

# Aircraft Loss-of-Control: Analysis and Requirements for Future Safety-Critical Systems and their Validation

Christine M. Belcastro  
NASA Langley Research Center  
Dynamic Systems and Control  
Hampton, Virginia  
christine.m.belcastro@nasa.gov

**Abstract**—Loss of control remains one of the largest contributors to fatal aircraft accidents worldwide. Aircraft loss-of-control accidents are complex, resulting from numerous causal and contributing factors acting alone or more often in combination. Hence, there is no single intervention strategy to prevent these accidents. This paper summarizes recent analysis results in identifying worst-case combinations of loss-of-control accident precursors and their time sequences, a holistic approach to preventing loss-of-control accidents in the future, and key requirements for validating the associated technologies.

**Keywords**—Aircraft loss of control; Loss-of-control accident analysis; Integrated systems solution to aircraft loss of control; Validation of safety-critical systems operating under off-nominal conditions

## I. INTRODUCTION

Aircraft loss of control (LOC) is one of the largest contributors to fatal accidents across all vehicle classes and operational categories [1], [2], and [3]. The 2010 Boeing report of Ref. [1] summarizes commercial jet airplane accidents that occurred worldwide between 1959 and 2009 involving aircraft that are heavier than 60,000 pounds maximum gross weight. In this report, aircraft loss-of-control is the leading fatal accident category, with 20 accidents occurring in this time period that resulted in 1,848 fatalities. The 2008 report of Ref. [2] on worldwide fatal accidents by the Civil Aviation Authority (CAA) Safety Regulation Group in the United Kingdom (UK) determined LOC to be the second-leading consequence (38.9%, 110 of 283 accidents) resulting from numerous causal and contributing factors – second only to post-crash fire. The report by Alliant Techsystems of Ref. [3] looked across all U.S. operational categories (Part 121, Scheduled Part 135, Non-Scheduled Part 135 and Part 91) between 1988 and 2004 and found that aircraft loss of control accidents “were responsible for more than half of the aviation fatalities during that time period” – despite having contributed to less than 20% of the U.S. aviation accidents in the data set.

Aircraft LOC is also complex, resulting from numerous causal and contributing factors acting alone or more often in combination. In Reference [4], 74 LOC accidents were reviewed for the time period 1993 – 2007, which resulted in

42 hull loss accidents and 3241 fatalities. The analysis of this reference groups the accidents into the categories aerodynamic stall, flight control system, spatial disorientation of the crew, contaminated airfoil, and atmospheric disturbance. There is also a detailed discussion of accidents in each of these categories and a comparison with older accidents that occurred prior to 1993 in order to identify emerging trends. This reference also provides a definition of aircraft upset conditions, which is defined therein as “any uncommanded or inadvertent event with an abnormal aircraft attitude, rate of change of aircraft attitude, acceleration, airspeed, or flight trajectory”. Due to the complexity of LOC accidents, no single intervention strategy can be identified to prevent them.

This paper summarizes key recent results presented in References [5], [6], and [7] to address aircraft loss of control. Ref. [5] presents a detailed analysis of LOC accidents in which worst case combinations of causal and contributing factors are identified as well as how they sequence in time. Future potential risks are also identified. Ref. [6] presents a future integrated systems concept for preventing aircraft LOC accidents, and Ref. [7] presents requirements and a process for their validation and verification (V&V), with an emphasis on validation. Key results from these references are summarized in Sections II, III, and IV, respectively. Section V provides a summary and some concluding remarks.

## II. AIRCRAFT LOC ACCIDENT ANALYSIS

A review of 126 LOC accidents (predominantly from Part 121, including large transports and smaller regional carriers) occurring between 1979 and 2009 (30 years) that resulted in 6087 fatalities was performed for the analysis, and a listing of these accidents is provided in the Appendix of Ref. [5]. This accident set does not represent an exhaustive search throughout this time period, and it does not include military, private, cargo, charter, and corporate accidents. Russian aircraft accidents were also excluded due to a general lack of detailed information in the associated reports. Of this total accident set, 91 accidents resulting in 4190 fatalities occurred between 1994 and 2009 (15 years). The review was based on accident reports available on the Aviation Safety Network [8] and National Transportation Safety Board (NTSB) [9]

websites. The level of detail in analyzing each accident was therefore dependent on the level of detail provided in the accident reports. Information from each report was transcribed into a categorized set of causal and contributing factors, using the following scheme. The causal and contributing factors were grouped into three categories: adverse onboard conditions, vehicle upsets, and external hazards and disturbances.

Adverse onboard conditions included:

- vehicle impairment (including inappropriate vehicle configuration, contaminated airfoil due to icing, and improper vehicle loading);
- system faults, failures, and errors (resulting from design flaws, software errors, or improper maintenance actions);
- vehicle damage to airframe and engines (resulting from fatigue cracks, foreign objects, overstress during upsets or upset recovery, etc.); and
- inappropriate crew response (including pilot-induced oscillations, spatial disorientation, mode confusion, ineffective recoveries, crew impairment, and failures to take appropriate actions).

External hazards and disturbances included:

- poor visibility;
- wake vortices;
- wind shear, turbulence, and thunderstorms;
- snow and icing conditions; and
- abrupt maneuvers for obstacle avoidance or collisions.

