



An Evaluation of Flight Safety Assessment and Management to avoid Loss of Control during Takeoff

Sweewarman Balachandran* and Ella M. Atkins†

This paper illustrates the application of a novel flight safety assessment and management (FSAM) system designed to assist a flight crew in avoiding loss of control (LOC) situations. Nominally, this system serves as a passive monitor, but in high-risk situations, warnings and ultimately override actions are initiated to recover a lower-risk state of operation. In this work, FSAM is applied to the task of preserving safety during takeoff. This paper presents logic and physics-based models that enable FSAM for takeoff. Case studies motivated by takeoff accidents described in National Transportation Safety Board (NTSB) accident dockets are presented to evaluate how well FSAM is able to identify risk, generate context-appropriate warnings, and override only when needed and only when such override will critically reduce risk.

Nomenclature

EA	Envelope Aware feedback controller
FDR	Flight Data Recorder
FMS	Flight Management System
FSAM	Flight Safety Assessment and Management
LOC	Loss of Control
NTSB	National Transportation Safety Board
α, β	Angle of attack, side slip angle
δ_a, δ_r	Aileron and rudder inputs
δ_{BL}, δ_{BR}	Left and right brake inputs
\mathcal{A}_{lg}	Longitudinal automaton
\mathcal{A}_{lt}	Lateral-directional automaton
ϕ, θ, ψ	Roll, pitch and yaw angles
g	Acceleration due to gravity
x, y, z	Aircraft position in the inertial frame

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 type of aircraft, avionics design, crew behavior, 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 an aircraft stall on takeoff, overshoot of the runway, or excursion off the side of the runway. Organizations such as the Flight Safety Foundation² have compiled accident statistics aimed at informing the aviation community of contributing factors leading to loss of control during each phase of flight. 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 under nominal aircraft functionality and environmental conditions.³⁻⁵ During failure, damage, or other exceptional events, decisions have to be made within a short time window. The wrong decisions could lead to an accident. Current Flight Management Systems (FMS) provide substantial data to the flight crew. Information about the flight plan, weather, local terrain, airports, fuel usage and more are available at the press of a button. The crew can use all relevant data to make the appropriate decisions during in-flight

*Graduate Student, Aerospace Engineering, University of Michigan, Ann Arbor, MI 48109, Student Member

†Associate Professor, Aerospace Engineering, University of Michigan, Ann Arbor, MI 48109, Associate Fellow

emergencies although workload and information overload can be issues. These systems form a convenient aid to the manual decision-making process. In case of emergencies, current systems may fail to provide critical information. For example, current FMS were never designed to provide an assessment of the risk 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.⁴ Such information is vital to guide the flight crew in the decision making process during emergencies particularly when real time decisions are required.

Several approaches that address one or more factors that contribute to LOC have been researched. The notion of Safety Augmentation System for aircraft (SafAS) was introduced by Borst et al.⁶ SafAS is an integrated and automated pilot support system that prevents aircraft from veering off course into external hazards like unfavorable weather conditions. The notion of Icing Contamination Envelope Protection (ICEPro) was proposed by Ratvasky et al.⁷ ICEPro helps identify degradations in airplane performance and flying qualities resulting from ice contamination, providing cues to pilots. The concept of Aircraft Integrated Resilient Safety Assurance and Failsafe Enhancement (AIRSAFE) was proposed by Belcastro et al.⁸ AIRSAFE focuses on online modeling, safety assessment and resilient control in situations with appreciable LOC risk.

The Flight Safety Assessment and Management (FSAM) system proposed in our previous publication⁹ is consistent with the ideals of AIRSAFE. FSAM is designed to constantly monitor flight conditions for anomalies and to assess risk associated with the current flight conditions. A capable FSAM module improves situational awareness of the flight crew with integrated rather than multiple disparate warnings about potential hazards, and suggests specific recovery actions to the flight crew that will reduce risk. If the flight crew does not respond with the appropriate control actions, FSAM continues to monitor and warn, but it has the ability to override the flight crew in scenarios with high LOC risk.

This paper describes the physical and logic models enabling a prototype FSAM to monitor, warn, and react as needed to enhance the safety of the takeoff phase of flight. Despite the safety-critical nature of the takeoff phase, very little literature has been devoted towards safety management of takeoff. Srivatsan et al¹⁰ proposed a takeoff performance monitoring system that constantly monitors the ground roll performance parameters. Milligan et al¹¹ developed an instrument that predicts the nominal takeoff performance using analytical models and aids the crew in making a safe GO-NO GO decision. For takeoff, LOC translates to a situation in which the aircraft veers off the side or end of the runway, or leaves the ground but in a condition (e.g., insufficient speed) that introduces substantial risk in the subsequent initial departure climb.

FSAM logic is based on timed automata¹² to detect transitions representing nominal flight sequences and transitions between anomalous states of varying risk levels. Timed automata provide tools for analyzing important properties of the underlying real time system over all possible inputs. They are widely used in model checking¹³ to verify properties such as correctness (satisfaction of design requirements), safety (nothing bad will happen) and liveness (something good will eventually happen). The usage of timed automata for modeling the FSAM logic has several advantages. Systems that are used on airplanes undergo a rigorous testing process to ensure that the safety of the aircraft is not compromised. The timed automata framework along with a wide variety of model checking tools, facilitates the safety verification process in a systematic manner. Secondly, representation of the flight control logic as a directed graph also may facilitate flight crew understanding of the Flight Management System and thus may contribute to a better decision making process.

This paper focuses on development and evaluation of takeoff logic in a graphical form understandable to flight crews as well as engineers and on characterizing the interactions between the logic module and the physics of the takeoff model. Section II provides a brief overview of FSAM and introduces the syntax and semantics of the timed automata framework. Section III presents the synthesis of a decision making logic for the takeoff phase of flight using timed automata. Section IV illustrates an application of the logic models with the help of a case study. Section IV also discusses the physics model and control law that we developed for the case study. Finally, section V presents conclusions and extensions of the FSAM logic models for takeoff.

II. Background

A. Flight Safety Assessment and Management (FSAM)

Flight Safety Assessment and Management (FSAM) is part of the Envelope Aware Flight Management System (EA-FMS) proposed in our previous publication⁹ and shown in Fig 1. The EA-FMS consists of a suite

of modules including: FSAM, Adaptive Planning and Guidance, Envelope Estimation, System Identification and Adaptive control. These modules interact with each other as a single unified system with the ultimate goal of preventing LOC. FSAM is the high level decision making module which primarily monitors the aircraft systems, instruments, pilot, autopilot control inputs, and activates warnings under off nominal conditions (i.e., off nominal conditions not identified by conventional flight management computers). FSAM issues resilient control override directives if necessary. Fig 2 illustrates the high level architecture of the FSAM module.

