Towards a new paradigm of UAV safety

Thomas Gurriet,Eric Feron, Eric Johnson,Laurent Ciarletta,Dmitry Bershadsky,Juan-Pablo Afman

In 2013 in the US, the number of fatal accidents was only 236 for roughly 64 million flights. One can be proud of such an achievement, only if the challenges of tomorrow are addressed in a timely and appropriate manner. Among these challenges, the explosion of the civilian UAV market and the possibility for virtually anyone to access the sky poses safety problems never encountered before. The current airspace will have to adapt to this paradigm shift, where people do not operate from inside the vehicle but from the ground or some other location: safe and ubiquitous human-system interaction remains the core requirement. Although system safety requirements, as they are currently performed in aviation may appear to be overly strict for UAVs, we believe it is possible to leverage the specific aspects of unmanned aviation to meet such requirements. For example, the fact that human operators stand outside the vehicle completely redefining the requirements and operational constraints for UAVs.

In this paper, we begin by analyzing the operational and safety issues arising from the growing usage of UAV in the civilian airspace. This then leads us to discussing the safety requirements arising from this new paradigm. By definition, safety is inherently an implicit property of any given system. Therefore, it becomes an important challenge to explicitly define what it means for a system to be safe, and to explore the entire range of safety-enhancing mechanisms. While self-destruction may not be an attractive concept for a traditional airplane, it may become a totally reasonable approach in the context of UAVs.

Next, we explore the new range of approaches to ensuring system safety from a vehicle-centric viewpoint. Considering hardware first, no real requirements or tests are currently conducted to assess the quality of the entire system and its parts. Hardware redundancy for safety-critical functions is largely lacking in commercial products , although it may be an important part of a safe unmanned solution. Dynamic sets of requirements (geographic flight restrictions and flight envelope protection for example) involve making decisions in real time. This decision process relies on the ability for the vehicle to determine its full state, or at least a critical part of it, including full knowledge of failed components. To achieve that goal, sensors play a fundamental role, especially since remote human presence make it more difficult for the pilot/operator to detect a failure on the vehicle using "seed of the pants". The question is then: which sensors should be mandatory? An interesting approach to determining vehicle state, including failure modes, is the development of analytic redundancy via online state estimation, as it allows to get information on the full vehicle state without full-state sensing. Such safety-enhancing features come at a cost in terms of needed accuracy and computational resources, and it will be interesting to quantitatively determine the tradeoffs in terms of weight, cost, performances, computational load between direct sensing and state estimation for equivalent safety levels.

The foregoing leads this paper directly to software considerations. As safety requirements for UAVs differ from those applied to conventional aviation, they open the door to develop previously unexplored control algorithms and decision making strategies. For example, a vehicle crash is no longer necessarily catastrophic if its effects can be mitigated by good vehicle guidance and appropriate operational constraints. Such constraints may include enforcing operational altitude minima allowing a vehicle to glide out of trouble in case of engine failure, for example. Geofencing and damage-tolerant control are other examples of software-enabled, safety-enhancing features. The Verification and Validation (V&V) of all these algorithms and their implementation could be similar to today's industry standards, but the associated costs should be measured against the overall UAV market value for the industry to remain competitive. Minimizing the cost of system certification via extensive process automation and component-based system safety evaluation are definitely two of the main challenges in this area. Changing a propeller should not void the safety certificate for the entire craft, as long as the concept of equivalent level of safety, currently in use by manned aviation, can be extended to unmanned aviation.

The outcome of this paper will be a detailed set of recommendations for the development of safe unmanned vehicles. These recommendations will be applied to a prototype unmanned system currently under development at Georgia Tech.