Vehicle upsets included:

- abnormal attitude;
- abnormal airspeed, angular rates, or asymmetric forces;
- abnormal flight trajectory;
- uncontrolled descent (including spiral dive); and
- stall/departure from controlled flight.

A basic analysis of the contributions of each causal/contributing factor to the 126 accidents is given in Table 1. It should be noted in Table 1 that the factors are not mutually exclusive. For example, 119 LOC accidents involved one or more adverse onboard conditions, and the frequency of each individual factor within this category is listed. These numbers do not add up to 119, however, because there were many accidents involving more than one subfactor. Similarly, adding the number of accidents listed for the three categories exceeds the 126 total because many accidents involved multiple categories. The 23 accidents related to vehicle damage consisted of 20 airframe and system damage conditions, and 3 engine damage conditions. Table 1 is useful for determining the number of accidents and fatalities associated with individual causal and contributing factors, but it does not provide any information on combinations or sequencing of these factors. Nonetheless, this table identifies System Faults/Failures/Errors, Vehicle Impairment/Damage, Inappropriate Crew Response, Stall/Departure, Atmospheric Disturbances related to Wind Shear/Gusts, and Snow/Icing as the most significant contributors to the number of fatalities.

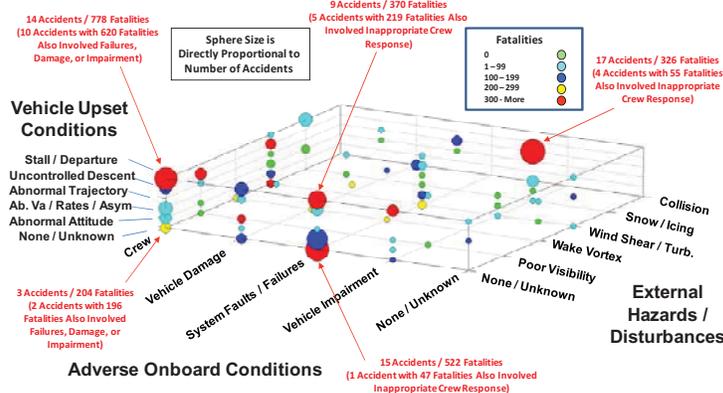
The following subsections A and B address combinations and sequencing of LOC causal and contributing factors, respectively. Subsection C addresses future risks.

**Table 1. Contributions to LOC Accidents and Fatalities by Individual Causal and Contributing Factors [5]**

Factor	Accidents	%	Fatalities	%
<b>Adverse Onboard Conditions</b>	<b>119</b>	<b>94.4</b>	<b>5683</b>	<b>93.4</b>
Vehicle Impairment	33	26.2	1134	18.6
System Faults / Failures / Errors	57	45.2	2807	46.1
Vehicle Damage	23	18.2	1780	29.2
Inappropriate Crew Response	54	42.8	2818	46.3
<b>Vehicle Upsets</b>	<b>98</b>	<b>77.8</b>	<b>4523</b>	<b>74.3</b>
Abnormal Attitude	18	14.3	219	3.60
Abnormal Airspeed / Angular Rates / Asymmetric Forces	14	11.1	701	11.5
Abnormal Flight Trajectory	4	3.2	272	4.47
Uncontrolled Descent	15	11.9	773	12.7
Stall / Departure	49	38.9	2622	43.1
<b>External Hazards &amp; Disturbances</b>	<b>61</b>	<b>48.4</b>	<b>3246</b>	<b>53.3</b>
Poor Visibility	9	7.1	556	9.1
Wake Vortices	4	3.2	402	6.6
Wind Shear / Gusts / Thunderstorms	18	14.3	1126	18.5
Snow / Icing	28	22.2	595	9.8
Abrupt Maneuver / Collision	3	2.4	189	3.1

*A. Worst Case Analysis*

In order to identify worst case combinations of LOC causal and contributing factors (as defined by number of accidents and resulting fatalities), 3-dimensional scatter plots were generated. Figure 1 shows the key result from this analysis.



**Figure 1. Identification of Overlap in LOC Causal and Contributing Factor Combinations, 1979 – 2009 [5].**

The three dimensions are aligned with the three categories identified in Table 1. Sphere size is directly proportional to the number of accidents, and sphere color depicts the number of fatalities as indicated by the legend. As indicated in Figure 1, worst case combinations include: system faults and failures occurring alone and in combination with upsets, icing conditions resulting in vehicle impairment, and inappropriate crew response combined with upset conditions. There are also a significant number of accidents and fatalities resulting from:

vehicle damage occurring alone and combined with upsets, icing combined with inappropriate crew response and upsets, and wind shear and turbulence combined with inappropriate crew response and vehicle upsets. As noted in Figure 1 with red text, there is some overlap (i.e., some combinations that are not mutually exclusive) in the scatter plot, especially within the adverse onboard conditions dimension. This overlap is due to a significant number of accidents that involved multiple adverse onboard conditions. For example, some of the accidents shown for system faults and failures also involved inappropriate crew response. Alternatively, many of the accidents shown for inappropriate crew response also involved other adverse onboard conditions, such as vehicle impairment, failure, or damage. While there is some overlap in the external hazards and disturbances and the vehicle upset dimensions, it is generally much smaller than the onboard dimension.