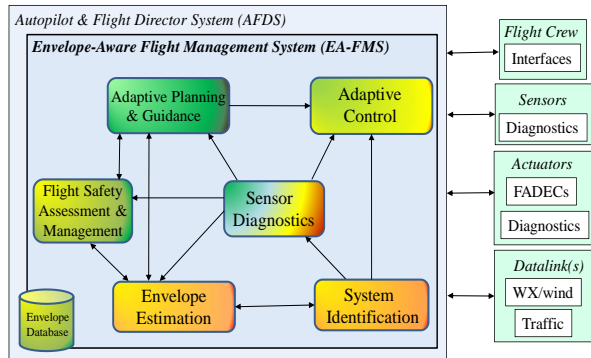


Figure 1. Envelope Aware Flight Management System (EA-FMS)

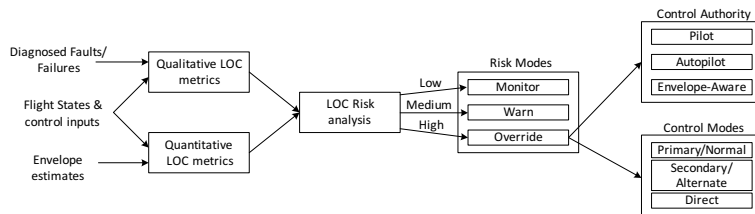


Figure 2. FSAM architecture

B. Deterministic Timed Büchi Automaton

A Deterministic Timed Büchi Automaton (DTBA) is a variant of the timed transition table/timed automaton.¹² A timed automaton can be viewed as an abstraction of a real-time physical system. A DTBA is formally represented as a tuple $(\Sigma, S, S_0, C, F, E)$, where

- Σ is a finite alphabet.
- S is a finite set of states.
- $S_0 \subset S$ is an initial state ($|S_0| = 1$).
- C is a finite set of clocks.
- $E \subseteq S \times S \times \Sigma \times 2^C \times \Phi(C)$ is the set of all transitions. An edge $\langle s, s', a, \lambda, \delta \rangle$ represents a unique transition from a state s to a state s' triggered by the action/event/input symbol a . $\lambda \subseteq C$ is the set of clocks to be reset on this transition, and δ is a clock constraint over C .
- $F \subseteq S$ is a set of final states.

The finite alphabet Σ consists of a non empty set of *symbols*. Each symbol $\sigma_i \in \Sigma$, ($i \in \mathbb{N}$) characterizes an observable event of a process/system. A sequence of symbols is called a *word* or *string* σ . A set of strings chosen from the given alphabet defines a *language* L . A *time sequence* τ is defined as a sequence of strictly monotonically increasing time values τ_i ($i \in \mathbb{R}$). A *timed word* (σ, τ) is a sequence of ordered pairs (σ_i, τ_i)

which is interpreted as the occurrence of the word σ_i at time τ_i . The states in S are chosen to reflect values of the various variables of the system that are of interest. States help to “remember” different configurations of the system. The behavior of the system can be represented by defining *runs* of the timed automaton. A run r , denoted by (\bar{s}, \bar{v}) , of a timed automaton over a timed word (σ, τ) is a sequence of the form

$$r : (s_0, v_0) \xrightarrow[\tau_1]{\sigma_1} (s_1, v_1) \xrightarrow[\tau_2]{\sigma_2} (s_2, v_2) \xrightarrow[\tau_3]{\sigma_3} \dots$$

A run logs the sequence of states s_i and the value of the clocks v_i at the transitions as the physical system executes its tasks.

III. Deterministic Timed Büchi Automata for Takeoff

Takeoff and landing are the highest-risk phases of flight. Contributing factors to loss of control during the takeoff phase have been identified in the literature.² For an aircraft with a given takeoff configuration (takeoff weight, flap/slat settings), several airspeed checkpoints called V-speeds¹⁴ are established to guide the flight crew in making the appropriate decisions for a safe takeoff/rejected takeoff. The most important V speed is V_I , the decision speed by which the flight crew must commit to or reject a takeoff. The flight crew may need to reject a takeoff due to several factors such as single/multiple engine failure, tire burst or a runway incursion.¹⁵ A rejected takeoff initiated after V_I will leave the aircraft with insufficient runway length remaining to stop safely. V_R represents the speed at which the pilot flying (PF) can safely rotate (pull back on the control column/stick) to attain a climb attitude. A premature rotation initiated before V_R can result in a takeoff stall due to insufficient lift.¹⁶

In this section, we present automata that represent a manually constructed strategy to identify and mitigate serious risk due to LOC during takeoff. These strategies are formulated based on a rigorous analysis of numerous aviation accident surveys, accident/incident reports, flight data obtained from the NTSB accident database, aircraft operating manuals, pilot handbooks, checklist procedures and flight control laws from the literature.^{3-5,16,17} The overall takeoff logic is decomposed into two automata for simplicity. Fig 3 illustrates the longitudinal automaton and Fig 4 illustrates the lateral automaton. We assume that the longitudinal and lateral states of the aircraft can be controlled separately.

A. Longitudinal Automaton

The longitudinal automaton governs the decision making process with respect to the longitudinal dynamics of the aircraft during the takeoff phase. It is designed to prevent events that could severely affect the ground roll performance of the aircraft, including inappropriate crew inputs such as improper rejected takeoff procedures and improper rotations. Each state of the automaton captures the critical V speed thresholds described above.

We represent the longitudinal (lg) automaton (\mathcal{A}_{lg}) as the tuple $(\Sigma_{lg}, S_{lg}, S_{lg0}, C_{lg}, F_{lg}, E_{lg})$ where

$$\Sigma_{lg} = \{V_{mcg}, V_1, V_R, V_{lof}, V_2, V_{fp}, T_{idle}, T_{max}, c, c', e, e', \hat{\theta}, \bar{\theta}\} \quad (1)$$

$$S_{lg} = \{s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8, s_9, s_{10}, s_{11}, s_{12}, s_{13}, s_{14}, s_{15}\} \quad (2)$$

$$S_{lg0} = \{s_1\} \quad (3)$$

$$C_{lg} = \{t_1, t_2\} \quad (4)$$

$$F_{lg} = \{s_1, s_{13}, s_{14}, s_{15}\} \quad (5)$$

The transitions E_{lg} are illustrated as edges in the directed graph (Fig 3). The definition of each alphabet symbol in the set Σ_{lg} is provided in Table 1. Table 2 provides descriptions of each state in S_{lg} . In Fig 1, the circles in the directed graph represent a state of the aircraft. A state s in the longitudinal automaton is defined as the quadruple $[\bar{v}, \mathcal{M}, \mathcal{R}, \mathcal{P}]$ where \bar{v} represents an airspeed range and takes values as shown below

$$\bar{v} \in \{\bar{v}_i\}, i = 1, \dots, 8 \quad (6)$$

$$\bar{v}_1 = \{V \in \mathbb{R} \mid V = 0\} \quad (7)$$

$$\bar{v}_2 = \{V \in \mathbb{R} \mid 0 < V \leq V_{mcg}\} \quad (8)$$

$$\bar{v}_3 = \{V \in \mathbb{R} \mid V_{mcg} < V \leq V_1\} \quad (9)$$

$$\bar{v}_4 = \{V \in \mathbb{R} \mid V_1 < V \leq V_R\} \quad (10)$$

$$\bar{v}_5 = \{V \in \mathbb{R} \mid V_R < V \leq V_{lof}\} \quad (11)$$

$$\bar{v}_6 = \{V \in \mathbb{R} \mid V_{lof} < V \leq V_2\} \quad (12)$$

$$\bar{v}_7 = \{V \in \mathbb{R} \mid V_2 < V \leq V_{fp}\} \quad (13)$$

$$\bar{v}_8 = \{V \in \mathbb{R} \mid V > V_{fp}\} \quad (14)$$

\mathcal{M} represents the control mode.

$$\mathcal{M} \in \{\bar{p}, \bar{ap}\} \quad (15)$$

Here \bar{p} denotes that the pilot is in command of the aircraft and \bar{ap} denotes that an “envelope-aware” autopilot system is in command of the aircraft that is sufficiently adaptable or situationally aware to be capable of recovering from the LOC situation. \mathcal{R} represents the risk level associated with the current state.

$$\mathcal{R} \in \{\varepsilon, low, med, high\} \quad (16)$$

ε represents a zero risk state. “*low*, *med* and *high*” represent low, medium and high risk states respectively. \mathcal{P} represents a flag,

$$\mathcal{P} \in \{0, 1\} \quad (17)$$

where $\mathcal{P} = 1$ represents a condition where continuing takeoff is no longer safe because of inappropriate configuration/component failures. $\mathcal{P} = 0$ represents a condition where it is safe to continue takeoff.

