Safety Science 108 (2018) 129–139

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/safety

STPA for continuous controls: A flight testing study of aircraft crosswind takeoffs

Diogo Silva Castilho[a,*], Ligia M.S. Urbina[b], Donizeti de Andrade[b]

[a] MIT (Massachusetts Institute of Technology), USA
[b] ITA (Instituto Tecnológico da Aeronáutica), Brazil

ARTICLE INFO

Keywords:
STPA
Hazard analysis
Continuous control
Flight testing
Crosswind takeoff

ABSTRACT

A light aircraft crosswind takeoff is a risky operation. The purpose of this paper is to demonstrate the feasibility of applying STPA (Systems-Theoretic Process Analysis) to closed-loop continuous controls, identifying the hazards of crosswind takeoffs with light aircraft and the mitigating actions that could make its execution safer. The paper analyzes the variables that affect the response of the aircraft when subjected to severe crosswind, considering how aircraft characteristics affect its stability. The hazard analysis technique STPA is a tool based on the conceptual accident causality model called STAMP (System-Theoretic Accident Model and Processes), which in turn is based on systems theory. To deal with closed-loop actions on continuous control systems, a new approach to STPA was developed and effectively used to analyze data collected on a crosswind flight test campaign. This campaign, conducted by the Flight Test and Research Institute, led to a flight envelope extension of the Embraer's training aircraft Super Tucano. The demonstration analysis showed the need for new, previously unidentified mitigating measures to be assigned to aircraft manufacturers, operators or owners, and their pilots.

1. Introduction

The aviation safety attitude is guided by individual experiences and stories about mishaps. Maturity comes as each professional find the borders of safe behavior and understands the variables that affect them. In aviation, crossing such borders is often catastrophic. Therefore, safety mentality must be motivated to guarantee conservative attitudes in decision-making processes.

Crosswind is the component of the wind that is perpendicular to the runway alignment, as shown in Fig. 1. Modern aviation manufacturers face a competitive market and must be efficient, reducing costs even with flight testing campaigns. That is why the highest crosswind experienced during the prototype flights has been frequently set as the crosswind limit of the aircraft.

The study of crosswind is opportune because, due to global warming, the meteorological phenomena become more severe and strong winds and gusts might come from directions that are different[1] from the predominant winds of decades ago when most runways were built (Edenhofer et al., 2014). It would be safer if every airport had three runways with different headings, but for most airports, residential and commercial areas forbid the construction of new runways.

Moreover, the Brazilian Government's Center for Aeronautical Accidents Investigation and Prevention (CENIPA) published statistics for 2015 with loss of control on the ground as a contributing factor in 13% of all accidents and 23% of all severe incidents (CENIPA, 2015). Accidents during crosswind takeoffs are expected to be more frequent as new aircraft become lighter, pilots more dependent of automation (less handling abilities) and manufacturers explore the borders of the standards to be more competitive.

The Brazilian Aeronautical Manufacturer EMBRAER produces the Super Tucano, which was developed to serve the Brazilian Air Force needs, but was also sold to at least a dozen other Air Forces. Its purpose is to be a training tool for fighter and test pilots schools, as well as performing the interception of low-performance aircraft, air combat maneuvers, and interdiction missions. One of its operators, the Flecha Squadron has suffered operational constraints due to crosswinds that exceeded the original limits of the Super Tucano. This squadron is in the Campo Grande Airbase, which has only one runway.

According to Brazilian Air Force documents, the squadron requested an extension of the crosswind envelope to the Flight Test and Research Institute - *Instituto de Pesquisas e Ensaios em Voo* (IPEV). The test was performed and a higher new limit was established. Pilots described the

* Corresponding author at: 77 Massachusetts Ave., Cambridge, MA 02139, USA.
E-mail address: castilho@mit.edu (D.S. Castilho).

[1] According to statistics from NTSB Aviation Accident and Incident Database, between 2003 and 2007, crosswinds were reported 371 times and winds were a causal factor in 216 takeoff accidents (FAA, 2010).

https://doi.org/10.1016/j.ssci.2018.04.013
Received 22 September 2017; Received in revised form 29 January 2018; Accepted 20 April 2018
0925-7535/ © 2018 Elsevier Ltd. All rights reserved.

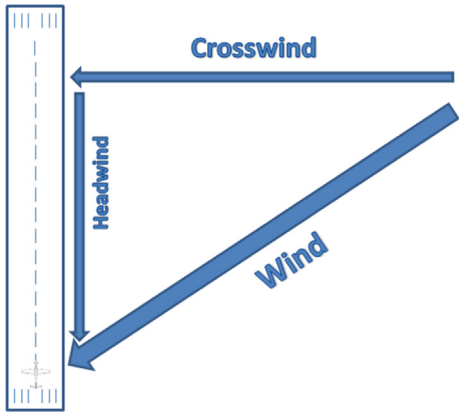


Fig. 1. Wind components in relation with runway alignment.

aircraft's handling qualities in extreme conditions and the test report analysis presented the results from the perspective of the testing activity. The report was issued and the Super Tucano squadrons have been using the extended limit for the aircraft flight envelope, which means that the new limit was considered safe for operation.

The analysis of parameters collected by the data acquisition system provided the identification of risks and the relationship between the variables involved. Close to the limit, the aircraft is controllable, but there is less room for mistakes and any mishap could bring severe consequences. The taxi showed no difficulties and the landings showed the same behavior already explored in books and manuals, but the takeoffs results presented issues that are not covered enough in the material offered by the current civilian and military courses verified in this research.

Light aircraft usually have single wheels in each landing gear leg, are often conducted by less experienced pilots and are more susceptible to the effects of lateral forces imposed by crosswinds. Therefore, it is highly advisable to conduct a risk analysis about light aircraft takeoffs with strong crosswinds. The technique based on systems theory and called Systems-Theoretic Process Analysis (STPA) was used for the task (Leveson, 2011) because, when analyzing interactions among components, it also considers human factors and hazards which are not related to failures. STPA uses a model of the hierarchical relationship between components of a system and is applied in this research to map handling techniques, safety constraints and requirements that should be applied to reduce the vulnerability of the light aircraft.

In this context, this research identifies opportunities to mitigate the risk of crosswind takeoffs of light aircraft using a risk analysis based on STPA. Forces and moments acting on an aircraft during crosswind takeoffs were analyzed using the data collected in a flight testing campaign. Then, the output of STPA determined which safety requirements and constraints could be applied to mitigate unsafe control actions.

This research is limited to single-engine clockwise propeller aircraft with low wing and positive dihedral, single-wheel landing gear and no spoilers. Ultimately, its contribution relies on the application of the STPA on handling qualities, dealing with variables that are not discrete and the human factors related to the non-linear behavior of the variables. This new approach to STPA might be used for continuous control actions in many different fields.

2. Hazard analysis tools

"Flight safety is everyone's duty" (CENIPA, 2015). This CENIPA motto tries to increase the number of people thinking about the identification of hazardous conditions that may lead to an accident. Traditional accident causality models explain accidents in terms of a chain-of-failure-events and have been described using concepts of easy understanding, like dominoes (Heinrich) and slices of Swiss cheese (Reason). These models are still taught in flight safety courses and used by aviation carriers.

