta^{(k)}_{ref,\min}, \theta^{(k)}_{ref,\max})$, if either:
   - $\max\limits_{i\in\{1,2\}} J_i^*(\boldsymbol{x}_0; \theta^{(k)}_{ref,\min}, \theta^{(k)}_{ref,\max}) \leq 0$
   - the lower margin limit hits the upper margin limit, i.e. $\theta^{(k)}_{ref,\min} = \theta^{(k)}_{ref,\max}$, and $\max\limits_{i=1,2} J_i^*(\boldsymbol{x}_0; \theta^{(k)}_{ref,\min}, \theta^{(k)}_{ref,\mathrm{r}}$ 0.
3. Depending on the sign of $J_1(\boldsymbol{x}_0)$, update the margin limits with one degree increments in the

following way:

$$\theta'_{ref,\min} = \begin{cases} \theta^{(k)}_{ref,\min} + 1^\circ & \text{if } J_1^*(\boldsymbol{x}_0; \theta^{(k)}_{ref,\min}, \theta^{(k)}_{ref,\max}) > 0 \\ \theta^{(k)}_{ref,\min} - 1^\circ & \text{if } J_1^*(\boldsymbol{x}_0; \theta^{(k)}_{ref,\min}, \theta^{(k)}_{ref,\max}) \leq 0 \end{cases}$$

$$\theta'_{ref,\max} = \begin{cases} \theta'_{ref,\min} & \text{if } J_1^*(\boldsymbol{x}_0; \theta^{(k)}_{ref,\min}, \theta^{(k)}_{ref,\max}) > 0 \\ & \text{and if } \theta^{(k)}_{ref,\min} = \theta^{(k)}_{ref,\max} \\ \theta^{(k)}_{ref,\max} & \text{otherwise} \end{cases}$$

4. Compute $J_i^*(\boldsymbol{x}_0; \theta'_{ref,\min}, \theta'_{ref,\max})$ for $i = 1, 2$.

5. If $k > k_{min}$, break the iteration at this point and return the safety margins $(\theta'_{ref,\min}, \theta'_{ref,\max})$, if either

   - $\max_{i \in \{1,2\}} J_i^*(\boldsymbol{x}_0; \theta'_{ref,\min}, \theta'_{ref,\max}) \leq 0$
   - the lower margin limit hits the upper margin limit, i.e. $\theta'_{ref,\min} = \theta'_{ref,\max}$, and $\max_{i=1,2} J_i^*(\boldsymbol{x}_0; \theta'_{ref,\min}, \theta'_{r}$ 0.

6. Depending on the sign of $J_2(\boldsymbol{x}_0)$, update the margin limits with one degree increments in the following way:

$$\theta^{(k+1)}_{ref,\max} = \begin{cases} \theta'_{ref,\max} - 1^\circ & \text{if } J_2^*(\boldsymbol{x}_0; \theta'_{ref,\min}, \theta'_{ref,\max}) > 0 \\ \theta'_{ref,\max} + 1^\circ & \text{if } J_2^*(\boldsymbol{x}_0; \theta'_{ref,\min}, \theta'_{ref,\max}) \leq 0 \end{cases}$$

$$\theta^{(k+1)}_{ref,\min} = \begin{cases} \theta^{(k+1)}_{ref,\max} & \text{if } J_2^*(\boldsymbol{x}_0; \theta'_{ref,\min}, \theta'_{ref,\max}) > 0 \\ & \text{and if } \theta'_{ref,\min} = \theta'_{ref,\max} \\ \theta'_{ref,\min} & \text{otherwise} \end{cases}$$

V. Simulation results

In this section, simulation results are presented for the GTM example where safety margins are computed for the reference pitch attitude along the followed state trajectory. The margins are

determined using the algorithm presented in the previous section. The simulation results display how the margins change dynamically to the control actions and system degradation.

A. The test scenario

In the simulation, a scenario is considered wherein a certain failure leads to a sudden degradation of the system dynamics. In this failure condition, which occurs after 10 seconds in the simulation, the system makes a transition from the nominal condition, i.e. as in (12), to the off-nominal condition described in (13). This transition happens instantaneously, and the simulation is extended for 40 more seconds, resulting in an overall simulation duration of 50 seconds.