Table 1. Alphabet symbols for the Takeoff automata

Alphabet (Σ)	Description
V_{mcg}	Minimum controllable ground speed 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}	Maximum takeoff thrust setting
T_{idle}	Idle thrust setting
c	Aircraft configured for takeoff
c'	Improper takeoff configuration
e	Envelope protection de-activated
e'	Envelope protection activated
$\hat{\theta}$	Positive pitch attitude
$\bar{\theta}$	Maximum allowable pitch attitude reached during rotation
d'	Crossing 1st directional threshold
\bar{d}	Crossing 2nd directional threshold

The longitudinal automaton starts initially in a state of rest (s_1). If the aircraft is configured for takeoff (c) and takeoff thrust is established (T_{max}), the aircraft starts accelerating down the runway and the automaton progresses through the various states sequenced by the V speeds. Thus, the top row of states in Fig 3 represent the nominal transitions the automaton goes through in a typical takeoff phase. At subsequently

higher speeds, the logic monitors the crew inputs to avoid scenarios leading to premature rotation and tail strikes (s_4 and s_5). After liftoff, conventional envelope protection features such as angle of attack and overspeed protections become active.^{3,4} Pushing the aircraft to the limits of the envelope during the 1st and 2nd climb segments (s_6, s_7) leads to a temporary override where control is transferred to the “envelope aware” controller (s_{11}, s_{12}) which prevents the aircraft from crossing envelope boundaries. FSAM reverts control to the flight crew after the aircraft is stabilized on climbout. After the first and second departure climb segments, the takeoff automaton terminates in the climb phase (s_{15}) and the next logic model for the climb phase engages. If the aircraft was inappropriately configured for takeoff, the automaton goes into the takeoff configuration warning state (s_8). s_8 is a state where FSAM issues warnings to the flight crew, alerting them to the risk associated with the inappropriate configuration. If no further action is taken, the automaton goes into the abort state (s_{13}) where it safely rejects the takeoff. This will be safe but surprising to a crew that did not heed warnings.

Table 2. Examples of state representations

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

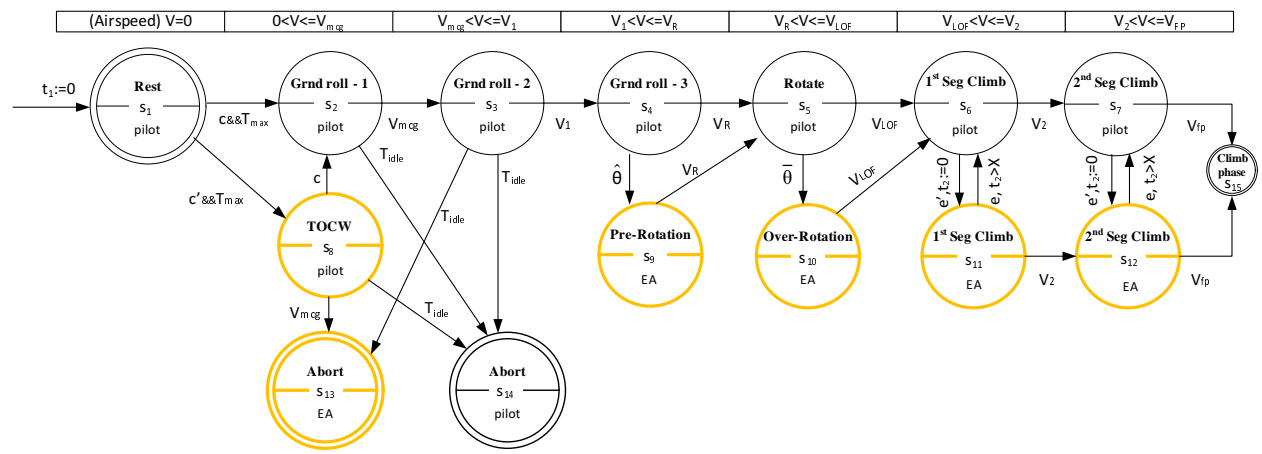


Figure 3. Timed automata for longitudinal takeoff dynamics

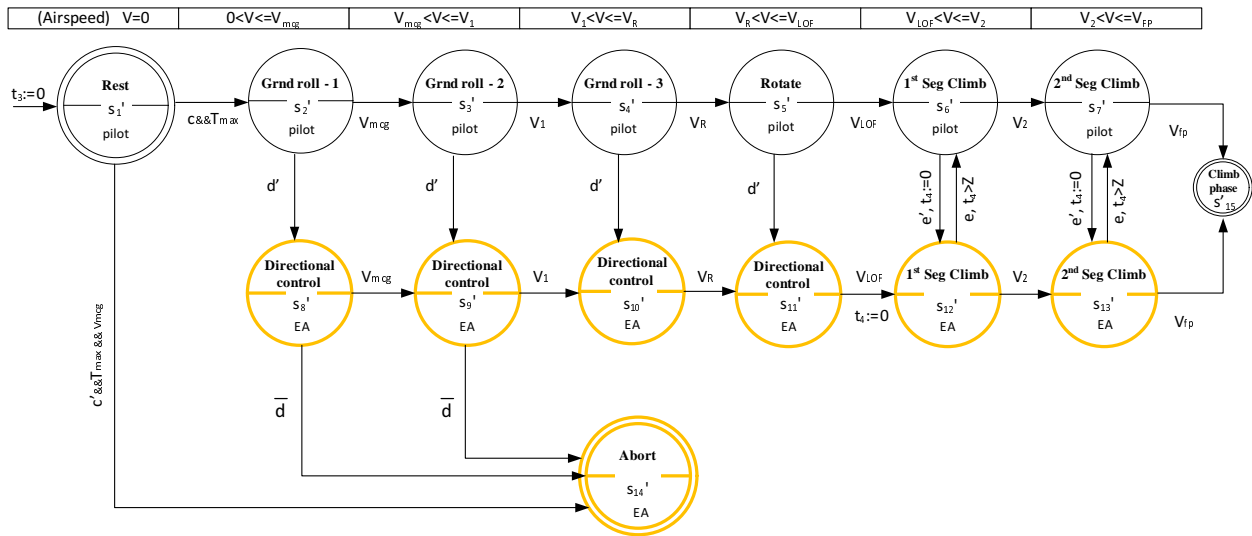


Figure 4. Timed automata for lateral-directional takeoff dynamics

B. Lateral Automaton

The lateral takeoff logic aims to prevent directional control losses during the initial ground roll. Directional control losses can be caused due to severe cross winds/gusts, engine thrust asymmetry, or mistrimmed rudder. Each state imposes bounds on the lateral position of the aircraft from the runway center line, deviations in aircraft's heading from runway heading, and the lateral acceleration of the aircraft (see Fig 5).

