# Safe Set Protection and Restoration for Unimpaired and Impaired Aircraft

Robert C. Allen* and Harry G Kwatny†

*Drexel University, MEM Department, 3141 Chestnut Street,Philadelphia, PA, 19104, USA*

Gaurav Bajpai‡

*Techno-Sciences, Inc., 11750 Beltsville Drive, Beltsville, MD, 20705, USA*

**The flight envelope can be viewed as a set within the state space of an aircraft. For various safety considerations an aircraft is required to remain within its prescribed flight envelope. The safe set is the largest controlled invariant set within the flight envelope. Thus, if an aircraft is to remain within its envelope it must stay within the safe set. When an aircraft is impaired, e.g., a jammed elevator or an engine loss, the safe set shrinks as would be expected. In this paper we consider strategies to prevent the aircraft from departing the safe set - the envelope protection problem - and strategies to restore the aircraft to a desired trim point within the safe set should it find itself outside the safe set - the envelope restoration problem. Note that an aircraft may be driven outside of the safe set by a disturbance, a loss-of-control incident, or by a component failure in which the safe set shrinks. The problems of envelope protection and restoration are substantially different. Envelope protection requires avoiding close proximity to certain critical boundary segments of the safe set. Restoration is more straightforward involving steering the aircraft to a target trim condition along trajectories that minimize the excursion from the flight envelope. Precise formulations of both problems will be given and alternative solutions will be compared. Examples are given using a model derived from the the longitudinal dynamics of NASA's Generic Transport Model.**

## Nomenclature

| | |
|---|---|
| $V$ | airspeed, ft/s |
| $\gamma$ | flight path angle, deg |
| $\alpha$ | angle of attack, deg |
| $\theta$ | pitch angle, deg |
| $q$ | pitch rate, deg/s |
| $T$ | engine thrust, lb |
| $\delta_e$ | elevator position, deg |
| $m$ | vehicle mass, slugs |
| $I_y$ | principal moment of inertia Y-axis, $lb - ft^2$ |
| $g$ | gravitational constant, ft/s/s |
| $C_D, C_L, C_M, C_X$ | aerodynamic coefficients |
| $x$ | state vector |
| $u$ | control vector |
| $z$ | regulated output vector |
| $\mathcal{C}, \mathcal{S}$ | $R^n$ state space domains for flight envelope and safe sets |
| $\partial\mathcal{C}, \partial\mathcal{S}$ | boundaries of $\mathcal{C}$ and $\mathcal{S}$ |
| $\mathcal{U}$ | control constraint set |

*Graduate Student, AIAA Member, rca28@drexel.edu.

†S. Herbert Raynes Professor, AIAA Member, hkwatny@coe.drexel.edu.

‡Senior Scientist, AIAA Member, bajpai@technosci.com.

| | |
|---|---|
| $\phi(x)$ | cost function associated with time dependent Hamiltonian-Jacobi equation |
| $H(x,u)$ | Hamiltonian |
| $p = \nabla\phi(x)$ | gradient of $\phi$ at $x$ |

# I. Introduction

Ensuring that an aircraft remains within its flight envelope is called *envelope protection.* Recent flight control research contains many examples of safe set envelope protection schemes.[1–7] The idea of a *safe*[3] or *viable*[2] invariant set derives from a decades old control problem in which the plant controls are restricted to a bounded set $\mathcal{U}$ and it is desired to keep the system state within a convex, not necessarily bounded, subset $\mathcal{C}$ of the state space. Feuer[8] studied the question: under what conditions does there exist for each initial state in $\mathcal{C}$ an admissible control producing a trajectory that remains in $\mathcal{C}$ for all $t > 0$? When $\mathcal{C}$ does not have this property it is desired to identify the safe set, $\mathcal{S}$, that is, the largest subset of $\mathcal{C}$ that does. Clearly, if it is desired to keep the aircraft in $\mathcal{C}$, it must be insured that it remains in $\mathcal{S}$. If an aircraft finds itself outside of $\mathcal{S}$, due to an impairment or disturbance, then there is no admissible control which will prevent departure from $\mathcal{C}$. This will require initiation of a restoration control which is to designed to return the aircraft to a safe equilibrium state in $\mathcal{C}$ when possible.

