Online safe flight envelope prediction for damaged aircraft: A database-driven approach

Zhang, Y; de Visser, CC; Chu, QP

DOI
10.2514/6.2016-1189

Publication date
2016

Document Version
Accepted author manuscript

Published in
Proceedings of the AIAA modeling and simulation technologies conference

Online Safe Flight Envelope Prediction for Damaged Aircraft: A Database-driven Approach

Y. Zhang[*], C.C. de Visser[†], and Q.P. Chu[‡]

Delft University of Technology, Delft, Zuid-Holland, 2629HS, The Netherlands.

This paper proposed a framework of database-driven approach to solve the problem of online safe flight envelope prediction for aircraft safe recovery under abnormal conditions. On occurrence of sudden accidents like structural damages, conventional systems have neither enough measurements for the online reidentification of global damaged models, nor enough time for the onboard safe flight envelope computation. To circumvent these technical bottlenecks and make online applications more feasible in such emergency situations, some information, like global damaged models and the corresponding safe flight envelops, could be stored offline in a database for later online retrieval.

I. Introduction

Statistics of past aircraft accidents[1,2] have shown that many fatal aircraft accidents could be traced back to a similar reason: the aircraft loss-of-control (LOC). There are a wide spectrum of factors and series of events that could potentially give rise to LOC accidents, like vehicle impairments, damages, icing, inappropriate crew responses and vehicle upset,[3] which are deeply coupled and vary under different conditions. Therefore, the definitions of LOC accidents still remain vague and it is not yet possible to find out one single solution that prevents all accidents. However, efforts have been made to monitor and prevent some specific LOC accidents, especially for large fixed-wing transports and airliners, to which safety is of paramount importance. The National Aeronautics and Space Administration's (NASA) Aviation Safety Program is developing technologies that address aircraft LOC prevention and recovery under a wide range of hazards and uncertain conditions.[3–5] Furthermore, some researchers are trying to quantify LOC events from flight data by defining metrics consist of five envelopes that are related to airplane flight dynamics, aerodynamics, structural integrity and flight control use.[6,7] Their results can help investigators decide whether or not the accident should be classified as a LOC, and identify the axis in which each event started as well as the chain of events that led to the lost controls, which will suggest valuable clues on how best to prevent future LOC events. However, this quantitative approach still reveals some limitations, so we still need more insights on how damages and faults have impact on the performance of aircraft.[5]

Despite the unclear definitions in analytical terms, the LOC accidents are generally related to situations in which the aircraft flew out of the current flight envelopes with external hazards or pilots' unwise behaviours. The Commercial Aviation Safety Team (CAST) describes in-flight LOC as a ”significant deviation of the aircraft from the intended flight path or operational envelope”.[8] The conventional definition of the flight envelope is the area of altitude and airspeed where an airplane is constrained to operate,[9] which is usually presented by the famous doghouse-plot.[10] In many other literatures, the flight envelope is not restricted to specific states, but a subset of the state space where the aircraft can be safely controlled and LOC accidents can be avoided.[10] In nominal cases, the flight envelope is characterised by the aerodynamic and kinematics models of the aircraft as well as its control authorities. Currently, most aircraft is equipped with flight software under nominal conditions, which reveals the shortcomings under off-nominal and even near-LOC

[*] PhD Student, Control and Simulation Section, Faculty of Aerospace Engineering, Delft University of Technology; Kluyverweg 1, 2629HS, Delft, The Netherlands.

[†] Assistant Professor, Control and Simulation Section, Faculty of Aerospace Engineering, Delft University of Technology; Kluyverweg 1, 2629HS, Delft, The Netherlands, Member.

[‡] Associate Professor, Control and Simulation Section, Faculty of Aerospace Engineering, Delft University of Technology; Kluyverweg 1, 2629HS, Delft, The Netherlands.

cases. To compensate for this, a flight envelope prediction and protection system is needed to provide necessary information and support to the flight control system or pilots.

As an important branch and one of the most promising techniques of LOC prevention project, several safe flight envelope protection systems[6] have been designed and proposed. The task of envelope protection can be generally divided into two steps: one is the determination of safe flight envelopes; and the other is to guarantee that the aircraft states stay within the safe flight envelope.[10] As to the second step, there exist literatures[6,10,11] covering how to help keep aircraft flying within pre-defined state boundaries and detect potential hazards through constant health monitoring, during which warnings will be given if certain boundaries[7] are violated due to some aggressive manoeuvres like abrupt pitch down and up of high angles. The research of this paper, on the other hand, focuses on the first step, which is the prerequisite of flight envelope protection system.

In literatures, the estimation of flight envelopes were proposed in many ways. Initially, the computation and clearance results can be obtained by conducting flight tests, wind tunnel and CFD experiments. Alternatively, there are also various analytical methods to calculate the flight envelopes due to different definitions and numerical tools.[4,11,12] One important research in the area was the computation of attainable equilibrium/trim states and observing how control properties change with flight conditions and parameters via bifurcation analysis,[5,13,14] which has been developed to examine equilibrium structure of the aircraft at or near bifurcation points, indicating highly nonlinear upset conditions. Moreover, many nonlinear methods based on Lyapunov's stability theory have been proposed as a region of attraction (ROA) prediction tool. The ROA method is designed to predict a stable set in the vicinity of a given equilibrium point, which has been applied to the NASA GTM with linear parameter varying model investigating the boundaries of safe flight envelopes.[15,16]

Another class of approach is more directly related to safety, which defines the flight envelope as a set of states that will reach the aircraft's target set within a certain time horizon, based on reachability analysis. Some researchers[10,17] extends the definition as the intersection between the forward and backward reachable set of the aircraft trim set, which evaluates the possibility of manoeuvring and recovering in a potential unsafe region. Another group explicitly links safe set to the calculation of viability set, and name it as "maximum controlled invariant set". By this definition, the safe set is a collection of states from which the trajectories are guaranteed not to leave the accepted operation envelope, which, unlike the former one, forms a safety-preserving problem.[11,18] Both the reachability analysis and viability theory provided a solid framework for control synthesis and trajectory analysis of constrained dynamical systems in a set-value fashion.[19] The solutions to computing reachable set and viability set are basically classified into two categories: Lagrangian method and Euler method. The latter one, represented by level set method, has been developed and utilised by many researchers.[20,21] The level set method computes the reachable set as the zero level set of a viscosity solution of the Hamilton-Jacobi-Isaacs(HJI) partial differential equation, which is derived from the close connection between reachability analysis and optimal control theory.[22,23] This method is capable of handling complex nonlinear models and control strategies, yet it relies on grids of state space. Therefore, the computational load will increase exponentially with the dimension of states and is hardly feasible for systems with more than four states.[19] Despite efforts on both improvements on numerical methods and simplifications on system models like semi-Lagrangian particle level set method[10] and time scale separation,[17,24] the "curse of dimensionality" still hinders the implementation of online applications. Alternatively, Lagrangian methods (e.g. the ellipsoidal method) take advantage of compact set representations that follow the vector field's flow, thus its computation complexity is usually polynomial in time and space, allowing for calculation of reachable sets with high dimensions in a relatively efficient way.[19,25,26]