Ref. [5] also analyzed the most recent 15 years of accident data in the set, as well as those involving no fatalities, in order to identify any emerging issues. No significant emergent trends were evident.

### B. Time Sequence Analysis

An analysis of the time sequencing of the LOC causal and contributing factors was performed for the 30-year data set. Table 2 provides a summary of this sequencing.

**Table 2. Sequencing of LOC Causal & Contributing Factors [5]**

Factor	1st	2nd	3rd	4th	5th
<b>Adverse Onboard Conditions</b>	<b>69</b>	<b>69</b>	<b>24</b>	<b>6</b>	<b>0</b>
Vehicle Impairment	3	29	3	0	0
System Faults / Failures / Errors	42	11	4	0	0
Vehicle Damage	6	7	5	5	0
Inappropriate Crew Response	18	22	12	1	0
<b>External Hazards &amp; Disturbances</b>	<b>54</b>	<b>6</b>	<b>0</b>	<b>0</b>	<b>0</b>
Poor Visibility	7	0	0	0	0
Wake Vortices	3	1	0	0	0
Wind Shear / Gusts / Thunderstorms	14	3	0	0	0
Snow / Icing	27	1	0	0	0
Abrupt Maneuver / Collision	3	1	0	0	0
<b>Vehicle Upsets</b>	<b>3</b>	<b>36</b>	<b>47</b>	<b>15</b>	<b>1</b>
Abnormal Attitude	0	12	3	3	0
Abnormal Airspeed / Angular Rates / Asymmetric Forces	0	3	7	4	0
Abnormal Flight Trajectory	1	1	3	1	0
Uncontrolled Descent	0	5	7	2	1
Stall / Departure	2	15	27	5	0

It should be noted that these sequences were identified without overlap. That is, there is no “double bookkeeping” of sequences in Table 2. Thus, the total number of initiating factors under column 1 sums to the total number of LOC accidents, since all LOC accidents result from at least 1 causal or contributing factor. Table 2 indicates that LOC events are usually first precipitated by an adverse onboard condition or an external hazard or disturbance. Moreover, external hazards and disturbances rarely occur further downstream in LOC sequences. Vehicle upsets are rarely the initial factor but

rather an outcome of an external hazard or adverse onboard condition. Within adverse onboard conditions, system faults, failures, and errors are the leading initial factor, and inappropriate crew response is the second most likely initial event. Relative to external hazards and disturbances, the leading initial factor is icing, followed by wind shear, gusts, and thunderstorms. Adverse onboard conditions are also the most likely factor to occur second in the chain of events leading to aircraft LOC, with vehicle impairment being the most likely secondary factor to occur. This is due to vehicle impairment resulting from icing conditions (i.e., contaminated airfoil or reduced engine performance), faults or damage. Vehicle upsets most often occur as the second, third, or fourth factor in the LOC sequence. Only one 5-factor sequence was identified in this data set.

An analysis was also performed of each LOC sequence. This analysis is summarized in Table 3.

**Table 3. Summary of LOC Accident Sequences [5]**

Initial Factor in LOC Sequence	Accidents	%	Fatalities	%
<b>Adverse Onboard Conditions</b>	<b>69</b>	<b>54.8</b>	<b>3733</b>	<b>61.3</b>
Vehicle Impairment	3	2.4	186	3.1
System Faults / Failures / Errors	42	33.3	1544	29.0
Vehicle Damage	6	4.8	908	14.9
Inappropriate Crew Response	18	14.3	1095	14.3
<b>External Hazards &amp; Disturbances</b>	<b>54</b>	<b>42.8</b>	<b>2228</b>	<b>36.6</b>
Poor Visibility	7	5.5	438	7.2
Wake Vortices	3	2.4	137	2.2
Wind Shear / Gusts / Thunderstorms	14	11.1	874	14.4
Snow / Icing	27	21.4	590	9.7
Abrupt Maneuver / Collision	3	2.4	189	3.1
<b>Vehicle Upsets</b>	<b>3</b>	<b>2.4</b>	<b>126</b>	<b>2.1</b>
Abnormal Attitude	0	0	0	0
Abnormal Airspeed / Angular Rates / Asymmetric Forces	0	0	0	0
Abnormal Flight Trajectory	1	0.8	117	1.9
Uncontrolled Descent	0	0	0	0
Stall / Departure	2	1.6	9	0.2
<b>Totals</b>	<b>126</b>	<b>100</b>	<b>6087</b>	<b>100</b>

Table 3 provides the number of accidents and fatalities (and associated percentages) relative to each causal and contributing factor as the initial factor in the LOC sequence. Defining the LOC sequences in terms of the initiating factor allowed a comprehensive assessment without overlap. As indicated in Table 3, LOC events initiated by adverse onboard conditions comprised 54.8% of the accidents and 61.3% of the fatalities within the data set considered in this analysis. Of these, system failures, faults, and errors initiated 33.3% of accidents and 29% of fatalities, followed by inappropriate crew response, vehicle damage, and vehicle impairment. External hazards and disturbances initiated 42.8% of the accidents and 36.6% of the fatalities in the LOC accidents considered. Within this category, icing represented 21.4% of accidents and 9.7% of fatalities, whereas wind shear, turbulence, and thunderstorms initiated 11.1% of accidents and 14.4% of fatalities. These factors were followed in

