WORKSHOP: New Visions for Software Design and Productivity
DATE: December 13-14, 2001
LOCATION: Vanderbilt University, Nashville, Tennessee

TITLE: New Directions in Avionics Software Design and Productivity

NAME (Authors): George Kasai (george.h.kasai@boeing.com) and Mahesh Reddy (mahesh.reddy@boeing.com), Boeing

ABSTRACT: Recent events significantly affect the direction of aircraft software design and productivity and open new avenues for the development and maintenance of more secure aircraft systems. Boeing is considering several new perspectives for aircraft systems design including advanced integration of mission, vehicle and ground software for predictive monitoring and prevention of catastrophic events. Software is the integrating force in future aircraft systems and current federated aircraft systems do not fully allow the desired integration, redundancy, monitoring and override capability required to assure aircraft safety and protection from attack. Radical improvements in current aircraft software design and productivity such as interface registration, integrated functions, partitioning and incremental verification allow insertion of monitoring and override systems required to provide safe and secure aircraft and airport systems. Barriers include provable isolation of integrated components from digital corruption and necessary improvements to aircraft system verification and certification methods. This paper provides a forum for discussion of the issues and possible approaches to new software design and development models and methods for aircraft systems.

TITLE: New Directions in Avionics Software Design and Productivity
NAME (Authors): George Kasai and Mahesh Reddy, Boeing

Driven by recent events, the Boeing Company is processing several thousand suggestions for improvement in aviation and airport safety. Aircraft and ground-based software will have a major role in integrating and implementing the best of these changes. Another driver for modification of Boeing's software design and development approach is the commercialization of military aircraft. The dual use of military transports with the option for rapid reconfiguration in extraordinary circumstances is currently in work and involves coordinating military and commercial methods of software development and acceptance. A key software design area in this commercial and military merge is compliance with the RTCA/DO-178 software standard and working with the Federal Aviation Agency. As another change, the military and air transport industries are implementing Global Air Traffic Management (GATM) that proposes a reduction in the physical spacing of aircraft in the global airspace by 2003. The implications of this reduction in relation to recent events will need to be evaluated. As another example requiring changes to aircraft systems, system dynamics modeling indicates that factors external to the software process are significant causes of software implementation failure and the entire system must be considered to assure successful realization.

Software provides the integration catalyst for large aircraft systems while emerging guidelines like the Capability Maturity Model Integration (CMMI) demand coordinated system and software processes. Boeing is evaluating the CMMI system and software assessment model for future developments. System and software integration is critical to the realization of systems that can provide monitoring and prevention of catastrophic events. These changes in software architecture and design methods include the elimination of the current federated nature of avionics systems in favor of an integrated system of systems approach. This approach provides advanced integration, alternative operation and intercommunication between systems especially during emergency modes. The first step in this process is the integration of critical and non-critical software systems. Current aircraft vehicle and mission systems are deliberately loosely coupled to allow segregation of safety critical systems from less critical mission systems. These two systems typically reside in separate hardware boxes with limited communication and shared services.

The Boeing Vehicle and Mission Management teams are investigating the use of a single hardware platform using software mediated partitioning to increase the integration of these systems and allow for rapid reconfiguration and upgrade while reducing the risk of execution or memory corruption. Under the current verification regime, safety critical aircraft systems contain only necessary and sufficient functionality required without any extra functionality. This means that additional, non-value added functions such as status monitoring, override and testability are absent because they increase the complexity of system verification. The area of formal analysis has great potential here to assure that execution sequence and component interaction are predictable. Boeing is monitoring the progress of the DARPA Model Based Integration of Embedded Software in both the formal methods and model based approach to future software development.

For systems that are not safety critical, Boeing's open architecture approach enables efficient insertion of new software and hardware. For example, web based transmission of weather data can be utilized to replace existing untimely weather information. The extension of these networking concepts is fundamental to change of aircraft operation during extraordinary circumstances. The locus of control in current aircraft systems is also under investigation. Current systems place the pilot in absolute control and revoking this authority requires the most severe circumstances but has been shown to be necessary based on recent events. Ground-based monitoring and control of aircraft in flight is a potential area for providing alternatives in these critical situations. Using this scenario, several options, up to aircraft automated landing could be provided. Also, existing collision avoidance systems assist the pilot in prevention of accidental collisions during flight and on the ground. Extensions of these systems to prevent intentional collisions in flight are under consideration.

The social and legal aspects of some drastic measures for public safety provide challenging areas and the ramifications of software modifications capable of harming passengers will need considerable scrutiny. There is no debate that the aircraft industry will require considerable change in the future to thwart potential terrorist threats. Boeing is looking forward to participation in this workshop and the associated forum to provide valuable information on the future of software design and development methods used to significantly improve the protection and security of aircraft and ground based systems.