During the entire simulation, a switching block signal is provided as a reference command to the pitch hold system. The following two cases are distinguished:

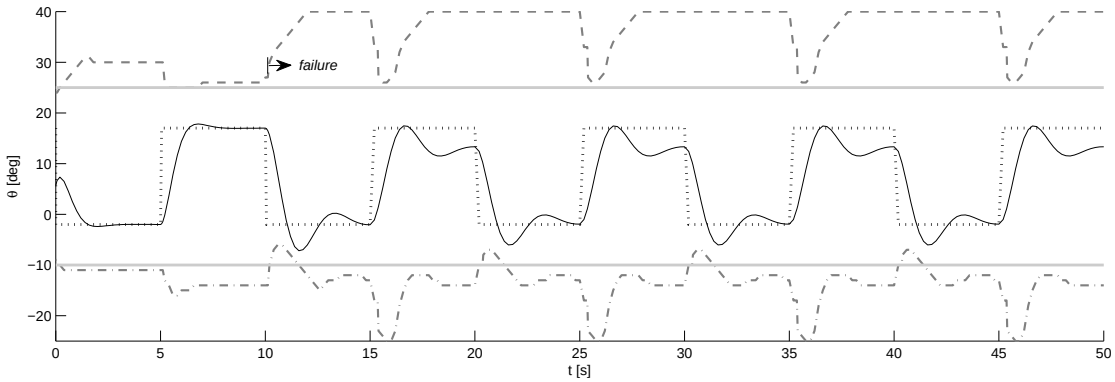
- Case I: the reference command *satisfies* the command margins, and hence stays *within* the computed margin limits at all times.
- Case II: the reference command occasionally *violates* the command margins, and sometimes goes *outside* of the computed margin limits.

Simulations are conducted representing both cases. The simulations are conducted using the sub-scale model of the GTM given by (12) and (13) for the nominal and off-nominal condition respectively. Subsequently, the provided example purely focuses on the system performance for the pitch attitude, and neglects the effects on the angle of attack and load factor envelopes. The remaining subsections discusses the dynamic behavior of the margins for case I and II separately.

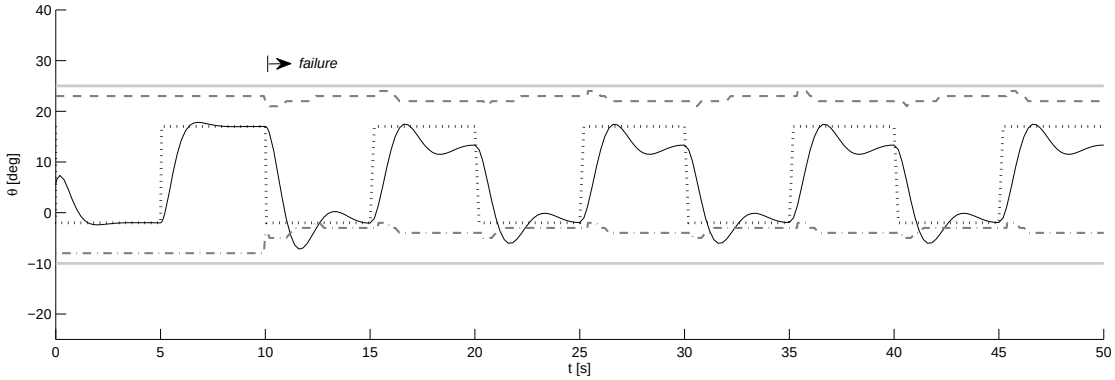
B. Case I: the reference command satisfies the command margins

Figure 4 shows simulation results for case I. In the figure, the envelope boundaries (as defined in (16)) are denoted by the thick, gray continuous lines. Furthermore, the state trajectory is denoted by a black continuous line, and the reference command signal is denoted by the black dotted line. The margins themselves are denoted by the gray dashed lines. Clearly noticeable in the figure is that the reference command always remains within the margins (i.e. between the dashed gray

