Journal of Aerospace Information Systems
Vol. 12, No. 9, September 2015

Flight Safety Assessment and Management for Takeoff Using Deterministic Moore Machines

Sweewarman Balachandran* and Ella. M. Atkins†
University of Michigan, Ann Arbor, Michigan 48105

DOI: 10.2514/1.I010350

This paper presents a novel flight safety assessment and management augmentation to the flight management system designed to assist a flight crew in avoiding or recovering from impending loss-of-control situations. Nominally, this system serves as a passive monitor but, in high-risk situations, warnings and (ultimately) override actions are initiated to mitigate the high-risk situation. In this work, flight safety assessment and management is applied to the task of preserving safety during takeoff, which is one of the highest-risk phases of flight. Flight safety assessment and management is specified as a deterministic Moore machine that can ultimately be certified using existing software certification processes. To facilitate understanding and to reduce state-space complexity, flight safety assessment and management's state machines are split into longitudinal and lateral-directional submachines that identify and mitigate loss-of-control contributing factors associated with aircraft dynamics and control constraints. Case studies based on documented takeoff accidents are presented to evaluate flight safety assessment and management's ability to maintain safe flight in realistic loss-of-control scenarios. Results from these case studies illustrate that flight safety assessment and management could have averted the takeoff accidents that were considered. A discussion of other factors that must be considered before realizing a comprehensive flight safety assessment and management capability for takeoff is provided.

Nomenclature

$\mathcal{A}_{\mathrm{lg}}$	=	longitudinal takeoff logic
$\mathcal{A}_{\mathrm{lt}}$	=	lateral takeoff logic
$\overline{ap}$	=	envelope aware autopilot control
C_L, C_D	=	lift and drag coefficients
h	=	altitude
p, q, r	=	angular rates
$\bar{p}$	=	pilot control
T, W	=	thrust and weight
u, v, w	=	velocities in the body frame
V	=	true airspeed
V_{lof}	=	liftoff speed
V_R	=	takeoff rotation speed
V_1	=	takeoff decision speed
X	=	longitudinal position on runway
Y	=	lateral position on runway
y	=	crosstrack error
α, β, γ	=	angle of attack, sideslip angle, and flight-path angle
δ_a, δ_r	=	aileron and rudder inputs
ρ, μ, S_{ref}	=	atmospheric density, friction coefficient, and planform area
ϕ, θ, ψ	=	roll, pitch, and yaw angles

I. Introduction

LOSS of control (LOC) is the leading cause of commercial aviation accidents today. Although common contributors exist, many causal factors that have historically led to LOC are a function of the type of aircraft, avionics design, crew behavior, weather conditions, and phase of flight [1]. LOC during takeoff can be attributed to several factors such as improper takeoff configuration, delayed execution of rejected takeoff procedures, engine failures during takeoff, bird strikes, severe crosswinds, etc. Such circumstances may result in aircraft stall after takeoff, runway overrun, or excursion off the side of the runway. Today, flight management decisions are made by the flight crew, with the exception of certain envelope protection logic to prevent events such as pilot-induced stall given a nominally functioning aircraft [2–4]. During failure, damage, or other exceptional events, decisions have to be made within a short time window, as the wrong decisions could lead to an accident. Current flight-deck automation provides substantial data to the flight crew and augments the manual decision-making process. In case of emergency, however, current systems may fail to provide critical information. For example, current flight management systems (FMSs) were not designed to provide an assessment of risks associated with the current flight conditions and control choices, nor do they inform the flight crew about possible actions that would improve safety of flight, except in specific cases such as the traffic collision-avoidance system [3,5,6]. Such information is vital to guide the

Presented as Paper 2014-0785 at the AIAA Guidance, Navigation, and Control Conference, National Harbor, MD, 14–17 January 2014; received 23 October 2014; revision received 3 May 2015; accepted for publication 31 July 2015; published online 24 September 2015. Copyright © 2015 by Swee Balachandran. Published by the American Institute of Aeronautics and Astronautics, Inc., with permission. Copies of this paper may be made for personal or internal use, on condition that the copier pay the $10.00 per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923; include the code 2327-3097/15 and $10.00 in correspondence with the CCC.

*Graduate Student, Department of Aerospace Engineering. Student Member AIAA.

†Associate Professor, Department of Aerospace Engineering. Associate Fellow AIAA.

flight crew in the decision-making process during emergencies, particularly when the workload is high and real-time safety-critical decisions are required.

Flight safety assessment and management (FSAM) is part of the envelope-aware (EA) flight management system (EA-FMS) originally proposed in our previous work [7] (see Fig. 1). The EA-FMS consists of modules including FSAM [7,8], adaptive planning and guidance [9], Envelope estimation [10], system identification [11] and adaptive control [12]. FSAM is designed to constantly monitor flight conditions for anomalies and to assess risks associated with the current flight conditions. FSAM warns the flight crew when risk is present and, if the flight crew does not respond with appropriate control actions in time to assure recovery, FSAM overrides with the EA-FMS until the LOC risk is mitigated. FSAM is effectively a "watchdog" system with LOC avoidance override capabilities such as flight envelope protection (FEP) [3], in a more general context.

For takeoff, LOC translates to a situation in which the aircraft veers off the side of the runway, overshoots the runway, or leaves the ground in a condition (e.g., insufficient speed/inappropriate rotation attitude) that introduces substantial risk in the subsequent departure climb. The work presented in this paper contributes a deterministic decision-making framework that addresses the aforementioned LOC factors in a holistic manner with an approach that can be certified using existing processes in DO-178B or DO-178C [13]. The deterministic Moore machines (DMMs) [14] realizing FSAM in this paper characterize the evolution of aircraft states to support safe takeoff decisions with FSAM warning or override to avoid LOC risk. The DMMs are formulated based on analysis of aviation accident surveys, accident/incident reports, flight data obtained from the National Transportation Safety Board (NTSB) accident database [15,16], aircraft operating manuals, pilot handbooks, checklist procedures, and flight control laws from the literature [2–4]. Furthermore, this paper introduces envelopes for the takeoff phase that enable the identification of safe and unsafe states. Note that a discussion of suitable human–machine interfaces that could make use of FSAM to improve the situational awareness of the flight crew is beyond the scope of this paper. This work assumes that the aircraft dynamics and the relevant flight envelopes remain static throughout takeoff. Consequently, this work does not illustrate the interactions between the various subsystems and the full capability of the EA-FMS.

Section II surveys related literature, whereas Sec. III provides a discussion of factors that contribute to LOC during takeoff. Section IV discusses the development of flight envelopes to efficiently and intuitively identify risk during takeoff. Section V presents the FSAM DMMs used to avoid LOC during takeoff. Section VI presents case studies illustrating the application of FSAM to real-world scenarios, whereas Sec. VII discusses results and their implications. Section VIII presents conclusions and future work required to realize a comprehensive FSAM capability.

II. Background

A. Flight Safety Architectures

Several approaches to identify and mitigate LOC risk have been investigated in the past, with most focused on providing cues to the pilot. The safety augmentation system [17] is an automation aid to prevent entry into hazardous conditions such as unfavorable weather. It identifies flight plan deviations and issues warning and haptic feedback upon hazard detection. Icing contamination envelope protection [18] identifies airplane performance degradations resulting from ice contamination with online system identification and provides associated cues to pilots. The runway overrun prevention system (ROPS) was developed by Airbus to provide warnings to the flight crew about degraded landing performance during final approach [19].

Bak et al. [20] proposed a sandbox architecture, where an unverified controller was augmented with a safety controller and a decision module that enabled switching to the safety controller when unsafe states were encountered. The switching strategy was obtained using hybrid systems and optimal control principles. The sandbox architecture was conceptually similar to FSAM, although it was not used in a flight safety context. The aircraft integrated resilient safety assurance and failsafe enhancement (AIRSAFE) [21] conceptual architecture for LOC avoidance includes online modeling, safety assessment, and resilient control in situations with appreciable LOC risk. FSAM realizes the role of AIRSAFE's safety assessment and risk mitigation concepts.

Several researchers have also focused on developing individual techniques that address different aspects of LOC. For example, Govindarajan et al. [22] proposed an optimal control framework to analyze flight control laws and estimate constraints on the reference commands. These constraints were then used by the autopilot to ensure that the aircraft stayed within safe operating envelopes. McDonough et al. [10], McDonough and Kolmanovsky [23], and Lombaerts et al. [24,25] proposed methods to estimate degrading envelope constraints under conditions such as icing.

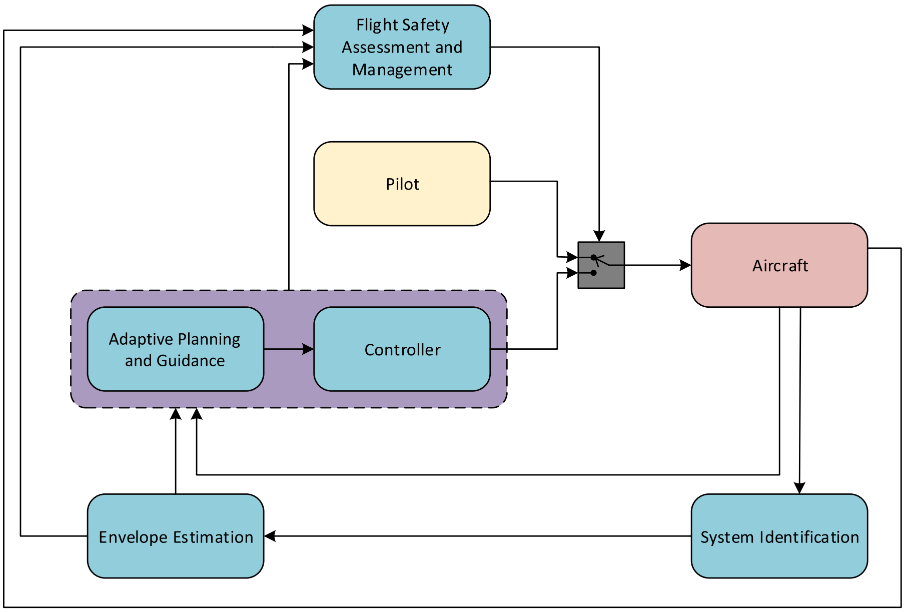

Flight Safety Assessment and Management
Pilot
Aircraft
Adaptive Planning and Guidance
Controller
Envelope Estimation
System Identification

Fig. 1 Envelope-aware flight management system architecture.

Yu et al. [11] and Schuet et al. [26] developed system identification techniques to estimate the dynamics of an aircraft following adverse onboard conditions. Information from these systems can be used by FSAM to make efficient decisions to prevent catastrophes.

B. Flight Safety Systems for Takeoff

Despite the safety-critical nature of takeoff, very little literature has been devoted toward LOC risk mitigation specifically for takeoff. Srivatsan et al. [27], Milligan et al. [28], and Zammit-Mangion and Shelby. [29] proposed systems that constantly monitored takeoff ground roll performance parameters and detected anomalies by comparing the current performance with a precomputed nominal performance profile. Verspay and Khatwa [30] evaluated the merits of various types of takeoff performance monitoring systems (TOPMs), as well as characteristics of a TOPM that improved pilot decision making during takeoff. It was found that a system with the ability to predict continued takeoff status and stopping performance had the potential to improve safety. Inagaki and Itoh [31] investigated automating go/no-go decisions using a situation-adaptive autonomy framework [32]. These publications focused on aiding the flight crew in making safe go/no-go decisions during takeoff and did not consider other LOC risks, such as loss of directional control or inappropriate rotation, which are both case studies in our work.