This paper is mostly concerned about the safety analysis after a sudden accident or an abrupt structural damage, with stability margins and control authorities degrading rapidly overtime. Under such off-nominal conditions, pilots and flight control systems need to stay aware of the aircraft performance characteristics, so updated reliable information is essential onboard for emergency flight planning and fault tolerant control fast enough to prevent LOC accidents. One important message is the safe flight envelope, i.e., a set of states from which the aircraft can safely fly to the target area with bounded control inputs. While determined beforehand, both the envelope and trim/target set could no longer remain constant due to the overall change of aerodynamic model and control authorities. Therefore, online obtaining the new safe flight envelope as well as the shrunken trim set as fast as possible is one of the key factors of saving the impaired aircraft from LOC accidents. Considering the low efficiency of reachable set computation methods reviewed above, it is hardly feasible for online calculation. Moreover, there's another significant technical challenge associated with this problem. Since the safe flight envelope is an entire set of safe aircraft states and control input combinations, it requires an accurate valid aerodynamic model based on measurement data covering all flight conditions of interest. However, in the presence of failures and damages, measurement data can only be attained in a limited region around the current flight condition given the fact that the impaired aircraft can no longer fly freely without losing control. Therefore, the onboard computer is only able to identify the local model at the current flight condition, which contradicts the fact that the estimated aerodynamic model has to be valid for the current aircraft configuration over the entire flight envelope to enable an evolution algorithm to estimate the boundary of safe flight envelope and changed trim sets.[27] Some researchers[12] have come up with a progressive updating method, in which they extrapolate the aerodynamic coefficients linearly. Nevertheless, this method doesn't take into considerations the highly nonlinear aircraft dynamics after damage. In this respect, even if the "curse of dimensionality" could be tackled by any chance, determining the new bounds of safe flight envelopes online under abnormal conditions would still remain as one of the main challenges of aircraft loss-of-control prevention and recovery.[3,4]

This paper presents an early stage in the development of the new Flight Envelope Anticipative Controller (FENCE) that is being developed at the Control & Simulation division of TU-Delft and provides an innovative process of predicting safe flight envelopes based on advanced database generation and retrieval techniques. Our approach is different from others in many respects. First, we circumvent the problem of solving complex HJI equations online. Instead, we transform part of online activities into offline calculations and store the results in the database, from which the information of safe flight envelopes could be retrieved online. Secondly, the database is designed to cover global models and trim sets of a wide range of faults and damages that may happen during flight.[4] In this paper we investigate airframe damage and its influence on aerodynamics in particular,[28,29] which is much more difficult to model and estimate compared with actuator faults. Thirdly, with our new database approach, we can use the local model of impaired aircraft to find out the corresponding global damaged model offline, rather than having to perform global model identification after an abnormal event. Besides, we present a possible way of identifying physical damage cases using only the locally updated aircraft model which is used as a retrieval key into the envelope database. In full generality, the novelty of this approach is highlighted in the integration of physical phenomenon of aircraft damages and the corresponding aerodynamic changes together with database techniques as a potential solution to the problem of online safe flight envelope prediction. Regarding the importance of aircraft safety, our approach could also be included as part of future design of primary flight displays(PFD).[30]

II. System Overview

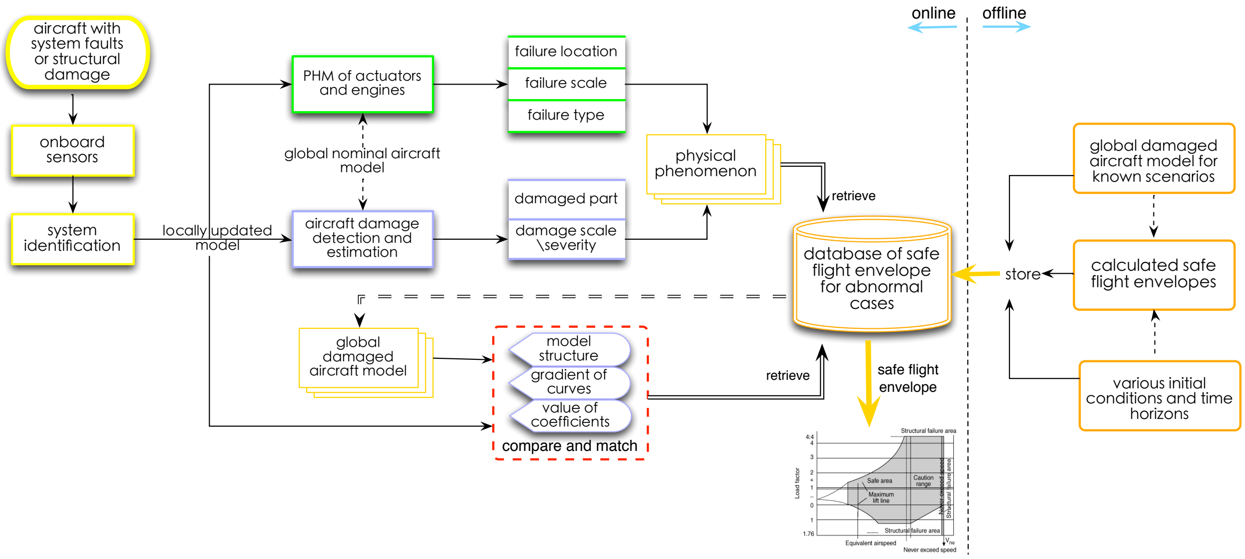


Figure 1. Architecture of the online database-driven safe flight envelope prediction system

The general process of online safe flight envelope prediction is illustrated in figure 1, where the onboard system is supported by an off-line database. When some off-norminal cases suddenly occur, it is highly desirable to first characterize the adverse conditions of the aircraft. Assuming that the sensors can function well due to the redundant networks onboard, new measurements are first sent to the system identification module to locally update the aircraft model. The identification method used in our study is called two-step method, which has been continuously developed at Delft University of Technology over the last 20 years. What makes this method successful and eligible for online applications is that it decouples the joint of nonlinar state estimation and model parameter estimation into two separate optimization problems. At the first step, aircraft states and sensor bias are estimated by Kalman filter and kinematic models. After this, the estimated states are used to calculated the total moments and forces along each axis, allowing the identification of aerodynamic model in the second step to be simplified as an equation error problem. According to a series of experiments and reports, the aerodynamic model can be regarded as a direct indication of the the completeness of an airplane's components and structure. Hence in our research, the second step, i.e., the estimation of aerodynamic model structures and coefficients, is thoroughly investigated. Identifying the aerodynamic model consists of two parts: the description of model structure and the estimation of parameters defined in the model structure. For the first part, polynomial model is commonly used in many literatures, which can be easily implemented and interpreted using physical knowledge, yet still suffers from locally updating problems. Other algorithms like neural networks and kernel methods have variant shortcomings and limitations. Multivariate simplex splines[31–33] have recently been used to defined and approximate the aerodynamic model with higher accuracy than ordinary polynomials in both local and global scale and avoid the over-fitting problem at the same time. A simplex spline is an analytical function that is the weighted sum of polynomial basis functions. Based on the data, any number of single simplex can form a geometric net with predefined continuity, which is called triangulation. The approximation power is not only proportional to the polynomial degree, but also to the size and density of the triangulation. Another great advantage of this method is that once the structure is set, it can be easily integrated into standard parameter estimation routines using advanced least square algorithms.