In linear models, accidents are assumed to result from a chain of directly related events, each one necessary and sufficient for the occurrence of the next. In these models, the causes of accidents are derived from a structural failure, human error, software "failure" or energy problem. Using these approaches, the appropriate action to increase the safety of a system is to increase the reliability of its components (Rasmussen, 1997). The failures of the components are considered random. Therefore, the safety of each system is based on the calculated reliability for each component. Thus, the general technique to reduce risk is to raise each system component's reliability to reduce the chances of an occurrence that would initiate or propagate the chain of events.

Analysis techniques based on this causality model, such as Fault Tree Analysis, Event Tree Analysis, Hazard and Operability Analysis (HAZOP), Failure Modes and Effects Analysis (FMEA) and Failure Modes and Effects Criticality Analysis (FMECA), as well as probabilistic models based on these tools, are still widely used (Altabbakh, 2013). They explain basic concepts of flight safety but fail to analyze the operation of complex systems currently in use (Montes, 2015).

Specialists in human factors, in contrast, usually consider the operator's behavior to be the result of social, psychological and even environmental scenarios. Therefore, human error should not be treated statistically because it is not random. The standard causality models do not consider how financial or competitive pressures affect people's behavior, which might lead to attitudes that make the system as a whole move to a state of higher risk (Leveson, 2011).

The role of systemic risk analysis is to identify dependencies or relationships that are more complex than direct relations. The complexity of today's engineering systems requires the use of systemic analyses to analyze the operation of modern products. The Systems-Theoretic Accident Model and Processes (STAMP) is based on Systems Theory, which can be used to analyze a system for emergent properties. This theory includes both technical and social aspects, explaining the interaction between components and behavioral events. In this model, systems are seen as a hierarchy of organizational levels. Each hierarchical level controls the relationship between the lower level components, imposing constraints on their degrees-of-freedom and controlling their behavior (Checkland, 1981). Systems theory allows the identification of relationships between components not as a simple and direct connection, but as a complex relationship.

Systems-Theoretic Process Analysis (STPA) is the hazard analysis technique based on STAMP. STPA covers not only the accidents caused by component failures but also the ones caused by a bad interaction between components of a system that is functioning properly, as a consequence of design flaws. It recognizes safety as an emergent property of a complex system caused by the interaction of its components.

STPA begins by identifying the possible accidents to be considered and their associated hazards. Then, using a model of the safety control structure for the system, the STPA analysis identifies in step 1 potentially unsafe control actions and their causal scenarios. Each unsafe control action is explored in step 2 to generate scenarios that explain the contexts, causal factors and rationale for those actions. Finally, system and component safety requirements and constraints are generated, as well as design changes that can eliminate or mitigate the causal scenarios. (Leveson, 2015). STPA includes humans in the analysis and can include human factors and psychological issues that contribute to the causal scenarios.

Emergent properties in complex systems do not fit a Newtonian framework. They have limited predictability because they do not behave linearly. Instead, their chaotic behavior is better explained with complexity theory because the system is adaptive and it works as a network. An aircraft taking off is complex because a pilot influenced by fatigue and external factors acts based on limited information and

applies techniques learned by tacit training restricted by operational procedures (Dekker et al., 2011).

The evolution of accident causality models is important because the difference between considering an accident as an unfortunate inevitable event (Perrow, 1984), as a result of individual failure of components of a system (linear model) or as the result of dysfunctional interaction between components (systemic model) determines how to apply mitigating measures to prevent accidents. Moreover, basic STPA has been augmented for additional properties such as security (Young, 2014), human factors and flight testing (Montes, 2015), and coordination among multiple controllers (Johnson, 2017). This paper suggests an approach to applying STPA to continuous, closed-loop systems, using crosswind analysis to demonstrate the approach.

3. Flight testing campaign

For the flight testing campaign considered in this paper, two IPEV's Super Tucano aircraft were outfitted with Flight Testing Instrumentation (FTI) containing sensors, accelerometers, differential GPS, strain-gauges and recorders on the MIL-STD-1553B bus (Castilho, 2015). Also, cameras were installed in the arch of the canopy (internal) and at the tail cone of the aircraft (external).

In November 2013, both aircraft flew to an airfield in southern Chile called Punta Arenas Air Base. Among many takeoff test events, one performed with a right crosswind of 26 kt and gusts of 29 kt, which were considered as the most critical of the whole campaign and chosen for this study. The collected parameters allowed full analysis of the forces and displacements of flight controls. The pilot applied up to 25% of the right pedal range (DDN). Directional force (FDN) showed that the pilot applied the pedal to the right at low speeds and to the left at high speeds (Fig. 2). The control stick was held centered (DDL) with no significant force applied to it (FDL). It was found that the aircraft rolled about 2.5° (ϕ) to the left, even while still in contact with the ground. After 80 kt, the aircraft was clearly skidding to the left until rotation at 90 kt of airspeed.

4. Hazard analysis

For certification, all measured forces must be within the limits of the requirements based on the MIL-HDBK-1797 - Handbook Flying Qualities of Piloted Aircraft. But, to achieve a clear understanding of the hazards involved in crosswind takeoffs, it is important to determine which forces and moments acting on the aircraft are important in analyzing the stability of the aircraft.

4.1. Aircraft response to wind

When the wind is constant in direction and intensity, the lateral force experienced by the aircraft throughout the takeoff is constant, but the total lift (L) depends on the square of speed (V), as shown in the following equation.

$$L = \frac{\rho}{2} V^2 S C_L$$

Total lift of the aircraft can be taken as a force applied on its aerodynamic center, but normal force decreases differently among the legs of the main gear and the nose gear (Anderson, 1985). Considering the aircraft symmetric, when there is no crosswind, the reduction of the normal force on the two legs of the main landing gear depends only on the torque of the propeller. If the propeller rotates clockwise as observed from behind, the aircraft will undergo a rolling moment to the left.

During takeoff with wind from the right, three other factors make the aircraft roll left. The first is the lateral force caused by the wind that