frequency of occurrence by poor visibility, wake vortices, and abrupt maneuver or collision (with the last two having the same frequency of occurrence). It is interesting to note that icing initiated more accidents, but wind-related disturbances resulted in more fatalities. This is because the predominance of icing-induced accidents in the data set of this study involved smaller aircraft, whereas the preponderance of wind-induced accidents in this data set involved large transports. As indicated previously, vehicle upsets are rarely the precipitating factor in the LOC sequence, with these comprising 2.4% of the accidents and 2.1% of the fatalities considered in this study. Within this category, stall/departure initiated 1.6% of the accidents and 0.2% of fatalities, and abnormal flight trajectory initiated 0.8% of accidents and 1.9% of fatalities in the data set. While upsets are not usually the precipitating factor, many LOC sequences include vehicle upset somewhere in the chain of events (as indicated in Table 2).

Ref. [5] identified 52 unique LOC sequences from the accident data. In order to condense these sequences into smaller, more actionable groupings, they were also combined and generalized. The generalized sequences from Ref. [5] are shown in Figure 2 along with the associated number of accidents and fatalities.

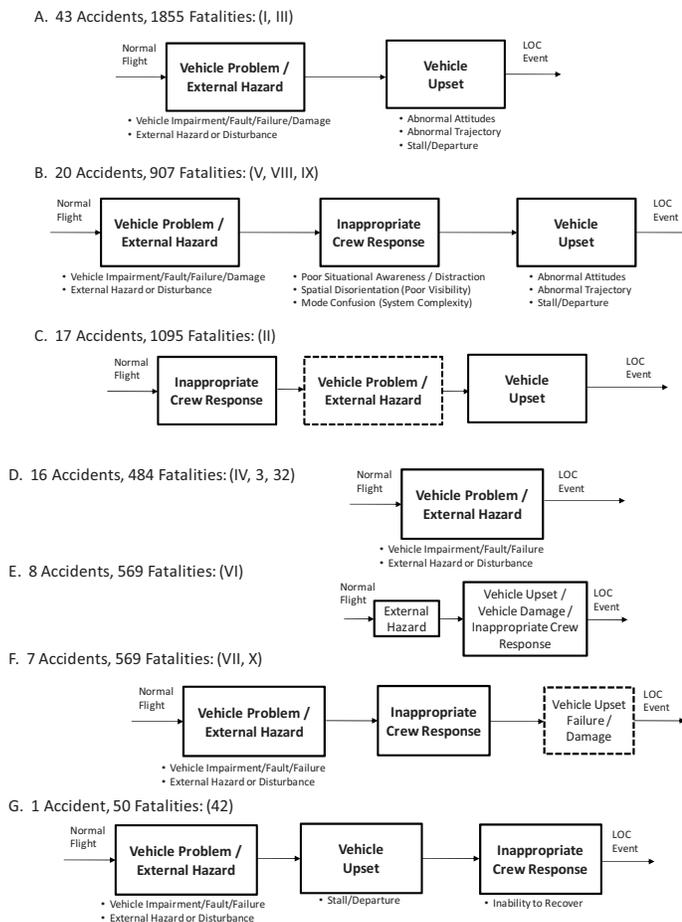


Figure 2. Generalized LOC Accident Sequences [5].

Dashed boxes in Figure 2 represent factors that occurred in some subset within the sequence. These 7 generalized sequences represent 112 accidents (88.9%) and 5529 fatalities (90.8%).

### C. Future Potential Risks

In addition to looking at historical accident data, potential future LOC accident risks should be identified relative to known (as well as new) precursors. This is more difficult, because (without data) it becomes more speculative. However, the identification of potential areas of vulnerability might enable the development of a comprehensive intervention strategy that anticipates and mitigates these future potential risks. One area of consideration is airspace operation under the Next Generation (NextGen) Air Transportation System [10]. The NextGen concept of operations provides an integrated view of airspace operations in the 2025 timeframe and includes high-density, all-weather, and self-separation operational concepts. There is also expected to be mixed-capability aircraft operating within the same airspace, including piloted aircraft and unmanned aircraft systems. High-precision 4-D trajectories are envisioned that will enable safely flying with closer spacing to inclement weather, terrain, and other aircraft, and these trajectories can be altered if necessary during the flight. Other areas of consideration include increasing airspace and vehicle system complexity without developing comprehensive methods for their validation and verification (V&V), and increased automation without improved crew interfaces.

In an effort to identify areas of potential future LOC risk in terms of known precursors, Figure 3 illustrates several areas of possible increase in causal and contributing factors with the potential for increased LOC accidents or incidents.

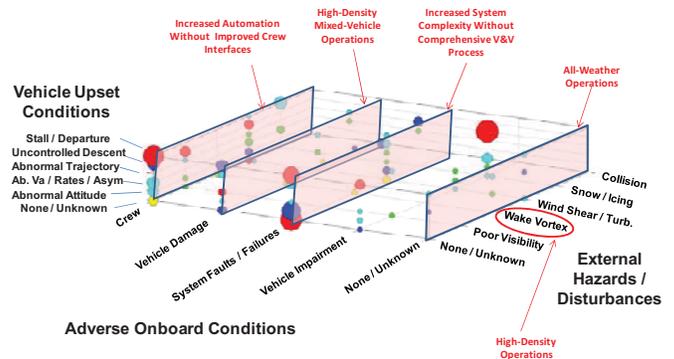


Figure 3. Potential Areas of Future Increased LOC Risk [5].