III. Takeoff

Takeoff is one of the hazardous phases of flight, second only to final approach and landing. Current takeoff regulations require that the flight crew follow standard operating procedures to configure the aircraft appropriately, obtain clearances, and manually fly the aircraft through initial departure climb [33]. In a commercial transport aircraft, a typical takeoff ground roll lasts 20–35 s. The Federal Aviation Regulations define several airspeed checkpoints called V speeds [34,33] to guide the flight crew in making appropriate decisions during takeoff. The most important V speed is V_1, which is the decision speed by which the flight crew must decide to continue or reject a takeoff, i.e., make a go/no-go decision with sufficient remaining runway to safely reject the takeoff. The flight crew may need to reject a takeoff due to several factors such as engine failure(s), tire burst(s), runway incursion, etc. A rejected takeoff initiated after V_1 will leave insufficient runway length to stop safely. Rotation initiated before the appropriate V speed can result in an early departure stall [15]. Figure 2 graphically represents takeoff V speeds. A listing of V speeds is provided in Sec. V (Table 1).

The aircraft takeoff dynamics used in this work are presented in [8] and the Appendices at the end of this paper. However, to study the longitudinal dynamics of the aircraft during the takeoff ground roll, these equations can be simplified as described in [34]. Let (X, Y) represent the longitudinal and lateral runway directions, respectively, with $(0, 0)$ as the ground roll initiation point on the runway centerline. Let V represent the airspeed and V_{lof} represent the lift off airspeed. The simplified equations can be described as follows:

$$\begin{aligned}\dot{X} &= V\cos(\gamma)\\ \dot{V} &= \begin{cases} A_1 - B_1 V^2 & V < V_{\text{lof}}\\ A_2 - B_2 V^2 & V \geq V_{\text{lof}}\end{cases}\end{aligned} \tag{1}$$

where A_1, B_1 and A_2, B_2 are defined as

$$\begin{aligned}A_1 &= g\left(\frac{T}{W} - \mu\right)\\ B_1 &= \frac{g}{W}\left(\frac{1}{2}\rho S_{\text{ref}}(C_{D_g} - \mu C_{Lg})\right)\\ A_2 &= g\left(\frac{T}{W} - \sin(\gamma)\right)\\ B_2 &= \frac{g}{W}\left(\frac{1}{2}\rho S_{\text{ref}} C_{D_g}\right)\end{aligned}$$

Table 1 Input alphabet symbols for the takeoff Moore machine

Alphabet (Σ)	Description
V_{mcg}	Minimum controllable groundspeed with one engine inoperative
V_1	Takeoff decision speed (go/no-go speed)
V_R	Rotation speed
V_{lof}	Liftoff speed
V_2	Takeoff safety speed
V_{fp}	Minimum flap retraction speed
$T_{\max}$	Takeoff thrust setting
T_{idle}	Idle thrust setting
c	Aircraft configured for takeoff
c'	Improper takeoff configuration
d	Crossing first directional threshold
d'	Crossing second directional threshold
e	Envelope protection deactivated
e'	Envelope protection activated
f	Inadequate acceleration performance
o'	Stall
θ	Positive pitch attitude
$\bar{\theta}$	Maximum allowable pitch attitude reached during rotation
θ'	Safe rotation attitude

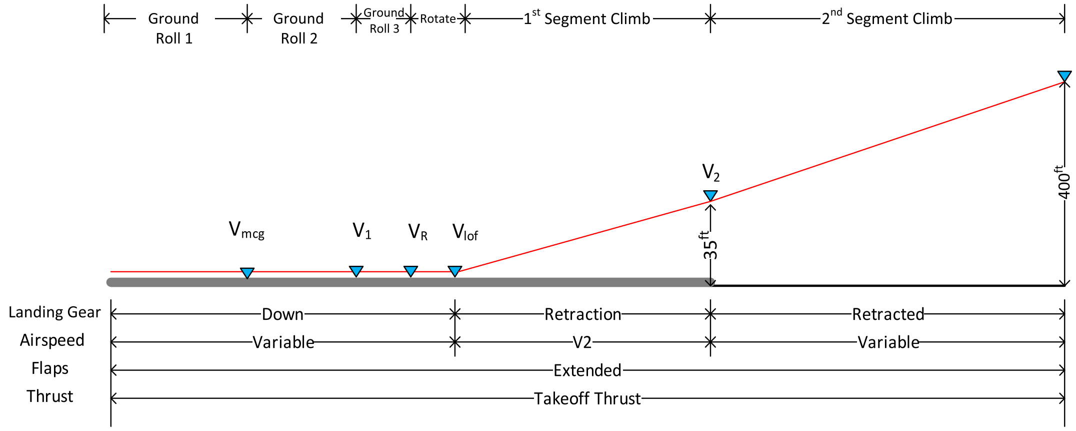


Fig. 2 Takeoff phase of flight.

Here, T represents the takeoff thrust or idle thrust for rejected takeoff (RTO), W represents the aircraft's takeoff weight, ρ represents the atmospheric density, μ represents the rolling friction coefficient for continued takeoff or braking friction coefficient for RTO, and γ is the flight-path angle. We assume $\gamma = 0$ when $V \leq V_{\mathrm{lof}}$ and $\gamma = \gamma_0$ $(\gamma_0 > 0)$ when $V > V_{\mathrm{lof}}$. The angle of attack is represented by α; S_{ref} is the planform area; and C_{L_g} and C_{D_g} are the coefficients of lift and drag, respectively, including ground effects and nominal flaps/slat settings for takeoff.

To investigate FSAM for takeoff, we first examined causal factors in takeoff-related accidents. Ninety-seven rejected takeoff runway overrun accidents and incidents have been reported from 1960 to 2000, resulting in more than 400 fatalities [1,35]. Takeoff accident causal factors are summarized in Fig. 3 [36].

The goal of FSAM is to identify LOC risk and assure its mitigation. In this initial work, we make the following simplifying assumptions:

1) There are no electromechanical or structural failures, and all software is functioning according to specification.

2) The control authority and aerodynamics are nominal, indicating no reduction in the flight envelope.

3) The aircraft is cleared for takeoff and faces no risk due to obstacles or other aircraft.

These assumptions would be relaxed in a comprehensive takeoff FSAM beyond the scope of this work.

Below, in Sec. IV, we present envelopes for the takeoff phase that are essential to prevent factors such as improper rejected takeoff decisions, degraded acceleration performance (due to reduced engine performance or other factors such as weight calculation errors), tail strikes, poor rotation procedures, and directional control issues.

IV. Takeoff Flight Envelopes

To achieve an effective FSAM capability, we first need to prescribe safe flight envelopes for takeoff. Translational dynamics [Eq. (1)] with $\gamma = 0$ yields the ground roll distance between two airspeeds, V_a and V_b, given by

$$\frac{\dot{V}}{\dot{X}} = \frac{\mathrm{d}V}{\mathrm{d}X} = \frac{A - BV^2}{V} \tag{2}$$

Equation (2) can be rearranged as

$$\mathrm{d}X = \frac{V\mathrm{d}V}{A - BV^2} \tag{3}$$

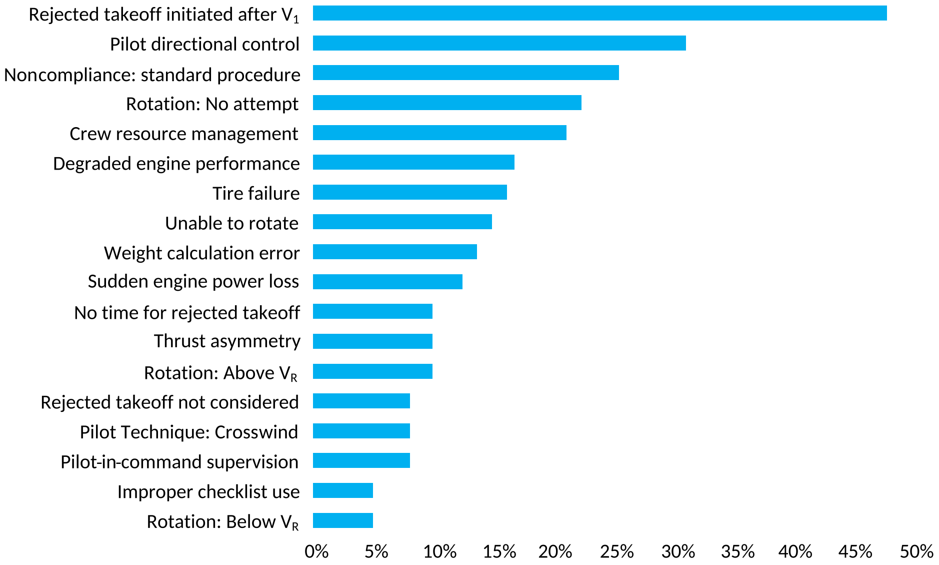


Fig. 3 LOC contributing factors for takeoff [36].

Integrating Eq. (3) yields

$$X_b - X_a = \frac{1}{2B} \ln\left(\frac{A - BV_a^2}{A - BV_b^2}\right) \tag{4}$$

Using Eq. (4) for a given takeoff configuration (weight, thrust, and flap/slat settings), one can estimate the maximum airspeed at which a rejected takeoff must be initiated to stop safely within the available runway space. The Fig. 4 vector field illustrates how V and X evolve after a rejected takeoff is initiated. The solid curve in Fig. 4 defines the partition of the V-X space for which a rejected takeoff will enable the aircraft to stop safely at or before the end of the runway.

Analogously, one can estimate the minimum airspeed beyond which a one-engine-inoperative (OEI) takeoff can be safely continued (see Fig. 5). All trajectories to the left of this envelope will overshoot the runway before attaining airspeed V_2.

Figure 6 combines the constraints in Figs. 4 and 5 to partition safe regions in the V-X space with respect to RTO and OEI conditions. The intersection of the two curves represents V speed V_1.

When operating with all engines operative (AEO), the aircraft must always stay in an envelope where at least one safe action can be executed. Figure 7 defines a minimum thrust boundary, assuming AEO to avoid the zone that is unsafe with respect to RTO and OEI. If the aircraft deviates outside this minimum thrust boundary under the AEO condition before V_1, takeoff must be rejected.

Rotational dynamics can be similarly analyzed to segregate safe and unsafe operating regions. For example, Fig. 8 illustrates a constraint on pitch during rotation. Overrotation leads to tail strike, imposing a maximum tail strike pitch constraint.

Similarly, lateral runway excursions due to poor directional control can be managed by enforcing constraints on lateral motion primitives. Figure 9 illustrates safety constraints on cross track position Y and heading ψ. Bounds $|y| \leq |y_1|$ and $|\psi| \leq |\psi_1|$ represent transitions to moderate risk states for FSAM, whereas either $|y| > |y_2|$ or $|\psi| > |\psi_2|$ represent an unacceptable lateral traversal condition.

V. DMM Formulation of FSAM

In this work, the FSAM decision logic is modeled as a deterministic Moore machine. DMMs are finite-state machines in which each state has a prescribed discrete output [14]. Also, DMMs are modular and composable [7,37], and use of a deterministic specification for FSAM will facilitate its verification and certification using well-established tools in model checking, which is a topic studied in another work [38]. The DMM is defined below and the FSAM formulation for takeoff is specified.

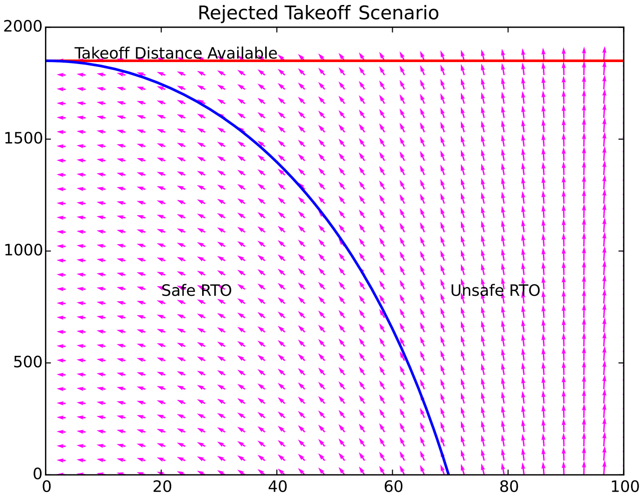


Fig. 4 Rejected takeoff envelope.