The lateral (lt) automaton \mathcal{A}_{lt} is represented by the tuple $(\Sigma_{lt}, S_{lt}, S_{lt0}, C_{lt}, F_{lt}, E_{lt})$.

$$\Sigma_{lt} = \{V_{mcg}, V_1, V_R, V_{lof}, V_2, V_{fp}, T_{idle}, T_{max}, c, c', e, e', d', \bar{d}\} \quad (18)$$

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

$$S_{lt0} = \{s'_1\} \quad (20)$$

$$C_{lt} = \{t_3, t_4\} \quad (21)$$

$$F_{lt} = \{s'_1, s'_{14}, s'_{15}\} \quad (22)$$

Each state s' is defined as the 7 tuple $[\bar{y}, \bar{y}, \bar{\psi}, \bar{g}, \mathcal{M}, \mathcal{R}, \mathcal{P}]$. \bar{y} , \mathcal{M} , \mathcal{R} and \mathcal{P} are defined as in Eqns (6)-(17). \bar{y} represents a range of cross track errors (lateral distance away from the runway center line) as shown below.

$$\bar{y} \in \{\bar{y}_i\}, i = 1, 2, 3 \quad (23)$$

$$\bar{y}_1 = \{y \in \mathbb{R} \mid |y| \leq |y_1|\} \quad (24)$$

$$\bar{y}_2 = \{y \in \mathbb{R} \mid |y_1| < |y| \leq |y_2|\} \quad (25)$$

$$\bar{y}_3 = \{y \in \mathbb{R} \mid |y| > |y_2|\} \quad (26)$$

y_1 and y_2 represent an inner and outer threshold, respectively (see Fig 5). $\bar{\psi}$ represents an inertial heading range

$$\bar{\psi} \in \{\bar{\psi}_i\}, i = 1, 2, 3 \quad (27)$$

$$\bar{\psi}_1 = \{\psi \in [-\pi, \pi] \mid |\psi| < |\psi_1|\} \quad (28)$$

$$\bar{\psi}_2 = \{\psi \in [-\pi, \pi] \mid |\psi_1| \leq |\psi| \leq |\psi_2|\} \quad (29)$$

$$\bar{\psi}_3 = \{\psi \in [-\pi, \pi] \mid |\psi| > |\psi_2|\} \quad (30)$$

Here ψ_1 and ψ_2 represent bounds on the aircraft's heading (see Fig 5). $\bar{\mathcal{G}}$ represents a lateral acceleration range

$$\bar{\mathcal{G}} \in \{\bar{g}_i\}, i = 1, 2 \quad (31)$$

$$\bar{g}_1 = \{\dot{y} \in \mathbb{R} \mid |\dot{y}| \leq |\dot{y}_1|\} \quad (32)$$

$$\bar{g}_2 = \{\dot{y} \in \mathbb{R} \mid |\dot{y}| > |\dot{y}_1|\} \quad (33)$$

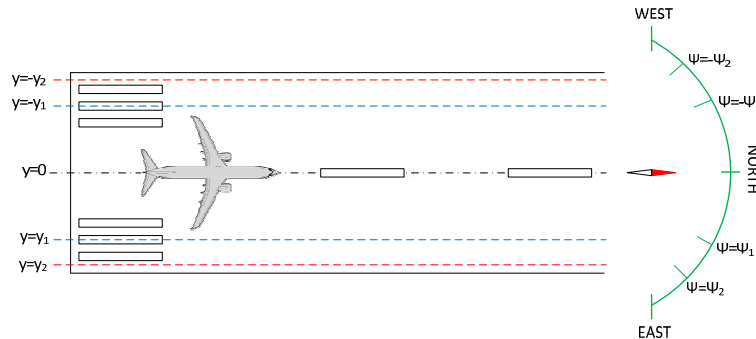


Figure 5. Lateral constraints

Directional control issues during the takeoff roll often arise due to the violation of one or more of the bounds specified above. A directional control loss may result from a pilot induced oscillation (PIO) which eventually leads to the aircraft veering off the side of the runway as in the FL1404 case study discussed below. If one or more of these thresholds were to be violated (d'), FSAM logic transfers control to the envelope-aware controller which then attempts to bring the aircraft within the specified bounds. If the envelope-aware control authority is not able to maintain the aircraft within the specified bounds (\bar{d}), then FSAM aborts the takeoff before the aircraft veers off the runway.

The overall automaton for the takeoff phase comprises the parallel composition of both \mathcal{A}_{lg} and \mathcal{A}_{lt} . We denote this parallel composition as $\mathcal{A}_{lg} \parallel \mathcal{A}_{lt}$. A parallel composition denotes the concurrent execution of the two automata as the aircraft executes a takeoff. Although the two automata (\mathcal{A}_{lg} and \mathcal{A}_{lt}) have a similar structure, they may not have the same transitions. For example, in case of an imminent tail strike during rotation, \mathcal{A}_{lg} transitions from $s_5 \xrightarrow{\bar{\theta}} s_{10} \xrightarrow{V_{lof}} s_6$ and \mathcal{A}_{lt} transitions from $s'_5 \xrightarrow{V_{lof}} s'_6$.

IV. Application of FSAM to prevent LOC during takeoff

In this section we present a case study that illustrates the application of FSAM's timed automata models to prevent LOC during a takeoff roll.

A. Case study: Continental Airlines FL1404

In December 2008, a Boeing 737 (B737) aircraft failed to complete an attempted takeoff from Denver International Airport.¹⁷ During the initial ground roll, the aircraft experienced severe crosswinds (above 35 knots) which pushed the aircraft towards the side of the runway. The pilot was not able to maintain directional control of the aircraft with the appropriate stick and rudder inputs and so the aircraft veered off the side of the runway. There were no fatalities but the aircraft was severely damaged. Fig 6 illustrates select parameters extracted from the Flight Data Recorder (FDR), obtained from the NTSB accident database, to provide a graphical understanding of the events that led to the accident starting from the takeoff roll. The graph shows the crosswind speed, the rudder inputs from the pilot and aircraft heading during the first 14 seconds of the takeoff roll. It is evident from Fig 6 that after 10 seconds, the aircraft deviates from the runway heading (heading deviates from 0^0 to -30^0) when the crosswinds reach over 30 knots. The NTSB determined the probable cause of the accident as “*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 6 as it is evident at around 7 seconds, the pilot relaxes the rudder pedals after the large rudder input at roughly 5 seconds.

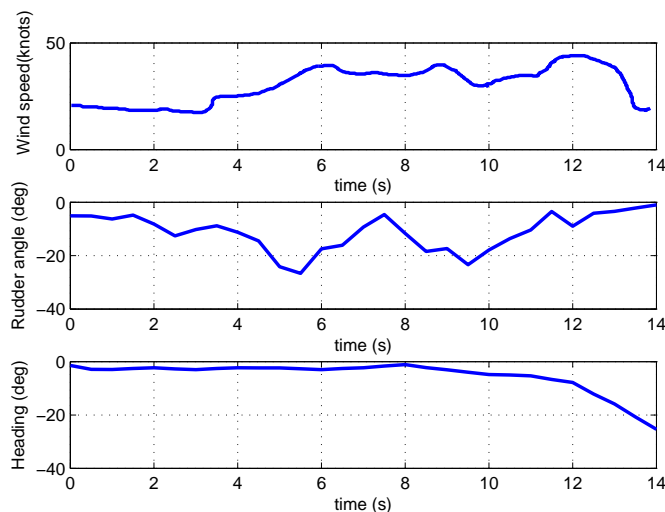


Figure 6. Parameters obtained from Flight Data Recorder(FDR)¹⁷

The aim of this case study is to analyze the behavior of FSAM's timed automata models in response to a LOC scenario, similar to that of FL1404 described above. We developed the following models, described below, to analyze the interactions of FSAM's timed automata with the aircraft dynamics and flight control laws.

- A physics-based model of the takeoff phase to simulate the aircraft's dynamics during the takeoff ground roll and also its responses to crosswinds and gusts.
- A nonlinear controller that is capable of tracking the runway center line in the presence of strong crosswinds to demonstrate FSAM's resilient override capabilities.