If all-weather operations and highly precise trajectories that enable closer spacing to inclement weather increase the probability of an aircraft actually encountering a weather hazard during flight, this could result in a larger number of weather-related LOC accidents (particularly in the terminal area). If airspace and vehicle system complexity is increased without comprehensive methods for their V&V, this could

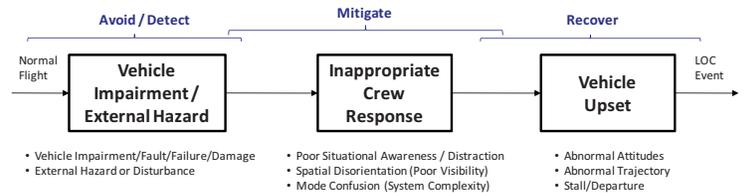
lead to a larger number of LOC events initiated by system faults, failures, and errors. If high-density mixed-vehicle operations and high-precision tracking that enables closer spacing between aircraft increase the probability of aircraft encountering other aircraft during flight, this could result in a larger incidence of wake-induced LOC events or ultimately those initiated by vehicle damage resulting from mid-air collisions. Increased automation without improved crew interfaces could result in a higher incidence of LOC events precipitated by inappropriate crew actions. New LOC precursors associated with failure modes of future vehicle and airspace systems must also be identified and considered during V&V of these systems, and their potential ramifications considered under off-nominal operating conditions. New types of crew-induced LOC precursors must also be considered.

### III. FUTURE SYSTEM CONCEPT

Due to the complexity of aircraft LOC events (i.e., accidents and incidents), no single intervention strategy can be identified to effectively prevent them. Moreover, there are currently no coordinated or integrated systems or research efforts for addressing aircraft LOC. Current aircraft control systems are primarily designed for operation under nominal conditions, and often disengage (i.e., return control authority to the pilot) under off-nominal conditions. Current flight deck systems provide limited information under off-nominal conditions associated with aircraft LOC. While many current systems have built-in tests for assessing system, subsystem, or component health, these lack the integrated capability for assessing vehicle health across them, or for the prevention of cascading failures across multiple systems. There is also no existing capability to assess vehicle health and external hazards in terms of their impact on flight safety. Improved crew training and operational procedures for off-nominal conditions might enable improved crew response during LOC events, but this is dependent on the capability to effectively characterize vehicle dynamics and control characteristics under off-nominal conditions. Advanced onboard systems that provide effective detection and resilience under off-nominal conditions could enable improved situational awareness and vehicle response under LOC events, but this requires the effective integration and validation of the associated technologies.

The analysis of Section II can provide insight into preventing LOC accidents. Figure 4 shows an example generalized sequence from Figure 2 with an intervention strategy defined to break the sequence at all stages via avoidance, detection, mitigation, and recovery technologies. Avoidance technologies include enhanced models and simulations for characterizing LOC conditions for improved crew training, advanced vehicle and system design methods that reduce failures and damage, and forward-looking sensors for avoidance of external hazards and disturbances. Detection technologies include vehicle health management technologies that provide the capability to prevent catastrophic failure through early anomaly detection as well as rapid failure

detection and isolation onboard the aircraft. Mitigation technologies include failsafe guidance and control systems that ensure stability, maximize vehicle performance and handling qualities, and enable safe maneuvering under LOC conditions, as well as flight deck interface systems that provide improved crew situational awareness, countermeasures for crew errors, and variable autonomy to optimize the synergy between the crew and automation. The mitigation technologies would also include specific functions for upset prevention under LOC conditions. Recovery technologies include guidance and control algorithms for safe and reliable upset recovery. These algorithms would prevent entry into unrecoverable conditions, and would include vehicle constraints during the recovery (e.g., normal structural loading constraints as well as vehicle constraints resulting from impairment or damage). Variable autonomy interface functions would be utilized to optimize involvement between the crew and the system. Figure 5 presents a holistic approach for developing the technologies needed to prevent LOC accidents using this intervention strategy. Advanced modeling and simulation technologies must be developed for characterizing off-nominal condition effects on vehicle dynamics and control characteristics, including vehicle failures and damage, vehicle upset conditions, wind shear and turbulence, wake vortices, icing, and key combinations of these (as identified in Reference [3]). This capability can be utilized for improved crew training under off-nominal conditions, and for the development and validation of advanced onboard integrated systems technologies. Databases, models, and real-time modeling methods can also be utilized onboard the aircraft for characterizing and assessing the effects of off-nominal conditions. Enhanced models, databases, and simulations can also be utilized for improved crew training under LOC conditions.



**Figure 4. Example Generalized LOC Accident Sequence and Intervention Strategy [6].**

Vehicle health management (VHM) technologies must be developed for continually assessing and predicting the health of the airframe, propulsion system, and avionics systems in real-time, as well as remaining useful life. In-situ sensing and estimation methods are needed for distinguishing between anomalous system behavior and external disturbances. These technologies provide the capability to prevent catastrophic failures and damage through the early detection of anomalies, as well as the capability to rapidly detect, identify, characterize, and contain failures and damage when they do

occur.