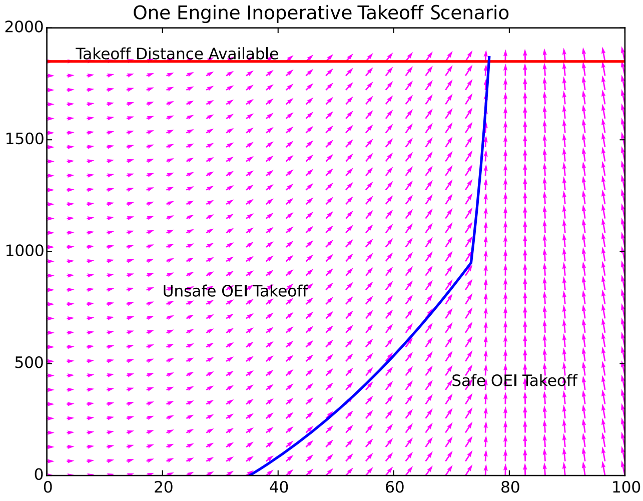


Fig. 5 Takeoff with one engine inoperative.

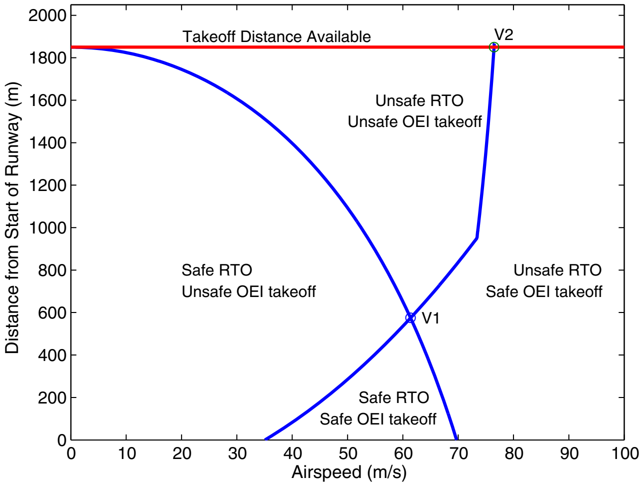


Fig. 6 Safe and unsafe regions of takeoff flight envelopes.

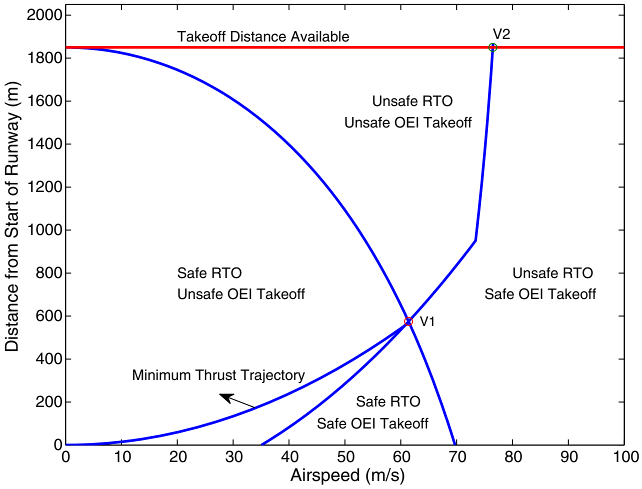


Fig. 7 RTO, OEI, and AEO envelopes.

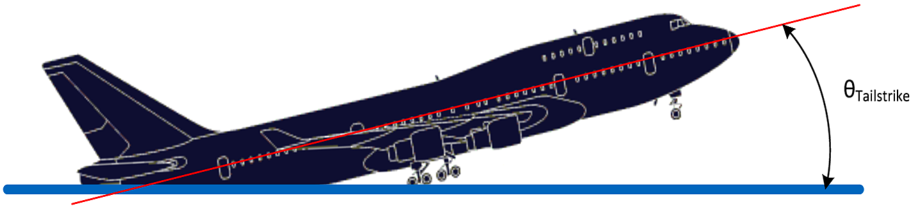


Fig. 8 Tail strike constraints.

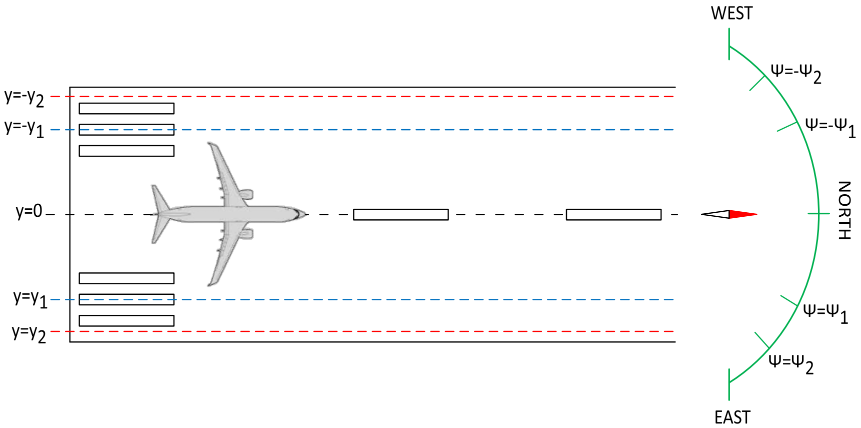


Fig. 9 Lateral takeoff constraints to avoid runway excursion.

A. Deterministic Moore Machine

A deterministic Moore machine [14,39,40] is defined by the tuple ($\mathcal{S}$, $\mathcal{S}_0$, Σ, Λ, $\mathcal{T}$, $\mathcal{G}$), where $\mathcal{S}$ represents a discrete set of states, $\mathcal{S}_0 \subset \mathcal{S}$ represents an initial state, Σ is a finite input alphabet, Λ is a finite output alphabet, $\mathcal{T} \subseteq \mathcal{S} \times \Sigma \times \mathcal{S}$ represents the set of state transitions, and $\mathcal{G}$: $\mathcal{S} \times \Lambda$ is the output function mapping each state to a unique output character (control action). For FSAM, inputs from Σ trigger state transitions. Outputs of $\mathcal{G}$ represent FSAM control authority decisions. For simplicity, FSAM is split into longitudinal and lateral DMMs to identify associated LOC risk.

B. Longitudinal Deterministic Moore Machine

The longitudinal takeoff FSAM DMM identifies LOC risk with respect to the longitudinal aircraft state. Takeoff stages are correlated with V speeds, as shown in Fig. 2. We represent the longitudinal Moore machine $\mathcal{A}_{\mathrm{lg}}$ by the tuple ($\mathcal{S}_{\mathrm{lg}}$, $\mathcal{S}_{\mathrm{lg}\,0}$, Σ_{lg}, Λ_{lg}, $\mathcal{T}_{\mathrm{lg}}$, $\mathcal{G}_{\mathrm{lg}}$), where

$$\mathcal{S}_{\mathrm{lg}} = \{s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8, s_9, s_{10}, s_{11}, s_{12}, s_{13}, s_{14}, s_{15}\} \tag{5}$$

$$\mathcal{S}_{\mathrm{lg}\,0} = \{s_1\} \tag{6}$$

$$\Sigma_{\mathrm{lg}} = \{V_{\mathrm{mcg}}, V_1, V_R, V_{\mathrm{lof}}, V_2, V_{\mathrm{fp}}, T_{\mathrm{idle}}, T_{\mathrm{max}}, c, c', e, e', f, \theta, \bar{\theta}\} \tag{7}$$

$$\Lambda_{\mathrm{lg}} = \{P, \mathrm{EA}\} \tag{8}$$

$$\mathcal{G}_{\mathrm{lg}} = \begin{cases} P & \text{if } s_i \in \{s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8, s_{14}\} \\ \mathrm{EA} & \text{otherwise} \end{cases} \tag{9}$$

Transitions $\mathcal{T}_{\mathrm{lg}}$ represent edges in a directed state transition graph (Fig. 10). The definition of each alphabet symbol in the set Σ_{lg} is listed in Table 1. Table 2 provides descriptions of each state. A state $s \in \mathcal{S}_{\mathrm{lg}}$ is defined by the triplet $[\bar{\mathcal{V}}, \mathcal{P}, \mathcal{R}]$. $\bar{\mathcal{V}}$ represents an airspeed range, with values shown in Eqs. (10–18). Here, $\mathcal{P} \in \{0, 1\}$ is a flag set to true when continuing the takeoff is no longer safe because of inappropriate aircraft configuration; and $\mathcal{R} \in \{\varepsilon, \mathrm{low}, \mathrm{med}, \mathrm{high}\}$ represents the risk level associated with the current state, where ϵ denotes a zero risk state:

$$\bar{\mathcal{V}} \in \{\bar{v}_i\}, \qquad i = 1, \ldots, 8 \tag{10}$$

$$\bar{v}_1 = \{V \in \mathbb{R} | V = 0\} \tag{11}$$

$$\bar{v}_2 = \{V \in \mathbb{R} | 0 < V \leq V_{\mathrm{mcg}}\} \tag{12}$$

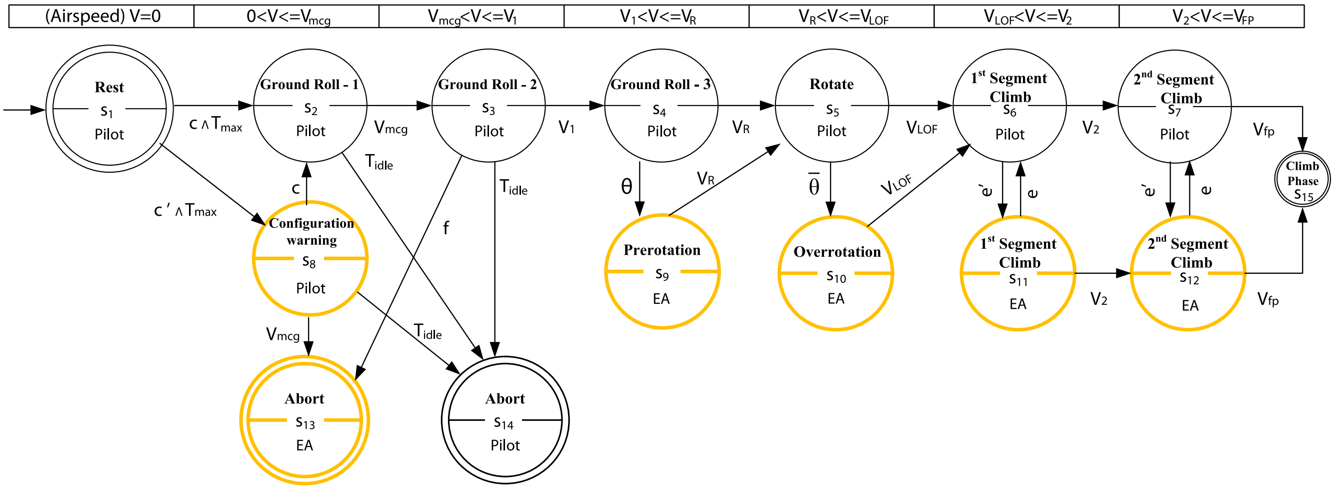


Fig. 10 DMM for longitudinal takeoff dynamics (see Table 1).

