Transportation CPS: Insights from Aviation on Major Challenges and Directions

Dr. Krishna Sampigethaya, Cyber Security & Network Tech., Boeing Research & Technology
Professor Radha Poovendran, Network Security Lab (NSL), University of Washington

Aviation is envisioning bold and exciting future concepts for the 21st century. We have recently envisioned an aviation cyber-physical system (CPS) framework for understanding the major challenges, problems, and solutions, identifying fertile research areas from small-scale (e.g., aircraft) to large-scale CPS (e.g., air traffic control or ATC systems).[1] This position paper summarizes research challenges as: (*i*) problems faced by existing CPS that warrant investigation and new solutions, and, (*ii*) emerging needs and opportunities that potentially benefit from CPS advances. We anticipate these challenges, insights, and directions to apply across transportation.

Major Research Challenges

Modern aircraft avionics enable automation and provide pilots with comprehensive, timely, and relevant information that improves pilot situation awareness, decision-making, and workload in critical flight phases. Pilot error, however, remains a major cause of aircraft incidents and accidents. Recent FAA studies identify a significant challenge to be the pilot interaction with automation and information sources, noting pilot addiction to automation and deterioration of pilot skills and knowledge to manually maneuver aircraft and monitor flight in critical scenarios. We also identify pilot fatigue management, intelligent layers of automation, and airborne information sharing as long-term research areas for combating pilot-errors.

Recent FAA and NTSB investigations bring to light some underlying challenges of the existing cyber-physical integration in the National Airspace System (NAS). Various procedures, policies, and technologies related to cyber-physical interactions of ATC functions, such as separation of aircraft, are exhibiting weaknesses. FAA recently noted the number of observed aircraft near-misses and runway incursions and pilot reports of observed weaknesses in ATC ground system, such as ground-based navigation aids, have increased. These reported trends can be attributed to a new enhanced FAA safety monitoring and reporting system; but they do indicate there is scope and need for improving the cyber-physical interactions of airspace systems. With predicted air traffic growth and ongoing transition to the FAA's NextGen in the next decade, NAS challenges from existing, emerging, and potentially undiscovered weaknesses must be understood and fixed.

Another clear transformation in the NAS is use of cloud computing in the real-time, safety-critical decision making triad formed by pilot, air traffic controllers, and airline operations center crew. This raises new challenges in the use of cloud computing for CPS that will be documented in a future NSF report (www.isis.vanderbilt.edu/workshops/cc4cps). Furthermore, another emerging need of the NAS is to control and closely coordinate a geographically spread network of sensors (e.g., Automatic Dependent Surveillance Broadcast or ADS-B ground stations and airborne transponders) to track flights and manage air traffic in real-time in an increasingly hostile and unpredictable airspace physical environment and vulnerable cyberspace.

Recent usage of cyberspace advances in modern aircraft warranted that the airworthiness as well as "ground-worthiness" and "space-worthiness" of the off-board systems interacting with aircraft be certifiable in the presence of potential threats and vulnerabilities in cyberspace. Regulatory guidance for aircraft certification was as a result updated to handle cyber threats to e-enabled

aircraft airworthiness. FAA special conditions 25.401-SC and 25.421-SC, which use safety fundamentals of FAR 25.1301 and FAR 25.1309, are some recent advances made by aviation sector in addressing the strong linkage between safety and cyber security certification. However, as future aircraft models exploit the benefits of tight cyber-physical integration, new challenges emerge in relating cyber-physical security with safety. For example, it is unclear how to present security requirements and functions in the context of a safety analysis. A major challenge for certification is sufficiently integrating safety and security processes to maintain consistency and ensuring outputs of safety process include all hazards identified in security analyses. Cyber-physical security challenges across transportation sectors are also being considered; we organized a symposium on this topic recently (http://sites.ieee.org/c4tti/).

Aviation also presents several new challenges that benefit from CPS advances. An exemplary area is that of future passenger health, comfort, and convenience. In-flight medical emergencies incur high costs for airlines and this concern can potentially escalate with the forecast increase in aging travelers. Fatigue caused by air travel is a prevalent issue in an increasingly health-aware society. CPS applications combining advances, such as mobile-health and personal electronics usage in cabins, can enable new passenger services to be embedded into door-to-door transport.

Acknowledgements

Any findings, conclusions or recommendations in this material are those of the authors, and should not be interpreted as of The Boeing Company.

[1] K. Sampigethaya, R. Poovendran, "Aviation CPS: Foundations for Future Aircraft and Air Transport, Proceedings of the IEEE, Aug. 2013.