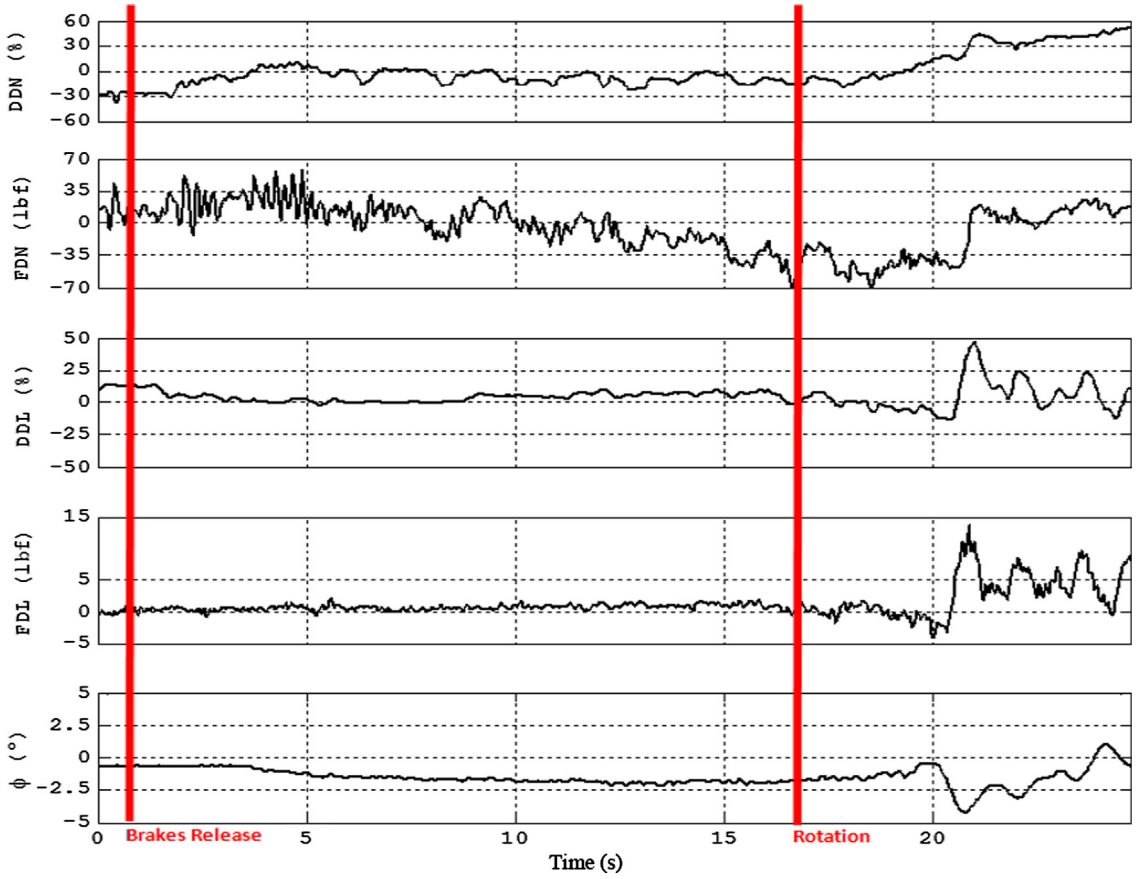


Fig. 2. Bank angle, forces and control positions during a right crosswind takeoff (Castilho, 2015).

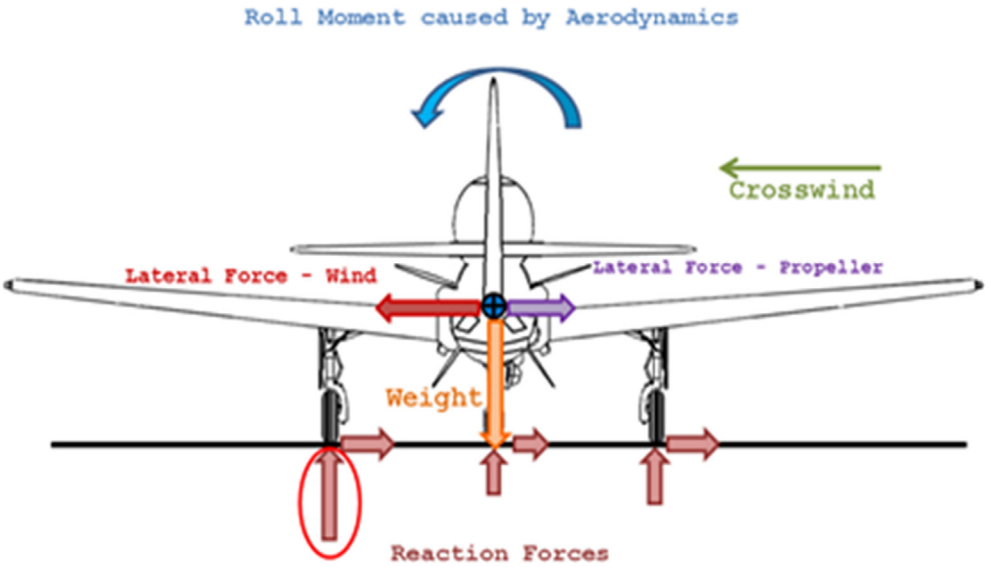


Fig. 3. Forces and moments caused by the right crosswind.

hits all the lateral area of the aircraft while its tires are in contact with the ground. Second, as most conventional aircraft have a vertical stabilizer above the longitudinal stability axis, right wind promotes a left roll moment. The third characteristic that makes the aircraft roll left is the dihedral effect caused by a different angle of attack on each wing. For low-wing aircraft with positive dihedral, as the Super Tucano, right crosswind impacts the right wing with higher AoA (angle-of-attack) and the left wing with lower AoA. The lift provided by the right wing becomes higher than on the left, also causing the aircraft to roll left.

The consequence of these effects together is a decrease of normal force on the right landing gear leg and its increase on the left one, resulting in more drag of the left gear, as shown in Fig. 3, that causes the aircraft to yaw even more to the left.

With respect to the directional control, the airflow from a clockwise propeller impacts considerably more the left side of the vertical stabilizer causing the aircraft to yaw left. The gyroscopic effect of a clockwise propeller also causes the aircraft to yaw left. When the engine is accelerated for takeoff, the rolling and yawing moments due to torque are perceived by the pilot, who needs to apply force on pedals and flying stick to keep the aircraft moving straight and with wings leveled.

At 60 kt on Super Tucano, an electronic system called ARTU (Auto Rudder Trim Unit) engages and acts on yaw trim according to speed and torque to reduce the necessary force on pedals and, consequently, the slip during flight. In this case, the yaw moment is to the right and the pilot must react on the pedals to maintain runway alignment. Moreover, as the aircraft gains speed, lift reduces the adherence of all tires and the aircraft drifts more to the left. When this happens, pilots press even more the right pedal, skidding the aircraft to bring it to the dashed line in the center of the runway.

All these described reactions are dynamic and require the pilot to be in the loop to control all three axes while performing other tasks such as checking engine parameters and speed. The takeoff used for the analysis took 21 s from brakes release until lift off.

4.2. System foundations

This hazard analysis identifies behavioral peculiarities for operational and training contexts. To apply STPA to this context, one starts from a safety functional control structure (Fig. 4), which shows the interactions between different levels of system components hierarchically. From Air Force Command to the Pilot, the downward arrows represent orders and policies while the up arrows are different kinds of feedback, from sensory information to standard reports. Brazil's safety center CENIPA receives prevention reports and performs technical surveys, provides courses and distributes awareness material about flight safety. The pilot's actions are also influenced by the tower and eventually by an instructor. The runway grip conditions and winds affect the aircraft directly and are part of the context. A civil structure would be similar, replacing the squadron by the operator or the owner of the aircraft and the upper hierarchical structure by the government regulatory agencies.

This analysis focuses on the control loop between the pilot and aircraft depicted in Fig. 5, including aspects related to human factors, responsibilities and devices that act on the flying stick and pedals. The pilot operates the throttle, brakes, control stick, rudder pedals, and its trims and feels the evolution of the aircraft position on the runway and its linear and angular accelerations in all axes. When the ARTU (Auto Rudder Trim Unit) is engaged above 60 kt, it acts only directionally. The autopilot is shown with a dashed line because it is not engaged operationally during takeoffs.

Based on the experience on a specific aircraft and gusts or crosswind experience, the pilot decides to abort the takeoff before losing control of the aircraft or damaging it. The aircraft responds to pilot inputs and environment conditions (e.g. wet surface) depending on its characteristics like stability derivatives, loads configuration (military), weight, balance and tire wear.