After the local model is updated, it will be sent to a prognostic and health monitoring (PHM) system to detect and evaluate the faults and failure of actuators and engines. With faults diagnosis method, the system can locate the failure position, identify the failure type (control effectiveness loss, actuator runaway, actuator jam or stuck, etc.) and asses the current level of damage severity associated with each failure type, as is demonstrated in the green part of the figure. A variety of techniques have been developed for aircraft fault detection and failure evaluations.[34–38] In the presence of more severe situations like airframe damages resulting form fatigue cracks, foreign objects and overstress during upsets, which normal PHM cannot diagnose, we need a process to implement the detection, isolation and estimation of those damages. Few researchers focus on this problem, part of the reason is that the structural damage causes the change of not only aerodynamic coefficients but also the overall structure, and it always couples with the paralysis of actuators. For instance, if one part of the wing is damaged by external attacks, the whole aircraft will become asymmetric and an incremental rolling moment will be generated, thus an additional component should be considered in the model of aircraft. Furthermore, with actuators being used to compensate for the asymmetrical moment, the remaining control authorities will become quite limited. In our approach, we designed a process to roughly identify a few typical scenarios of structural damages with the results of system identification and fault detection. As shown in figure 1, the updated local model in the vicinity of current flight conditions will be compared with the onboard global nominal model to measure the change in the model. The key step that follows is to identify the physical phenomenon of the damage including the damaged position and severity, i.e., the representative physical phenomenon of impaired aircraft, which will be used as the retrieval index to the database and for further interpolations.

However, the above routine, which we may refer to as event-based approach, is based on the assumption that only one damage/failure case happens at a time and each case has distinguished features from one another that could avoid potential ambiguity. Yet, this is not always the case. If damages and failures occur at multiple locations simultaneously,[3,4] it is hardly possible to correctly isolate them from each other by simply using nominal model as the reference. Instead we could use an offline database to store a wide range of global damaged models covering complex situations. In NASA's design of safety-critical systems for aircraft LOC prevention and recovery,[3,4] a preliminary set of 60 LOC test scenarios were developed based on the past accidents analysis[39] and the initial sets of potential future LOC risks. The preliminary set contains scenarios involving from one to four LOC precursors from various hazards categories, which can be considered as the baseline of our database. The data of global damaged models could be generated by CFD/wind tunnel experiments and will be used by advanced system identification methods to determine their mathematical approximations. It is noticed that these models are generated out of single or compound abnormal cases of the aircraft, yet it's not necessary for them to have exact physical interpretations when being connected to safe flight envelopes in the database. Instead of finding out the physical conditions of the aircraft as the index to the database, the alternative model-based approach is more like a black-box problem, where we only need to look for the very safe flight envelope calculated from the global model that mostly matches the locally identified model in terms of model structure, gradient of curve (in case different global models have the same local model) and value of coefficients. The model-based approach can be used when the aircraft encountered multiple damages and simple event-based approach is unable to detect or determine the current situation. However, searching throughout the whole database for the right model can be time-assuming, so the event-based approach can be used as a rough selection to scale down the searching area, and the model-based approach can in turn help to validate the identification result of event-based approach. In general, both processes could be integrated to find out the most suitable safe flight envelope in the database.

III. Database Design

A. Overview of the Design Process

The design of database is one of the most crucial and complex parts of the system, involving a whole process of transforming high-level application requirements into lower-level application programs of database. Figure 2 displays the general process of database design.[40]

- The initial phase of database design is to investigate user requirements, in this context would be to retrieve safe flight envelope based on identified adverse conditions, as is illustrated previously.
- Next, we need to translate the requirements into a conceptual schema of the database, which is graphically represented by entity-relationship (E-R) model. This stage is reviewed to ensure that all data requirements are indeed satisfied and are not in conflict with one another.
- The conceptual design is followed by specification of functional requirements, which describes the operations, or transactions that will be performed on the data.
- In the logical-design phase, the high-level conceptual schema is linked to the implementation of the database through relational data model.
- Finally comes the physical-design phase, including the form of file organization and choice of index structures, which leads to the application program of database that is ready for practical use.

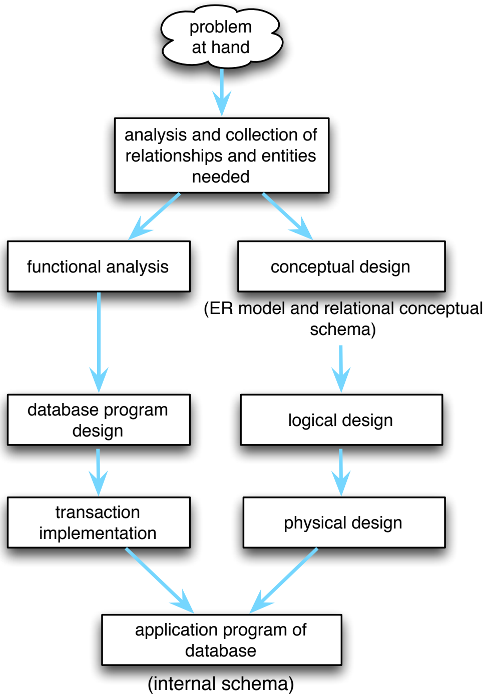
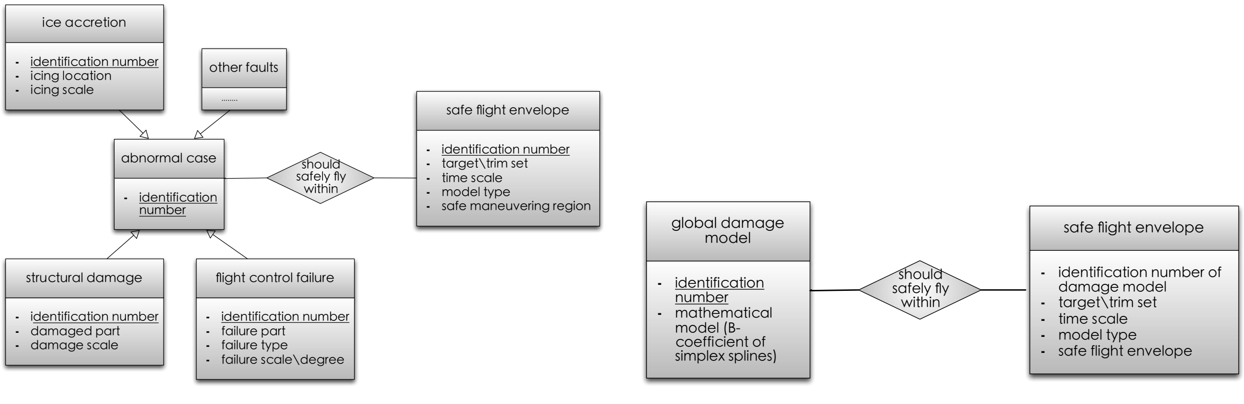

problem at hand
analysis and collection of relationships and entities needed
functional analysis
conceptual design
(ER model and relational conceptual schema)
database program design
logical design
transaction implementation
physical design
application program of database
(internal schema)

Figure 2. General process of database design

B. Entity-Relationship Model Design

A major part of the database design is to represent various things and relationships in between with entity-relationship (E-R) model.[40] In ER model, an entity is a distinguishable object having unique identifiers, and a set of entities of the same type form a entity set. An entity is described by a set of attributes with values, one of which will be used as the key to uniquely identify each entity from one another. In some occasions, subclasses of entities may exist in an entity set if they have



(a) (b)

Figure 3. Entity-relationship diagram of the database

attributes that are not shared by all. A relationship is an association among several entities (sets). One important property of relationship is the mapping cardinality, expressing the number of entities to which another entity can be associated via a relationship.