To illustrate concepts in this paper, we presume we are given a hypothetical four dimensional flight envelope which defines the state constraints $\mathcal{C}$, for the longitudinal dynamics of an aircraft. We consider aircraft impairments in the form of control constraints on either the elevator or the engine thrust and show how the boundary of the safe set changes. For envelope recovery, we will employ a linear quadratic regulator. We illustrate that when the aircraft state is outside $\mathcal{S}$,the state constraints, $\mathcal{C}$ will be exceeded. For envelope protection we give a mathematical formulation for the admissible safe set control, that is the control required to prevent envelope departure. We also show that for a stabilizing controller there are cases where a trajectory starting in $\mathcal{S}$, $\mathcal{C}$ might be departed in in order to reach an admissible trim state. It is noted that safe set theory says nothing about reachability within the safe set, that is whether all points in $\mathcal{S}$ can be reached from any point in $\mathcal{S}$ without departing $\mathcal{C}$. So the safe set might not always be 'safe' when one considers maneuverability within $\mathcal{S}$. We present examples of safe set protection utilizing a stabilizing, discontinuous switching control law for which sliding manifolds exist on portions of the trajectory, however chattering remains an impediment to safe set control as has been observed by previous research.[3,9]

This paper is organized as follows. Section II introduces some background material for this paper. Safe set mathematical formulation and examples are presented in section III. Section III also discusses the methodology used in this paper to to determine the proximity to $\partial\mathcal{S}$ and the admissible safe set control, $u_{safe}(x)$ when on $\partial\mathcal{S}$. Sections IV and V provide simulation results of safe set restoration and protection respectively. Section VI is the conclusion.

# II. Mathematical Preliminaries and Model

Consider a nonlinear system defined by

$$\dot{x} = f(x,u) \tag{1}$$
$$y = g(x) \tag{2}$$
$$z = h(x) \tag{3}$$

where $x \in R^n$ is the state, $u \in \mathcal{U} \subset R^m$ is the control, $y \in R^p$ is the vector of measured variables, and $z \in R^m$ is the vector of regulated variables. It is assumed that the number of controls equals the number of regulated variables. The control constraint set $\mathcal{U}$ is assumed to be bounded. The functions $f, g, h$ are assumed smooth in all variables. A steady motion or trim condition is generated by selecting $x^*(t), u^*(t)$ such that

$$\dot{x}^* = f(x^*, u^*) = 0 \tag{4}$$
$$z = h(x^*) \tag{5}$$

The trim condition is *admissible* if $u^*(t) \subset \mathcal{U}$ and $x^*(t) \subset \mathcal{C}$.

## II.A. Sliding Modes

Consider a square multi-input multi-output affine form of (1,3)

$$\begin{aligned} \dot{x} &= f(x) + G(x)\,u \\ z &= h(x) \end{aligned} \tag{6}$$

where $f, h$ and $G = [g_1, ..., g_m]$ are smooth functions of the state $x$. Define a smooth switching surface, $s_i(x) = 0$ for the $i^{th}$ control with the following discontinuous control strategy across $s_i(x)$

$$u_i(x) = \begin{cases} u_i^+(x), & \text{if } s_i(x) > 0 \\ u_i^-(x), & \text{if } s_i(x) < 0, \end{cases} \tag{7}$$

As stated in[10] if there exists an open manifold, $M$, of any intersection of the discontinuity surfaces, $s_i(x) = 0$ for $i = 1, ..., p \le m$ such that $\dot{s}_i s_i \le 0$ in the neighborhood of almost every point in $M$, then it must be true that once entering $M$, a trajectory remains in it until a boundary is reached. $M$ is called a sliding manifold and the motion in $M$ is called a sliding mode. If a trajectory lies in a sliding manifold, then its motion is characterized by the constraint $s(x) = 0$. Note the control in (7) is not defined when $s(x) = 0$. However, when in a sliding mode it is also true that $\dot{s}(x) = 0$. Using this fact one can show that the equivalent control is

$$u_{eq} = -\left[\frac{\partial s(x)}{\partial x} \cdot G(x)\right]^{-1} \frac{\partial s(x)}{\partial x} \cdot f(x) \tag{8}$$

and the motion in sliding is

$$\dot{x} = \left[I - G(x)\left[\frac{\partial s(x)}{\partial x} \cdot G(x)\right]^{-1} \frac{\partial s(x)}{\partial x}\right] f(x) \tag{9}$$

In sliding mode control, the equivalent control is not applied, but a switching control strategy is employed such that the trajectories are forced into a sliding manifold. This allows the a sliding mode controller to inherit certain robustness properties. The design of sliding control is a typically two step process which involves: (a) design of 'sliding mode' dynamics by the choice of switching surfaces, and (b) design of reaching dynamics the the specification of the control functions $u^+(x)$ and $u^-(x)$, typically accomplished by applying Lyapunov methods.