Table 2 Examples of state representations

$\mathcal{A}_{\mathrm{lg}}$ states	Representation	$\mathcal{A}_{\mathrm{lt}}$ states	Representation
s_1	$[\bar{v}_1, 0, \varepsilon]$	s'_1	$[\bar{v}_1, \bar{y}_1, \bar{\psi}_1, \bar{g}_1, \varepsilon]$
s_2	$[\bar{v}_2, 0, \varepsilon]$	s'_2	$[\bar{v}_2, \bar{y}_1, \bar{\psi}_1, \bar{g}_1, \varepsilon]$
s_3	$[\bar{v}_3, 0, \varepsilon]$	s'_3	$[\bar{v}_3, \bar{y}_1, \bar{\psi}_1, \bar{g}_1, \varepsilon]$
s_4	$[\bar{v}_4, 0, \varepsilon]$	s'_4	$[\bar{v}_4, \bar{y}_1, \bar{\psi}_1, \bar{g}_1, \varepsilon]$
s_5	$[\bar{v}_5, 0, \varepsilon]$	s'_5	$[\bar{v}_5, \bar{y}_1, \bar{\psi}_1, \bar{g}_1, \varepsilon]$
s_6	$[\bar{v}_6, 0, \varepsilon]$	s'_6	$[\bar{v}_6, \bar{y}_1, \bar{\psi}_1, \bar{g}_1, \varepsilon]$
s_7	$[\bar{v}_7, 0, \varepsilon]$	s'_7	$[\bar{v}_7, \bar{y}_1, \bar{\psi}_1, \bar{g}_1, \varepsilon]$
s_8	$[\bar{v}_2, 0, \mathrm{med}]$	s'_8	$[\bar{v}_2, \bar{y}_2, \bar{\psi}_2, \bar{g}_2, \mathrm{med}]$
s_9	$[\bar{v}_4, 0, \mathrm{low}]$	s'_9	$[\bar{v}_3, \bar{y}_2, \bar{\psi}_2, \bar{g}_2, \mathrm{med}]$
s_{10}	$[\bar{v}_5, 0, \mathrm{low}]$	s'_{10}	$[\bar{v}_4, \bar{y}_2, \bar{\psi}_2, \bar{g}_2, \mathrm{med}]$
s_{11}	$[\bar{v}_6, 0, \mathrm{low}]$	s'_{11}	$[\bar{v}_5, \bar{y}_2, \bar{\psi}_1, \bar{g}_2, \mathrm{med}]$
s_{12}	$[\bar{v}_7, 0, \mathrm{low}]$	s'_{12}	$[\bar{v}_6, \bar{y}_2, \bar{\psi}_2, \bar{g}_2, \mathrm{med}]$
s_{13}	$[\bar{v}_3, 1, \mathrm{med}]$	s'_{13}	$[\bar{v}_7, \bar{y}_2, \bar{\psi}_2, \bar{g}_2, \mathrm{med}]$
s_{14}	$[\bar{v}_3, 1, \varepsilon]$	s'_{14}	$[\bar{v}_{2,3}, \bar{y}_3, \bar{\psi}_3, \bar{g}_1, \mathrm{med}]$
s_{15}	$[\bar{v}_8, 0, \varepsilon]$	s'_{15}	$[\bar{v}_8, \bar{y}_1, \bar{\psi}_1, \bar{g}_1, \varepsilon]$

$$\bar{v}_3 = \{V \in \mathbb{R} | V_{\mathrm{mcg}} < V \leq V_1\} \tag{13}$$

$$\bar{v}_4 = \{V \in \mathbb{R} | V_1 < V \leq V_R\} \tag{14}$$

$$\bar{v}_5 = \{V \in \mathbb{R} | V_R < V \leq V_{\mathrm{lof}}\} \tag{15}$$

$$\bar{v}_6 = \{V \in \mathbb{R} | V_{\mathrm{lof}} < V \leq V_2\} \tag{16}$$

$$\bar{v}_7 = \{V \in \mathbb{R} | V_2 < V \leq V_{\mathrm{fp}}\} \tag{17}$$

$$\bar{v}_8 = \{V \in \mathbb{R} | V > V_{\mathrm{fp}}\} \tag{18}$$

Each state $s \in \mathcal{S}$ is mapped to an output by function $\mathcal{G}_{\mathrm{lg}}$. P represents the "pilot-in-control" command, and EA represents the "envelope-aware autopilot" command output. The output of each state is indicated on the lower half of each state depicted in Fig. 10. This work assumes the envelope-aware controller has sufficient situational awareness to recover from the LOC triggers/hazards.

As shown in Fig. 10, the aircraft starts from an initial state of rest s_1 at $(X, Y) = (0, 0)$. If the aircraft is configured for takeoff c and takeoff thrust is established T_{max}, the aircraft accelerates down the runway and the DMM state transitions through the nominal V-speed state progression.. The top row of states in Fig. 10 represents the nominal V-speed sequence The additional states represent offnominal conditions with LOC risk. If the aircraft is inappropriately configured, the DMM enters a configuration warning state s_8, inducing a corresponding alert to the crew. If the configuration problem persists, the DMM transitions into the abort state s_{13}, where it overrides and rejects the takeoff. During the initial ground roll ($V_{\mathrm{mcg}} < V \leq V_1$), if the aircraft has inadequate acceleration, FSAM rejects the takeoff f to prevent entry into the Fig. 7 zone that is unsafe with respect to RTO and OEI. At higher speeds, the DMM monitors crew inputs to avoid premature rotation and tail strike (s_4 and s_5). After liftoff, conventional envelope protection features such as angle of attack (stall) and overspeed become active [2,3]. Pushing the aircraft to the stall boundary during the climb (s_6, s_7) results in override, with the envelope-aware controller (s_{11}, s_{12}) analogous to stall or envelope protection capabilities found on existing aircraft. FSAM reverts control to the flight crew after the aircraft is stabilized on climbout.

The DMM models presented here are a subcomponent of the FSAM system covering all phases of flight. Consequently, after takeoff, FSAM switches to a climb DMM that is beyond the scope of this work.

C. Lateral Deterministic Moore Machine

The lateral FSAM DMM ensures directional control is sufficient to prevent lateral or crosstrack runway excursions. Directional control loss can result from high crosswinds or gusty winds, engine thrust asymmetry, and inappropriate rudder inputs. Figure 9 provides partitions on the crosstrack error and heading error, indicating LOC risk level.

The lateral DMM $\mathcal{A}_{\mathrm{lt}}$ is represented by the tuple ($\mathcal{S}_{\mathrm{lt}}$, $\mathcal{S}_{\mathrm{lt}0}$, Σ_{lt}, Λ_{lt}, $\mathcal{T}_{\mathrm{lt}}$, $\mathcal{G}_{\mathrm{lt}}$), where

$$S_{\mathrm{lt}} = \{s'_1, s'_2, s'_3, s'_4, s'_5, s'_6, s'_7, s'_8, s'_9, s'_{10}, s'_{11}, s'_{12}, s'_{13}, s'_{14}, s'_{15}\} \tag{19}$$

$$S_{\mathrm{lt}0} = \{s'_1\} \tag{20}$$

$$\Sigma_{\text{lt}} = \{V_{\text{mcg}}, V_1, V_R, V_{\text{lof}}, V_2, V_{\text{fp}}, T_{\text{idle}}, T_{\text{max}}, c, c', e, e', d', \bar{d}\} \tag{21}$$

$$\Lambda_{\text{lt}} = \{P, \text{EA}\} \tag{22}$$

$$\mathcal{G}_{\text{lt}} = \begin{cases} P & \text{if } s_i' \in \{s_1', \ldots, s_7'\} \\ \text{EA} & \text{otherwise} \end{cases} \tag{23}$$

Transitions $\mathcal{T}_{\text{lt}}$ are shown as edges in the Fig. 11 DMM graph. Each state s' is defined as the quintuple $[\bar{\mathcal{V}}, \bar{\mathcal{Y}}, \bar{\Psi}, \bar{\Upsilon}, \mathcal{R}]$. $\bar{\mathcal{V}}$ and $\mathcal{R}$ are defined as in DMM $\mathcal{A}_{\text{lg}}$. $\bar{\mathcal{Y}}$ represents discretized crosstrack errors, with y_1 and y_2 defined as in Fig. 9:

$$\bar{\mathcal{Y}} \in \{\bar{y}_i\}, \qquad i = 1, 2, 3 \tag{24}$$

$$\bar{y}_1 = \{y \in \mathbb{R} | |y| \leq |y_1|\} \tag{25}$$

$$\bar{y}_2 = \{y \in \mathbb{R} | |y_1| < |y| \leq |y_2|\} \tag{26}$$

$$\bar{y}_3 = \{y \in \mathbb{R} | |y| > |y_2|\} \tag{27}$$

$\bar{\Psi}$ represents discrete inertial heading intervals with deviation constraints ψ_1, ψ_2, also shown in Fig. 9:

$$\bar{\Psi} \in \{\bar{\psi}_i\}, \qquad i = 1, 2, 3 \tag{28}$$

$$\bar{\psi}_1 = \{\psi \in [-\pi, \pi] | |\psi| < |\psi_1|\} \tag{29}$$

$$\bar{\psi}_2 = \{\psi \in [-\pi, \pi] | |\psi_1| \leq |\psi| \leq |\psi_2|\} \tag{30}$$

$$\bar{\psi}_3 = \{\psi \in [-\pi, \pi] | |\psi| > |\psi_2|\} \tag{31}$$

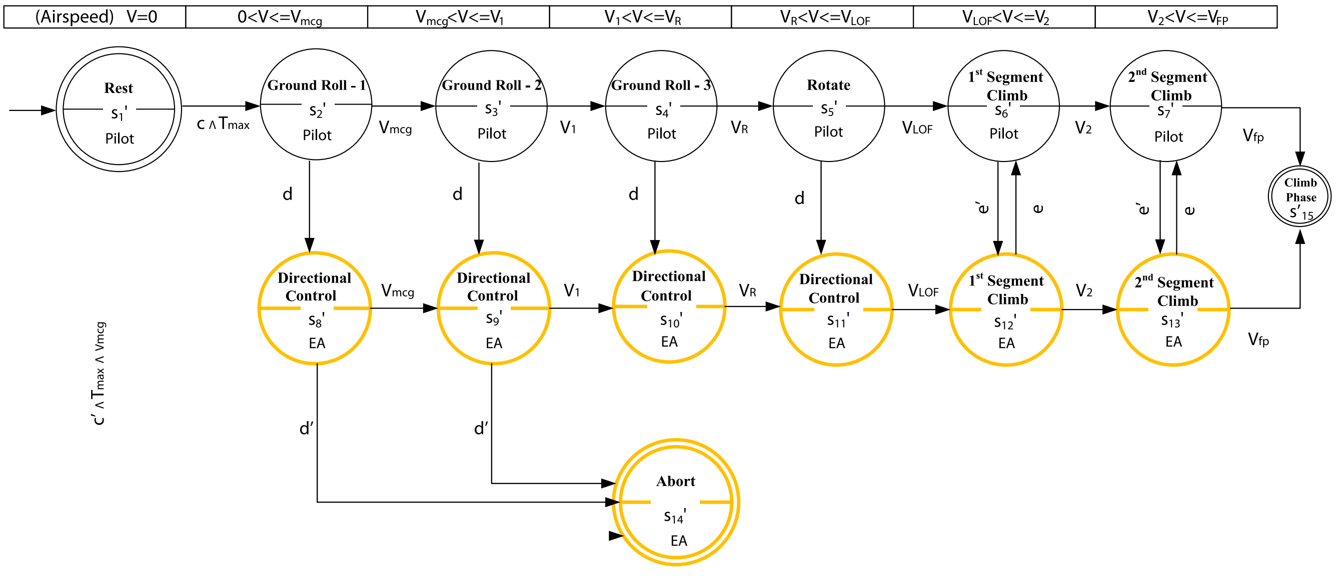


Fig. 11 DMM for lateral-directional takeoff dynamics (see Table 1).