Flight safety assurance (FSA) technologies must be developed to provide the capability of continually assessing and predicting the impact of off-nominal conditions on vehicle flight safety, and to provide resilient guidance and control capabilities under off-nominal conditions. These capabilities can be utilized onboard the aircraft for mitigation of system failures and vehicle impairment or damage, external disturbance rejection, and upset prevention and recovery. They can also be utilized to support improved crew training, especially for providing insight into non-intuitive control strategies required for upset recovery. Resilient guidance functions, such as trajectory generation under vehicle constraints (e.g., vehicle impairment or damage), must also be developed.



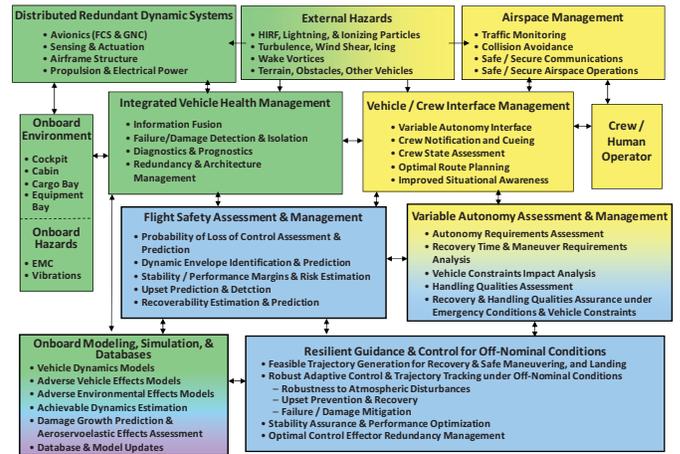
**Figure 5. A Holistic Approach to Prevent Aircraft LOC Accidents [6].**

Effective crew-system interface technologies must be developed for providing improved situational awareness and crew response under off-nominal conditions. These technologies include effective visual and aural methods for notification and cueing, and variable autonomy systems that enable optimal partitioning of authority between the crew and automation. Effective information exchange and coordination between the vehicle and airspace operations must also be achieved. Remote sensing technologies must be developed for avoidance of external hazards and disturbances.

Validation and verification (V&V) technologies must be developed for the comprehensive evaluation of these technologies for operation under off-nominal conditions, and to enable the identification of system limitations and constraints as well as safe and unsafe operating conditions (and their boundaries).

Based on the holistic approach of Figure 5, an onboard integrated systems concept can be developed. One such concept, called AIRSAFE, is presented in Figure 6, including a detailed depiction of subsystem functions and capabilities. The core subsystems include vehicle health management

(shown in green), vehicle flight safety management and resilient control (shown in blue), and crew-system interfaces (shown in yellow).



**Figure 6. Aircraft Integrated Resilient Safety Assurance & Failsafe Enhancement (AIRSAFE) System Concept and Functions [6].**

Onboard modeling capability is reflected by purple. These core functions and capabilities directly correlate to those depicted in Figure 5. Multi-colored boxes represent shared functions between the associated subsystems. A detailed description of the AIRSAFE System concept, including subsystem interfaces, is given in Reference [11], and Ref. [6] provides a synopsis description as well as an initial assessment of the potential effectiveness of the AIRSAFE System concept in providing LOC sequence interventions.

#### IV. VALIDATION AND VERIFICATION (V&V)

V&V becomes much more difficult for safety-critical resilient systems operating under off-nominal conditions, such as the AIRSAFE System Concept of Section III. Due to the huge operational space, there are too many conditions to fully analyze, simulate, and test. While there are numerous technical challenges associated with this problem, some key technical challenges are summarized below.

- Development and Validation of Physics-Based Off-Nominal Conditions and Effects Models
  - Requires modeling of
    - » adverse onboard conditions (e.g., faults, failures, damage)
    - » abnormal flight conditions (e.g., unusual attitudes, stall, stall/departure, other vehicle upset conditions)
    - » external hazards and disturbances (e.g., icing, wind shear, wake vortices, turbulence)
    - » Worst-Case Combinations (as Determined from LOC Accident/Incident Data)
  - Requires data and/or experimental methods for off-nominal conditions, which may not be available
  - Can involve multidisciplinary coupled effects
  - Cannot fully replicate in-flight loss-of-control environment
- V&V of Adaptive Diagnostic, Prognostic, and Control Algorithms Operating under Off-Nominal Conditions

- Involves a variety of nonlinear mathematical constructs (inference engines, probabilistic methods, physics-based, neural networks, artificial intelligence, etc.)
- May involve onboard adaptation that can result in stochastic system behavior
- Involves fusion and reasoning algorithms for sensor data, information processing, and decisions
- Requires methods for establishing probabilities of
  - » false alarms and missed detections
  - » incorrect identifications and decisions
  - » loss of stability, recoverability, and control
- Requires methods & metrics for establishing off-nominal condition coverage, reliability, and accuracy for diverse algorithms & multiple objectives
- Requires integrated multi-disciplinary system assessment methods
  - » performance assessment
  - » error propagation and effects assessment
  - » inter-operability effectiveness assessment
- System Verification and Safety Assurance
  - Involves large-scale complex interconnected software systems
  - Involves potentially fault tolerant and reconfigurable hardware
  - May involve adaptive and reasoning algorithms with stochastic behavior
  - Requires verification methods for a complex system of systems
- V&V Predictive Capability Assessment
  - Requires methods to demonstrate compliance to certification standards for an extensive set of off-nominal conditions (and their combinations) that cannot be fully replicated
  - Requires methods for determining (and quantifying) level of confidence in V&V process and results for demonstrating compliance