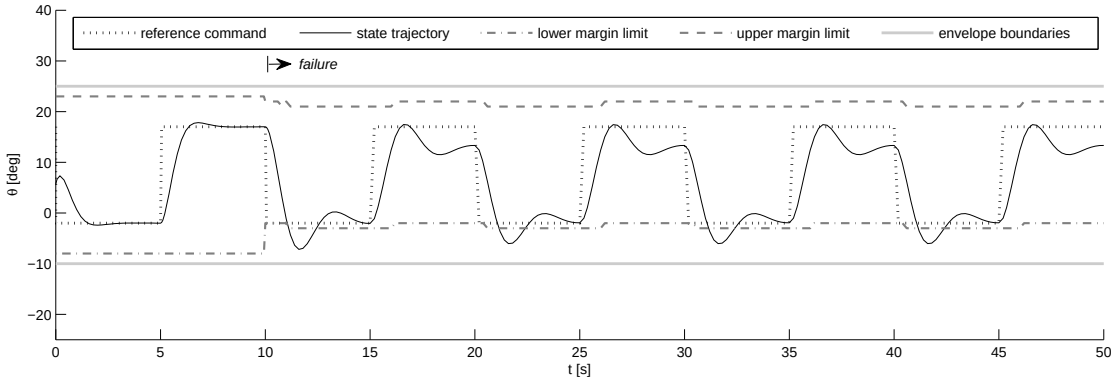
lines) for the entire simulation. Coincidentally, the state trajectory never exceeds the envelope in this particular simulation. This observation is consistent with our expectations since the margins provide a guarantee of not violating the envelope for a specified time period. Hence, if the reference command continuously satisfies the margins, so will the state trajectory continuously remain within the envelope.



a) Results for a prediction horizon of $T = 1$ second.



b) Results for a prediction horizon of $T = 3$ seconds.



c) Results for a prediction horizon of $T = 5$ seconds.

Figure 4. The command margins estimated with different prediction horizon settings for case I.

Figure 4 displays the command margins for three different prediction horizons. The general trend seen in the figure is that increasing the prediction horizon leads to more restrictive margins. This holds true particularly for the prediction horizon of $T = 1$ second in figure 4a, where the margins are extremely large and exceed even the flight envelope. This result suggests that extremely large reference commands (that which even exceed the envelope) are required to steer the aircraft out of the envelope within a one second time frame. When increasing the prediction horizon to $T = 3$ seconds, figure 4b shows that it is also possible to steer the aircraft out of the envelope with less extreme reference command signals. Clearly, a one second prediction is simply too small to encompass all transient effects in the pitch dynamics. Using such a small prediction horizon can be very misleading and sends out false signals concerning vehicle safety and operational freedom.

For the example consider in this paper, a larger prediction horizon of $T = 5$ seconds (figure 4c) gives a much better indication of safety. For a prediction horizon of $T = 5$ seconds, the margins clearly shrink after the failure at $t = 10$ seconds. This shrinkage of the margins gives an indication that the system dynamics has been degraded and that the aircraft has entered an off-nominal condition.

C. Case II: the reference command violates the command margins

Figure 5 shows the simulation results for Case II. This time, the margins are computed only for a prediction horizon of $T = 5$ seconds. Furthermore, the provided reference command no longer satisfies the safety margins for the entire duration of the simulation. As can be seen in figure 5, after the failure condition at $t = 10$ seconds, the reference command repeatedly violates the lower limit set by the margins. In compliance with expectations, results indicate that envelope excursions may occur under prolonged neglect of the margins. For instance, an envelope excursion happens at approximately $t = 11.5$ seconds, when the margins are ignored for the first time. The broken lines at approximately $t = 12$ seconds point out that there is no reference signal that will keep the system inside the envelope boundaries. In the simulation, the aircraft returns back into the envelope as if nothing significant has occurred. However, note that in practice this envelope excursion could have been a precursor to a LOC incident.

