Multi-Quality Verification: The Convergence of Security, Reliability and Safety

Engineering a large, embedded, real-time distributed air traffic management system involves looking at properties which must be built into and tested at a component level, then assembled and integrated together, in the context of an environment, in order to achieve quality assurance. The National Airspace System (NAS) is an example of a software-intensive, safety-critical real time system which is a part of the nation's critical infrastructure that poses several specialized concerns in terms of security, reliability and other performance-based characteristics (such as availability, quality of service, etc.). The safety critical nature of aeronautical engineering must consider the fact that an overt security breach could result in a loss of availability, thereby leading to a mishap, as safety and liveness become equivalent.

When the systems providing vital services to an organization are down (due to either random errors or malicious attacks) the cost can be devastating: lost opportunities, lost revenues, non-compliance penalties, high maintenance cost. More importantly partners, customers, and suppliers affected by the system shutdowns perceive the organization as poorly run and not suited to meet their needs. If the organization is concerned with public health or safety, lives can be lost. Consequently, a prominent point for discussion on reliability, safety and security has to be the cost of information system downtime and information loss or unauthorized discloser.

The transition from research and development to deployment is critical to the success of any modernization to take place in the National Airspace System. Revolutionizing a high-availability, safety-critical infrastructure system is a non-trivial task, as operation of the present system must continue simultaneous to the upgrade process. Functionality cannot be lost at any stage of the upgrade, and backward compatibility must be furnished along with quality guarantees.

We must develop processes and methods of assuring safety, security and reliability properties in a possibly distributed, safety-critical, real-time infrastructure. The characteristics of an air vehicle network populated by commercial, military and general aviation aircraft that can be either human-piloted or computer-controlled, need to be accurately modeled, analyzed and validated, including the interaction between components, such as autonomous and non-autonomous vehicles. Qualities such as safety, security and reliability must be maintained throughout the development, operation and evolution of such a system, in the face of control, computational, and communication challenges inherent to atmospheric flight in a shared environment. Our goal must be to develop techniques that enable the validation and eventual certification of safety, security and reliability properties via (formal) modeling and analysis as well as simulation and experimentation.

Quality Assessment with Measurement Driven Analysis and Design. There is a great need to develop a methodology that enables the assessment and enforcement of a specified level of safety, security and reliability for complex software, as well as its interactions with avionics hardware and human supervisors. One of the most difficult tasks is assuring that the system requirements specification matches the implementation [nat99, lev95]. Furthermore, in order to assure that the properties are maintained throughout the lifecycle of the system, metrics must be developed to assess the safety, security and reliability qualities of the implementation. These metrics, if developed early enough in the design process, can potentially be used to evaluate and perform tradeoffs of design options in terms of maintainability or even certification of the system. Finally, a rigorous framework must be established to maintain the system's safety, security and reliability throughout its evolution via fully documented property tracablility, including new software releases, and equipment upgrades. Central to this problem will be the viability of this structure to enable certification and eventual deployment of any new technologies.

High Reliability and Security Infrastructure. Rapid response to random errors and malicious attacks entail that the system must make correct decisions in an automated and autonomous manner. Integrity of the reliability and security infrastructure becomes paramount and is typically the most difficult quality to assure, as the precise conditions of field failures and security threats are difficult to anticipate or reproduce with enough realism to verify the capabilities of the infrastructure. The infrastructure must be designed to manage redundant resources across interconnected nodes, foil security threats, detect errors in both the user applications and the infrastructure components, and recover quickly from failures when they occur, in order to qualify and quantify benefits in terms of assessment, verification and maintenance of reliability, security and safety constraints.

Fault Diagnosis, Recovery and Performance Degradation. Safe, secure and reliable aircraft composed with several other safe, secure and reliable aircraft do not necessarily make a safe, secure and reliable networked airspace system in a distributed environment where component interactions are not regulated by a central authority. Furthermore, software for aircraft flight management systems, collision avoidance and pilot/controller alerting functions are complex in nature. A fault protection envelope for both hardware and software is necessary so that a failure does not trigger a hazardous situation. Interface requirements and constraints must be developed which take into account all possible software, avionics and pilot and ground controller interactions under degraded conditions**.** In the near future, human-piloted vehicles will be required to share the same airspace with computer controlled, autonomous vehicle. Interactions between a human piloted plane and an autonomous vehicle must be modeled in order to design for a 'fault containment region' to contain violations of trustworthiness, such as a human's reluctance to trust a purely automated entity, and an autonomous vehicle's response to any 'irrational behavior' displayed by a piloted plane.

Natasha Neogi is an Assistant Professor in Aerospace Engineering and Computer Science at the University of Illinois, Urbana-Champaign. She received her B.Eng. Honours, in Mechanical Engineering from McGill University, and a M.Phil in Physics from Cambridge University. She attained both an M.S. and Ph.D in Aeronautical and Astronautical Engineering from MIT.

Contact Information:
Coordinated Science Laboratory
103 West Main St.
Urbana, IL 61801
Phone: 217-333-4741
E-mail: neogi@uiuc.edu