Using STPA, accidents or incidents that could occur in a takeoff with strong crosswind are identified, along with the hazards associated with each accident. The high-level accidents considered are damage to the aircraft and pilot death or injury. The system safety requirements and constraints are created from the hazards. Considering the characteristics of Super Tucano's missions, piloted by experienced pilots as well as by students, the high-level hazards related to crosswind takeoffs are presented in Table 1.

The H1-type of hazard can lead to several consequences. It is possible that the aircraft leaves the runway undamaged, but skidding in an attempt to return to the runway. This attempt can be exaggerated and cause the aircraft to turn, increasing the severity of consequences. A tire burst severely aggravates directional controllability.

The bursting of an aircraft tire is not always clearly noticed. The perception of the pilot varies from aircraft to aircraft. The Super Tucano has a pressurized cockpit. That means that the sound of a tire bursting (Fig. 6) is barely perceived by a pilot using a helmet. The perception is limited to a vibration and a directional instability. The problem lies in the fact that strong crosswinds are constantly accompanied by gusts and turbulence. Therefore, vibration and directional instability as symptoms

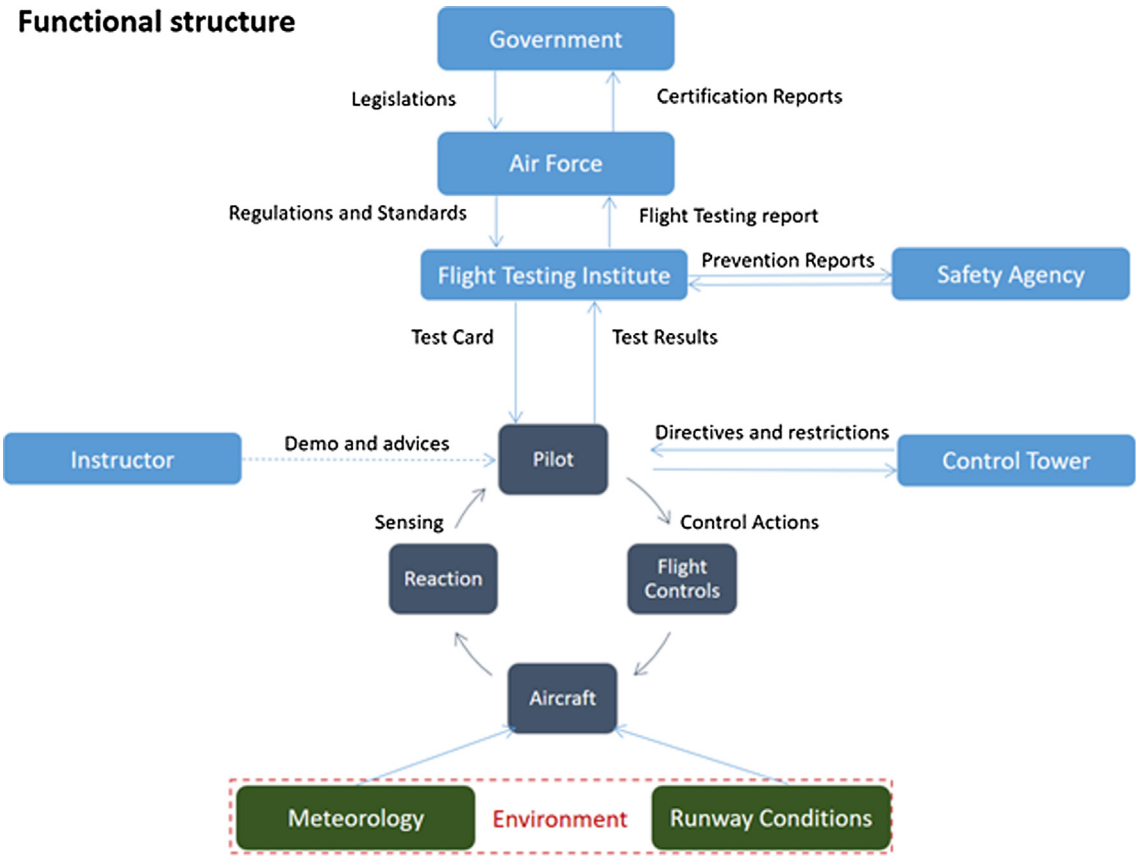


Fig. 4. Functional structure of operational control.

of a tire burst can easily be confused with effects of wind gusts, especially for inexperienced pilots, who are the typical users of lighter aircraft.

The control action C1 refers to an aborted takeoff. When a pilot decides to abort a takeoff, the first action is the reduction of the throttle to minimum or reverse and the immediate application of brakes. If the decision is made at high speed and the runway is short, brakes must be applied severely to stop the aircraft. When aborting with crosswinds, if

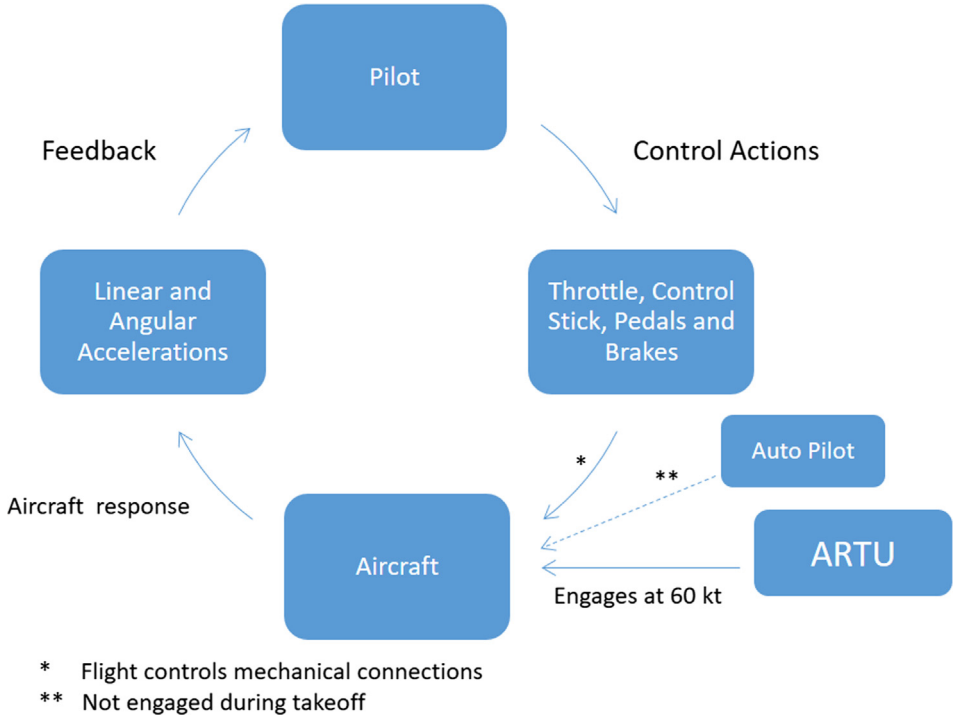


Fig. 5. Pilot-aircraft control loop.

Table 1
Relation between hazards and control actions leading to the hazards.