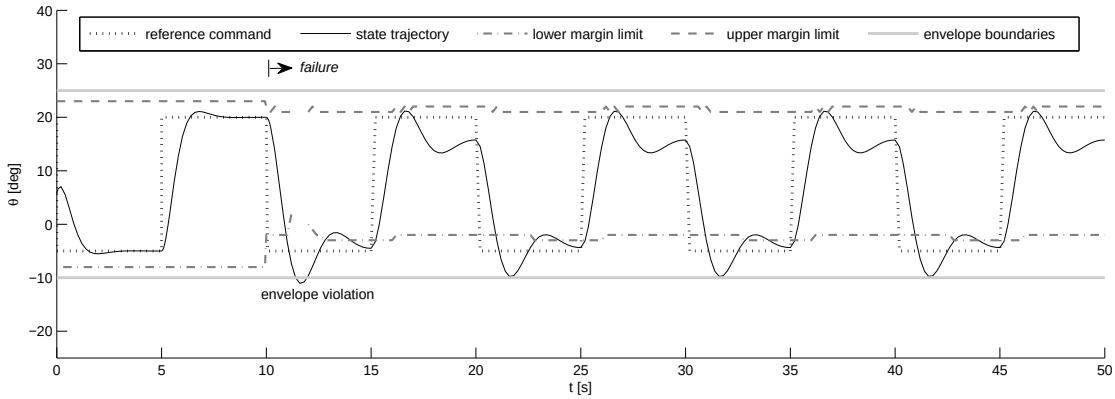
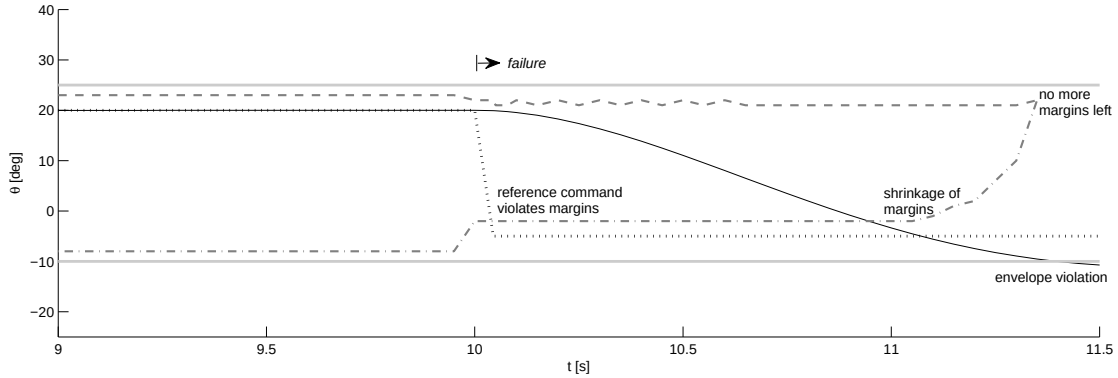


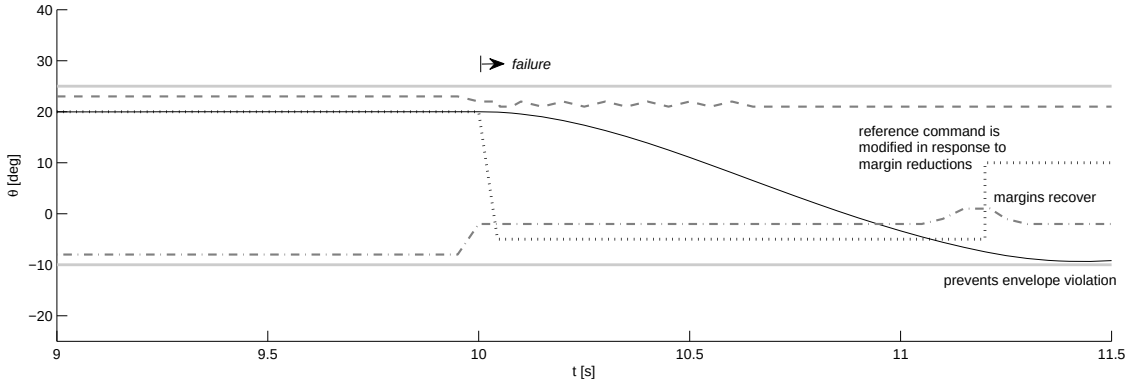
Figure 5. Command margins estimated with a prediction horizon of $T = 5$ seconds for case II.