## II.B. GTM Longitudinal Dynamics

In this paper we use a model of longitudinal dynamics of a rigid body aircraft written in path coordinates:

$$\begin{aligned} \dot{V} &= \tfrac{1}{m}\left(T\cos\alpha - \tfrac{1}{2}\rho V^2 S C_D(\alpha, \delta_e, q) - mg\sin\gamma\right) \\ \dot{\gamma} &= \tfrac{1}{mV}\left(T\sin\alpha + \tfrac{1}{2}\rho V^2 S C_L(\alpha, \delta_e, q) - mg\cos\gamma\right) \\ \dot{q} &= \tfrac{M}{I_y}, \\ \dot{\alpha} &= q - \dot{\gamma} \end{aligned} \tag{10}$$

where

$$\begin{aligned} M = \tfrac{1}{2}\rho V^2 S\bar{c} C_M(\alpha, \delta_e, q) &+ \tfrac{1}{2}\rho V^2 S\bar{c} C_Z(\alpha, \delta_e, q) \\ &(x_{cgref} - x_{cg}) - mgx_{cg}\cos(\theta) + l_t T \end{aligned}$$

and $\theta = \alpha + \gamma$. To illustrate safe set computations in this paper we assume that we are given an operating envelope

$$\begin{aligned} \mathcal{C} = \{(V, \gamma, q, \alpha) | 90 \le V \le 120, -10 \le \gamma \le 10, \\ -20 \le q \le 20, -6 \le \alpha \le 22\} \end{aligned} \tag{11}$$

and a control restraint set specified by

$$\mathcal{U} = \{(T, \delta_e)\,| 0 \le T \le 30, -40 \le \delta_e \le 20\} \tag{12}$$

## III. Safe Set Formulation and Examples

The safe set is defined as the largest positively control-invariant set contained in $\mathcal{C}$. Several investigators have considered the computation of the safe set, the most compelling of which involve solving a time dependent Hamilton-Jacobi (HJ) partial differential equation (PDE). In[2] it is shown that the safe set

$$\mathcal{S}\left(t,\mathcal{C}\right) = \left\{x \in R^n \left|\phi\left(x,t\right) > 0\right.\right\} \tag{13}$$

can be obtained by the solution of the terminal value problem

$$\frac{\partial \phi}{\partial t} + \min\left\{0, H\left(x,p\right)\right\} = 0, \quad \phi\left(x,T\right) = l\left(x\right) \tag{14}$$

Define the Hamiltonian of (14) as

$$H\left(x,p\right) = \sup_{u\in\mathcal{U}} \mathcal{H}\left(x,p,u\right) \tag{15}$$

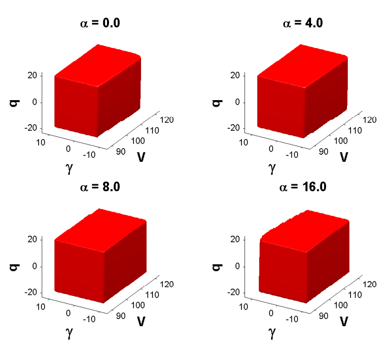
then

$$\mathcal{H}\left(x,p,u\right) = p^T \cdot f(x,u) = \left(p_1\dot{V} + p_2\dot{\gamma} + p_3\dot{q} + p_4\dot{\alpha}\right) \tag{16}$$

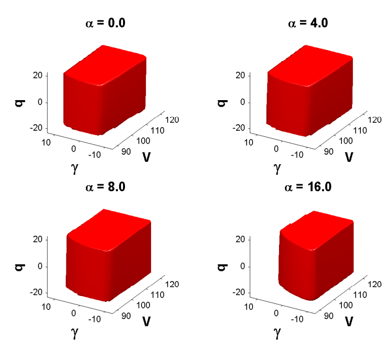
where

$$p = \nabla\phi(x) \tag{17}$$

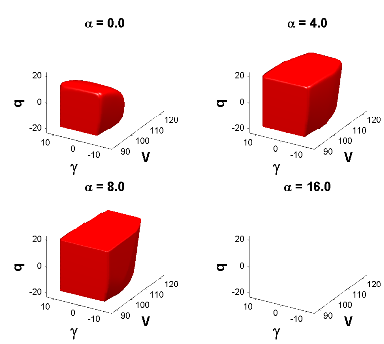
When the control of the Hamiltonian in (15) is applied to a state along any trajectory initially inside of $\mathcal{S}$ it is ensured that the resulting trajectory will remain in $\mathcal{S}$. It follows that this control should be applied for states on its boundary to ensure that the trajectory does not leave $\mathcal{S}$. Obtaining analytic solutions to (14) is difficult for realistic models of dimension higher than two. The four dimensional results obtained in this paper employ the numerical level set framework developed by[11] based on algorithms in[12] to approximate the safe set. Figure 1 illustrates a four dimensional safe set as a sequence of four three dimensional surfaces for constant angles of attack values, $S(V,\gamma,q)(\alpha_{const})$ for an unimpaired and impaired aircraft. These examples are generated over a 37x27x47x65 grid in $x$.




(a) Unimpaired




(b) Loss of Thrust




(c) Jammed Elevator

**Figure 1. The figure shows the four dimensional safe sets for slices of constant $\alpha$=(0,4,8,16) for three different aircraft configurations. The figure on the left shows the safe set for the unimpaired aircraft. In the center figure, the aircraft has no thrust, and in the rightmost figure the elevator is stuck at -2 deg.**

### III.A. Determining Distance to Safe Set Boundary and Admissible Control

A safe set protection or restoration strategy must be able to determine the aircraft's proximity to the safe set boundary, $\partial\mathcal{S}$ and characterize the admissible control to prevent envelope departure, $\mathcal{C}$. In higher dimensional state space, the meaning of Euclidean distance is not easily interpreted, so the approach taken here is to determine whether $x$ is in the interior of the safe set ($x \in \mathcal{S}^\circ$), or the exterior of the safe set ($x \in \mathcal{S}^-$), or on the safe set boundary ($x \in \partial\mathcal{S}$).