Hazards	Related Control Actions
Loss of control on ground (H1)	– Severe braking (C1) – Late or no decision to abort (C2) – Flight controls misuse during takeoff run (C3) – Blown tire procedure not followed (C4)
Loss of control in the air (H2)	– Mistaken flight controls use during rotation (C5) – PIO[a] (Pilot Induced Oscillation) (C6)
Following landing with landing gear partially retracted (H3)	– Landing gear retraction with blown tire (C7)

[a] Pilot Induced Oscillation (PIO), occurs when controls are applied in phase with the delayed response of the aircraft on the respective axis. The lag in the response is more significant in dynamic maneuvers at low speeds.



Fig. 6. Blown Super Tucano tire.

the weight is divided differently in the main gear, there is a high possibility of locking one wheel and bursting one tire. Most of the light aircraft do not have antiskid systems. With a tire burst, directional control may be restricted and not adequate to keep the aircraft on the runway (C2).

Another cause of H1 relates to the pilot's reaction when releasing the brakes (C3). Using the rudder, inexperienced pilots are expected to release the brakes, observe the yawing and react to it. The delay in doing these things varies from pilot to pilot and slow reactions require a larger correction to bring the aircraft back to the center of the runway. Experienced pilots push the right pedal just after releasing the brakes, before any directional movement, because they are conditioned to counter the yawing movement induced by torque. A pilot's aggressive directional corrections may cause damage to tires and aircraft, compromising its controllability.

C4 involves situations where a pilot realizes that the tire blew out at high speed and decides to proceed with the takeoff because his ability to reduce speed is unknown. In this case, the correct procedure for most aircraft is to keep the landing gear down. The procedure for landing with blown tire includes circling to spend fuel and allow some time to prepare the runway. It also leads to such considerations as landing on the side of the runway opposite to the blown tire and applying ailerons (lateral controls) to reduce the weight over the blown tire. Landing as soon as possible and not following completely the guidelines provided may result in loss of control of the aircraft on the ground (H1).

The second hazard is the loss of control in flight, just after the rotation. If the pilot rotates while applying predicted lateral input and not attempting to keep wings leveled, a sudden roll movement[2] will reduce lift and lead to a dangerous condition (C5).

The coupling between a pilot and the aircraft (C6), known as PIO, is dynamic and safety critical. As the aircraft lifts off with low speed, PIO could be induced just after rotation and lead to a dangerous condition.

The third hazardous control action (C3) also refers to the situation when, at high speed, the tire bursts and the pilot decides to proceed. In this case, the difference is that the landing gear is retracted. This may happen when the pilot does not perceive the tire burst,[3] when the retraction of the landing gear is performed as a conditioned behavior, or when reduction of drag is needed to gain height to avoid obstacles. In this case, depending on tire conditions, the gear may damage the aircraft and compromise the subsequent lowering of the landing gear, resulting in a landing with one or more legs not locked down, which is an even riskier procedure.

When approaching for landing, if the landing gear lowers and the pilot does not know that the tire is blown, the touchdown and the use of brakes are critical. It is important to remember that the subsequent landing will probably be performed at the same aerodrome the aircraft took off from, where strong crosswinds may still be present.

4.3. STPA Step 1

STPA step 1 identifies potential Unsafe Control Action (UCA). Therefore, the actions are organized in four different types, as shown in Table 2. This framework provide an understanding of how each of the controlling actions might be unsafe, depending on the context in which the actions are taken.

Discrete controls were explored in many previous hazard analysis with STPA considering on/off switches or opening and closing doors and valves. The retraction of the landing gear in this analysis is considered in the same way as in previous analyses and the four columns have a very straightforward meaning. In this study, however, in contrast to the usual application of STPA, the cockpit operation has discrete and continuous closed-loop flight controls. Elevators, ailerons, rudder, and brakes have infinite positions and dynamic behaviors. The time and frequency of an input of these surfaces also matter. High amplitudes are not necessarily unsafe if they last a short period. This is common when pilots are learning to fly, in normal operation in bad weather or in maneuvers that require a higher gain, like formation flight.

Therefore, continuous variables, such as the use of pedals for brakes and rudder or side stick force to move the ailerons, need a new interpretation. The ideal position of the rudder pedals along the takeoff run, for instance, varies non-linearly even when there are no gusts. The pilot acts continuously to keep the dashed central line, correcting the deviation. Thus, the analysis considered as "provided" is the control action which is adequate for the desired target.

Second, the delayed correction was identified in the "too early/soon or out of order" classification, even though this title does not explain the exact meaning of a late reaction, e.g. to yaw. The late reaction is important and might be catastrophic in systems where dynamic stability is critical. For elevator and rudder, the delayed reaction could happen in phase with the natural frequency of the aircraft and cause a pilot-aircraft coupling.

Finally, the poor combination of amplitude and duration, which is

[2] If the pilot applies directional input to maintain a straight takeoff, when the wings get sufficient lift and the nose wheel leaves the ground, the balance of forces and moments changes abruptly and the pilot must react in all axes skillfully. Any yawing or rolling affects other axes because lateral and directional derivatives are correlated.

[3] The Super Tucano and many other aircraft in the same category are not equipped with tire pressure sensors.

Table 2
Unsafe Control Actions.

Control action	Not provided causes hazard	Provided causes hazard	Too early/soon or out of order	Stopped too soon/applied too long
Reduce throttle	Not Applicable	Not Applicable	Late decision to abort (UCA 1)	Not Applicable
Applying brakes	Not Applicable	Brake severely when aborting (UCA 2)	Not Applicable	Not Applicable
Yaw + Steer at brakes release	Not Applicable	Aggressive directional corrections (UCA 3)	Delayed pedal application (UCA 4)	Not Applicable
Ailerons - lateral force on stick	Keep the stick in neutral during takeoff run (UCA 5)	Not Dangerous	Not Dangerous	Keep full lateral deflection on stick until rotation (UCA 6)
Applying controls simultaneously	Not Applicable	Not Dangerous	Allow banking while alignment with wind (UCA 7)	Induce PIO by wide controls input (UCA 8)
Retract the landing gear	Landing without following complete blown tire procedure (UCA 9)	Retract landing gear with blown tire (UCA 10)	Not Dangerous	Not Applicable