These technical challenges can be utilized in defining V&V process requirements. Key components of the V&V process include system/subsystem validation, system/subsystem verification, and V&V predictive capability assessment. Each of these V&V components requires the development of methods, tools, and testbeds to perform analysis, simulation / ground testing, and flight testing. Moreover, each method, tool, and testbed must be developed to assess system mitigation effectiveness under off-nominal precursor conditions to aircraft loss-of-control accidents in order to reduce (or prevent) them in the future. V&V metrics must be defined for the diverse set of algorithms associated with the subsystems and integrated system, and new methods, tools, and testbeds developed (as needed) to assess these metrics. Based on an analysis of the V&V problem [12], the V&V process requirements for future systems designed for operation under off-nominal conditions (such as the AIRSAFE System concept) can be defined as depicted in Figure 7. This figure shows V&V process components, methods, and some example algorithm validation metrics that are required for AIRSAFE subsystem and integrated system technologies. The core V&V methods of analysis, simulation/ground testing, and flight testing are applicable to each of the core V&V components and take on different meanings for each. Metrics must be

developed for assessment of each core component using the appropriate methods. Although Figure 7 shows some example metrics for algorithm validation, and illustrates that these are dependent on the algorithm type, metrics are needed for each core V&V component.

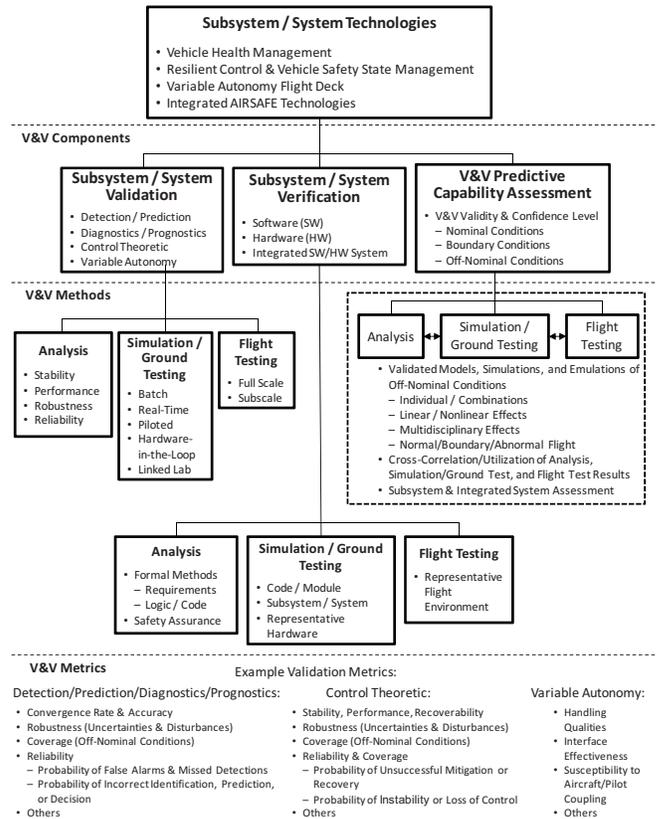


Figure 7. V&V Process Requirements for the AIRSAFE System Concept [7].

Based on the V&V process requirements of Figure 7, a detailed V&V process can be developed for complex integrated resilient systems, such as the AIRSAFE System concept of Figure 6. A high-level overview of the integrated V&V process is presented in Figure 8. The colors of the blocks correlate to the associated AIRSAFE subsystem functions depicted in Figure 6 – that is, blue correlates to integrated resilient control and flight safety management functions, green represents vehicle health management functions, and yellow is associated with crew interface functions. Multi-colored boxes in Figure 8 represent evaluation of the associated integrated subsystem functions. Analysis, simulation, and experimental V&V components are organized in the V&V process of Figure 8 moving from left to right, and system evaluation becomes more highly integrated moving to the center (from above and below) and to the right. Also as indicated in Figure 8, results from the V&V process are utilized as an iterative process for refining the algorithm design of each subsystem. Ref. [7] presents a more detailed description of the controls-related components of the V&V process (including methods and interfaces). This is depicted

in Figure 8 by the red box around the lower two rows of the process. A detailed summary of recent research accomplishments is also provided in Ref. [7]. Reference [12] provides a detailed description of the entire process.

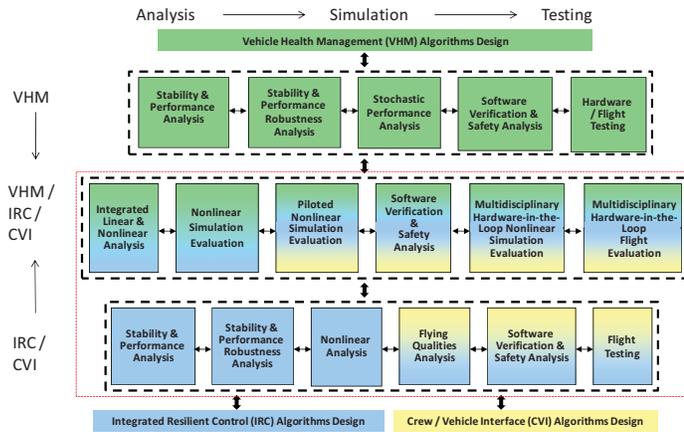


FIGURE 8. V&V PROCESS OVERVIEW [7].