The overall logical structure can be illustrated graphically by an E-R diagram. One of the most popular ways of drawing the diagram is Unified Modeling Language (UML), which our notation is based on. The entity sets are represented by a rectangular box with the name in the headline and the attributes listed below it, and the key attributes are underlined. The relationship is represented by a diamond connecting a pair of related entity sets. Based on the definitions above, we can map the requirements of the safe flight envelope prediction system to the corresponding elements of E-R diagram, which is depicted in figure 3. The relationship that links a specific abnormal condition to its corresponding safe flight envelope is defined as ”can safely flight within”. To make it more straightforward, the design of each entity is interpreted below:

- In the database of event-based approach (figure 3(a)), two entity sets are linked by one relationship. The one on the left denotes the abnormal cases of the aircraft, each of which has a unique identification number as the key attribute for retrieval. In real world, diverse contributing factors can lead to abnormal cases of the aircraft, which is why we need to specialize the entity into several subclasses, each possessing different attributes, which are listed below:

  1. The subclass named ”flight control failure” includes four attributes, which form the characteristics of a system failure accident. The attribute ”failure part” refers to the specific part of the aircraft that may have faults and failures ; the second attribute describes the current condition of faults and failures identified, like jammed or stuck actuators at various positions; the last attributes stores the scale of faults and failures. Examples of possible failure cases in form of domains and values of each attribute are displayed in table 1

     Table 1. Examples of possible failure cases

ID number	failure part	failure type	failure scale
1-1	right elevator	stuck	5 deg
1-2	left elevator	stuck	10 deg
1-3	left aileron	run away	25 deg
1-4	rudder	loss of control effectiveness	30%
1-5	right engine	thrust reduction	50%
1-6	double engine	thrust reduction	25%

  2. The second subclass entity describes the case of structural damage, which is characterized by two attributes: damaged part and its scale. Examples of possible damage scenarios that should be included in the database are listed in table 2 on the following page.

Table 2. Examples of potential structural damage cases

ID number	damaged part	damage scale
2-1	left horizontal tail	100% (full loss)
2-2	right horizontal tail	30% (tip loss)
2-3	left elevator	80%
2-4	vertical tail	50%
2-5	rudder	100% (off)
2-6	left wing tip	25%
2-7	left engine	total separation
2-8	wing leading-edge slat	100% (total loss)

3. Similar to the subclasses described above, the abnormal conditions caused by external hazard environment, such as ice accretion in this context, forms another entity bearing two attributes, which represent icing type and icing scale in the database. The constraint on the specialization of entity "abnormal case" is partial, which allows the entity not to belong to any of the three subclasses, because there are a lot more factors that could lead to off-normal conditions of the aircraft. That's why we leave some space for further study on other faults and future refinements.

- In the database of model-based approach (figure 3(b)), only one entity set should be considered, which contains two attributes. One is the damaged global model of different single or combined scenarios, and the other is the identification number of each model. The model structure in the database should be the same as the one used in online system identification. For instance, if we use spline model, then the B-coefficients for each component of the model will be stored.

- Another entity represents the safe flight envelopes computed offline. If we use event-based database, four attributes are used to determine the envelope of a specific aircraft model under certain failure or damage for a given time horizon. Examples of the attributes and their values can be seen in table 3. On the other hand, in the design of model-based one, there are still four attributes needed for retrieving the envelope, except that the identification number of abnormal case is replaces by the one of global damaged model matched before. Since the target set and safe flight region are both sets in form of figures, they are not explicitly shown in the table, but will be discussed in the next part of the paper.

Table 3. Examples of safe flight envelopes stored in the database

abnormal case number	target(trim) set	time horizon	model type (global)	safe flight region
1-3	(figures)	$1s$	full longitudinal failure model	(figures)
2-1	(figures)	$2s$	lateral damaged model	(figures)
2-4	(figures)	$2s$	short-period damaged model	(figures)
2-4	(figures)	$2s$	full longitudinal damaged model	(figures)
2-6	(figures)	$3s$	full damaged model	(figures)

IV. Computation of Safe Flight Envelopes

A. Notion of safety-related sets

The guarantee of safety has always been an important consideration when synthesizing controllers of complex safety-critical systems such as civil aircraft. Despite the existence of flight envelope protection systems, there are still problems when we try to achieve multiple control goals (e.g. envelope protection and stabilization) simultaneously.[41] In such case, physical constraints in conventional flight envelopes may not be enough for the control design, and simulations may also be inadequate to help predict the unanticipated problems with all possible initial conditions. Alternatively, reachability analysis can provide a new set-valued insight into the safety and control design of dynamic systems. On one hand, the theory can mathematically observe the system's behaviour by synthesizing states and input constraints. In other words, constraints, like stall speed, which come from aerodynamic envelope protection system, can be incorporated as the initial boundary on the continuous state space. On the other hand, with reachability analysis, all points belonging to all possible trajectories can be computed at once from all possible initial states, which differs itself from what simulation can achieve at one time and perfectly conform with the meaning of safety guarantee.[19]

Basically, the reachability analysis seeks to decide whether the trajectories of a system model can reach a certain target set from an initial set within given time horizons and input constraints.[18] To put it in a mathematical and more strict way, we first consider a continuous dynamic system,[22]

$$\dot{x} = f\left(x, u\right) \tag{1}$$

with $x \in \mathbb{R}^n$, $u \in U \subseteq \mathbb{R}^m$, $f\left(\cdot,\cdot\right) : \mathbb{R}^n \times U \rightarrow \mathbb{R}^n$, a bounded and Lipschitz continuous function, $l\left(\cdot\right) : \mathbb{R}^n \rightarrow \mathbb{R}$ and an arbitrary time horizon T. Let $\mathcal{U}_{[t,t']}$ denote the set of Lebesgue measurable functions from the interval $[t, t']$ to U, then for every $x \in \mathbb{R}^n$, $\tau \in [t, T]$ and $u \in \mathcal{U}_{[t,T]}$, the system admits a unique solution or trajectory ϕ, with $\phi\left(\tau, t, x, u\left(\cdot\right)\right) = x$.

Now we define a target set for our problem and it can be represented by the zero level set of the function as:

$$\mathcal{K} = \left\{x \in \mathbb{R}^n | l\left(x\right) > 0\right\} \tag{2}$$

In some literatures on differential game theory,[21, 42, 43] two counter inputs with opposing influences are considered, which usually come from controllers and disturbances respectively. To simplify the situation, we only focus on one positive input, and assumes that it will always endeavour to steer the system into the safe area. Based on those statements and settings, we can formulate four reachability sets by exchanging the type and order of quantifiers that operate on the time and input variables:[25, 26]

- The maximal reachable set is the set of initial states for which there exists at least *one* input such that the trajectories emanating from those states reach $\mathcal{K}$ at some time $\tau \in [t, T]$:

$$Reach_{max}\left(t, \mathcal{K}\right) := \left\{x \in \mathbb{R}^n | \exists u \in \mathcal{U}_{[t,T]}, \exists \tau \in \left[t, T\right], \phi\left(\tau, t, x, u\left(\cdot\right)\right) \in \mathcal{K}\right\} \tag{3}$$

- The minimal reachable set is the set of initial states such that for *every* input the trajectories emanating from those states reach $\mathcal{K}$ at some time $\tau \in [t, T]$:

$$Reach_{min}\left(t, \mathcal{K}\right) := \left\{x \in \mathbb{R}^n | \forall u \in \mathcal{U}_{[t,T]}, \exists \tau \in \left[t, T\right], \phi\left(\tau, t, x, u\left(\cdot\right)\right) \in \mathcal{K}\right\} \tag{4}$$

