Aircraft Certification Guidelines for the use of Commercial Off-The-Shelf Hardware / Software

**Background:** Commercial Off-The-Shelf (COTS) software / hardware are being used in aircraft avionics systems. Aircraft avionics designs are evolving into highly integrated complex systems that are becoming increasingly difficult to analyze for intended function and failure effects. Methods or processes to ensure that the COTS hardware / software components meet their intended function as installed in complex aircraft architecture need to be assessed at both the system and aircraft level.

**Historical Knowledge of Legacy Avionics Systems:** Legacy aircraft avionics systems relied on federated avionics architecture with mechanical backup systems. The strengths of this architecture included isolation of faults with enhanced failure analysis and fault detection. Weaknesses included duplication of hardware resource and dedicated software programs for each avionics computer. Many legacy airplanes including the B727, B737, B747, B757 and B767 series airplanes could continue safe flight and landing with all of the avionics systems failed with the exception of the standby instruments which are powered by the emergency battery buss.

**Inter-modular Avionics Computer Resource:** Inter-modular avionics systems strengths include shared hardware resource as software programs are "swapped" and execute concurrently on same computer platform. Weaknesses include complicated failure analysis, fault detection and isolation schemes and vulnerability to common mode failures.

**Avionics System Safety Assessments:** Avionics system safety assessments are based in part on numerical analysis and probability determinations. As the software error rate and integrated circuit failure modes probabilities cannot be determined by numerical analysis, the probability of software/integrated circuits failures should be mitigated by independent back-up systems.

We should develop policy to aid in standardization of complex avionics systems and fault mitigation. If single point or common mode integrated circuit failures for integrated avionics systems are determined to be "hazardous" or catastrophic than the design is not acceptable.

Peter Skaves 9/1/06