A violation of the margins by the reference command signal does not necessarily imply an inevitable envelope violation. As can be observed in figure 5, the pitch attitude reference command repeatedly violates the margins after $t = 20$ seconds, yet the state trajectory does not cross the envelope for those occasions. An envelope excursion is commonly preceded by a rapid shrinkage of the margins. This is noticeable also in the envelope violation at approximately $t = 11.5$ seconds in figure 5. The shrinkage is more clearly portrayed in figure 6a which zooms in to the time period of the transition from nominal to off-nominal dynamics. A fast shrinkage of the margins is a strong indication of the aircraft approaching the edge of the envelope; closer the aircraft is to the envelope boundary, smaller the margins become. The envelope excursion could have been prevented if the reference command was modified in time in order to comply with the margins. This is illustrated in figure 6b and 6c, wherein an envelope excursion is avoided by modifying the reference command at approximately $t = 11.2$ seconds.

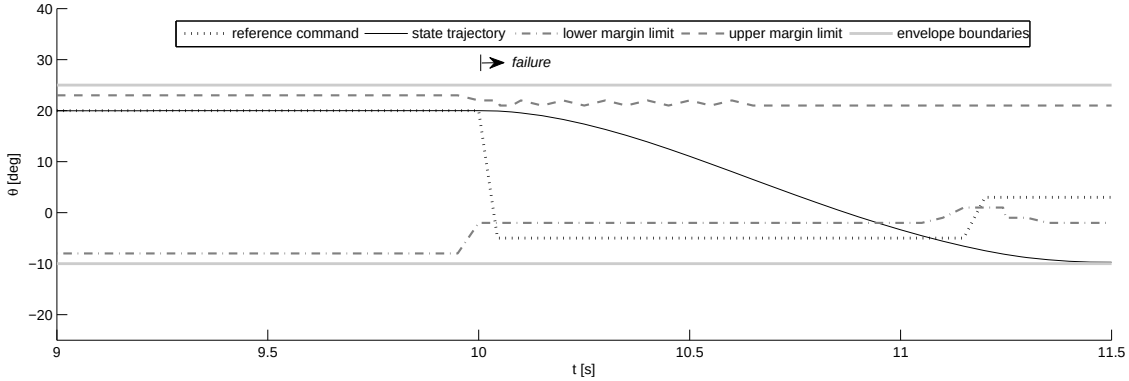
In future work, efforts will be geared towards designing effective cockpit displays that help portray the margin information to the pilots. Furthermore, efforts will be made to apply the framework on more complex, higher dimensional systems with potentially multiple reference command inputs. Eventually, the goal is to conduct human-in-the-loop experiments in order to test the concept in practice.



a) The reference command violates the margins continuously. The margins shrink rapidly followed by a envelope violation.



b) The reference command is modified in response to the changes in the margins.



c) The reference command is modified in response to the changes in the margins, but this time the reference command is only modified slightly so that it barely satisfies the margins.

Figure 6. Command margins estimated for case II with $T = 5$ seconds. The results are shown for the time interval: $[9, 11.5]$ **seconds where the transition occurs from nominal to off-nominal dynamics.**

VI. Conclusions

A methodology was proposed to compute "safety margins" for the reference command signals of aircraft control systems, such that certain predefined state constraints denoting a safe maneuvering

envelope are not violated. The methodology employs principles from optimal control to establish a set of margins that mathematically guarantee operation of the aircraft within the envelope for a specified prediction horizon. To estimate the margins correctly, complete information on the system dynamics is required, and hence, the methodology must be used in combination with a system identification procedure to estimate the anomalies during off-nominal conditions.