Solving the terminal value problem of (14) with numerical level set methods results in $\{x_i, \hat{\phi}_i(x_i)\}$ where $x_i$ represents a finite n-dimensional state space grid, and $\hat{\phi}_i(x_i)$ represents a numerical approximation to the exact solution $\phi(x)$. The boundary of $\partial\mathcal{S}$ is represented by an implicit function, $\hat{\phi}_i(x_i) = 0$ so it follows that $\hat{\phi}_i(x_i)$ provides a measure of distance from $\partial\mathcal{S}$. Since $\hat{\phi}_i(x_i)$ is a discrete set of points a simple way to compute the proximity to the safe set boundary is to linearly interpolate $\hat{\phi}_i(x_i)$ at the current state, $x$, resulting in $\hat{\phi}(x)$. Then using the sign conventions implied in (13), if $\hat{\phi}(x) > 0$ then $x \in \mathcal{S}^\circ$, if $\hat{\phi}(x) < 0$ then $x \in \mathcal{S}^-$, and when $\hat{\phi}(x) = 0$ then $x \in \partial\mathcal{S}$. The safe set boundary, $\partial\mathcal{S}$ is then given by the zero level isocontour of $\hat{\phi}(x)$, or when

$$\partial\mathcal{S} = \{x \in \mathcal{C} | \hat{\phi}(x) = 0\} \tag{18}$$

It is also necessary to know the gradient term $p(x) = \nabla\phi(x,t)$ in order to compute the safe set control when $x \in \partial\mathcal{S}$ from (15). To estimate this quantity, the numerical gradient was computed at each point over the state space grid yielding a table of the form $\{x_i, \hat{p}_i(x_i)\}$; $\hat{p}_i(x)$ was then estimated using a table lookup for each dimension.

Application of safe set control is necessary when $x \in \partial\mathcal{S} \setminus \partial\mathcal{C}$ to produce a trajectory tangent to $\partial\,S$ and prevent departure from $\mathcal{C}$. However when $x \in \partial\mathcal{S} \cap \partial\mathcal{C}$ the ensuing trajectory will not necessarily be tangent to $\partial\mathcal{S}$, since $H(x) > 0$, but towards the interior of $\mathcal{S}$. The admissible control to prevent safe set departure $u_{safe}$ can be computed from (16)

$$u_{safe}(x) = \{u \in \mathcal{U}, x \in \partial\mathcal{S} | \mathcal{H}(p(x), x, u) \geq 0\} \tag{19}$$

which collapses to a single value when $x \in \partial\mathcal{S} \setminus \partial\mathcal{C}$. Physically, (19) represents the ability of the control to keep the aircraft in $\mathcal{C}$. More than one solution can exist for the safe set control (19) when $x \in \partial\mathcal{S} \cap \partial\mathcal{C}$ and application of the control from (15) is not necessary to prevent envelope departure. Control constraints can then be estimated by the largest rectangle in (19) containing $u_{safe}$ if desired.

A simple choice for automated safe set protection is the following:

$$u(x) = \begin{cases} u_{stabilizing}(x), & \text{if } \hat{\phi}(x) > 0 & \text{(20a)} \\ u_{stabilizing}(x), & \text{if } \hat{\phi}(x) = 0 \text{ and } u_{stabilizing}(x) \in u_{safe}(x) & \text{(20b)} \\ u_{safe}(x), & \text{otherwise} & \text{(20c)} \end{cases}$$

where $u_{safe}(x)$ can be uniquely specified by (15) when more than one solution exists. In this strategy, $u_{stabilizing}(x)$ could be any linear or nonlinear control law designed to stabilize the system. Approaches similar to this have been referred to as multiobjective control[9] in the literature since the controller strategy is simultaneously trying to satisfy both performance and safety objectives. Section V will explore implications of this control strategy for safe set protection.

## IV. Safe Set Restoration

This goal of safe set restoration is to return the aircraft to a desired equilibrium condition $(x^*, u^*)$ when the aircraft finds itself outside of the safe set. This could occur when encountering a sudden disturbance such as a wind gust or when presented with a sudden failure, such as a jammed elevator or loss of engine thrust. It will be shown that with a stabilizing controller trajectories with initial conditions outside of $\mathcal{S}$ but inside $\mathcal{C}$ will temporarily depart the flight envelope $\mathcal{C}$ during restoration.