- The viability set is the set of all initial states *in* $\mathcal{K}$ for which there exists at least *one* input such that the trajectories emanating from those states remain within $\mathcal{K}$ for all time $\tau \in [t, T]$:

$$Via\left(t, \mathcal{K}\right) := \left\{x \in \mathbb{R}^n | \exists u \in \mathcal{U}_{[t,T]}, \forall \tau \in \left[t, T\right], \phi\left(\tau, t, x, u\left(\cdot\right)\right) \in \mathcal{K}\right\} \tag{5}$$

- The invariance set is the set of all initial states *in* $\mathcal{K}$ such that for *all* input the trajectories emanating from those states remain within $\mathcal{K}$ for all time $\tau \in [t, T]$:

$$Inv\left(t, \mathcal{K}\right) := \left\{x \in \mathbb{R}^n | \forall u \in \mathcal{U}_{[t,T]}, \forall \tau \in \left[t, T\right], \phi\left(\tau, t, x, u\left(\cdot\right)\right) \in \mathcal{K}\right\} \tag{6}$$

With $\mathcal{K}^c$ representing the complement of $\mathcal{K}$, we can clearly show that:

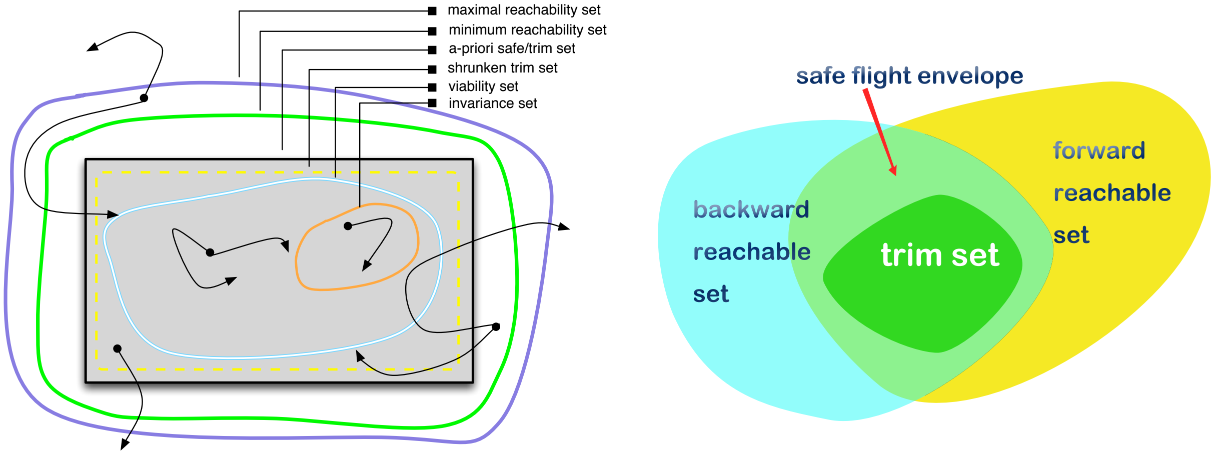
$$Reach_{max}\left(t, \mathcal{K}\right) \supseteq Reach_{min}\left(t, \mathcal{K}\right) \supseteq \mathcal{K} \supseteq Via\left(t, \mathcal{K}\right) \supseteq Inv\left(t, \mathcal{K}\right) \tag{7}$$

and more importantly,

$$Reach_{max}\left(t, \mathcal{K}\right) = \left(Inv\left(t, \mathcal{K}^c\right)\right)^c \tag{8}$$

$$Reach_{min}\left(t, \mathcal{K}\right) = \left(Via\left(t, \mathcal{K}^c\right)\right)^c \tag{9}$$

As a further step, we can establish a connection between these sets with practical safety problems, which is illustrated in figure 4(a). If the target set $\mathcal{K}$ is defined as the safe set where the system is aimed to reach, the viability set is often computed for 'safety-preserving' controllers that keep the trajectories of system within the safe region, so it is also called "the largest controlled invariant set".[41] However, the viability set is hardly useful when the aircraft has flown out of the pre-defined safe region or trim set. Alternatively we should calculate the boundary of maximum reachable set, which includes the states that have the potential of returning to the safe region. This set is more useful for the design of "safe-recovery" controllers that may steer the system from upset conditions. In some cases, the target set $\mathcal{K}$ is specified as "unsafe", and we want to find out the states that may give rise to dangerous situations and we should avoid when designing control strategies.[18] Thus the minimal reachable set should be computed that includes all the states that may reach the unsafe set no matter what the controller does within a certain time interval.[44] More importantly, the invariance set of the complement of a safe set is always used to find out the maximum reachable set of the safe set based on the duality relationship described in equation 8. Notice that all the above sets are in a *backward* sense, for they are all initial states with given terminal states, which means that the computation is in some way going backward in time.



(a)

(b)

Figure 4. Different types of safety-related sets based on reachability analysis

In this paper we pay the most attention to safety-recovery after the occurrence of abnormal conditions when the aircraft has left the previous safe region. So we need maximum reachable set, which is also referred to as backward reachable set in some papers,[10,45] to obtain all the possibilities that may guide the aircraft back to new trim sets under appropriate control allocations. On the other hand, the aircraft cannot stay in the trim set forever, it still needs to manoeuvre to other flight conditions like landing. So another set should be computed representing a set that all the states emanating from trim/target set may reach given a time horizon and control inputs. Since the evolution of system states is forward in time, this set is often called a forward reachable set.[46] In general, as is illustrated in figure 4(b), the intersection of forward and backward reachable set of a given trim set is the safe flight envelope we are looking for.[10,45]

B. Connection to optimal control

Based on the definitions in the previous section, let $l\left(\phi\left(\tau,t,x,u\left(\cdot\right)\right)\right)$ be the cost function of the state trajectory over time horizon $[t,T]$. Then two control problems can be formulated with value functions $V:\mathbb{R}^n\times[0,T]\to\mathbb{R}$,

$$V_1\left(x,t\right)=\sup_{u\in\mathcal{U}_{[t,T]}}\min_{\tau\in[t,T]} l\left(\phi\left(\tau,t,x,u\left(\cdot\right)\right)\right) \tag{10}$$

$$V_2\left(x,t\right)=\inf_{u\in\mathcal{U}_{[t,T]}}\min_{\tau\in[t,T]} l\left(\phi\left(\tau,t,x,u\left(\cdot\right)\right)\right) \tag{11}$$

where the minimum with respect to time is well defined by continuity. The connection between optimal control problems and reachable sets has been stated and proved clearly in:[22]

$$Via\left(t,\mathcal{K}\right)=\left\{x\in\mathbb{R}^{n}|V_{1}\left(x,t\right)>0\right\} \tag{12}$$

$$Inv\left(t,\mathcal{K}\right)=\left\{x\in\mathbb{R}^{n}|V_{2}\left(x,t\right)\geqslant 0\right\} \tag{13}$$

It is apparently shown that the boundary of reachable sets can be determined by solving for the value function V and obtaining its zero level set. A characterization of the value function as the viscosity solution to a time-dependent Hamilton-Jacobi-Isaacs (HJI) partial differential equation has been proposed and well developed, which is the key theory to solving reachability problems:

$$\frac{\partial V_{1}}{\partial t}+\min\left\{0,\sup_{u\in\mathcal{U}}\frac{\partial V_{1}}{\partial x}\left(x,t\right)f\left(x,u\right)\right\}=0 \tag{14}$$

with $V_1\left(x,T\right)=l\left(x\right)$ over $\left(x,t\right)\in\mathbb{R}^n\times\left[0,T\right]$. Similarly, for V_2:

$$\frac{\partial V_{2}}{\partial t}+\min\left\{0,\inf_{u\in\mathcal{U}}\frac{\partial V_{2}}{\partial x}\left(x,t\right)f\left(x,u\right)\right\}=0 \tag{15}$$

with $V_2\left(x,T\right)=l\left(x\right)$ over $\left(x,t\right)\in\mathbb{R}^n\times\left[0,T\right]$.