$\bar{\Upsilon}$ represents lateral acceleration given by

$$\bar{\Upsilon} \in \{\bar{g}_i\}, \qquad i = 1, 2 \tag{32}$$

$$\bar{g}_1 = \{\ddot{y} \in \mathbb{R} | |\ddot{y}| \leq |\ddot{y}_1|\} \tag{33}$$

$$\bar{g}_2 = \{\ddot{y} \in \mathbb{R} | |\ddot{y}| > |\ddot{y}_1|\} \tag{34}$$

Directional control constraint violations often arise due to pilot-induced oscillations [16]. If one or more constraint thresholds is violated d, FSAM logic transfers control to the envelope-aware controller, which then attempts to bring the aircraft within nominal (low risk) bounds. If the envelope-aware controller is not able to maintain the aircraft within the specified bounds d', then FSAM aborts the takeoff.

The overall FSAM DMM for the takeoff is defined by the parallel composition (concurrent execution) of both $\mathcal{A}_{\text{lg}}$ and $\mathcal{A}_{\text{lt}}$. Although the two machines ($\mathcal{A}_{\text{lg}}$ and $\mathcal{A}_{\text{lt}}$) have a similar structure, they may not follow analogous transition sequences. For example, in case of an imminent tail strike during rotation, $\mathcal{A}_{\text{lg}}$ transitions from

$$s_5 \xrightarrow{\bar{\theta}} s_{10} \xrightarrow{V_{\text{lof}}} s_6$$

and $\mathcal{A}_{\text{lt}}$ transitions from

$$s_5' \xrightarrow{V_{\text{lof}}} s_6'$$

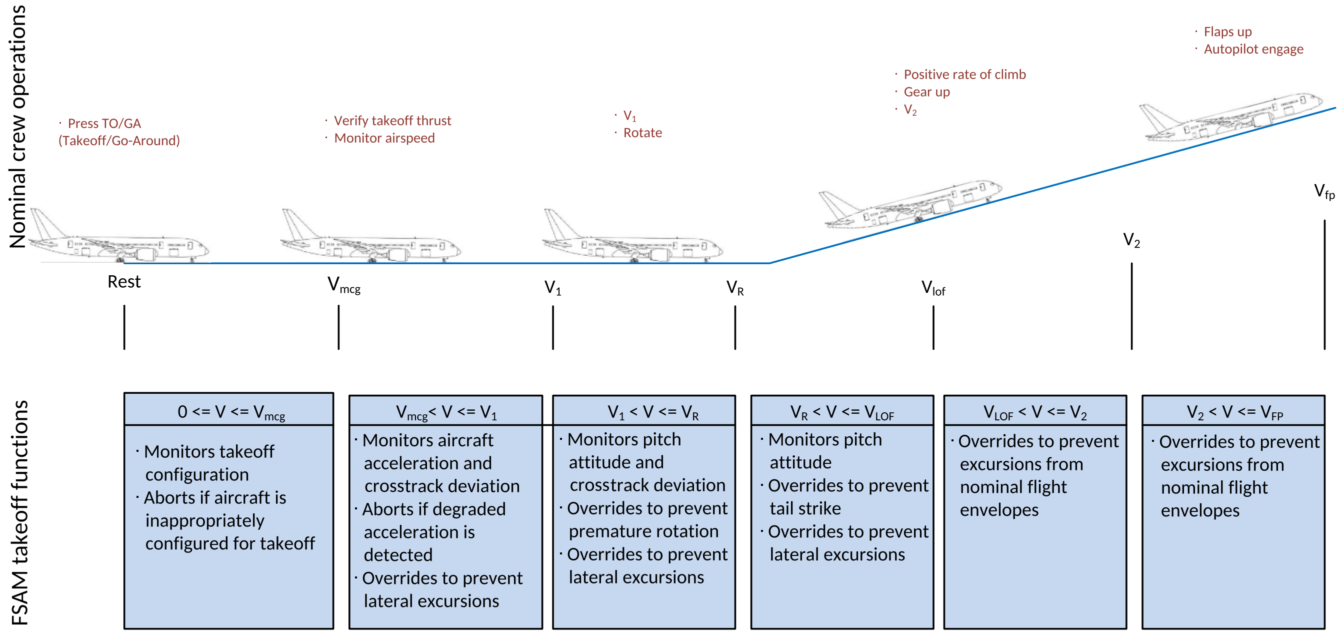
That is, FSAM transfers longitudinal control to the EA controller while retaining directional control with the pilot. This notion of decoupling the longitudinal and directional control authorities, though convenient from a system design perspective, may or may not be welcomed or easily understood by flight crews. Analyzing the benefits of a coupled versus decoupled FSAM formulation would require human subject evaluations beyond the scope of this work. Figure 12 indicates the role of the flight crew and FSAM during takeoff.

VI. Case Studies

In this section, we present case studies to illustrate and evaluate use of FSAM for takeoff. Each case study is based on accident data obtained from the flight data recorders.

A. Loss of Directional Control in Continental Airlines Flight 1404

The behavior and effectiveness of FSAM's takeoff DMM were first analyzed using a case study based on the Continental Airlines Flight 1404 accident [16]. Due to severe crosswinds during takeoff, the Boeing 737 veered off the side of the runway after the pilot failed to maintain directional control. Figure 13 illustrates relevant parameters extracted from the flight data recorder (FDR). After 10 s, the aircraft veered away from the runway heading (heading transitions from 0 to −30 deg) when the crosswinds exceeded 40 kt. The NTSB determined the probable cause of the accident as follows "The captain's cessation of rudder input, which was needed to maintain directional control of the airplane, about four seconds before the excursion, when the airplane encountered strong gusty crosswind that exceeded the captain's training and experience." This is reflected in Fig. 13, showing that the pilot relaxed the rudder pedals following a large rudder input at roughly 5 s.



$0 <= V <= V_{mcg}$
· Monitors takeoff configuration
· Aborts if aircraft is inappropriately configured for takeoff

$V_{mcg} < V <= V_1$
· Monitors aircraft acceleration and crosstrack deviation
· Aborts if degraded acceleration is detected
· Overrides to prevent lateral excursions

$V_1 < V <= V_R$
· Monitors pitch attitude and crosstrack deviation
· Overrides to prevent premature rotation
· Overrides to prevent lateral excursions

$V_R < V <= V_{LOF}$
· Monitors pitch attitude
· Overrides to prevent tail strike
· Overrides to prevent lateral excursions

$V_{LOF} < V <= V_2$
· Overrides to prevent excursions from nominal flight envelopes

$V_2 < V <= V_{FP}$
· Overrides to prevent excursions from nominal flight envelopes

Fig. 12 Flight crew and FSAM functions during takeoff.

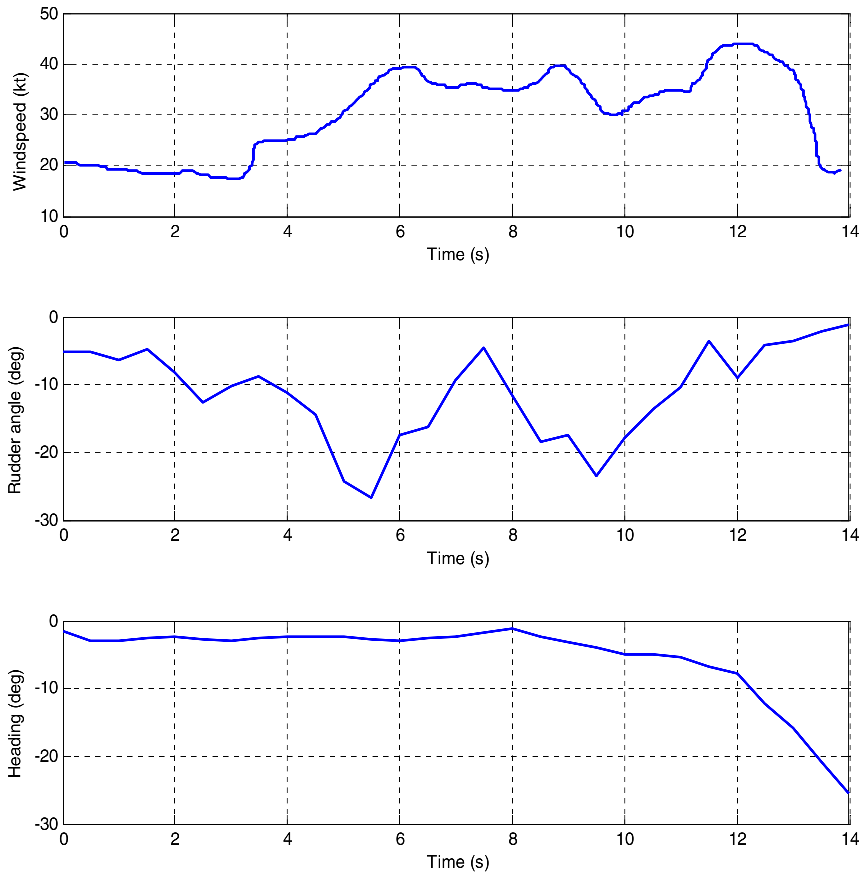


Fig. 13 Accident data from flight data recorder.

To study the behavior of the FSAM DMM for the Flight (FL) 1404 LOC scenario, a lateral runway excursion accident was simulated using data obtained from the FL 1404 FDR (Fig. 14). Details about the physical models, the controller design, and the simulation setup can be found in this paper's appendices. The results of the simulation are shown in Fig. 15. These plots illustrate the dynamics of an aircraft augmented with the FSAM DMM taking off in a severe crosswind. The FSAM DMM transfers lateral control of the aircraft from the pilot to the EA controller when the aircraft exits the inner threshold with respect to heading ($|\psi| > |\psi_1|$) (see Fig. 15). The envelope-aware controller is able to steer the aircraft back within the inner thresholds. After the aircraft is stabilized on the initial departure climb, lateral control is transferred back to the pilot. The execution sequence of the machines is illustrated in Fig. 15. To enable a sensitivity analysis, we also chose different thresholds and crosswind magnitudes. In each scenario, FSAM consistently rejected the takeoff whenever possible [8].

B. Tail Strike and Runway Excursion: Emirates Airlines Flight 407

On 20 March 2009, an Airbus A340 operated by Emirates Airlines failed to takeoff safely from Melbourne Airport, Australia [41]. The flight crew had programmed the flight computer with the wrong weight, which resulted in inadequate thrust application for takeoff. Consequently, the aircraft overshot the runway during the initial takeoff roll and experienced a tail strike due to overrotation. The subsequent flight was uneventful, and the aircraft returned for an emergency landing at the same airport. The actual weight of the aircraft was determined to be 362.9 tons, and the weight entered into the flight computer was 262.9 tons. Figure 16 illustrates the takeoff envelopes of the aircraft for the weight that was entered into

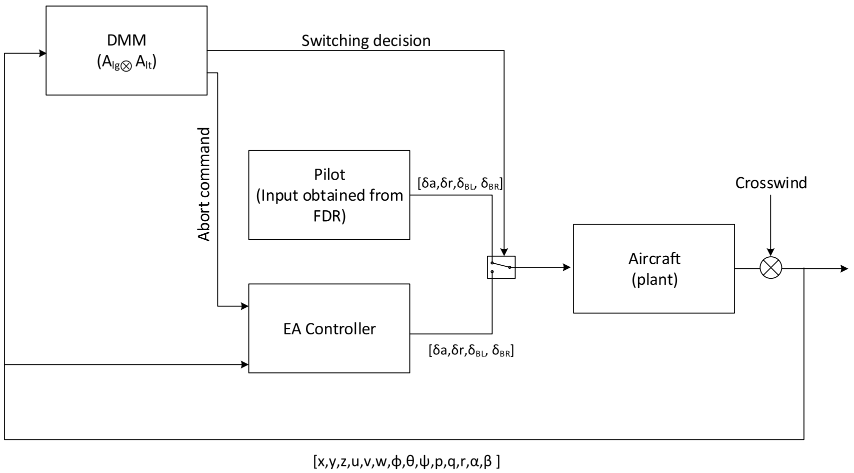


Fig. 14 Simulation setup.