The approach we take here is to apply smooth state feedback stabilizing control of the form $u = K\delta x$ where $K$ is derived from a linear design technique, to the nonlinear system in (1). We derive $K$, using linear quadratic design techniques, where $K$, the Kalman Gain, is chosen to minimize a cost function,

$$J = \frac{1}{2}\int_0^\infty (\delta x^T Q \delta x + \rho \delta u^T R \delta u)\,\mathrm{d}t. \tag{21}$$

where $Q \in R^{nxn}$, and $R \in R^{mxm}$, are symmetric, positive definite matrices, which represent cost weights for perturbations of the state, $\delta x$, and control vectors, $\delta u$, respectively.

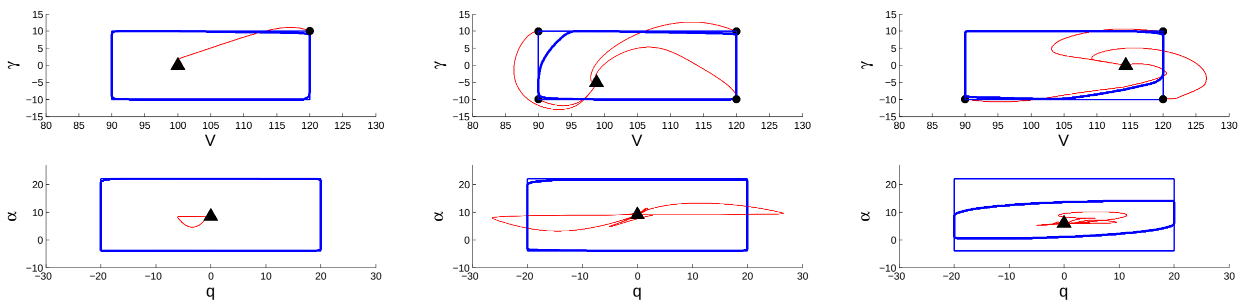
It is assumed that the desired trim state, $x^*$ is known and we that have full state feedback. The feedback term in (1) will then take the form,

$$u = u^* - K(\delta x) \quad (22)$$
$$\quad (23)$$

resulting in the following closed loop dynamics

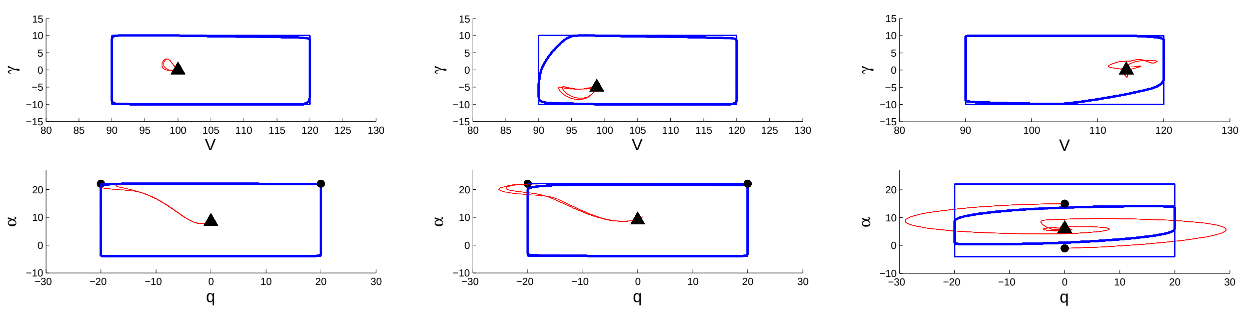
$$\dot{x} = f(x, u^* - K(\delta x)) \quad (24)$$
$$z = h(x) \quad (25)$$

Figures 2 and 3 represent parametric plots of trajectories that result from perturbations from $x^*$ in flight path variables $(V, \gamma)$ and $(\alpha, q)$ states respectively. Note in each case when the initial state is outside the safe set, the trajectory departs the flight envelope.




(a) Unimpaired (b) Loss of Thrust (c) Jammed Elevator

**Figure 2. These figures shows trajectories resulting from trim state (black triangles) perturbations in $V, \gamma$ (starting at circles) for an unimpaired aircraft and two different control impairments. The trajectory and safe set are shown in 2 2-dimensional parametric plots. The top shows a projection of the safe set onto the $V, \gamma$ plane at the point $\alpha^*, q^*$, while the bottom plot also shows a projection of the safe set onto the $\alpha, q$ plane at the point $V^*, \gamma^*$. When the the trajectory starts outside the safe set it departs the flight envelope before returning to the desired trim point.**




(a) Unimpaired (b) Loss of Thrust (c) Jammed Elevator

**Figure 3. These figures shows trajectories resulting from trim state (black triangles) perturbations in $\alpha, q$ (starting at circles) for an unimpaired aircraft and two different control impairments. The trajectory and safe set are shown in 2 2-dimensional parametric plots. The top shows a projection of the safe set onto the $V, \gamma$ plane at the point $\alpha^*, q^*$, while the bottom plot also shows a projection of the safe set onto the $\alpha, q$ plane at the point $V^*, \gamma^*$. When the the trajectory starts outside the safe set it departs the flight envelope before returning to the desired trim point.**