The practical application of the entire framework was illustrated on a simplified pitch dynamics model with state limitations on the pitch attitude. Simulations were conducted wherein margins were computed for the reference pitch attitude command of the pitch hold system. These margins were computed along the actual flown state trajectory, while the aircraft enters into a failure condition. In line with theory and expectations, simulation results confirmed that envelope excursions are avoided when the reference command signals remain within the margins. On the other hand, a prolonged neglect of the margins is capable of steering the aircraft out of the flight envelope. The excursions can be anticipated by a rapid shrinkage of the margins prior to an envelope violation. The computed margins can be used to improve the situational awareness by displaying the information on cockpit displays. The margins can also be used to directly limit the commands provided to the autopilot system. This all depends on which design philosophy is applied in the FEP architecture.

Acknowledgements

The authors would like to thank Q.P. Chu and J.H. van Schuppen for their useful suggestions and feedback on this work.

References

[1] Belcastro, C. M. and Foster, J. V., “Aircraft Loss-of-Control Accident Analysis,” in “AIAA Guidance, Navigation and Control Conference, Toronto, Canada,” AIAA 2010-8004.

[2] Kwatny, H. G., Dongmo, J.-E. T., Chang, B.-C., Bajpai, G., Yasar, M., and Belcastro, C., “Nonlinear Analysis of Aircraft Loss of Control,” *Journal of Guidance, Control, and Dynamics*, Vol. 36, No. 1, 2012, pp. 149–162. DOI: 10.2514/1.56948.

[3] Wilborn, J. E. and Foster, J. V., “Defining Commercial Transport Loss-of-Control : A Quantitative Approach,” in “AIAA Atmospheric Flight Mechanics Conference and Exhibit, Providence, Rhode Island,” AIAA 2004-4811, 2004. DOI: 10.2514/6.2004-4811.

[4] 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. 248–261. DOI: 10.2514/1.35265.

[5] Falkena, W., Borst, C., Chu, Q., and Mulder, J., "Investigation of Practical Flight Envelope Protection Systems for Small Aircraft," *Journal of Guidance, Control, and Dynamics*, Vol. 34, No. 4. DOI: 10.2514/1.53000.

[6] Sharma, V., Voulgaris, P. G., and Frazzoli, E., "Aircraft autopilot analysis and envelope protection for operation under icing conditions," *Journal of guidance, control, and dynamics*, Vol. 27, No. 3, 2004, pp. 454–465.

[7] Kirk, D. E., *Optimal Control Theory - An Introduction*, Dover Publications, Inc., New York, 1970.

[8] Bardi, M. and Capuzzo-Dolcetta, I., *Optimal Control and Viscosity Solutions of Hamilton-Jacobi-Bellman Equations*, Birkhauser, Boston, 2008. DOI: 10.1007/978-0-8176-4755-1.

[9] Barlow, J., Stepanyan, V., and Krishnakumar, K., "Estimating Loss-of-Control: a Data-Based Predictive Control Approach," in "AIAA Guidance, Navigation, and Control Conference, Portland, Oregon," AIAA 2011-6408, 2011. DOI: 10.2514/6.2011-6408.

[10] Krishnakumar, K., Stepanyan, V., and Barlow, J., "Piloting on the Edge: Approaches to Flight Control Solutions," in "Space Mission Challenges for Information Technology (SMC-IT), 2011 IEEE Fourth International Conference on," , 2011, pp. 103–110. DOI: 10.1109/SMC-IT.2011.28.

[11] Unnikrishnan, S., *Adaptive Envelope Protection Methods for Aircraft*, PhD thesis, Georgia Institute of Technology, 2006.

[12] Yavrucuk, I. and Prasad, J., "Online Dynamic Trim and Control Limit Estimation," *Journal of Guidance, Control, and Dynamics*, Vol. 35, No. 5, 2012, pp. 1647–1656. DOI: 10.2514/1.53116.

[13] Jordan, T., Langford, W., Belcastro, C., Foster, J., Shah, G., Howland, G., and Kidd, R., "Development of a Dynamically Scaled Generic Transport Model Testbed for Flight Research Experiments," Nasa technical report, 2004.

[14] Morelli, E. A. and Smith, M. S., "Real-time dynamic modeling: Data information requirements and flight-test results," *Journal of Aircraft*, Vol. 46, No. 6, 2009, pp. 1894–1905. DOI: 10.2514/1.40764.