B. Takeoff Dynamics

This section discusses the development of the mathematical model that describes the dynamics during the takeoff phase. Modeling the ground roll dynamics of the aircraft requires the knowledge of the reaction forces and moments exerted by the ground on the airframe¹⁸ as well as aerodynamic forces that become significant as airspeed progressively increases during the takeoff roll.

The aircraft is considered as a spring-mass-damper model.^{19,20} The massless springs and damping units represent the oleo struts of the nose, left and right landing gear assemblies. 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 thus 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

$$F_{z_i} = -K_i z_i - C_i \dot{z}_i \quad i = N_w, L_w, R_w \quad (34)$$

K_i and C_i are the spring constants and the damping coefficients of the nose, left and right oleo struts of the landing gear. z and \dot{z} are the compression and rate of compression of the oleo struts expressed in the inertial frame. N_w , L_w and R_w represent the nose, left and right wheels. The gear model is shown in Fig 7.

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.²¹ The longitudinal force acting on the wheels are due to the longitudinal slip and the normal force experienced by the wheels. The longitudinal slip ratio is given by:

$$\sigma_s = \frac{V_x - \omega R_0}{V_x} \quad (35)$$

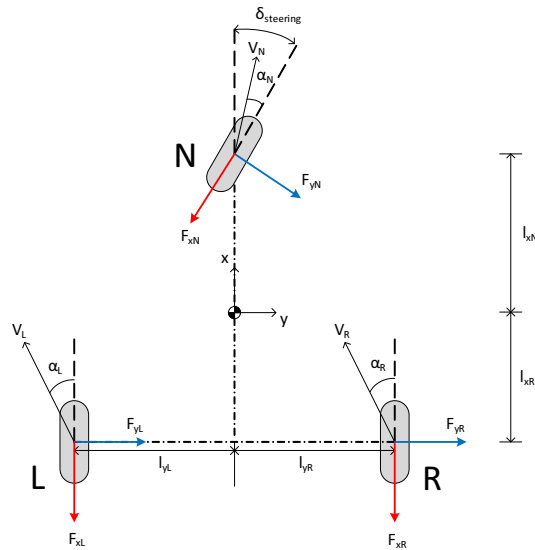


Figure 7. Tri-cycle landing gear configuration

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

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”.²²

$$\mu = \bar{D} \sin(\bar{C} \tan^{-1}(\bar{B} \sigma_s)) \quad (36)$$

Here \bar{B}, \bar{C} and \bar{D} are constants pertaining to the runway surface and are obtained from experimental data. The longitudinal frictional force F_x exerted by the ground on the wheel is given by:

$$F_{x_i} = \mu_i F_{z_i} \quad i = N_w, L_w, R_w \quad (37)$$

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

$$\alpha_{s_i} = \tan^{-1} \left(\frac{v + r l_{x_i}}{u - r l_{y_i}} \right) \quad i = L_w, R_w \quad (38)$$

$$\alpha_{s_{N_w}} = -\delta_{steer} + \tan^{-1} \left(\frac{v + r l_{x_{N_w}}}{u} \right) \quad (39)$$

Here u, v are the x, y components of the aircraft’s velocity in the body frame respectively. l_{y_i} and l_{x_i} are distances of the wheels from the CG as shown in Fig 7. δ_{steer} is the nose wheel steering angle. The side force F_y is given by^{19,20}

$$F_{y_i} = \frac{2F_{y_{max_i}} \alpha_{s_{opt_i}} \alpha_{s_i}}{\alpha_{s_{opt_i}}^2 + \alpha_{s_i}^2} \quad i = N_w, L_w, R_w \quad (40)$$

Here $F_{y_{max}}$ is the maximum attainable side force at the optimal slip angle α_{opt} . The expressions for $F_{y_{max}}$ and α_{opt} are given by^{19,20}

$$F_{y_{max}N_w} = -3.53 \times 10^{-6} F_{z_{N_w}}^2 + 8.33 \times 10^{-1} F_{z_{N_w}} \quad (41)$$

$$F_{y_{max}L_w, R_w} = -7.39 \times 10^{-7} F_{z_{L_w, R_w}}^2 + 5.11 \times 10^{-1} F_{z_{L_w, R_w}} \quad (42)$$

$$\alpha_{s_{opt_N}} = 3.52 \times 10^{-9} F_{z_{N_w}}^2 + 2.8 \times 10^{-5} F_{z_{N_w}} + 13.8 \quad (43)$$

$$\alpha_{s_{optL, R}} = 1.34 \times 10^{-10} F_{z_{L_w, R_w}}^2 + 1.06 \times 10^{-5} F_{z_{L_w, R_w}} + 6.72 \quad (44)$$

The net ground reaction force components F_x , F_y and F_z can be computed as shown in Eqns (34),(37) and (40). The moment components M_x , M_y , 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 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 motion²³ 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 as follows:

- Translational Momentum

$$m(\dot{u} - vr + wq) = -(\sin\theta)mg - (\cos\beta)(\cos\alpha)\mathcal{D} + (\sin\alpha)\mathcal{L} + (\cos\phi_T)F_T + F_{x_{gear}} \quad (45)$$

$$m(\dot{v} + ur - wp) = (\sin\phi)(\cos\theta)mg - (\sin\beta)\mathcal{D} + F_{y_{gear}} \quad (46)$$

$$m(\dot{w} - uq + vp) = (\cos\phi)(\cos\theta)mg - (\cos\beta)(\sin\alpha)\mathcal{D} - (\cos\alpha)\mathcal{L} - (\sin\phi_T)F_T + F_{z_{gear}} \quad (47)$$

- Rotational Momentum

$$I_{xx}\dot{p} + (I_{zz} - I_{yy})qr - I_{xz}(\dot{r} + pq) = L_{aero} + L_{thrust} + L_{gear} \quad (48)$$

$$I_{yy}\dot{q} + (I_{xx} - I_{zz})pr + I_{xz}(p^2 - r^2) = M_{aero} + M_{thrust} + M_{gear} \quad (49)$$

$$I_{zz}\dot{r} + (I_{yy} - I_{xx})pq + I_{xz}(qr - \dot{p}) = N_{aero} + N_{thrust} + N_{gear} \quad (50)$$

- Wheel Dynamics

$$I_{w_N}\dot{\omega}_N = F_{x_N}R_{wheel_N} \quad (51)$$

$$I_{w_L}\dot{\omega}_L = F_{x_L}R_{wheel_L} + \tau_{brake_L} \quad (52)$$

$$I_{w_R}\dot{\omega}_R = F_{x_R}R_{wheel_R} + \tau_{brake_R} \quad (53)$$

Here u, v and w are the components of translational velocity in the aircraft body frame. p, q and r are angular rates. ϕ, θ and ψ are the roll, pitch and yaw attitude angles. \mathcal{L}, \mathcal{D} are lift and drag. F_T is the thrust force and ϕ_T is the angle the thrust vector makes with the longitudinal axis. L, M and N are the roll, pitch and yaw moments. 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. τ_{brake} is the braking torque produced on the wheels due to the application of brakes. Eqns (51)-(53) model the effect of differential braking during the ground roll.¹⁸

C. Controller Design

This section describes the development of a lateral-directional controller for the takeoff phase. We are interested in demonstrating loss of control prevention due to directional control issues as in FL1404 so we focus on the development of a lateral-directional controller to track the runway center line in the presence of disturbances such as crosswinds and gusts. We assume that the longitudinal control of the aircraft is open loop.

