2014 NSF National Workshop on Transportation Cyber-Physical Systems
January 23-24, 2014

Safety-Assured Autonomy Technologies for Future Air Transportation

Dr. Christine M. Belcastro
NASA Langley Research Center
Hampton, VA 23681

I. Motivation[1]

Global demands on air transportation are expected to grow at unprecedented levels due to trends in economic growth and urbanization throughout the world, particularly in China and India. By 2050, it is envisioned by the International Air Transportation Association (IATA) that traditional, commercial air transport utilization will increase from 2.4 billion to 16 billion passengers annually. Future technologies must enable safe, energy efficient, and environmentally sustainable global air travel that can meet this demand. In addition, emerging Unmanned Aircraft Systems (UAS) offer the potential to provide services and to transform the mobility of goods, and possibly people, on local and regional scales. Moreover, progress in automation, information, and communication technologies provide an opportunity for safety-critical autonomous systems.

Safety-assured autonomy technologies could provide transformational capabilities to meet the demands of future air transportation. These technologies could enable: 1.) simplified single-pilot and pilot-optional operations in the current and future National Airspace System (NAS); 2.) improved performance under off-nominal and hazardous conditions; 3.) improved disaster response and long-duration science observation in the current and future NAS; 4.) point-to-point autonomous transportation and on-demand door-to-door transportation of people and goods in the future NAS; and 5.) real-time system-wide safety assurance at all levels of the current and future NAS. The use of safety assured autonomy technologies to implement integrated multi-modal ground and air transportation will enable future on-demand, door to door transportation.

II. Safety-Assured Autonomy Technologies

Technology advancement is needed in three key areas to enable safety-assured autonomy in the NAS: 1.) Vehicle-centric safety-assured autonomy; 2.) Real-time safety assurance at all levels of the NAS; and 3.) comprehensive validation and verification (V&V) of autonomy technologies. Each of these technology areas is discussed below.

Vehicle-Centric Safety-Assured Autonomy

Autonomy technologies are needed for assured vehicle safety under all conditions, including situations characterized by hazards, off-nominal conditions, and elevated uncertainty. Vehicle-level safety encompasses flight safety assurance that enables accident prevention and risk mitigation under a wide spectrum of hazards and their combinations, as well as obstacle and traffic detection and avoidance. Examination of current hazards and challenges in all phases of operation, both surface and ground, provides a useful wish list of autonomous technologies that are necessary to enable acceptable future operational systems. For example, a compilation of hazards that can lead to aircraft loss of control (LOC) provide a good starting point since this is the largest fatal accident category across all aircraft classes.[2] These hazards include onboard system failures and malfunctions, vehicle impairment and damage, external hazards and disturbances, abnormal vehicle dynamics and control response, and abnormal flight (or upset) conditions. For autonomous aircraft operations involving a single pilot or remote operator, hazards related to inappropriate pilot / operator actions and inactions would be included in the list of potential hazards. Analysis of hazards based on aircraft accidents and incidents provides an identification of worst-case hazards combinations and how they sequence in time. [3,4] The analysis results can lead to the identification of comprehensive technology solutions, and to the development of a comprehensive set of test scenarios for use in their V&V. Integrated autonomy technologies for LOC accident prevention and risk mitigation include vehicle health management, hazards effects detection, identification, and prediction, resilient aircraft control for hazards mitigation, and upset prevention, detection, and recovery. Mitigation of multiple hazards and upset recovery will require advanced integrated control methods that utilize all available control authority to preserve stability, handling qualities, and performance to the greatest extent possible while enabling the prevention and recovery from upset and LOC conditions. Upset prevention methods should incorporate dynamic envelope protection. This will require real-time safe envelope estimation. Upset recovery methods should utilize upset onset detection information, and should provide for early upset recovery as well as recovery from fully developed upsets for both nominal and impaired aircraft. Initial integrated technology concepts for loss of control accident prevention and flight safety recovery for piloted operations have been developed. [5,6] An independent supervisory system for vehicle safety assurance is also needed. This is discussed in the next sub-section. The extension of these methods to hazards peculiar to remotely or even optionally piloted aircraft is possible. Emergency path planning and path following leading to a "best case" outcome for an autonomous but damaged vehicle is a key enabling concept.

Autonomous obstacle detection and conflict/collision avoidance (i.e. comprehensive sense and avoid) would require operation under hazardous conditions, including loss of global positioning system (GPS) information, and must be effective for static and moving obstacles, both in flight and during surface operations. Moreover, avoidance maneuvers must be cognizant of vehicle constraints arising from passenger or cargo susceptibility, system failures, vehicle impairment, and vehicle damage. This will require real-time trajectory planning and generation.

For single pilot operations, variable autonomy decision processes and interfaces would be needed to maximize aircraft safety and mitigate human and machine errors. For fully autonomous operations, autonomous mission planning would be needed for nominal, off-nominal, and hazardous conditions.

Real-Time Safety Assurance

Autonomy technologies are needed at all operational levels, from individual vehicles through the entire NAS operation, for continual real-time optimization of system performance and safety monitoring, risk identification, and active safety assurance. At the vehicle level, safety monitoring would include flight safety assessment and prediction (in faster-than-real-time) of the impacts of onboard and external hazards, as well as safety state in terms of proximity and trajectory predictions relative to fixed and moving obstacles. External hazards include not only other traffic and obstacles, but also adverse weather which may be easily detected (e.g., severe convective activity) or may not be easily detected or predicted with precision (e.g., icing or turbulence) will need to be detected by, or communicated to, vehicles. Assessment of flight safety (from a dynamics and control perspective) is inherently challenging because of the lack of a quantifiable / measurable definition and due to the inherent nonlinear nature of combinatorial events and factors that lead to unsafe flight conditions. Moreover, to be useful, flight safety assessments must be predictive to assure that recoverability, safe landing or other successful outcomes (e.g., descent via ballistic chute), are always achievable. At the NAS operational level, safety risks associated with infrastructure malfunctions and failures as well as security threats need to be identified and mitigating actions taken to reduce safety risk.