The minimization term with zero in the equation is to guarantee that the subset enclosed by the zero level set of the value function cannot decrease as time marches backward. This is to prevent some states that have already entered the target from leaving it before time horizon by "freezing" the evolution of the trajectory.[18, 47] More specifically, if the target set is defined as the undesired region, then the restriction is to make sure that some unsafe states will be tagged as "unwanted" once it enters the unsafe area and tries to leave. Similarly, if the target set is defined as a safe set, the restriction will include all the potential safe sets correctly.

As is mentioned before, under nominal conditions, the reachable set rather than the viability set should be considered as the indication of survivability. Clearly, the invariance and reachability problem are duals of one another and is unnecessary to be dealt with separately.[22] Therefore, we should firstly calculate the invariance set of $\mathcal{K}^c$ and take the complement of it to obtain the reachable set.

C. Level set methods

Due to the discontinuity of the right-hand side of HJI PDE as well as the switching of the optimal control, the value function may not remain continuous even if the boundary condition is differentiable. In order to obtain discontinuous solutions, a "weak" solution to the HJI PDE was developed and is named "viscosity" solution. By adding an additional term to the right-hand side of the HJI equation, a solution will be derived even when classical smooth solutions do not exist.[42]

Several numerical techniques have been proposed to compute the viscosity solution to the HJI equation. In this paper we discuss and use the one developed by Osher and Sethian[20] and is called level set methods, which has been successfully applied to the reachability analysis of many systems including aircraft. The level set method is one of the subclasses of Euler method, which discretizes the state space into grids and calculates in a dimension-by-dimension manner. One of the key process of the numerical scheme is the approximation of the spatial gradient $\partial V\left(x,t\right)/\partial x$ defined on grids, especially for discontinuity points. Upwinding differencing is usually used to choose the approximation of spacial derivatives from forward and backward differencing by looking at the flow direction of $V\left(x,u\right)$ indicated by the sign of dx/dt. By each grid, the minimum or maximum value of $\frac{\partial V_2}{\partial x}\left(x,t\right)\cdot f\left(x,u\right)$ is calculated by choosing optimal control inputs. After evaluating the analytical optimal value of the Hamiltonian function, a Lax-Friedrichs approximation of the Hamiltonian is often used to ensure stability of the numerical scheme by adding an artificial viscosity term to the Hamiltonian. In the end, based on the equation:

$$\frac{\partial V}{\partial t}=-\min\left\{0,\sup_{u\in\mathcal{U}}\frac{\partial V}{\partial x}\left(x,t\right)f\left(x,u\right)\right\} \tag{16}$$

the value of V for each grid node can be evaluated via time integration performed by second or higher order total variation diminishing (TVD) explicit Runge-Kutta schemes.

D. Generation of safe flight envelope database

To illustrate how the level set method works on reachable sets computation for the generation of safe flight envelope database, we present a example based on a nonlinear RCAM (Research Civil Aircraft Model).[30,48] The longitudinal dynamic model of the simulated aircraft is presented below:

$$\frac{d}{dt}\begin{bmatrix} V \\ \gamma \\ \alpha \\ q \\ z \end{bmatrix} = \begin{bmatrix} \frac{1}{m}\left[T\cos\alpha - D\left(\alpha, V\right) - mg\sin\gamma\right] \\ \frac{1}{mV}\left[T\sin\alpha + L\left(\alpha, V\right) - mg\cos\gamma\right] \\ -\frac{1}{mV}\left[T\sin\alpha + L\left(\alpha, V\right) - mg\cos\gamma\right] + q \\ \frac{M}{I_{yy}} \\ V\sin\gamma \end{bmatrix} \tag{17}$$

where the detailed polynomial model parameters of lift force, drag force and pitching moment can be found in papers[22,23,30,48] and they will be substituted in the above equation to solve for the optimal value of Hamiltonian function. Since the level set method is hardly feasible for system with more than four states and the computation load could become tremendously heavy, as a proof of concept, we can apply structure decomposition, or time scale separation skills to the problem. Thus, only three states are used for safe flight envelope computation, which the velocity, the flight path angle and the altitude, denoted by $x^T = [V, \gamma, z]$. Also, the virtual control inputs have been simplified as T and α. To compute reachable sets, the first thing is to decide on the target/initial sets, or safe trim sets K, which are usually described by an signed distance function, in our simulation it is taken as the area between the boundaries of states :

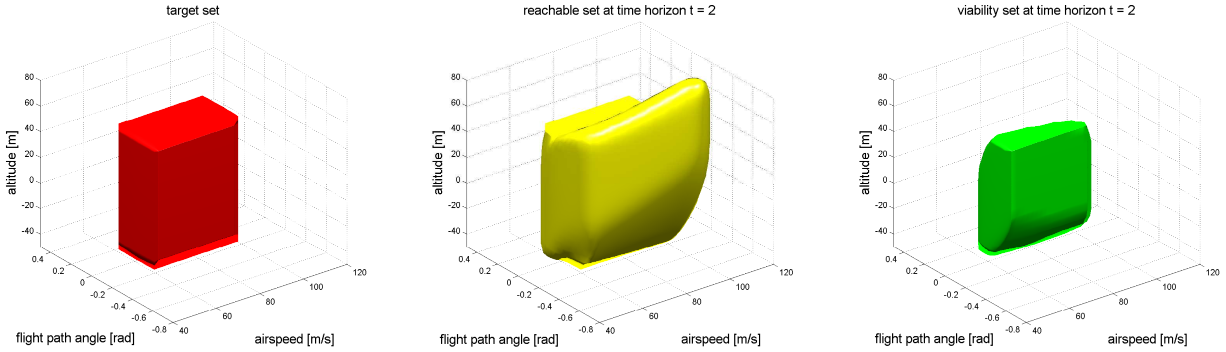
$$l\left(x\right) = \min\left\{x_1 - x_{1min}, x_{1max} - x_1, x_2 - x_{2min}, x_{2max} - x_2, x_3 - x_{3min}, x_{3max} - x_3,\right\} \tag{18}$$

Thanks to a well-developed toolbox by Mitchell et al.,[44] we can handle level set methods in a very convenient way. Figure 5 shows the computed reachability set and viability set with three-dimensional aircraft model introduced above. To make it more clearly, we can simply use the first two states to compute safe flight envelopes in slow dynamics. Figure 6 illustrates the two-dimensional invariance set, viability set and reachable set in a backward sense, and it clearly presents the relationships indicated in equation 7. All three sets are computed based on the model and trim set in nominal cases, which can only be used as a reference. To build up a database of safe flight envelops for various abnormal conditions, we must first establish a collection of global model for different cases. For primary phase of the research, we first compute safe flight envelopes based on two simple modifications of the original model or look up table, one is magnitude scaling, and the other is variable scaling:[49]

$$C_{act}\left(x\right) = \left(1 + \lambda_{mag}\right) C_{nom}\left(x\right) \tag{19}$$