[15] Tang, L., Roemer, M., Ge, J., Crassidis, A., Prasad, J. V. R., and Belcastro, C., "Methodologies for Adaptive Flight Envelope Estimation and Protection," in "AIAA, Guidance, Navigation and Control Conference, Chicago, Illinois," AIAA 2009-6260, 2009. DOI: 10.2514/6.2009-6260.

[16] Tang, Y., Atkins, E. M., and Sanner, R. M., "Emergency Flight Planning for a Generalized Transport Aircraft with Left Wing Damage," in "AIAA Guidance, Navigation and Control Conference and Exhibit, Hilton Head, South Carolina," AIAA 2007-6873, 2007. DOI: 10.2514/6.2007-6873.

[17] Bayen, A. M., Mitchell, I. M., Oishi, M., and Tomlin, C. J., "Aircraft Autolander Safety Analysis Through Optimal Control-Based Reach Set Computation," *Journal of Guidance, Control, and Dynamics*, Vol. 30, No. 1, 2007, pp. 68–77. DOI: 10.2514/1.21562.

[18] Lygeros, J., "On reachability and minimum cost optimal control," *Automatica*, Vol. 40, 2004, pp. 917 – 927. DOI: 10.1016/j.automatica.2004.01.012.

[19] Oort, E., Chu, Q., and Mulder, J., "Maneuver Envelope Determination through Reachability Analysis," in Holzapfel, F. and Theil, S., eds., "Advances in Aerospace Guidance, Navigation and Control," Springer Berlin Heidelberg, pp. 91–102, 2011. DOI: 10.1007/978-3-642-19817-5_8.

[20] Lombaerts, T. J., Schuet, S. R., Wheeler, K. R., Acosta, D. M., and Kaneshige, J. T., "Safe Maneuvering Envelope Estimation based on a Physical Approach," in "AIAA Guidance, Navigation, and Control Conference, Boston, Massachusetts," AIAA 2013-4618, 2013. DOI: 10.2514/6.2013-4618.

[21] 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, 2005, pp. 947–957. DOI: 10.1109/TAC.2005.851439.

[22] Osher, S. and Fedkiw, R., *Level Set Methods and Dynamic Implicit Surfaces*, Vol. 153, Springer-Verlag, New York, 2003.

[23] Wang, F., Zhang, H., and Liu, D., "Adaptive Dynamic Programming : An Introduction," *IEEE Computational Intelligence Magazine*, Vol. 4, No. 2, 2009, pp. 39–47. DOI: 10.1109/MCI.2009.932261.

[24] Govindarajan, N., de Visser, C. C., and Krishnakumar, K., "A sparse collocation method for solving time-dependent HJB equations using multivariate B-splines," *Automatica, In Press*.

[25] Lai, M. J. and Schumaker, L. L., *Spline Functions on Triangulations*, Cambridge University Press, 2007.

[26] de Visser, C., Chu, Q., and Mulder, J., "A new approach to linear regression with multivariate splines," *Automatica*, Vol. 45, No. 12, 2009, pp. 2903–2909. DOI: 10.1016/j.automatica.2009.09.017.

[27] Betts, J. T., "Survey of Numerical Methods for Trajectory Optimization," *Journal of Guidance, Control, and Dynamics*, Vol. 21, No. 2, 1998, pp. 193–207. DOI: 10.2514/2.4231.

[28] Rao, A. V., "A survey of numerical methods for optimal control," *Advances in the Astronautical Sciences*, Vol. 135, No. 1, 2009, pp. 497–528.

[29] Benson, D., *A Gauss Pseudospectral Transcription for Optimal Control*, PhD thesis, Massachusetts Institute of Technology, 2005.

[30] Benson, D. A., Huntington, G. T., Thorvaldsen, T. P., and Rao, A. V., "Direct Trajectory Optimization and Costate Estimation via an Orthogonal Collocation Method," *Journal of Guidance, Control, and Dynamics*, Vol. 29, No. 6. DOI: 10.2514/1.20478.