An aircraft flying at a trim condition is in equilibrium so one can compute a linearized feedback control law to achieve the required closed loop behavior. However, an aircraft accelerating down the runway during the takeoff phase is not in equilibrium. Moreover, due to increasing airflow over the control surfaces, the effectiveness of the control surfaces is not constant. Friction between the wheels and the runway surfaces adds further non-linearities into the model. All these factors make it difficult to design a linear control law that would achieve a tracking behavior to stay on the runway center line. However, if one assumes that there are no disturbances (crosswinds), and the aircraft's wheels do not have lateral slip, the aircraft would remain in equilibrium with respect to the lateral axis (i.e if the aircraft starts on the runway center line, it will stay on the center line if there are no disturbances). Thus, the aircraft's lateral dynamics can be approximated by linearizing Eqns (46), (48) and (50) about the lateral equilibrium.

The lateral-directional model obtained after linearization is dependent on the forward speed of the aircraft. Thus, for each forward speed, one can find a linear lateral-directional model. This implies that there is a continuum of linear lateral-directional models that describe the behavior of the accelerating aircraft about the lateral equilibrium. For takeoff, we are interested in the airspeed range $[0, V_{fp}]$ (i.e. from rest till the flap

retraction speed after lift off). We divide this airspeed range into $n = 10$ partitions. We select the mean value of the airspeed u in each partition and then linearize Eqns (46), (48) and (50) about the lateral equilibrium $v = 0, p = 0, r = 0$ for the selected mean airspeed u . We assume that this linearized model approximates the lateral-directional dynamics of the aircraft within the selected partition. Informally, this approach can be considered as taking a snapshot of the longitudinal dynamics at various locations in the ground roll and then computing the linear lateral-directional models for each snapshot. We obtain n piecewise affine linear lateral-directional models of the form shown below.

$$\delta \dot{x} = A_i \delta x + B_i \delta u_i, \quad i = 1, \dots, n$$

δx represents perturbation from the equilibrium and δu is the input.

$$\begin{aligned} \delta x &= [\delta v, \delta p, \delta r, \delta \phi, \delta \psi, \delta y] \\ \delta u &= [\delta a, \delta r] \end{aligned}$$

A control law developed for the non-linear plant (aircraft) using the above linear models is guaranteed to stabilize the equilibrium of the plant as long as the perturbations acting on the aircraft are small. However, to stabilize the aircraft on the runway center line in the presence of large crosswinds, we need a robust controller that can handle large uncertainties. We use a Linear Quadratic Regulator (LQR)²⁴ approach to design a control law that tracks the runway center line. An LQR controller guarantees certain stability margins and is robust to some uncertainties. For each pair (A_i, B_i) $i = 1, \dots, n$ we compute a state feedback control law of the form $\delta u_i = -k_i \delta x$ that renders the equilibrium stable and also optimizes the cost

$$J_i = \int_0^{\infty} \delta x^T \bar{Q}_i \delta x + \delta u^T \bar{R}_i \delta u \quad i = 1, \dots, n$$

where \bar{Q}_i and \bar{R}_i are weighting matrices that impose penalties on the states and controls respectively. We then use all the δu_i , $i = 1, \dots, n$ to control the nonlinear aircraft plant model described in Eqns (45)-(53) by scheduling the gains according to the airspeed partitions. As a lateral control law, δu_i only provides control inputs for the ailerons and rudder. We also use a PID controller to control the differential braking action to help achieve runway center line tracking. Fig 8 illustrates the takeoff control architecture. From the results illustrated in the following section, it can be seen that the controller developed above is indeed robust and can stabilize the aircraft on the runway center line in the presence of a 40 knot steady crosswind.

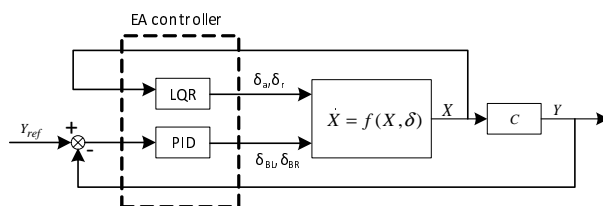


Figure 8. Envelope Aware (EA) controller architecture used on the non-linear aircraft plant

D. Simulation Setup and Results

Using the above non-linear aircraft plant and controller, we then simulated the accident scenario with data obtained from FL1404's Flight Data Recorder (FDR). We used rudder and aileron inputs from the FDR to represent the pilot's inputs. We extracted crosswind data from the NTSB data report to simulate similar environmental conditions. We did not have access to an exact B737 simulation model. We used parameters that approximate B737 characteristics. We also approximated runway surface and friction characteristics. Nevertheless, this simulation supports credible analysis of the behavior of an aircraft subjected to heavy crosswinds and gusts during a takeoff ground roll. Fig 9 illustrates the simulation framework in which we augment the FSAM modules with the aircraft model and the controller.

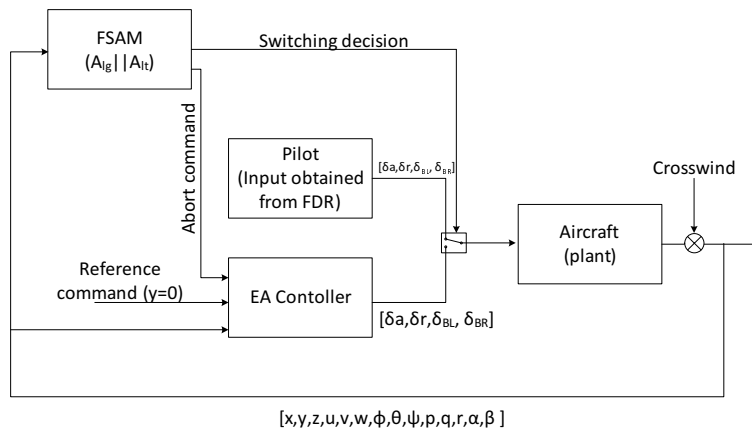


Figure 9. Simulation framework

Parameters of our aircraft model closely resemble the physical properties (mass, inertia, wingspan and mean aerodynamic chord) of a B737 type aircraft. Based on performance calculations, the following V speeds were chosen for the automata; $V_{mcg} = 60$ knots, $V_1 = 140$ knots, $V_R = 180$ knots, $V_{lof} = 200$ knots, $V_2 = 220$ knots, $V_{fp} = 230$ knots. We chose the following thresholds for the lateral automaton; $y_1 = 30$ m and $\psi_1 = 22.92^\circ$ (inner thresholds), $y_2 = 45$ m, and $\psi_2 = 28.65^\circ$ (outer thresholds). Figures 10 and 11 illustrate the results of our simulation. Figure 10 illustrates a continued takeoff sequence of an aircraft subjected to a crosswind similar to the one experienced by FL1404. Here, FSAM identifies that the flight crew is no longer able to achieve directional control of the aircraft when the aircraft violates the inner threshold in lateral displacement (shown in the second graph on the left in Fig 10); i.e transitions $s'_3 \xrightarrow{d'} s'_9$ in \mathcal{A}_{lt} . It then overrides the flight crew by transferring control authority to the envelope-aware controller which then drives the aircraft back towards the runway center line. After the aircraft lifts off the ground and is stabilized on the initial departure climb segment, control is reverted back to the pilot; i.e $s'_{12} \xrightarrow{e} s'_6$. The aircraft starts to drift due to the crosswind after control is transferred back to the pilot (after $t = 40s$). This is due to the fact that the pilot's rudder input is zero after $t = 40s$. The above decisions made by FSAM are important because by overriding the pilot, the controller helps make the appropriate corrections to the flight trajectory so that the aircraft can takeoff safely.