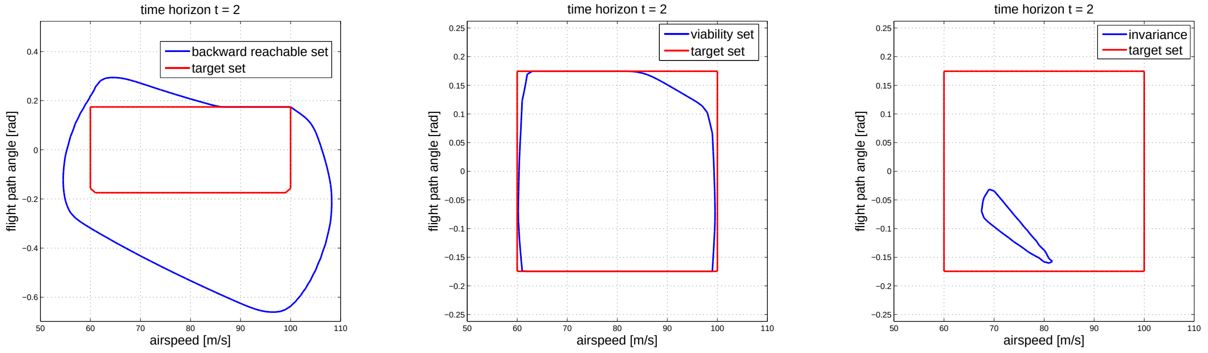
$$C_{act}\left(x\right) = C_{nom}\left(\left(1 + \lambda_{var}\right) x\right) \tag{20}$$

For some typical failure or damage cases, it is possible to related them with certain models with changed parameters or additional terms. Nevertheless, when the accident is too complicated to find its physical explanation, we may need a black-box model stored in the database to match with the online identified model. Therefore, even though the models used for computing safe flight envelopes are modified according to equation 19 and may not have solid physical meanings, they still could provide valid information in complex situations. In our simulation example, we assume that the aerodynamic coefficients as well as input bounds have changed due to certain accidents like wing damage or icing, and the resulting safe flight envelopes are displayed in figure 7. From the simulation results we can see that the change of aircraft model will first influence the original shape of the trim set, and both changed model and shrunken trim set will become decisive factors of the final boundaries of safe flight envelopes. Following this method, we can generate the whole offline database containing different abnormal scenarios that may happen represented by either physical interpretations or mathematical equations, together with the corresponding safe flight envelopes. In the end we would be able to approximate the current safe flight envelope by searching for the model in the database that mostly match the identified model and interpolate the retrieved envelope. In this respect, the simulation proves the feasibility of our database-driven approach.



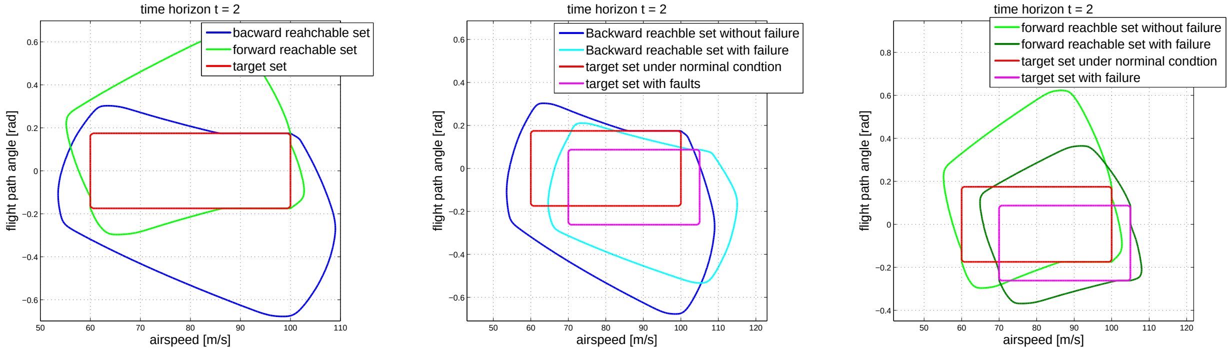
(a) (b) (c)

Figure 5. The reachability and viability set of three dimensional aircraft model



(a) (b) (c)

Figure 6. The reachability, viability and invariance set of two dimensional aircraft model



(a) (b) (c)

Figure 7. The comparisons of safe flight envelopes between nominal and abnormal cases

V. Conclusion

The paper presents a new approach for online prediction of safe flight envelopes in an database-driven manner to help deal with the problem of aircraft safe recovery under abnormal conditions, especially structural damage. The main contribution of our approach is that it proposes a feasible solutions to the problems that make instant calculation of safe flight envelopes hardly possible onboard. One problem we intend to fix is the "curse of dimensionality", which makes the time cost of the calculation far too long for emergency cases such as sudden system failures or abrupt structure changes. Another issue we may solve is the acquisition of global model when only limited measurements are available on occurrence of accidents. Through solid simulation results, the feasibility of our approach will be proved. Future work will be focused on advanced identification methods and searching techniques.

References

[1] Ranter, H., "Airliner Accident Statistics 2006," Tech. rep., Aviation Safety Network, 2007.

[2] Company, B., "Statistical Summary of Commercial Jet Airplane Accidents: Worldwide Operations since 1959." Tech. rep., Boeing Commercial Airplanes, 2009.

[3] Belcastro, C. M., "Validation of Safety-Critical Systems for Aircraft Loss-of-Control Prevention and Recovery," *AIAA Guidance Navigation and Control Conference*, 2012.

[4] Belcastro, C. M., "Validation and Verification of Future Integrated Safety-critical Systems Operating Under Off-nominal Conditions," *AIAA Guidance, Navigation, and Control Conference*, 2010.

[5] Kwatny, H. G., Dongmo, J.-E. T., Chang, B.-C., Bajpai, G., Yasar, M., and Belcastro, C. M., "Nonlinear Analysis of Aircraft Loss of Control," *Journal of Guidance, Control, and Dynamics*, Vol. 36, No. 1, 2013, pp. 149–162.

[6] Chongvisal, J. and Talleur, D., "Loss-of-control Prediction and Prevention for NASA's Transport Class Model," *AIAA Guidance, Navigation, and Control Conference*, 2014.

[7] Wilborn, J. and Foster, J., "Defining Commercial Transport Loss-of-control: A Quantitative Approach," *AIAA Atmospheric Flight Mechanics Conference*, 2004.

[8] Russell P., P. J., "Joint Safety Analysis Team- CAST Approved Final Report Loss of Control JSAT Results and Analysis," Tech. rep., FederalAviation Administration: Commercial Airline Safety Team, 2000.

[9] Ruijgrok, G. J. J., "Elements of Airplane Performance," Tech. rep., Delft Univeristy Press, 1996.

[10] Van Oort, E. R., *Adaptive Backstepping control And Safety Analysis For Modern Fighter Aircraft*, Ph.D. thesis, 2011.

[11] Govindarajan, N., *An optimal control approach for estimating aircraft command margins*, Ph.D. thesis, 2012.

[12] Tang, L., Roemer, M., Ge, J., Prasad, J., and Belcastro, C., "Methodologies for Adaptive Flight Envelope Estimation and Protection," *AIAA Guidance, Navigation and Control Conference*, 2009.