Comprehensive V&V of Autonomy Technologies

The comprehensive V&V of autonomy technologies for safety-critical applications poses significant challenges. [7,8] System validation is a confirmation that the algorithms are performing the intended function under all possible operating conditions. Validation is not merely a demonstration that the system works under the design condition and selected test conditions, but a comprehensive process that involves analytical, simulation / ground testing, and flight testing to identify potentially problematic regions of operation (and their boundaries) and expose technology limitations – particularly for operation under uncertain, hazardous, and even unforeseen conditions. New methods, tools, testbeds, and metrics must be established for algorithms that cannot be thoroughly evaluated using existing methods. For example, nonlinear time-varying control systems and stochastic decision-based diagnostic / prognostic systems will require new methods and metrics for their effective analysis. Moreover, methods and metrics may vary depending on the algorithm being considered. For example, stability of detection and prediction algorithms may imply convergence rate and accuracy rather than the traditional control-theoretic meaning of stability. Performance of diagnostic and prognostic algorithms may be characterized by probabilities associated with correct detection and diagnosis of system faults or failures, whereas performance of control systems may be characterized by tracking capability or evaluation of multiple control objectives. Robustness for all algorithms must be evaluated relative to uncertainties (e.g., parameter variations and unmodeled system dynamics) and disturbances (e.g., signal and system noise and turbulence). Coverage of representative off-nominal and hazardous conditions must also be clearly defined and evaluated for effectiveness in dealing with these specific conditions and, more importantly, the broad set of conditions and combinations that could be encountered in service. Variable autonomy algorithms and interfaces must be evaluated for handling qualities and effectiveness, and adverse pilot coupling (APC) susceptibility under off-nominal conditions. Moreover, real-time allocation of roles, responsibilities, and tasks between the human and automation (and the levels of automation that are engaged) must be evaluated under off-nominal (and emergency) conditions. Simulation and ground testing includes traditional batch, real-time, piloted (where applicable), and hardware-in-the-loop methods, as well as a linked lab capability for the integration and simultaneous evaluation of integrated multidisciplinary technologies. Flight testing includes traditional full-scale testing to evaluate pilot/system interactions (if applicable), as well as sub-scale testing to evaluate algorithm effectiveness (and dynamics models) under off-nominal conditions that are too hazardous for full-scale testing.

Research is therefore also needed for the development of multidisciplinary modeling and simulation methods for characterizing vehicle dynamics effects under individual and multiple hazards. Research in flight dynamics, airframe damage propagation, and propulsion system modeling is needed to address the limitations of conventional analytical and experimental methods where simplifying assumptions typically limit response prediction to relatively benign, steady, and/or linear flight regimes. More specifically, modeling research is needed to improve understanding of current aircraft under LOC hazards and to predict potential LOC risks in next-generation aircraft designs. It is expected that new methods of analysis and integration will be necessary to determine expanded parameters of interest using data from wind-tunnel testing, analytical methods, including computational fluid dynamics (CFD), and system identification. Verification of extensive software systems for safety-critical operation within the NAS also poses significant challenges, particularly for stochastic systems. Moreover, technology V&V must ultimately lead to certification and transition into the NAS.

References

[1] Pearce, Robert, "NASA's Aeronautics Research Strategy: A Reflection of Research Continuity, Strategic Analysis, and Community Dialogue," July, 2013.
URL: http://www.nasa.gov/sites/default/files/files/CSC_ARMD_July2013_TAGGED.pdf

[2] "Statistical Summary of Commercial Jet Airplane Accidents, Worldwide Operations, 1959-2012", Boeing Commercial Airplanes, July 2013. URL: http://www.boeing.com/news/techissues/pdf/statsum.pdf

[3] Belcastro, Christine M. and Foster, John V., "Aircraft Loss-of-Control Accident Analysis," *AIAA Guidance, Navigation and Control Conference*, Toronto, August 2-5, 2010.

[4] Belcastro, C. M., Groff, L., Newman, R. L., Foster, J. V., Crider, D. A., Klyde, D. H., and Huston, A. M., "Preliminary Analysis of Aircraft Loss of Control Accidents: Worst Case Precursor Combinations and Temporal Sequencing," *AIAA SciTech Conference*, National Harbor, MD, January 13-17, 2014. (To Appear)

[5] Belcastro, Christine M. and Jacobson, Steven, "Future Integrated Systems Concept for Preventing Aircraft Loss-of-Control Accidents," *AIAA Guidance, Navigation and Control Conference*, Toronto, August 2-5, 2010.

[6] Belcastro, Christine M., "Loss of Control Prevention and Recovery: Onboard Guidance, Control, and Systems Technologies," *AIAA Conference on Guidance, Navigation and Control*, Minneapolis, Minnesota, August 2012.

[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, 2010.

[8] Belcastro, Christine M., "Validation of Safety-Critical Systems for Aircraft Loss-of-Control Prevention and Recovery," *AIAA Guidance, Navigation, and Control Conference*, Minneapolis, Minnesota, August 2012.