## V. Safe Set Protection

In this section we discuss and show examples of employing the control specified by (20) to prevent envelope departure. If $x \in \mathcal{S}^\circ$, then no safe set control is necessary. Safe set protection is only necessary when $x \in \partial\mathcal{S}$. Here there are two cases of interest, the first of which occurs when $x \in \partial\mathcal{S} \cap \partial\mathcal{C}$ , i.e. when the system is in the intersection of $\partial\mathcal{S}$ and $\partial\mathcal{C}$. This implies that the admissible safe set control, $u_{safe}$ is a set valued quantity. This can be seen by examining (14). In (14) $\phi(x,T)$ is initialized to $\partial\mathcal{C}$. If the boundary of the safe set does not shrink, that implies that $H(x) \geq 0$. If $H(x) = 0$, then $u_{safe}$ is a single valued control which if applied will produce a trajectory tangent to both $\partial\mathcal{C}$ and $\partial\mathcal{S}$ at $x$. This is more of a pathological case. More typically $H(x) > 0$ when $x \in \partial\mathcal{S} \cap \partial\mathcal{C}$ which implies that there exists a set of controls $u_{safe}$ which can force the system into $\mathcal{S}^{\circ}$ and $\mathcal{C}^{\circ}$ simultaneously. If $u_{stabilizing} \in u_{safe}$ then $u_{stabilizing}$ can be selected and the safe set control is not necessary.

The other case of interest is when $x \in \partial\mathcal{S} \setminus \partial\mathcal{C}$. When this occurs the admissible safe set control specified in (20) is unique and required to prevent envelope departure. Moreover since in this case the Hamiltonian of (15) $H(x,p)$ is zero the trajectory will be tangent to the safe set boundary at $x$.

Figure 4 shows simulation results for an aircraft with and without application of a safe set automated envelope protection control law as in (20). Figure 4 (a) shows a trajectory for which $\mathcal{C}$ is departed and re-entered as a stabilizing control law restores the aircraft to a desired trim point. With a control strategy as in (20) Figure 4 (b) suggests the existence of switching surfaces and that the system is in a sliding mode for a portion of the trajectory where $x \in \partial\mathcal{S} \cap \partial\mathcal{C}$. The chattering occurs because the safe set control is trying to force the system into $\mathcal{S}$ by setting the thrust to zero, which in this particular case is at odds with the stabilizing control law. Previous research with safe set control strategies[9] has also shown chattering. In Figure 4 (b) the sliding domain occurs along a portion of $\partial\mathcal{C}$ where $V = 120$. The constraint here is $s(x) = V - 120$ which implies that $\dot{V}(x) = 0$.

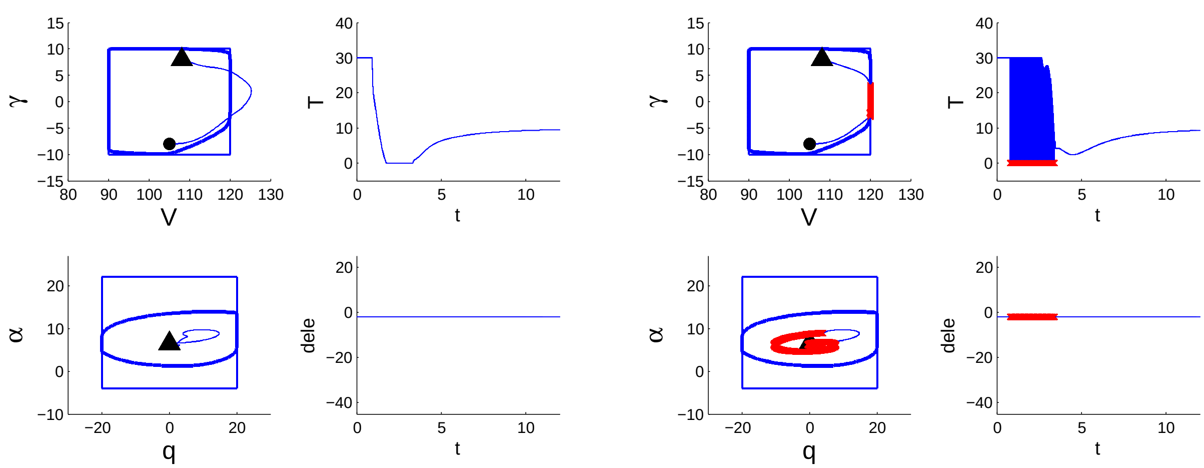
On this sliding manifold it can be shown that the switching control takes the form

$$u(x) = \begin{cases} Kx, & \text{if } \hat{\phi}(x) > 0 \\ \arg\max\limits_{u \in \mathcal{U}} \mathcal{H}\left(x, p, u\right) = 0, & \text{if } \hat{\phi}(x) \leq 0 \end{cases} \tag{26}$$

and that the equivalent control reduces to

$$T_{eq} = -\frac{1}{\cos\alpha}\left(-\tfrac{1}{2}\rho V^2 S C_D\left(\alpha, \delta_e, q\right) - mg\sin\gamma\right) \tag{27}$$