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

[14] Kwatny, H. G., Dongmo, J.-E. T., Allen, R. C., Chang, B.-C., and Bajpai, G., "Loss-of-Control: Perspectives on Flight Dynamics and Control of Impaired Aircraft," *AIAA Guidance, Navigation, and Control Conference*, 2010.

[15] Pandita, R. and Chakraborty, A., "Reachability and region of attraction analysis applied to GTM dynamic flight envelope assessment," *AIAA Guidance, Navigation and Control Conference*, 2009.

[16] Topcu, U., Packard, A. K., Seiler, P., and Balas, G. J., "Robust Region of Attraction Estimation," *IEEE Transactions on Automatic Control*, Vol. 55, No. 1, 2010, pp. 137–142.

[17] Lombaerts, T. and Schuet, S., "Robust Maneuvering Envelope Estimation Based on Reachability Analysis in An Optimal Control Formulation," *Conference on Control and Fault-Tolerant System*, 2013, pp. 318–323.

[18] Gillula, J. H., Hoffmann, G. M., Haomiao Huang, Vitus, M. P., and Tomlin, C., "Applications of hybrid reachability analysis to robotic aerial vehicles," *The International Journal of Robotics Research*, Vol. 30, No. 3, 2011, pp. 335–354.

[19] Kaynama, S., *Scalable Techniques for the Computation of Viable and Reachable Sets*, Ph.D. thesis, 2012.

[20] Fedkiw, S., *Level Set Methods and Dynamic Implicit Surfaces*, Vol. 153, Springer, 2003.

[21] Mitchell, I. M., *Application of Levle Set Methods to Control and Reachability Problems in Continuous and Hybrid Systems*, Ph.D. thesis, Stanford University, 2002.

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

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

[24] Kitsios, I. and Lygeros, J., "Launch-pad Abort Flight Envelope Computation for a Personnel Launch Vehicle Using Reachability," 2005, pp. 1–11.

[25] Kaynama, S., Mitchell, I. M., Oishi, M., and Dumont, G. a., "Scalable Safety-Preserving Robust Control Synthesis for Continuous-Time Linear Systems," Vol. 9286, No. 1, 2013, pp. 1–25.

[26] Kaynama, S., Oishi, M., Mitchell, I. M., and Dumont, G. a., "The continual reachability set and its computation using maximal reachability techniques," *IEEE Conference on Decision and Control and European Control Conference*, Vol. 0, 2011, pp. 6110–6115.

[27] Sun, L., *Model and Sensor Based Nonlinar Adaptive Flight Control with Online System Identification*, Ph.D. thesis, Delft Univeriety of Technology, 2014.

[28] Shah, G., "Aerodynamic Effects and Modeling of Damage to Transport Aircraft," *AIAA Guidance, Navigation and Control Conference and Exhibit*, 2008.

[29] Shah, G. and Hill, M., "Flight Dynamics Modeling and Simulation of a Damaged Transport Aircraft," *AIAA Modeling and Simulation Technologies*, 2012.

[30] Lombaerts, T., Schuet, S., Acosta, D., and Kaneshige, J. T., "Piloted Simulator Evaluation of Maneuvering Envelope Information for Flight Crew Awareness," *arc.aiaa.org*, 2015.

[31] de Visser, C. C., Chu, Q. P., and Mulder, J., "A New Approach to Linear Regression with Multivariate Splines," *Automatica*, Vol. 45, No. 12, 2009, pp. 2903–2909.

[32] de Visser, C. C., Mulder, J., and Chu, Q. P., "A Multidimensional Spline-Based Global Nonlinear Aerodynamic Model for the Cessna Citation II," *AIAA Atmospheric Flight Mechanics Conference*, 2010.

[33] Tol, H. J., de Visser, C. C., van Kampen, E., and Chu, Q. P., "Nonlinear Multivariate Spline-Based Control Allocation for High-Performance Aircraft," *Journal of Guidance, Control, and Dynamics*, Vol. 37, No. 6, 2014, pp. 1840–1862.

[34] Lopez, I. and Sarigul-Klijn, N., "A Review of Uncertainty in Flight Vehicle Structural Damage Monitoring, Diagnosis and Control: Challenges and Opportunities," *Progress in Aerospace Sciences*, Vol. 46, No. 7, 2010, pp. 247–273.

[35] Moncayo, H., Perhinschi, M. G., and Davis, J., "Artificial-Immune-System-Based Aircraft Failure Evaluation over Extended Flight Envelope," *Journal of Guidance, Control, and Dynamics*, Vol. 34, No. 4, jul 2011, pp. 989–1001.

[36] Lombaerts, T., Huisman, H., Chu, Q. P., Mulder, J., and Joosten, D., "Nonlinear Reconfiguring Flight Control Based on Online Physical Model Identification," *Journal of Guidance, Control, and Dynamics*, Vol. 32, No. 3, 2009, pp. 727–748.

[37] Tang, L., Roemer, M., Bharadwaj, S., and Belcastro, C., "An Integrated Health Assessment and Fault Contingency Management System for Aircraft," *AIAA Guidance Navigation and Control Conference*, 2008.

[38] Carl S. Byington, P. S., "A Model-Based Approach to Prognostics and Health Management for Flight Control Actuators," *IEEE Aerospace Conference Proceedings*, 2004.

[39] Belcastro, Christine M., F. J. V., "Aircraft Loss-of-Control Accident Analysis," *AIAA Guidance, Navigation and Control Conference*, 2010.

[40] Elmasri, R. and Navathe, S. B., *Fundamentals of Database Systems*, Addison-Wesley, 6th ed., 2010.

[41] 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," *Proceedings of the 45th IEEE Conference on Decision and Control*, 2006, pp. 3801–3807.

[42] Tomlin, C., Lygeros, J., and Sastry, S., "A game theoretic approach to controller design for hybrid systems," *Proceedings of the IEEE*, Vol. 88, No. 7, 2000.

[43] Lygeros, J., Tomlin, C., and Sastry, S., "Controllers for reachability specifications for hybrid systems," *Automatica*, Vol. 35, 1999, pp. 349–370.

[44] Mitchell, I. M., "A Toolbox of Level Set Methods (Version 1.1)," Tech. rep., 2007.

[45] Lombaerts, T., Schuet, S., Acosta, D., and Kaneshige, J., "On-Line Safe Flight Envelope Determination for Impaired Aircraft," *Advances in Aerospace Guidance, Navigation and Control*, 2015, pp. 263–282.

[46] Mitchell, I. M., "Comparing Forward and Backward Reachability as Tools for Safety Analysis," *Hybrid systems: computation and control*, edited by A. Bemporad, A. Bicchi, and G. Buttazzo, Springer Berlin Heidelberg, 2007, pp. 428–443.

[47] Tomlin, C., Mitchell, I. M., Bayen, A. M., and Oishi, M., "Computational techniques for the verification of hybrid systems," *Proceedings of the IEEE*, Vol. 91, No. 7, 2003, pp. 986–1001.

[48] Lombaerts, T., Schuet, S., and Wheeler, K., "Safe Maneuvering Envelope Estimation Based on A Physical Approach," *Guidance, Navigation, and Control and Co-located Conferences*, 2013.

[49] Tol, H. J., de Visser, C. C., Sun, L. G., Kampen, E. V., and Chu, Q. P., "Multivariate Spline Based Adaptive Control of High Performance Aircraft With Aerodynamic Uncertainties," .