Fig 11 illustrates a similar scenario, but this time tighter thresholds are placed on the lateral displacement and heading to reflect a narrower runway: $y_1 = 20$ m and $\psi_1 = 17.19^\circ$ (inner thresholds), $y_2 = 30$ m and $\psi_2 = 28.65^\circ$ (outer thresholds). Here, FSAM first identifies that the flight crew has lost directional control (violation of inner threshold in heading) and it transfers control to the envelope-aware controller; i.e $s'_3 \xrightarrow{d'} s'_9$. FSAM then identifies that the envelope-aware controller is also not able to gain directional control; Fig 11 shows that the controller is not able to prevent the lateral position of the aircraft from crossing the outer threshold. Thus a transition to the abort state is made in an attempt to reject the takeoff safely; i.e. $s'_9 \xrightarrow{\bar{d}} s'_{14}$. In the abort state, the controller sets the throttle to idle. While decelerating, the controller still tries to track the runway center line. In this scenario, FSAM has successfully prevented major excursions off the side of the runway even though it did not continue the takeoff. In Fig 12 we present a graphical representation of runs of the automata for the case illustrated in Fig 11. The shaded states indicate the sequence of states the automata visit during an execution.

V. Conclusion

In this paper, we have presented a detailed description of FSAM's automata for the takeoff phase of flight. These automata address only a very small subset of factors contributing to LOC during takeoff. The goal of this paper was not to develop a complete set of automata that address every possible contributing factor, but to illustrate a systematic approach to deal with LOC contributing factors. For a comprehensive safety management system, events such as engine failures, instrument failures and actuator failures have to be addressed simultaneously. The influence of other variables such as extreme weather conditions, air