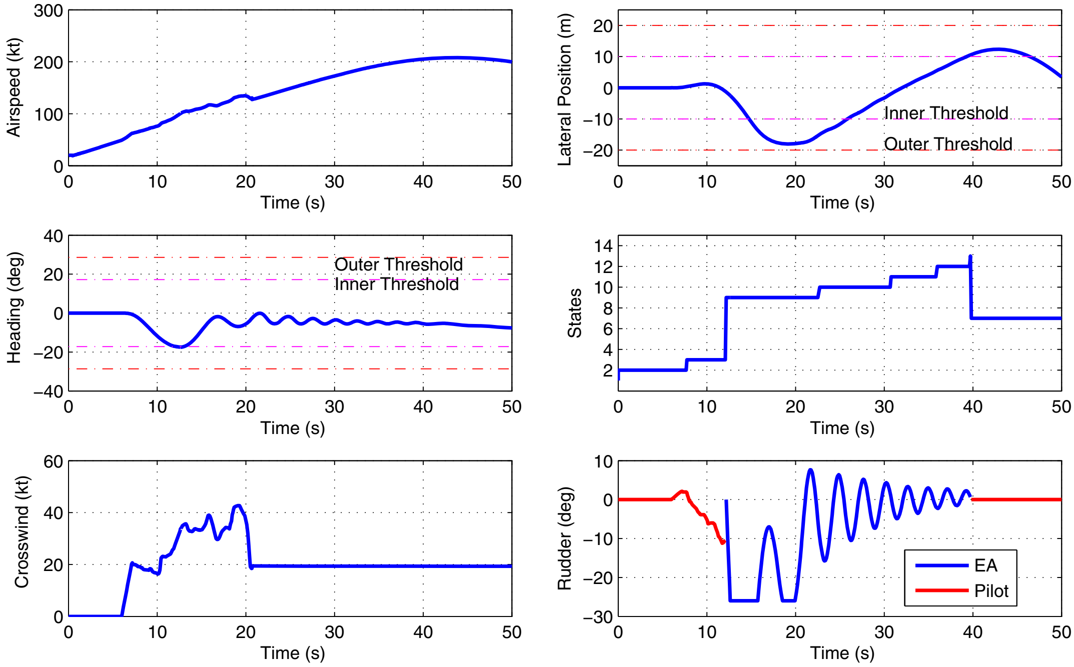


Fig. 15 Continued takeoff scenarios (case study 1).

the flight computer (262.9 tons). If the aircraft was actually loaded at 262.9 tons, it would have followed the trajectory indicated by the solid curve that lies in the safe region of the takeoff envelope. However, the actual trajectory of FL 407 (362.9 tons) veered into the region that is unsafe with respect to continued AEO takeoff. FL 407 began the ground roll with a thrust setting appropriate for a lower weight; hence, as seen in Fig. 16, the aircraft could not achieve a safe liftoff speed V_{lof} before overshooting the runway.

Figure 17 shows the trajectory of the aircraft augmented with both FSAM DMMs. As the aircraft exits the safe envelope with respect to AEO, FSAM triggers a rejected takeoff and the aircraft is safely brought to a stop.

VII. Discussion

The takeoff FSAM DMMs were able to avoid LOC for the two presented case study scenarios but are not yet complete. Although a DMM will only be capable of executing the LOC mitigation sequences for which it has been designed, it would be possible to construct a DMM database that identifies and reacts to a broad suite of known risk factors, e.g., see Fig. 3. Ultimately, if FSAM encounters a scenario it has not been designed to handle, FSAM must recognize this or at least ensure the crew remains in charge to handle the situation, which is a capability requiring further research. Verifying that FSAM never initiates an override in scenarios for which it was not designed will be the key to safety certification.

The DMMs illustrated in this paper were manually constructed. This process is not scalable to all known risks over all phases of flight. Furthermore, the full suite of FSAM DMMs needs to be collectively verified and validated to assure no unexpected interactions between DMMs will cause inappropriate FSAM response. We are pursing complementary work in verification to ensure FSAM decisions meet safety requirements [38].

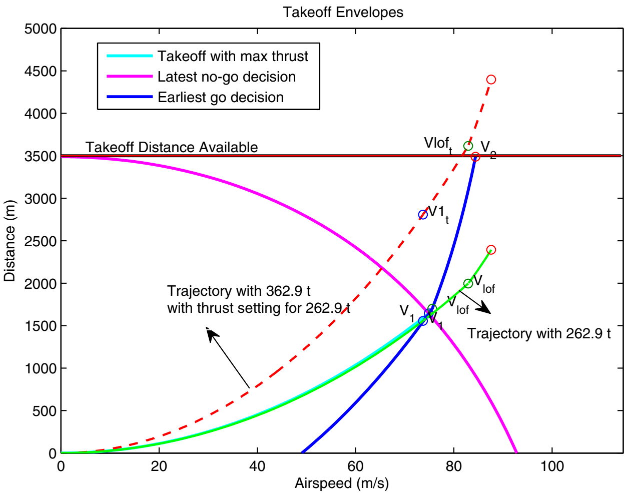


Fig. 16 Takeoff trajectories of Emirates Flight 407 (case study 2).

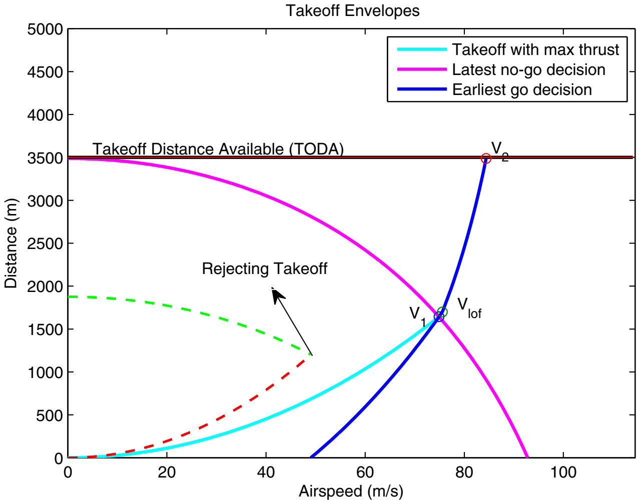


Fig. 17 Takeoff trajectory with FSAM augmentation (case study 2).

VIII. Conclusions

This paper has presented a flight safety assessment and management capability that identifies and mitigates risks associated with loss of control. FSAM initially warns the crew of imminent LOC risks. It overrides to an alternate recovery controller if the crew fail to mitigate the risk. FSAM is formulated as a deterministic Moore machine and applied to the takeoff phase of flight. The FSAM DMM machines are evaluated on case studies motivated by real-world aviation accidents and incidents. Results show that a capable FSAM implementation can potentially avert LOC. This paper contributes a novel formulation to ensure takeoff flight safety using deterministic Moore machines. The nominal sequence of states in the DMMs have a one-to-one correspondence with the typical V-speed decision sequence on which a pilot is trained. Furthermore, envelopes have been developed for the takeoff phase that simplify identification of safe and unsafe regions with respect to longitudinal takeoff dynamics. The takeoff phase in commercial aircraft is the only phase that remains manually flown. The work presented in this paper can play a significant role in ensuring manual control is safe.

For a more comprehensive safety management system, hazards associated with conditions such as instrument failures, actuator failures, structural problems, and other traffic must also be recognized and handled by FSAM. FSAM must also be extend to the other phases of flight. The DMM will ultimately require verification before certification and must be integrated into an informative crew interface display for manned transport applications. The decision system described in this paper can ultimately be extended to provide a comprehensive and verified means of avoiding LOC, which is the leading cause of aviation accidents today.

Appendix A: Takeoff Dynamics

This appendix describes aircraft dynamics for takeoff. Modeling ground roll dynamics of the aircraft requires the knowledge of the reaction forces and moments exerted by the ground on the airframe [43], as well as aerodynamic forces that become significant as airspeed progressively increases during the takeoff roll.

Aircraft landing gear is modeled as a spring-mass-damper system for each assembly [44,45]. Based on knowledge of inertial position and velocity of the center of gravity (CG) and attitude of the aircraft, one can estimate the compression and rate of compression of the oleo struts and then compute the normal forces and moments exerted by the ground on the airframe.

Assuming that the three struts are exactly vertical, the normal force F_z exerted by the ground on the aircraft (expressed in the inertial frame) is given by

$$F_{z_i} = -K_i z_i - C_i \dot{z}_i i = N_w, L_w, R_w \tag{A1}$$

K_i and C_i are the spring constants and the damping coefficients of the nose, as well as the left and right oleo struts of the landing gear. The compression and rate of compression of the oleo struts expressed in the inertial frame are z and $\dot{z}$. N_w, L_w, and R_w represent the nose, and the left and right wheels. The gear model is shown in Fig. A1.

The wheels experience friction due to contact between the tire and runway surface. We assume that the wheels are rigid to simplify the friction model [46]. Longitudinal forces acting on the wheels are due to the longitudinal slip and the normal forces experienced by the wheels. The longitudinal slip ratio is given by

$$\sigma_s = \frac{V_x - \omega R_0}{V_x} \tag{A2}$$

where V_x is the translational velocity of the wheel in the longitudinal direction, ω is angular velocity of the wheel, and R_0 is wheel radius including tire.