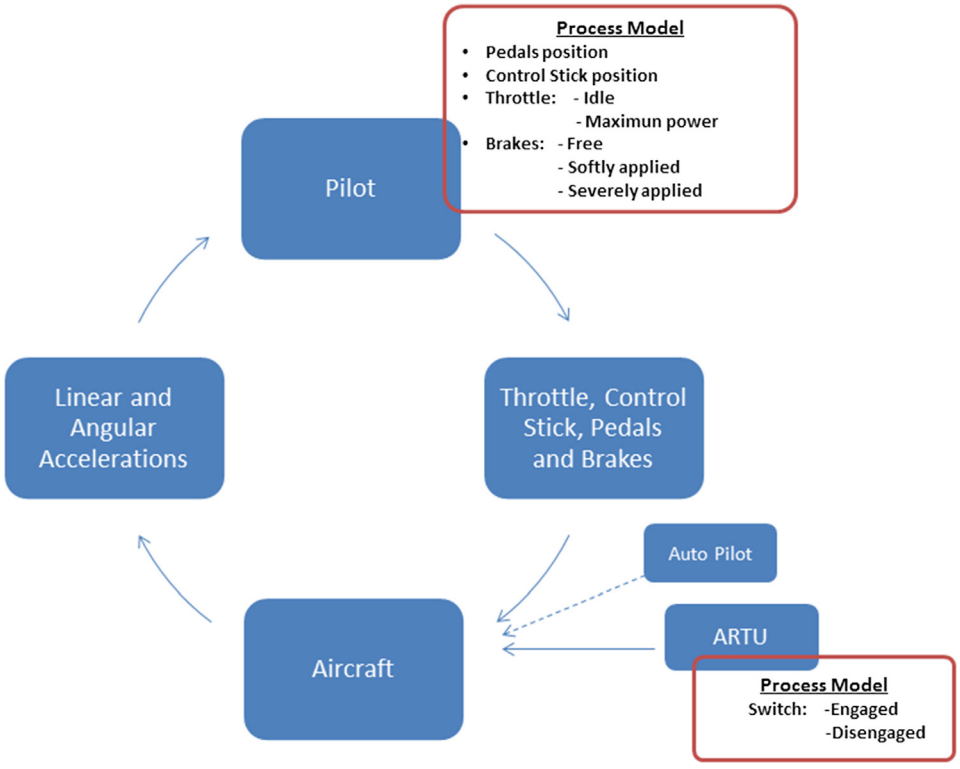


Fig. 7. Control loop pilot-aircraft with controller's process model.

common for less experienced pilots, was characterized as "stopped too soon / applied too long". It includes lack of experience, delayed response of the aircraft for any mechanical reason and stress on the pilot in critical situations.

The use of throttle in the middle range suffers from the same considerations when taking off in formation as a wingman. But when a leader is about to takeoff with strong crosswinds, the correct procedure is to command isolated takeoff. Thus, the acceleration and throttle reduction for RTO (Rejected takeoff) were considered as discrete for this analysis.

Another novelty for STPA is the actuation of two different continuous closed-loop controls to execute one specific maneuver. When an aircraft with considerable dihedral angle yaws, one wing receives local relative wind with a different angle of attack (AoA) than the other. At higher AoAs, that results in a rolling reaction. This explains why the application of ailerons while reducing the slip angle is important to keep the wings leveled just after takeoff, at a low height from the ground. The amplitude needed is hardly foreseen by the pilot because crosswinds are rare and slipping the aircraft is common only in acrobatic or flight testing.

For each UCA, a safety requirements or constraint (SRC) is set, as in the following examples:

SRC 1: The takeoff must be aborted at the first sign of loss of directional control.
SRC 2: Brakes cannot be applied severely when aborting with a strong crosswind.

Pilots are conditioned to apply severely and immediately the brakes when aborting because performance manuals are calculated considering maximum braking. Pilots should not perform takeoffs with strong crosswinds on short runways. The severe application of brakes at high speed, when the tires are already near their lateral grip limit may cause the wheels to lock and reduce braking efficiency or a tire to burst.

SRC 3: Directional deviations must be corrected smoothly and continuously.
SRC 4: Yawing at brakes release must be counteracted quickly.
SRC 5: Side stick command should be applied to the side of the wind after releasing the brakes.
SRC 6: Side stick command must be gradually reduced as the aircraft gains speed.

Table 3
Controls to avoid UCA 1.

Late decision to abort		
Scenario	Associated Causal Factor	Rationale/Notes
Pilot is able to control the aircraft for steady wind, but fails to consider the consequences of gusts because his/her mental model for gusts include less sliding (low intensity crosswinds).	1. Lack of experience with gusts and training on simulators that have only constant winds cause a flawed process model. 2. Wind information from tower is measured far from the aircraft.	1. Most simulators for training aircraft are low cost and don't simulate gusts. 2. Positioning wind sensors around runways is not practical as a new standard.
Mitigating measure **Pilot:** Include into the emergency briefing procedures to abort when wind gusts exceed the directional control authority.		
Scenario	Associated causal factor	Rationale/Notes
Pilot is surprised by unusual yaw movement at brakes release.	Rejected takeoffs due to lack of directional control authority are rare.	Standardized takeoff briefings leave pilots less prepared for the unexpected.
Mitigating Measure **Operator:** Give freedom for pilots to use a simple briefing guide, instead of using standard memorized takeoff briefings. Therefore special conditions receive more attention.		
Scenario	Associated causal factor	Rationale/Notes
Pilot delays the decision for abortion because nose is returning to the track, even if the path is still divergent.	Pilot wants to takeoff as planned, instead of wasting time and having to explain the reasons of a rejected takeoff.	If other pilots took off in equal conditions, some pilots feel motivated to take greater risks.
Mitigating measure **Operator:** Promote conservative attitudes and never motivate unnecessary bold attitudes.		

Table 4
Controls to avoid UCA 2.

Brake severely when rejecting a takeoff		
Scenario	Associated Causal Factor	Rationale/Notes
Rejecting a takeoff at high speed, pilots reduce the throttle and press brakes severely because the acceleration and stopping calculations consider this.	Takeoff abort is trained only in a simulator. There is no training of rejected takeoff with crosswinds.	Loss of control gets even more dangerous when runway is wet.
Mitigating measures **Manufacturer:** Develop calculations with a multiplication factor for accelerate-stop distances with crosswinds. **Operator (only military):** Promote the installation of stop barriers at the end of short runways. **Operator:** Standardize conservative procedures about accelerate-stop distances for each location.		
Scenario	Associated causal factor	Rationale/Notes
Pilot does not analyze takeoff charts when preparing for a crosswind takeoff.	No manual provides guidance on techniques or braking restrictions in cases of crosswind.	The decision to abort is a pilot judgment that is questionable by the operator, owner or customer.
Mitigating measure **Pilot:** Remember the set of actions that would be needed to reject a takeoff at high speed just before starting it.		

SRC5 aims to equalize the weight among the main gear. To keep the wings leveled and prevent the rotation with stick fully applied to one side, SRC6 must be followed. The optimal implementation depends on the pilot sensibility because, even assuming a constant acceleration, the rolling effectiveness is not linear.

SRC 7: After rotation, the skid angle must be reduced to keep wings leveled.
SRC 8: The transition of primary flight controls in the rotation should be performed smoothly and continuously.

To avoid PIO the pilot must establish a constant attitude in the rotation and apply other primary controls (aileron and rudder) smoothly and continuously. SRC 7 and 8 are synthesized in a single operation that is improved by experience for every pilot.

SRC 9: The procedure for landing with a blown tire must be completely followed.

SRC 10: When the bursting of a tire at high speed is suspected and the pilot decides to continue, the landing gear must not be retracted.

As the perception of a tire blown is doubtful, when taking off with gusty winds, any suspicion has to be considered as a tire blown.

4.4. Identifying UCA causal scenarios

Causal scenarios provide the information needed to eliminate or control unsafe behavior. Therefore, the process model, that is, the model of the controlled process that each controller has, must be incorporated in the control loop, as shown in Fig. 7. As described in Section 4.1, the ARTU is the only equipment that interferes with a surface (yaw trim) controlled by the pilot.

Despite the simplicity of this system, the fact that the controller is human increases its complexity because humans use dynamic control algorithms, which constantly adapt to the scenario perceived.

Table 5
Controls to avoid UCA 3.