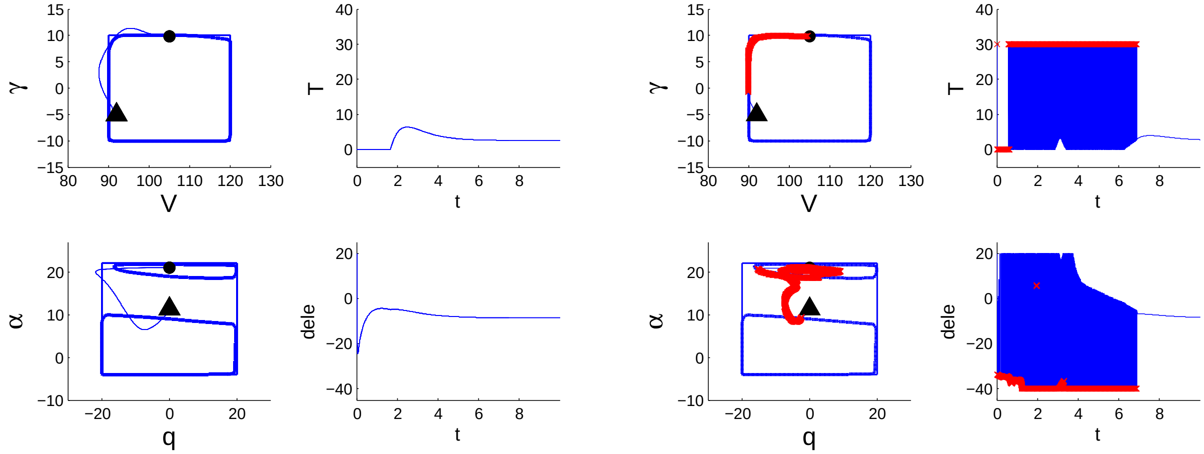
Figures 5 and 6 show similar results for an aircraft with no control impairments. It was also observed that chattering was sometimes observed when $x \in \partial\mathcal{S} \setminus \partial\mathcal{C}$. This suggests that discontinuities might exist along $\partial\mathcal{S}$.




(a) LQR Only

(b) LQR with safe set protection as in (20)

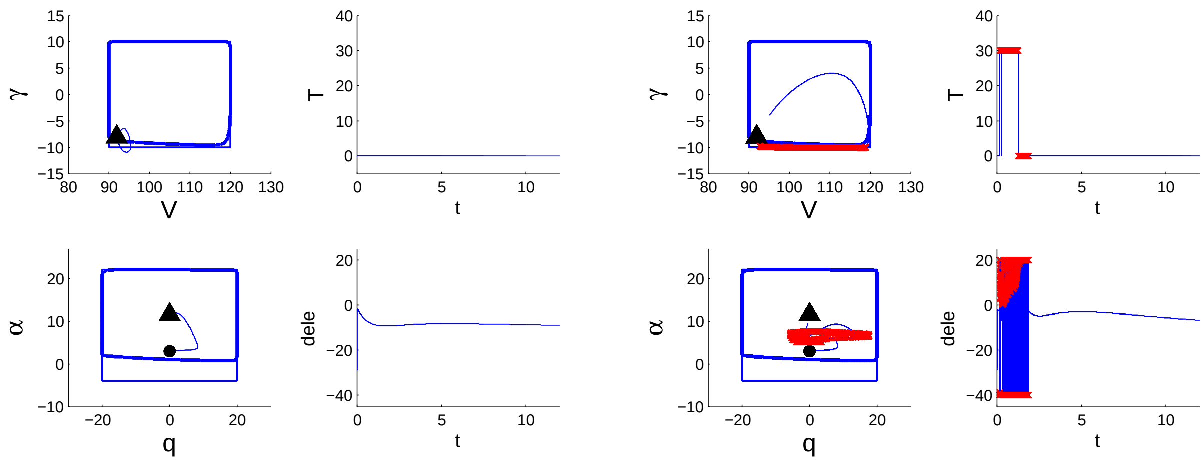
**Figure 4. This figure shows trajectories with and without safe set protection for a jammed elevator. The 4 dimensional safe set boundary is shown by 2 2-dimensional projections at the trajectory starting point. The trim state $x^*$ is denoted by black triangles. (a) shows a case where the trajectory starts in $\mathcal{S}$, but $\mathcal{C}$ is departed in order to attain, $x^*$. (b) has a switching control law to provide safe set protection. A red 'x' denotes application of safe set control.**




(a) LQR Only

(b) LQR with safe set protection as in (20)