The coefficient of friction μ is related to the longitudinal slip ratio σ_s of the wheels by the empirical formula known as the "magic formula" [47]:

$$\mu = \bar{D}\ \sin(\bar{C} \tan^{-1}(\bar{B}\sigma_s)) \tag{A3}$$

Here, $\bar{B}$, $\bar{C}$, and $\bar{D}$ are constants pertaining to the runway surface type. The longitudinal frictional forces F_x exerted by the ground on the wheel are given by

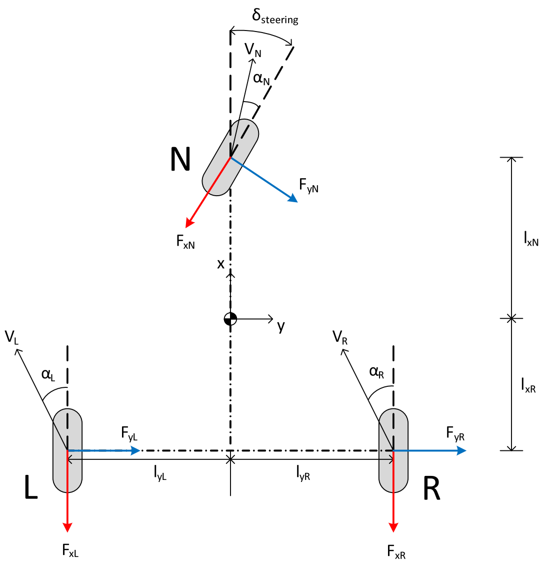


Fig. A1 Tricycle landing-gear configuration.

$$F_{x_i} = \mu_i F_{z_i} \qquad i = N_w, L_w, R_w \tag{A4}$$

The wheels also experience side force F_y due to lateral slip of the wheels. The lateral slip ratio α_s is given by

$$\alpha_{s_i} = \tan^{-1}\left(\frac{v + rl_{xi}}{u - rl_{yi}}\right) i = L_w, R_w \tag{A5}$$

$$\alpha_{s_{N_w}} = -\delta_{\text{steer}} + \tan^{-1}\left(\frac{v + rl_{xN}}{u}\right) \tag{A6}$$

Here, (u, v) are the (x, y) components of the aircraft velocity in the body frame, respectively. l_{yi} and l_{xi} are the distances of the wheels from the CG, as shown in Fig. A1. The nose wheel steering angle is δ_{steer}. The side force F_y is given by [45,46]

$$F_{y_i} = \frac{2F_{y_{\max_i}} \alpha_{s_{\text{opt}_i}} \alpha_{s_i}}{\alpha^2_{s_{\text{opt}_i}} + \alpha^2_{s_i}} \qquad i = N_w, L_w, R_w \tag{A7}$$

Here, $F_{y_{\max}}$ is the maximum attainable side force at the optimal slip angle α_{opt}. $F_{y_{\max}}$ and α_{opt} are experimentally derived parameters [44,45]:

$$F_{y_{\max} N_w} = -3.53 \times 10^{-6} F^2_{zN_w} + 8.33 \times 10^{-1} F_{zN_w} \tag{A8}$$

$$F_{y_{\max} L_w, R_w} = -7.39 \times 10^{-7} F^2_{zL_w,R_w} + 5.11 \times 10^{-1} F_{zL_w,R_w} \tag{A9}$$

$$\alpha_{s_{\text{opt}_N}} = 3.52 \times 10^{-9} F^2_{zN_w} + 2.8 \times 10^{-5} F_{zN_w} + 13.8 \tag{A10}$$

$$\alpha_{s_{\text{opt}_{L,R}}} = 1.34 \times 10^{-10} F^2_{zL_w,R_w} + 1.06 \times 10^{-5} F_{zL_w,R_w} + 6.72 \tag{A11}$$

The net ground reaction force components F_x, F_y, and F_z can be computed as shown in Eqs. (A1), (A4), and (A7). The moments M_x, M_y, and M_z, due to the reaction forces, can be obtained by taking the product of the reaction forces and the respective moment arms about the aircraft center of gravity.

The net ground reaction forces and moments are transformed into the aircraft body frame. The transformed forces and moments can then be added to the conventional six-degree-of-freedom aircraft equations of motion [48] to obtain the complete nonlinear set of equations that simulate the takeoff phase of flight. The takeoff equations of motion (expressed in body frame) are given by the following:

Translational momentum:

$$m(\dot{u} - vr + wq) = -(\sin\theta)mg - (\cos\beta)(\cos\alpha)\mathcal{D} + (\sin\alpha)\mathcal{L} + (\cos\phi_T)F_T + F_{x_{\mathrm{gear}}} \tag{A12}$$

$$m(\dot{v} + ur - wp) = (\sin\phi)(\cos\theta)mg - (\sin\beta)\mathcal{D} + F_{y_{\mathrm{gear}}} \tag{A13}$$

$$m(\dot{w} - uq + vp) = (\cos\phi)(\cos\theta)mg - (\cos\beta)(\sin\alpha)\mathcal{D} - (\cos\alpha)\mathcal{L} - (\sin\phi_T)F_T + F_{z_{\mathrm{gear}}} \tag{A14}$$

Rotational momentum:

$$I_{xx}\dot{p} + (I_{zz} - I_{yy})qr - I_{xz}(\dot{r} + pq) = L_{\mathrm{aero}} + L_{\mathrm{thrust}} + L_{\mathrm{gear}} \tag{A15}$$

$$I_{yy}\dot{q} + (I_{xx} - I_{zz})pr + I_{xz}(p^2 - r^2) = M_{\mathrm{aero}} + M_{\mathrm{thrust}} + M_{\mathrm{gear}} \tag{A16}$$

$$I_{zz}\dot{r} + (I_{yy} - I_{xx})pq + I_{xz}(qr - \dot{p}) = N_{\mathrm{aero}} + N_{\mathrm{thrust}} + N_{\mathrm{gear}} \tag{A17}$$

Wheel dynamics:

$$I_{w_N}\dot{\omega}_N = F_{x_N}R_{\mathrm{wheel}_N} \tag{A18}$$

$$I_{w_L}\dot{\omega}_L = F_{x_L}R_{\mathrm{wheel}_L} + \tau_{\mathrm{brake}_L} \tag{A19}$$

$$I_{w_R}\dot{\omega}_R = F_{x_R}R_{\mathrm{wheel}_R} + \tau_{\mathrm{brake}_R} \tag{A20}$$

Here, u, v, and w represent the translational velocity in the aircraft body frame; and p, q, and r are the body frame angular rates. The roll, pitch, and yaw angles are ϕ, θ, and ψ; $\mathcal{L}$ and $\mathcal{D}$ are the total lift and drag, respectively; F_T is the total thrust force; and ϕ_T represents the angl, the thrust vector makes with the longitudinal axis. L_i, M_i, and N_i are the roll, pitch, and yaw moments where $i =$ aero, $i =$ thrust, and $i =$ gear represent moments induced by aerodynamic, thrust, and gear forces, respectively. I_{xx}, I_{yy}, I_{zz}, and I_{xz} are the moments of inertia of the aircraft; I_w is the moment of inertia of the wheel; R_{wheel} is the radius of the wheel; and τ_{brake} is the braking torque produced on the wheels due to the application of brakes. Equations (A18–A20) model the effect of differential braking during the ground roll [43].

Appendix B: Controller Design

In Sec. VI.A, we used a simple proportional-integral derivative (PID) control framework, as illustrated in Fig. B1. There are two parallel PID controllers. One actuates the brakes to maintain a zero crosstrack error, whereas the other controller actuates the rudder to track a particular reference heading. The gains for the two PID controllers were tuned manually. The brake controller was tuned to yield reasonable runway centerline tracking performance in the low-airspeed regime. The rudder controller was tuned to yield adequate tracking performance in the high-airspeed regime during takeoff.

The use of differential braking enables the controller to counteract crosswind forces, especially while the rudder is ineffective at low airspeeds. Figure B2 illustrates the aircraft's lateral response (crosstrack error) to a constant crosswind of 16 kt under different scenarios. From Fig. B2, it can be seen that the aircraft veers off the runway due to the crosswind when no control input is applied. With braking input alone (right brake input of 800 N · m), the aircraft can maintain runway centerline at low airspeeds. At higher airspeeds, braking does not provide sufficient cornering forces to counteract the crosswind. The rudder input alone is ineffective at low airspeeds; however, as the airspeed increases, the rudder's effectiveness increases to provide a sufficient yawing moment to return to the runway centerline. When rudder and braking are both used to maintain the runway centerline, the aircraft can be controlled with very small deviations from the centerline.

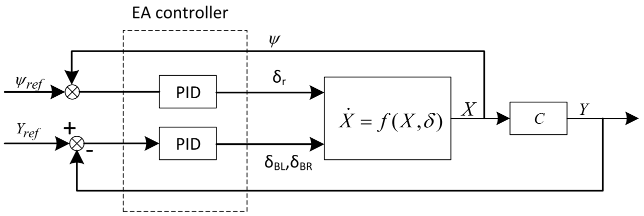


Fig. B1 Envelope-aware controller architecture used on the nonlinear aircraft plant.

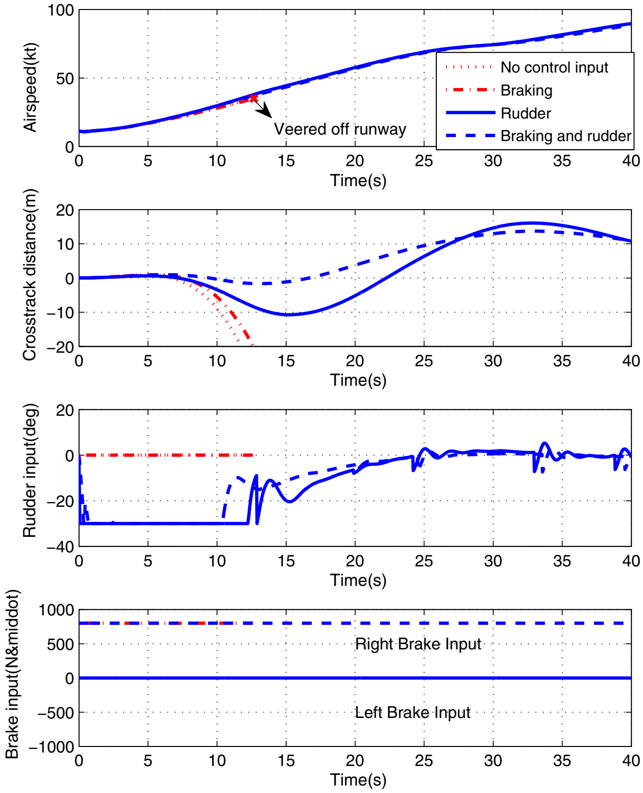


Fig. B2 Comparison of aircraft lateral response with braking and rudder control inputs.

Appendix C: Parameters Used

The takeoff weight of the aircraft is 45,420 kg. The inertia properties of the aircraft are $Ixx = 0.2262 \times 10^7$ Kg · m^2, $Iyy = 0.3172 \times 10^7$ Kg · m^2, $Izz = 0.3337 \times 10^7$ Kg · m^2, and $Ixz = -0.15 \times 10^4$ Kg · m^2. The planform area is 122.4 m^2, and wing span is 34.10 m. The mean chord length is 4.194 m. The aerodynamic forces and moments in Eqs. (A12–A17) are obtained from the NASA generic transport model [49]. The landing-gear parameters are chosen to ensure that the spring-mass-damper model, shown in Eq. (A1), has sufficient damping characteristics. The spring constants are $K_{L_w} = K_{R_w} = 2 \times 10^5$ N · m^{-1}, and $K_{N_w} = 4 \times 10^4$ N · m^{-1}. The damping coefficients are $C_{L_w} = C_{R_w} = 1.5 \times 10^5$ N · s · m^{-1}, and $C_{N_w} = 5.0 \times 10^4$ N · s · m^{-1}. Landing-gear offsets from the center of gravity, as shown in Fig. A1, are $l_{x_N} = 10$ m, $l_{xR} = l_{xL}\_= 2.932$ m, $l_{yL} = -3.795$ m, and $l_{yR} = -l_{yL}$. The friction parameters in Eq. (A3) correspond to a dry tarmac runway and are given by $B = 10$, $C = 1.9$, and $D = 1$. The total takeoff thrust over both engines is 160 kN.

Acknowledgments

This work was supported in part by NASA under cooperative agreement NNX12AM54A. The authors would like to thank Dennis Bernstein, Ilya Kolmanovsky, Kevin McDonough, Ming-Jui Yu, and Pedro Di Donato for their support and feedback. The authors gratefully acknowledge John Broderick for sharing his knowledge on friction models and the motion of ground robots.

References

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

[2] Gregg, F. B., “Boeing B-777: Fly-By-Wire Flight Controls,” *The Avionics Handbook*, CRC Press, Boca Raton, FL, 2001, Chap. 11.

[3] Briere, D., and Traverse, P., “AIRBUS A320/A330/A340 Electrical Flight Controls A Family of Fault Tolerant Systems,” *23rd International Symposium on Fault-Tolerant Computing (FTCS-23)*, IEEE Publ., Piscataway, NJ, 1993, pp. 616–623.

[4] Well, H. K., “Aircraft Control Laws for Envelope Protection,” *AIAA Guidance, Navigation, and Control Conference and Exhibit*, AIAA Paper 2006-6055, 2006.