## V. CONCLUSION

Aircraft loss of control is the largest aircraft accident category, and results in the highest number of fatalities among the worldwide commercial jet fleet. It is also the most complex accident category, resulting from numerous causal and contributing factors that act individually or (more often) combine to result in a loss of control event (accident or incident). These factors are off-nominal conditions that occur onboard the aircraft, as external disturbances, or as abnormal flight conditions. To address aircraft loss of control, a detailed LOC accident analysis was performed to identify worst-case combinations of causal and contributing factors as well as their temporal ordering or sequencing in time. The data set used in the analysis consisted of 126 LOC accidents that resulted in 6087 fatalities during the 30-year period 1979 – 2009. Scatter plots were used in identifying worst-case combinations of LOC accident precursors, and a set of 7 generalized LOC sequences was defined, which represent 88.9% of the accidents and 90.8% of the fatalities considered in this study. Future risks with the potential to increase LOC accidents were also considered.

A holistic research and technology development approach was presented for reducing aircraft LOC accidents, as well as an associated integrated system concept, called the Aircraft Integrated Resilient Safety Assurance and Failsafe Enhancement (AIRSAFE) System. The holistic approach requires the development of (i) modeling and simulation technologies for characterizing vehicle dynamics and control characteristics under off-nominal precursor conditions associated with LOC events; (ii) vehicle health management technologies for the detection, identification, characterization, and containment of vehicle and system failures and damage (as well as their prevention through improved maintenance, inspection, and vehicle design); (iii) flight safety management and resilient control technologies for the rapid assessment of

off-nominal condition effects and their mitigation; and (iv) crew interface technologies for improved situational awareness and variable autonomy under off-nominal conditions.

The AIRSAFE System technologies are being developed for safety-critical operation under off-nominal conditions, and their V&V poses significant technical challenges. The V&V problem and the research approach being taken to address it were described. V&V process requirements were presented, which integrated analytical, simulation, and experimental methods, software tools, and testbeds. A detailed V&V process was defined for application to the AIRSAFE System concept.

## ACKNOWLEDGMENT

The AIRSAFE System concept and V&V process presented in this paper were developed in collaboration with Dr. Celeste M. Belcastro of NASA Langley Research Center, who lost her courageous and selfless battle with cancer and passed from this life on August 22, 2008. Continued work in these areas, as well as in aircraft LOC accident prevention, is dedicated to her memory.

## REFERENCES

- [1] “Statistical Summary of Commercial Jet Airplane Accidents, Worldwide Operations, 1959-2009”; Boeing Commercial Airplanes, July 2010.
- [2] “Global Fatal Accident Review 1997-2006”, Civil Aviation Authority, Safety Regulation Group, CAP 776, July 21, 2008. URL: <http://www.caa.co.uk/docs/33/CAP776.pdf>
- [3] Evans, Joni K., “An Examination of In Flight Loss of Control Events During 1988–2004”, Alliant Techsystems, Inc., NASA Langley Research Center, Contract No.: TEAMS:NNL07AM99T/R1C0, Task No. 5.2, 2007. URL: <http://www.boeing.com/news/techissues/pdf/statsum.pdf>
- [4] Lambregts, A. A., Nesemeier, G., Wilborn, J. E., and Newman, R. L., “Airplane Upsets: Old Problem, New Issues”, *AIAA Modeling and Simulation Technologies Conference and Exhibit*, 2008, AIAA 2008-6867.
- [5] Belcastro, Christine M. and Foster, John V., “Aircraft Loss-of-Control Accident Analysis”, *AIAA Guidance, Navigation, and Control Conference*, Toronto, Canada, 2010.
- [6] Belcastro, Christine M. and Jacobson, Steven R., “Future Integrated Systems Concept for Preventing Aircraft Loss-of-Control Accidents”, *AIAA Guidance, Navigation, and Control Conference*, Toronto, Canada, 2010.
- [7] Belcastro, Christine M., “Validation and Verification of Future Integrated Safety-Critical Systems Operating under Off-Nominal Conditions”, *AIAA Guidance, Navigation, and Control Conference*, Toronto, Canada, 2010.
- [8] Aviation Safety Network (ASN) Database Available at <http://aviation-safety.net/database/>
- [9] National Transportation Safety Board (NTSB) Database Available at <http://www.ntsb.gov/ntsb/query.asp>
- [10] Joint Planning and Development Office, “Concept of Operations for the Next Generation Air Transportation System”, Version 3, October 2009, Available at <http://www.jpdo.gov/library.asp>
- [11] Belcastro, Christine M., and Belcastro, Celeste M.: Future Research Directions for the Development of Integrated Resilient Flight Systems to Prevent Aircraft Loss-of-Control Accidents, Part I: System Technologies; NASA TM (being finalized for publication).
- [12] Belcastro, Christine M., and Belcastro, Celeste M.: Future Research Directions for the Development of Integrated Resilient Flight Systems to Prevent Aircraft Loss-of-Control Accidents, Part II: Validation and Verification; NASA TM (in final preparation).