Aggressive directional corrections		
Scenario	Associated Causal Factor	Rationale/Notes
Gusts make the aircraft to yaw, requiring corrections with greater magnitude.	Pilot applies significant input on pedals as an overreaction to gusts, skidding the aircraft.	Wingman takeoffs require the pilot to maintain half the width of the track. A tire burst in this condition may cause a collision between aircraft.
Mitigating measures **Operator (only military):** Prohibit the Wingman takeoffs when the wind exceeds a limit set by the operator, depending on the aircraft characteristics. **Pilot:** React smoothly and continuously to yawing.		
Scenario	Associated causal factor	Rationale/Notes
It is not possible to predict that there will be strong crosswinds. So it is impossible to use a procedure for changing worn tires before the limit.	The limit for changing tires is the same regardless of the operating conditions.	A worn tire can be released for the flight and reach the condition for changing during the takeoff run.
Mitigating measures **Operator:** Guide maintenance personnel about the careful inspection of tires in the pre-flight and recommend its early replacement in crosswinds conditions. **Pilot:** When preparing for crosswind takeoff, perform a careful inspection of tires, asking for new ones if necessary.		

Table 6
Controls to avoid UCA 4.

Delayed pedal application		
Scenario	Associated Causal Factor	Rationale/Notes
Inexperienced pilots await the initial yaw of the aircraft to react acting on the pedals.	There is no specific instruction about crosswind takeoff in the manuals.	The crosswind simulator training is hardly reliable, especially while the aircraft is on the ground.
Mitigating measures **Manufacturer:** Include in the manual a description of the aircraft behavior to right and left crosswinds. **Operator:** Highlight to instructors the need to teach crosswind takeoff techniques during instruction, even when the wind is calm. **Operator:** Establish a conservative limit for pilots that have no significant crosswind experience. **Pilot:** Respond promptly to the initial yaw to decrease the necessary magnitude of the directional corrections.		
Scenario	Associated causal factor	Rationale/Notes
ARTU input causes yaw disturbances.	ARTU engages automatically with 60kt.	ARTU works in the entire flight envelope.
Mitigating measures **Manufacturer:** Decrease the ARTU gain during system engagement. **Manufacturer:** Set an ARTU engagement speed as low as possible. **Pilot:** Predict the engagement of ARTU on takeoff briefing, planning to reject the takeoff when the engagement occurs violently. **Pilot:** Consider engaging the ARTU manually after takeoff.		

Table 7
Controls to avoid UCA 5.

Keep stick in neutral during takeoff run		
Scenario	Associated causal factor	Rationale/Notes
Pilot holds the stick in neutral throughout the takeoff run, increasing the roll moment to the opposite side of the wind and the chances for a tire burst.	There is no written procedure in many manuals about aileron application in crosswind takeoffs.	The crosswind limit for each aircraft does not consider any application of lateral control.
Mitigating measures **Manufacturer:** Consider de technique of aileron to the side of the wind on tests and write its characteristics in flight manuals. **Operator:** Promote the training of aileron to the side of the wind on crosswind takeoffs. **Pilot:** Apply the aileron to the side of the wind technique during crosswind takeoff runs.		

Therefore, the continuous application of force on a pedal has a complex behavior. Human controllers have characteristics that differentiate them from machines, such as the need to experiment and to diagnose the system's problems, both of which are necessary to understand the best way to operate a system.

Near the limit, different behaviors among pilots are expected. Instructors and aircraft owners see bold and conservative postures differently as well. Aviation standards, weather conditions and the aircraft itself do not distinguish between new or experienced, able or restricted, healthy or sick pilots. Hence, the importance of applying human factors concepts to the critical conditions that happen to anyone and may lead to an aircraft accident.[4]

The identification of the UCAs in Step 1 is an exercise in logic while the development of scenarios in Step 2 requires operational experience in human behavior. Each of the unsafe control actions was explained to a group of four test pilots and four flight testing engineers at IPEV and the outcome of a brainstorm meeting was the contexts in which each scenario could occur. These contexts explore non nominal conditions like bad weather or equipment malfunction that would incur human factors issues like high workload or memory limitations. Tables 3–12 show part of the identified scenarios that lead to UCAs, their causal factors, and additional information about Rationale/Notes. Then, new barriers (Mitigating Measures) for each scenario of each UCA are suggested, identifying where the controls would be implemented in the safety control structure (manufacturer, operator or pilot).

5. Discussion

The Mitigating Measures (MM) for each scenario are key to avoiding the UCA and guaranteeing the accomplishment of the SRC. Each of the recommendations must be seen as an opportunity to reduce risk on crosswind takeoffs.

Today, some flight schools apply practices like a lower crosswind limit for students. Flying only in light wind conditions lowers the hazards during instruction, but one day this new pilot will face a crosswind condition and the lack of experience will put the instruction system in a state of higher risk. That is why all possible orientations

[4] More human factors scientific contributions, such as the development of mental models for control actions can be found in Thornberry (2012), Thomas (2013), Montes (2015), and France (2017).

Table 8
Controls to avoid UCA 6.

Keep full lateral deflection of stick until rotation		
Scenario	Associated causal factor	Rationale/Notes
The pilot applies the technique of aileron to the side of the wind but does not decrease the amplitude as the aircraft gains speed because believes that this is the correct procedure.	The lateral control is maintained at full deflection at high speed.	The aircraft banking with weight on wheels is not easily noticeable.
Mitigating measure **Operator:** instruct pilots about reducing the aileron inputs to keep wings leveled as aircraft gains speed.		
Scenario	Associated causal factor	Rationale/Notes
Pilot forgets to apply the correct technique due to high workload.	Takeoff is a dynamic maneuver that requires handling skills and monitoring of embedded systems.	Gusts may require more attention with directional control and less attention to other activities.
Mitigating measure **Pilot:** Brief the technique of lateral control to the side of the wind technique before takeoff.		

Table 9
Controls to avoid UCA 7.

Allow banking while alignment with wind		
Scenario	Associated causal factor	Rationale/Notes
After the rotation, pilot devotes his attention to reduce slippage, attitude acquisition, and gear retraction.	After the rotation, the aircraft yaw to the wind and the aircraft rolls to the same side.	Bank angle reduces lift and may cause the aircraft to touch the wing tip or a main gear on the runway.
Mitigating measure **Pilot:** Stay on the loop to keep wings leveled as aircraft heads the wind.		
Scenario	Associated causal factor	Rationale/Notes
The standardization of procedures and training in simulators cause mechanization of pilot actions.	The pilot brings the lateral control to neutral during rotation, rather than use it to keep wings leveled.	Pilots with less experience have slow crosschecks.
Mitigating measure **Pilot:** Focus attention on flying the aircraft from rotation to gear retraction.		
Scenario	Associated causal factor	Rationale/Notes
The trim triggers involuntarily by pilot action or systems failure.	Trim's runaway causes undesirable moments during rotation.	With high workload, it is possible that the pilot act on trim switches without noticing.
Mitigating measure **Pilot:** Grip throttle and stick keeping fingers out of trim switches.		

Table 10
Controls to avoid UCA 8.