[5] Kochenderfer, M. J., and Chryssanthacopoulos, J. P., “A Decision-Theoretic Approach to Developing Robust Collision Avoidance Logic,” *Annual Conference on Intelligent Transportation Systems*, IEEE Publ., Piscataway, NJ, 2010.

[6] Lygeros, J., and Lynch, N., “On the Formal Verification of the TCAS Conflict Resolution Algorithms,” *Proceedings of the 36th IEEE Conference on IEEE Decision and Control*, Vol. 2, IEEE Publ., Piscataway, NJ, 1997, pp. 1829–1834.

[7] Balachandran, S., and Atkins, E. M., “Flight Safety Assessment and Management During Takeoff,” *AIAA Infotech@Aerospace Conference*, AIAA Paper 2013-4805, 2013.

[8] Balachandran, S., and Atkins, E. M., “An Evaluation of Flight Safety Assessment and Management to Avoid Loss of Control During Takeoff,” *AIAA Guidance, Navigation, and Control Conference*, AIAA Paper 2014-0785, 2014.

[9] Yi, G., Zhong, J., Atkins, E. M., and Wang, C., “Trim State Discovery with Physical Constraints,” *Journal of Aircraft*, Vol. 52, No. 1, 2015, pp. 90–106. doi:10.2514/1.C032619

[10] McDonough, K., Kolmanovsky, I., and Atkins, E. M., “Recoverable Sets of Initial Conditions and Their Use for Aircraft Flight Planning After a Loss of Control Event,” *AIAA Guidance, Navigation, and Control Conference*, AIAA Paper 2014-0786, 2014.

[11] Yu, M. J., McDonough, K., Bernstein, D. S., and Kolmanovsky, I., “Retrospective Cost Model Refinement for Aircraft Fault Signature Detection,” *Proceedings of the American Control Conference*, IEEE Publ., Piscataway, NJ, 2014, pp. 2486–2491.

[12] McDonough, K., Kolmanovsky, I., and Atkins, E. M., “Recoverable Sets of Initial Conditions and Their Use for Aircraft Flight Planning After a Loss of Control Event,” *AIAA Guidance, Navigation, and Control Conference*, AIAA Paper 2014-0786, 2014.

[13] Gigante, G., and Pascarella, D., "Formal Methods in Avionic Software Certification: the DO-178C Perspective," *Leveraging Applications of Formal Methods, Verification and Validation. Applications and Case Studies*, Springer, New York, 2012, pp. 205–215.

[14] Hopcroft, J. E., *Introduction to Automata Theory, Languages, and Computation*, Pearson Education, Noida, India, 1979, pp. 38–83, Chap. 2.

[15] "Northwest Airlines, INC; McDonnnell Douglas DC 9-82, N312RC, Detroit Metropolitan Wayne County Airport, Romulus, Michigan, August 16, 1987," National Transportation Safety Board Accident Rept. NTSB/AAR-85/05, 1988, http://libraryonline.erau.edu/online-full-text/ntsb/aircraft-accident-reports/AAR88-05.pdf [retrieved Dec. 2012].

[16] "Runway Side Excursion During Attempted Takeoff in Strong and Gusty Crosswind Conditions-Continental Airlines Flight 1404, Boeing 737-500, N18611," National Transportation Safety Board Accident Rept. NTSB/AAR-10/04, 2008.

[17] Borst, C., Grootendorst, F. H., Brouwer, D. I. K., Bedoya, C., Mulder, M., and van Paassen, M. M., "Design and Evaluation of a Safety Augmentation System for Aircraft," *Journal of Aircraft*, Vol. 51, No. 1, 2013, pp. 12–22.
doi:10.2514/1.C031500

[18] Gingras, D. R., Barnhart, B., Ranaudo, R., Ratvasky, T. P., and Morelli, E., "Envelope Protection for In-Flight Ice Contamination," *47th AIAA Aerospace Sciences Meeting*, AIAA Paper 2009-1458, 2009.

[19] Armand, J., Lignee, R., and Villaume, F., "The Runway Overrun Prevention System," *Safety First: The Airbus Safety Magazine* [online database], No. 8, Airbus S.A.S, Blagnac, France, July 2009, http://www.ukfsc.co.uk/information/safety-briefings-presentations/335-airbus-safety-first-magazine.

[20] Bak, S., Manamcheri, K., Mitra, S., and Caccamo, M., "Sandboxing Controllers for Cyber-Physical systems," *2011 IEEE/ACM International Conference on IEEE Cyber-Physical Systems (ICCPS)*, IEEE Publ., Piscataway, NJ, 2011, pp. 3–12.

[21] Belcastro, C. M., and Jacobson, S. R., "Future Integrated System Concepts for Preventing Aircraft Loss-of-Control Accidents," *AIAA Guidance, Navigation, and Control Conference*, AIAA Paper 2010-8142, 2010.

[22] Govindarajan, N., De Visser, C., Van Kampen, E., Krishnakumar, K., Barlow, J., and Stepanyan, V., "Optimal Control Framework for Estimating Autopilot Safety Margins," *Journal of Guidance, Control, and Dynamics*, Vol. 38, No. 7, 2015, pp. 1197–1207.
doi:10.2514/1.G000271

[23] McDonough, K., and Kolmanovsky, I., "Integrator Resetting for Enforcing Constraints in Aircraft Flight Control Systems," *AIAA Guidance, Navigation, and Control Conference*, AIAA Paper 2015-1995, 2015.

[24] Lombaerts, T., Schuet, S. R., Wheeler, K. R., Acosta, D. M., and Kaneshige, J. T., "Safe Maneuvering Envelope Estimation Based on a Physical Approach," *AIAA Guidance, Navigation, and Control Conference*, AIAA Paper 2013-4618, 2013.

[25] Lombaerts, T., Schuet, S., Acosta, D., Kaneshige, J., Shish, K., and Martin, L., "Piloted Simulator Evaluation of Maneuvering Envelope Information for Flight Crew Awareness," *AIAA Guidance, Navigation, and Control Conference*, AIAA Paper 2015-1546, 2015.

[26] Schuet, S., Lombaerts, T., Acosta, D., Wheeler, K., and Kaneshige, J., "An Adaptive Nonlinear Aircraft Maneuvering Envelope Estimation Approach for Online Applications," *AIAA Guidance, Navigation, and Control Conference*, AIAA Paper 2014-0268, 2014.

[27] Srivatsan, R., Downing, R. D., and Bryant, H. W., "Development of Takeoff Performance Monitoring System," *Journal of Guidance, Control, and Dynamics*, Vol. 10, No. 5, 1987, pp. 433–440.
doi:10.2514/3.20237

[28] Milligan, M. W., Zhou, M. M., and Wilkerson, H. J., "Monitoring Airplane Takeoff Performance: Prototype Instrument with Learning Capability," *Journal of Guidance, Control, and Dynamics*, Vol. 32, No. 4, 1995, pp. 768–772.
doi:10.2514/3.46789

[29] Zammit-Mangion, D., and Eshelby, M., "Simplified Algorithm to Model Aircraft Acceleration During Takeoff," *Journal of Aircraft*, Vol. 45, No. 4, 2008, pp. 1090–1097.
doi:10.2514/1.22966

[30] Verspay, J., and Khatwa, R., "A Comparative Evaluation of Three Take-Off Performance Monitor Display Types," *Flight Simulation and Technologies: AIAA Guidance, Navigation, and Control and Colocated Conferences*," AIAA Paper 1993-3608, 1993.
doi:10.2514/6.1993-3608

[31] Inagaki, T., and Itoh, M., "Situation-Adaptive Autonomy: The Potential for Improving Takeoff Safety," *Proceedings of the 6th IEEE International Workshop on Robot and Human Communication, RO-MAN '97*, IEEE Publ., Piscataway, NJ, 1997, pp. 302–307.
doi:10.1109/ROMAN.1997.647000

[32] Inagaki, T., "Situation-Adaptive Autonomy: Dynamic Trading of Authority Between Human and Automation," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 44, Sage Publ., Thousand Oaks, CA, 2000, pp. 13–16.

[33] "Pilot Guide to Takeoff Safety," *Takeoff Safety Training Aid*, Federal Aviation Authority, Nov. 2012, http://www.faa.gov/other_visit/aviation_industry/airline_operators/training/media/takeoff_safety.pdf [retrieved 2015].

[34] Roskam, J., and Lan, C. T. E., *Airplane Aerodynamics and Performance*, DARcorporation, Lawrence, KS, 1997, pp. 435–507, Chap. 10.

[35] Belcastro, C. M., Newman, R. L., Crider, D. A., Groff, L., Foster, J. V., Klyde, D. H., and Huston, A. M., "Preliminary Analysis of Aircraft Loss of Control Accidents: Worst Case Precursor Combinations and Temporal Sequencing," *AIAA Guidance, Navigation, and Control Conference*, AIAA Paper 2014-0612, 2014.

[36] "Reducing the Risk of Runway Excursions: Report of the Runway Safety Initiative," Flight Safety Foundation, Alexandria, VA, 2009, http://www.skybrary.aero/bookshelf/books/900.pdf [retrieved Sept. 2012].

[37] Baier, C., and Katoen, J. P., *Principles of Model Checking*, Vol. 26202649, MIT Press, Cambridge, MA, 2008, pp. 19–82, Chap. 2.

[38] Balachandran, S., Ozay, N., and Atkins, E. M., "Verification Guided Refinement of a Flight Safety Assessment and Management System," *Journal of Aerospace Information Systems* (submitted for publication).

[39] Savage, J. E., *Models of Computation: Exploring the Power of Computing*, Addison-Wesley, Reading, MA, 1998, pp. 153–207, Chap. 4.

[40] Moore, E. F., "Gedanken-Experiments on Sequential Machines," *Automata Studies*, Vol. 34, Princeton Univ. Press, Princeton, NJ, April 1956, pp. 129–153.

[41] "Tailstrike and Runway Overrun, Melbourne Airport, Victoria," Australian Transportation Safety Bureau Accident Rept. AO-2009-012, Australian Capital Territory, Canberra, Australia, 2009, http://www.atsb.gov.au/publications/investigation_reports/2009/aair/ao-2009-012.aspx [retrieved 2015].

[43] York, B. W., and Alaverdi, O., "A Physically Representative Aircraft Landing Gear Model for Real Time Simulations," U.S. Naval Air Warfare Center Aircraft Division Rept. 19960916-028, 1996, http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA314062 [retrieved March 2012]; also AIAA Paper 1996-3506, 1996.

[44] Rankin, J., "Bifurcation Analysis of Nonlinear Ground Handling of Aircraft," Ph.D. Thesis, Univ. of Bristol, Bristol, England, U.K., 2010.

[45] Wong, J., *Theory of Ground Vehicles*, Wiley-Interscience, Hoboken, NJ, 2010, pp. 3–84.

[46] Canudas-de Wit, C., Tsiotras, P., and Velenis, E., "Dynamic Friction Models for Longitudinal Road/Tire Interaction: Theoretical Advances," *Vehicle System Dynamics*, Vol. 39, No. 3, 2003, pp. 189–226.
doi:10.1076/vesd.39.3.189.14152

[47] Pacejka, H., *Tyre and Vehicle Dynamics*, Elsevier, Oxford, 2006, pp. 150–202.

[48] Stevens, L. B., and Lewis, L. F., *Aircraft Control and Simulation*, Wiley, Hoboken, NJ, 2003.

[49] Grauer, J. A., and Morelli, E. A., "A Generic Nonlinear Aerodynamic Model for Aircraft," *Proceedings of AIAA Atmospheric Flight Mechanics Conference*, AIAA Paper 2014-0542, 2014.

J. How
Associate Editor