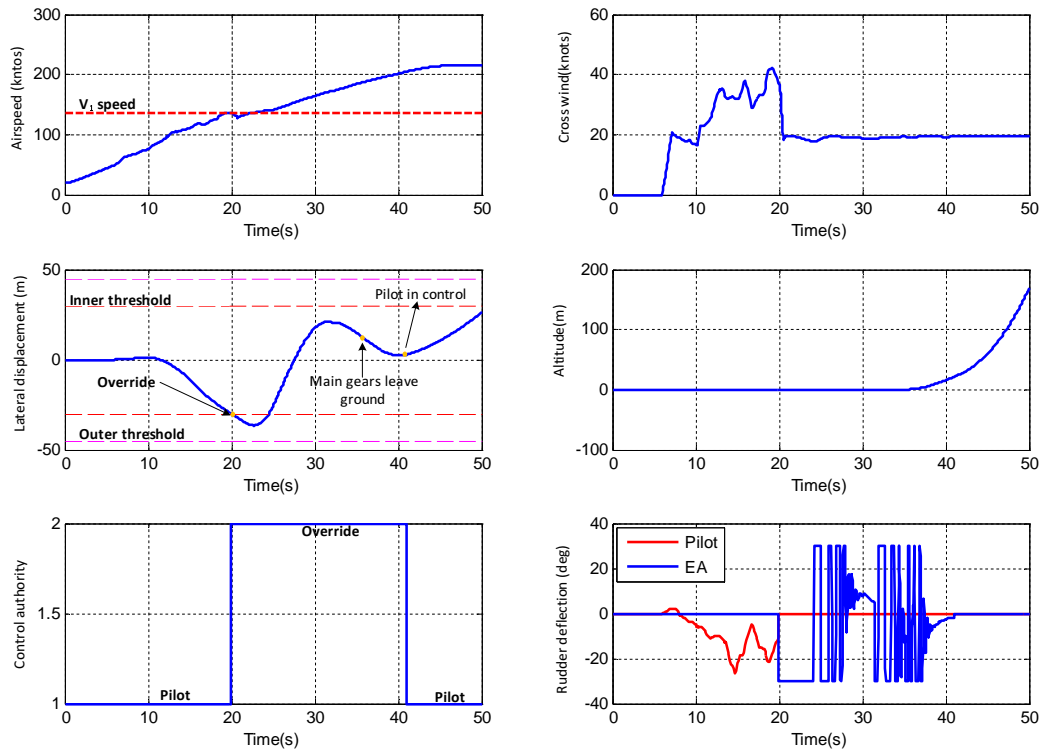


Figure 10. Continued takeoff after an override

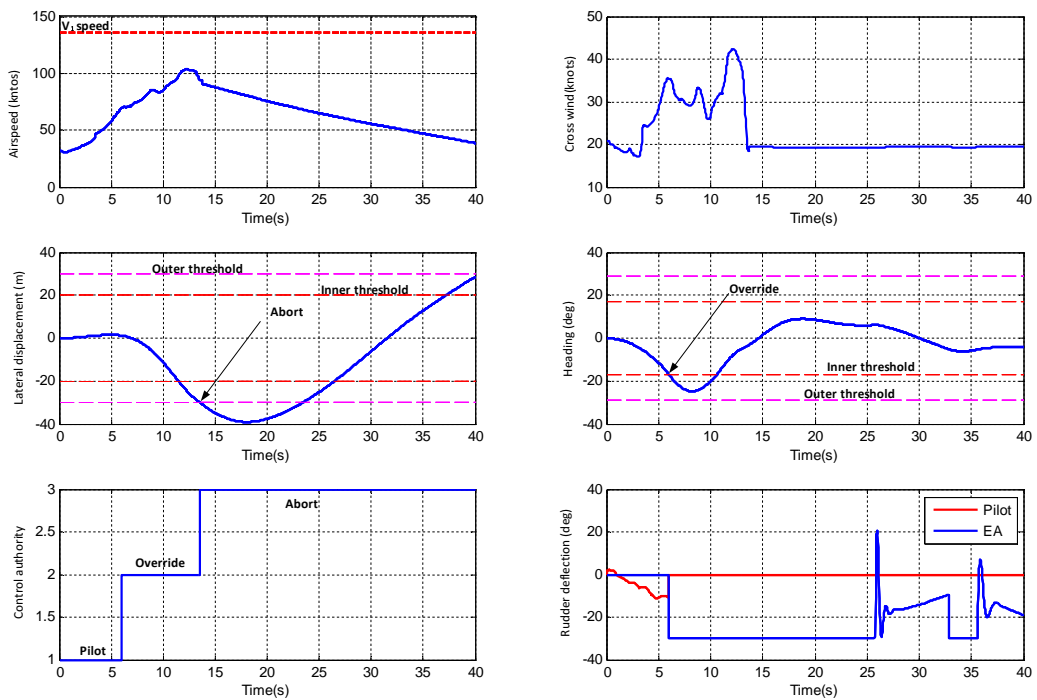


Figure 11. Aborting takeoff before LOC

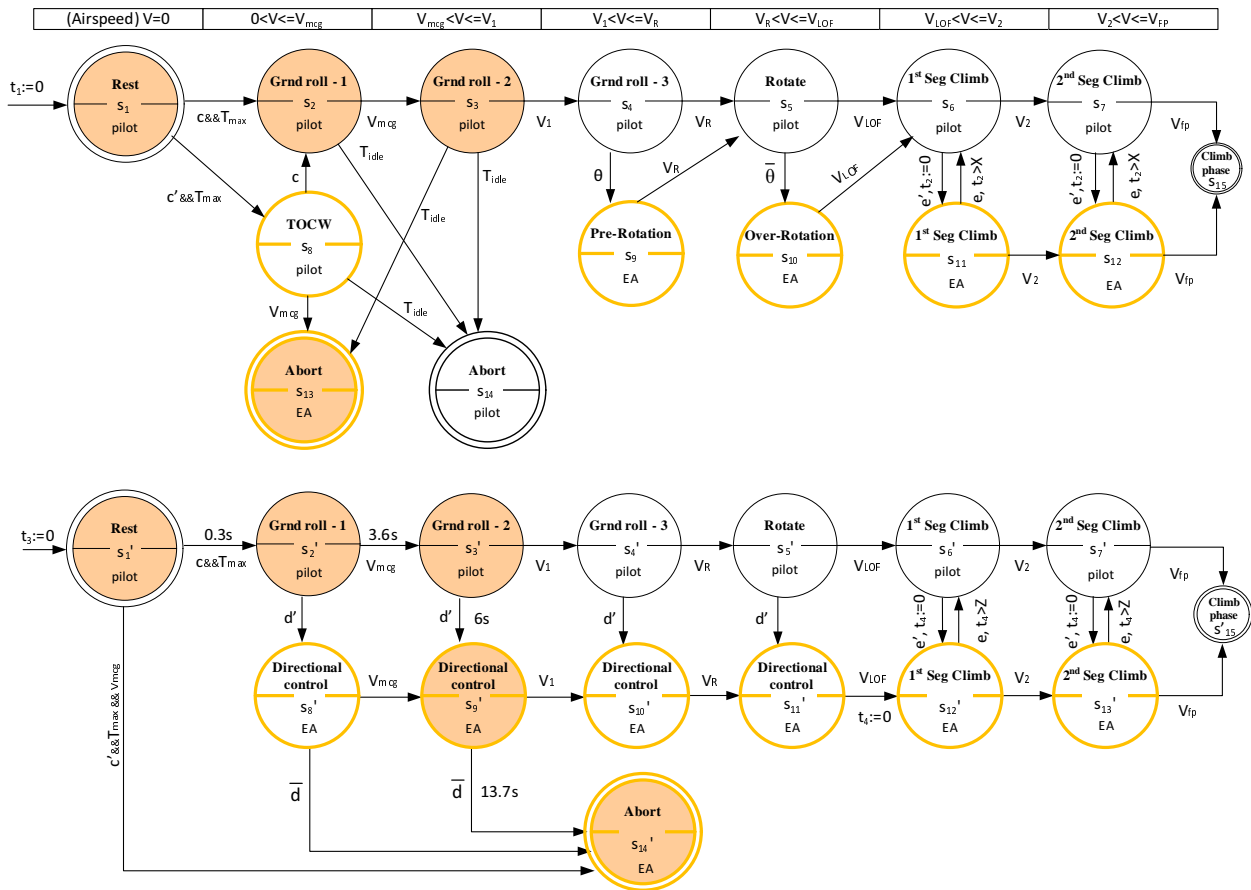


Figure 12. Concurrent execution of the two automata for the aborted takeoff scenario

traffic, pilot experience, workload and crew resource management have to be considered as well. The current hierarchical architecture of FSAM can be expanded by incorporating sub-automata that address the various events just mentioned, as illustrated in our previous publication.⁹

The simulations presented in this paper illustrate the utility of a deterministic, automata-driven Flight Safety Assessment and Management system. These simulations were performed using pilot input data obtained from the FDR of FL1404. Of course, human pilot in the loop simulations and numerous other issues in validation, verification, and pilot acceptance must be addressed before even the “simple” override logic presented here will be certified for operation. The goal in this paper was to present an intuitive, deterministic logic model that ultimately can be certified once accepted as reducing rather than increasing risk. As a future research direction, we will formally verify the above automata using well-established tools in model checking to ensure that these logic models meet certain safety and liveness properties. Also, we will relax the notion of determinism and consider the effects of uncertainties in the decision making process.

Acknowledgments

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

References

¹Belcastro, C. M. and Foster, J. V., “Aircraft Loss of Control Accident Analysis,” *Proc. AIAA Guidance Navigation, and Control Conference*, Toronto, Ontario, 2010.
²Flight Safety Foundation, “Reducing the Risk of Runway Excursions, Report of the Runway Safety Initiative,” May 2009, <http://www.skybrary.aero/bookshelf/books/900.pdf>, Sep 2012.

- ³Bartley, G. F., *The Avionics Handbook*, CRC press LLC, 2001, Chapter 11, Boeing B-777: Fly-By-Wire Flight Controls.
- ⁴Briere, D. and Traverse, P., "AIRBUS A320/A330/A340 Electrical Flight Controls A Family of Fault Tolerant Systems," *Proc. International Symposium on Fault-Tolerant Computing (FTCS)*, Toulouse, France, 1993.
- ⁵Well, H. K., "Aircraft Control Laws for Envelope Protection," *AIAA Guidance, Navigation and Control Conference and Exhibit*, Keystone, CO, 2006.
- ⁶Borst, 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*, 2013, doi: 10.2514/1.C031500.
- ⁷Ratvasky, P. T. and Morelli, E., "Envelope Protection for In-Flight Ice Contamination," *47th AIAA Aerospace Sciences Meeting Including the New Horizons Forum and Aerospace Exposition*, Orlando, FL, 2009.
- ⁸Belcastro, C. M. and Jacobson, S. R., "Future Integrated System Concepts for Preventing Aircraft Loss-of-Control Accidents," *Proc. AIAA Guidance Navigation, and Control Conference*, Toronto, Ontario, 2010.
- ⁹Balachandran, S. and Atkins, E. M., "Flight Safety Assessment and Management during Takeoff," *AIAA Infotech@Aerospace Conference*, Boston, MA, 2013.
- ¹⁰Srivatsan, 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.
- ¹¹Milligan, 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.
- ¹²Alur, R., "The Theory of Timed Automata," *Theoretical Computer Science*, Vol. 126, 1999, pp. 183–225.
- ¹³Baier, Christel Katoen, Joost-Pieter Larsen and Kim Guldstrand, *Principles of Model Checking*, MIT press, 2008.
- ¹⁴Roskam, J. and Edward Lan, C.-T., *Airplane Aerodynamics and Performance*, DARcorporation, 1997.
- ¹⁵Federal Aviation Authority, "Pilot Guide to Takeoff Safety," Online database, http://www.faa.gov/other_visit/aviation_industry/airline_operators/training/media/takeoff_safety.pdf, Nov 2012.
- ¹⁶"Northwest Airlines, INC; McDonnell Douglas DC 9-82,N312RC, Detroit Metropolitan Wayne County Airport, Romulus, Michigan," Accident report NTSB/AAR-85/05, 1988, <http://libraryonline.erau.edu/online-full-text/ntsb/aircraft-accident-reports/AAR88-05.pdf>, Dec 2012.
- ¹⁷"Runway Side Excursion During Attempted Takeoff in Strong and Gusty Crosswind Conditions- Continental Airlines Flight 1404,Boeing 737-500, N18611," Accident report, 2008, <http://www.ntsb.gov/doclib/reports/2010/AAR1004.pdf>, Feb 2013.
- ¹⁸York, B. W. and Alaverdi, O., "A physically representative aircraft landing gear model for real time simulations," American Institute of Aeronautics and Astronautics, Inc., Jun 1996, <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA314062>, March 2012.
- ¹⁹Rankin, J., *Bifurcation Analysis of Nonlinear Ground Handling of Aircraft*, Ph.D. thesis, University of Bristol, Bristol, United Kingdom, 2010.
- ²⁰Wong, J., *Theory of Ground Vehicles*, Wiley-Interscience, 2010.
- ²¹Canudas-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.
- ²²Pacejka, H., *Tyre and Vehcile Dynamics*, Oxford: Elsevier, 2006.
- ²³Stevens, L. B. and Lewis, L., *Aircraft control and Simulation*, Hoboken, NJ: Wiley, 2003.
- ²⁴Kirk, D. E., *Optimal Control Theory, An Introduction*, Prentice-Hall, Inc., 1970.