Induce pio by wide controls input		
Scenario	Associated causal factor	Rationale/Notes
When the nose gear loose contact with ground, pilot needs to compensate with rudder deflection.	Fast and wide applications of directional controls in sequence may cause the Dutch Roll (late roll response to yaw).	Dutch Roll gets worse when pilot inputs are in phase with aircraft reaction.
Mitigating measure **Pilot:** Apply pedal inputs smoothly and continuously.		

must be explained in the basic instruction, taking advantage of windy days to show the correct technique. Some aircraft operators and owners are already using the MMs presented to update doctrinal manuals and operational procedures to pilots and maintenance professionals. Even when fully loaded with external stores, the Super Tucano has a maximum takeoff weight bellow civilian standards for light aircraft, meaning that the amount of inertia in each axis should be similar. Thus, the MMs are applicable to every light single-engine low-wing aircraft.

Table 11
Controls to avoid UCA 9.

Land without following the blown tire procedure		
Scenario	Associated Causal Factor	Rationale/Notes
Realizing the bursting of a tire and keeping the gear down, pilot returns for an immediate landing.	In many aerobatic light aircraft, the complete emergency procedures are not taken on board.	Realizing that the flight will not continue as planned, the pilot wants to land as soon as possible to save time and fuel.
Mitigating measures **Operator:** When it is not feasible to keep all the aircraft manuals on board, provide a complete summary of the emergency procedures and its updating. **Pilot:** Request a holding area to follow carefully the complete emergency procedures for a blown tire.		

As strong crosswinds are rare in many places, constraints lose effectiveness with time. Therefore, these recommendations should be applied in a higher level of hierarchy, changing the doctrine and standards related to safety and followed by each operator, which might be interpreted as a formal learning opportunity (Maslen, 2014). Pilots

Table 12
Controls to avoid UCA 10.

Retract landing gear with blown tire		
Scenario	Associated causal factor	Rationale/Notes
Pilot retracts the landing gear with a burst tire by conditioned behavior or because did not realize the burst of one or more tires.	The landing gear is retracted with one or more blown tires causing damage to the aircraft and compromising the next lowering of the landing gear.	At high speed with gusts, it is natural that a pilot does not notice the bursting of a tire.
Mitigating measures		
Manufacturer: Develop a landing gear system that will not be damaged if the gear retracts with a tire burst.		
Manufacturer: Develop a pressure sensor that warns the pilot when the tire loses pressure.		
Operator: Check the possibility of installing a certified system of tire pressure monitoring.		
Pilot: Consider the tire burst as a critical emergency in the takeoff briefing.		

must be taught about the reasons behind constraints and MMs to be proactive when leading indicators (Leveson, 2015) of one of those scenarios is perceived.

The STPA analysis identified safety constraints that are not applied to current instructions and operations. Those findings could not be found with traditional chain-of-failure-events models because they relate to hazardous scenarios where no component has failed. This technique also leads to requirements that should be considered in future projects to guarantee safer crosswind takeoffs. Light aircraft manufacturers should follow those recommendations as a guide to develop more robust and reliable projects.

The new interpretation of the original classification of the Unsafe Control Actions on STPA's Step 1 was necessary to guarantee the complete understanding of pilots' mental models for the operation of single and multiple continuous close-loop controls. This understanding is necessary to explore the human factors related to each scenario in Step 2 because discrete inputs are related with decisions on applying or not a switch while in-the-loop continuous inputs are related with the deviation from a desired path and the experience of the controller on that machine. The same approach can be used in different fields, like the application of brakes on cars or steering on a boat.

6. Conclusion and future work

The new interpretation of the classification of Unsafe Control Actions (STPA's Step 1) applied to continuous closed-loop controls provides a better and more complete analysis of human factors issues. All future work with STPA considering similar control actions, even in different fields of study, might use the same approach to help in designing appropriate mitigating measures.

The hazard analysis technique STPA applied to the data collected in a flight test campaign permitted the identification of safer use of flight controls than the verified current instruction in civilian and military flight schools because it effectively maps control relations. The results are the new barriers that must be imposed and controlled by stakeholders to avoid accidents or reduce its consequences.

The advantages of considering continuous control actions in STPA are extended to similar analysis for light high-wing aircraft, widely used in civilian basic instruction, and light twin-engine aircraft. Heavier aircraft are less susceptible to crosswinds, but the mitigating measures might be adapted for executive, military and commercial aircraft.

Acknowledgments

The authors thank Professor Nancy Leveson for reviewing the manuscript and the pilots, engineers and mechanics from IPEV who participated in the crosswind flight testing campaign and validation of the analysis. The first author was funded by a CNPq – Brazil scholarship.

Appendix A. Supplementary material

Supplementary data associated with this article can be found, in the online version, at http://dx.doi.org/10.1016/j.ssci.2018.04.013.

References

Altabbakh, H.M., 2013. Risk Analysis: Comparative Study of Various Techniques. Missouri University of Science and Technology.
Anderson, J. Jr., 1985. Fundamentals of Aerodynamics, Fundamentals of aerodynamics, doi:10.1036/0072373350.
Castilho, D.S., 2015. Aplicação da técnica STPA na análise de risco da decolagem de aeronaves leves com vento cruzado limítrofe. Instituto Tecnológico da Aeronáutica.
CENIPA, 2015. Panorama Estatistico da Aviacao Civil Brasileira.
Checkland, P., 1981. Systems Thinking, Systems Practice, doi:10.1016/0143-6228(82)90039-X.
Dekker, S., Cilliers, P., Hofmeyr, J.H., 2011. The complexity of failure: implications of complexity theory for safety investigations. Saf. Sci. 49, 939–945. http://dx.doi.org/10.1016/j.ssci.2011.01.008.
Edenhofer, O., Pichs-Madruga, R., Sokona, Y., 2014. Climate Change 2014: Mitigation of Climate Change.
FAA, 2010. Weather-Related Aviation Accident Study 2003–2007.
France, M.E., 2017. Engineering for Humans: A New Extension to STPA. Massachusetts Institute of Technology, . , .
Johnson, K.E., 2017. Systems-Theoretic Safety Analyses Extended for Coordination. Massachusetts Institute of Technology.
Leveson, N., 2015. A systems approach to risk management through leading safety indicators. Reliab. Eng. Syst. Saf. 136, 17–34. http://dx.doi.org/10.1016/j.ress.2014.10.008.
Leveson, N.G., 2011. Engineering a safer world: systems thinking applied to safety. Vasa. http://dx.doi.org/10.1017/CBO9781107415324.004.
Maslen, S., 2014. Learning to prevent disaster: an investigation into methods for building safety knowledge among new engineers to the Australian gas pipeline industry. Saf. Sci. 64, 82–89. http://dx.doi.org/10.1016/j.ssci.2013.11.027.
Montes, D.R., 2015. Using STPA to Inform Developmental Product Testing. Massachusetts Institute of Technology.
Montes, D.R., 2015. Using STPA to Investigate Test Safety.
Rasmussen, J., 1997. Risk management in a dynamic society: a modelling problem. Saf. Sci. http://dx.doi.org/10.1016/S0925-7535(97)00052-0.
Thomas, J., 2013. Extending and Automating a Systems-theoretic Hazard Analysis for Requirements Generation and Analysis. Massachusetts Institute of Technology.
Thornberry, C.L., 2012. Extending the Human Controller Methodology in Systems - Theoretic Process Analysis (STPA).
Young, W., 2014. Applying System-Theoretic Process Analysis for Security (STPA-SEC) to Support Mission Assurance and Security.