**Figure 5. This figure shows trajectories with and without safe set protection for an unimpaired aircraft. The 4 dimensional safe set boundary is shown by 2 2-dimensional projections at the trajectory starting point. The trim state $x^*$ is denoted by black triangles. (a) shows a case where the trajectory starts in $\mathcal{S}$, but $\mathcal{C}$ is departed in order to attain, $x^*$. (b) has a switching control law to provide safe set protection. A red 'x' denotes application of safe set control.**




(a) LQR Only

(b) LQR with safe set protection as in (20)

**Figure 6. This figure shows trajectories with and without safe set protection for an unimpaired aircraft. The 4 dimensional safe set boundary is shown by 2 2-dimensional projections at the trajectory starting point. The trim state $x^*$ is denoted by black triangles. (a) shows a case where the trajectory starts in $\mathcal{S}$, but $\mathcal{C}$ is departed in order to attain, $x^*$. (b) has a switching control law to provide safe set protection. A red 'x' denotes application of safe set control.**

## VI. Conclusions

We have shown how aircraft impairments in the form of control constraints affect a four dimensional safe set boundary. For the envelope restoration problem we have verified by simulation that when the aircraft is outside of $\mathcal{S}$, $\mathcal{C}$ will be departed. However for small perturbations we show that $\mathcal{C}$ can be re-entered during stabilization. For envelope protection we present a mathematical formulation for the admissible safe set control, that is the control required to prevent envelope departure. To illustrate an automated envelope protection scheme, we show instances where a trajectory starts in $\mathcal{S}$, and subsequently departs $\mathcal{C}$ in order to reach an admissible trim state. We note that it might be possible that all points in $\mathcal{S}$ are not reachable from some points in $\mathcal{S}$ without departing $\mathcal{C}$ but this statement is not proven at this time and remains an area for further safe set research. For safe set protection problem we have shown the existence of sliding modes when switching between stabilizing and safe set based control strategies.

## References


[1] Tomlin, C., Lygeros, J., and Sastry, S., "Aerodynamic Envelope Protection using Hybrid Control," *American Control Conference*, Philadelphia, 1998, pp. 1793–1796.

[2] Lygeros, J., "On Reachability and Minimum Cost Optimal Control," *Automatica*, Vol. 40, 2004, pp. 917–927.

[3] Oishi, M., Mitchell, I. M., Tomlin, C., and Saint-Pierre, P., "Computing Viable Sets and Reachable Sets to Design Feedback Linearizing Control Laws Under Saturation," *45th IEEE Conference on Decision and Control*, IEEE, San Diego, 2006, pp. 3801–3807.

[4] Ding, J., Sprinkle, J., Sastry, S. S., and Tomlin, C. J., "Reachability calculations for automated aerial refueling," *Proc. 47th IEEE Conf. Decision and Control CDC 2008*, 2008, pp. 3706–3712.

[5] Kitsios, I. and Lygeros, J., "Final Glide-back Envelope Computation for Reusable Launch Vehicle Using Reachability," *Proc. and 2005 European Control Conf. Decision and Control CDC-ECC '05. 44th IEEE Conf*, 2005, pp. 4059–4064.

[6] Kitsios, I. and Lygeros, J., "Aerodynamic Envelope Computation for Safe Landing of the HL-20 Personnel Launch Vehicle Using Hybrid Control," *Proc. IEEE Int. Symp. Control and Automation Mediterrean Conf Intelligent Control*, 2005, pp. 231–236.

[7] Kwatny, H. G., Dongmo, J.-E. T., Chang, B. C., Bajpai, G., Yasar, M., and Belcastro, C., "Aircraft Accident Prevention: Loss-of-Control Analysis," *AIAA Guidance, Navigation and Control Conference*, Chicago, 10-13 August 2009.

[8] Feuer, A. and Heymann, M., "Ω-Invariance in Control Systems wiyh Bounded Controls," *Journal of mathematical Analysis and Applications*, Vol. 53, 1976, pp. 26–276.

[9] Oishi, M., Tomlin, C., Gopal, V., and Godbole, D. N., "Addressing Multiobjective Control: Safety and Performance through Constrained Optimization," *Proceedings of the 4th International Workshop on Hybrid Systems: Computation and Control*, HSCC '01, Springer-Verlag, London, UK, 2001, pp. 459–472.

[10] Kwatny, H. G. and Kim, H., "Variable Structure Regulation of Partially Linearizable Dynamics," *Systems & Control Letters*, Vol. 15, 1990, pp. 67–80.

[11] Mitchell, I. M., Bayen, R. M., and Tomlin, C. J., "A time-dependent Hamilton-Jacobi formulation of reachable sets for continuous dynamic games," *IEEE Transactions on Automatic Control*, Vol. 50, 2005, pp. 947–957.

[12] Osher, S. and Fedkiw, R., *Level Set Methods and Dynamic Implicit Surfaces*, Springer, 2003.