FILLING THE FAA GUIDANCE AND POLICY GAP FOR SYSTEMS INTEGRATION AND SAFETY ASSURANCE

Kirk Baker, Federal Aviation Administration, Washington D.C

Abstract

In 2010 the FAA formed the Airborne Systems Advisory Team (ASAT). The team consists of airborne system and safety specialists from FAA Headquarters, Directorates, and Aircraft Certification Offices (ACO). Our goal is to provide an efficient and standardized approach for establishing aircraft systems integration and safety assurance for the implementation of emerging technologies and the FAA NextGen operating environment.

Current airborne systems designs have become increasingly dependent on highly integrated systems architectures that share power, computing, networking, and input/output resources to support the needs for multiple aircraft functions. Establishing the relationships and transition points between the development, verification and validation activities for these functions throughout systems integration have become more difficult to define and trace to established safety objectives.

The ASAT identified SAE, ARP4754a, Development of Civil Aircraft and Systems as an acceptable method for constructing the regulatory compliance for highly-integrated or complex aircraft systems. Therefore, we published an Advisory Circular (AC) to formally recognize the methodology provided by the ARP and its part in demonstrating an acceptable means of compliance to the Title 14 CFR.

In the paper we will look at an actual incident and its causal factors to illustrate the challenges we face when we integrate systems and how important it is to thoroughly analyze and test that the safety objectives established for aircraft and system level functions are compliant with the applicable Title 14 of the Code of Federal Regulations (14CFR). We will indentify the regulatory requirement for safety in installations of systems and equipment and look at how our current policy and guidance applies to this challenge and what new policy and guidance may be needed.

Incident Case Study

The following case study provides an example of how important it is to properly integrate aircraft functions and evaluate their interactions and failure modes to properly assure safety. The information for the case study was gathered from the Serious Incident Investigation Report, CA18/3/2/0717 issued by the South African Civil Aviation Authority (SCCAA) [1].

The report offered the following executive summary of the incident:

On the 11th May 2009, a Boeing 747-400 aircraft operated by an airline with appropriate certification and holder of an Air Operator Certificate was involved in a serious incident during takeoff from OR Tambo Airport at Johannesburg, South Africa.

The serious incident involved the un-commanded retraction of the automatic Group ‘A’ leading edge flaps on rotation for a period of about 23 seconds. Subsequent to the initiation of the retraction of the Group ‘A’ leading edge flaps, the aircrew was faced with unexpected stall warnings. The pilot flying was able to prevent the aircraft from stalling, with support from the other crew member and to keep the aircraft flying until the leading edge flaps re-extended and normal performance capability returned.

At no time was the aircrew aware that the Group ‘A’ leading edge flaps had retracted or as to the circumstances leading to the stall warnings. They were however aware that the thrust reverser in-transit EICAS amber message on the P2- Pilots Center Instruments Panel did display during takeoff roll prior to rotation.

After discussing the occurrence and not being sure about what had been the cause of the event, the crew elected to return to the airport where an uneventful landing was carried out approximately 2 hours later.
Subsequent investigation revealed that two thrust reverser (TR) in-transit EICAS amber messages were received from the applicable sensors with the No.3 TR signal originating at 125.6kt and No.2 TR at 159.9kt. Ground testing revealed that the reversers were not fully stowed against the stops and that one of the four locking gearboxes on both No.2 and No.3 engines had unlocked. Note that the other thrust reverser locks were still in place and that the translating reverser cowls did not move during the event.

No evidence was found that the thrust reversers had in fact deployed.

The automatic retraction of the Group ‘A’ leading edge flaps based on dual thrust reverser in-transit signals from either both inboard or both outboard engines was part of the original 747-400 type design that was certified in January, 1989.

All model 747 airplanes will automatically retract the Group ‘A’ LE flaps upon movement of the reverse thrust handle. This is to prevent thrust reverser efflux air from impinging directly onto the flap panel surfaces in order to improve the fatigue life of the panels and their attachments. The original type design (certified in January, 1989) of the 747-400 airplane added the auto-retract feature based upon receipt of a thrust reverser unlock signal from engines No.1 & No.4 or from engines No.2 & No.3.

Factors that prevented this serious situation from becoming an accident include the timely and skillful response to the airplane’s performance loss by the pilot flying (PF), the activation of the airplane’s stall warning system (stick shaker), and that the Group ‘A’ leading edge flaps’ re-extended when the air/ground logic went to ‘air’ mode.

Following the event Boeing issued a service bulletin calling for the de-activation of the TR stow signal from the Flap Control Unit on Rolls Royce powered Boeing 747-400 aircraft to prevent a recurrence.

The probable cause for the occurrence of this serious incident is attributed to the loss of a significant amount of lift on rotation, during the takeoff, caused by the automatic LE flap retraction logic retracting the Group ‘A’ LE flaps on receipt of spurious thrust reverser unlock signals from the no. 2 and no. 3 engines. The possibility of such an occurrence had not been identified during amendment of the retraction logic.

The investigating authority acknowledges the action taken by The FAA and Boeing but does consider it essential that all software logic altered by amendments from the original type certification be revisited to identify any other hidden combinations that may lead to control issues and even possible loss of the aircraft.

In this case we can see that “software logic” allowed and un-identified functional state or failure “spurious thrust reverser unlock signals” to create an unintended interaction between two systems during a critical phase of aircraft operation causing “loss of a significant amount of lift on rotation, during the takeoff, caused by the automatic LE flap retraction logic retracting the Group ‘A’ LE flaps”. Was this a software logic problem or a design logic problem? The software logic in the Flap Control Unit (FCU) was working as it was programmed, X signal from TR = Retract LE flap. The logic is in the design. For example, the software logic in the FCU could have been designed to recognize an intermittent signal as erroneous and not retracted the flaps. It could have required that the TR handle and signal from the TR be active in order to retract the leading edge slates. Regardless of the inaccuracies with software design, the interaction between the FCU and TR should have been analyzed more thoroughly to assure that a aircraft level hazard condition such as un-commanded retraction of the leading edge slates during rotation would be mitigated. This was an integration of only two systems; imagine how much more challenging this becomes as the number of systems interfaces increase.

Regulatory Base

In aircraft and systems designs that incorporate high levels of systems integration and interactive capability, the safety analysis process and validation of aircraft and systems level safety objectives requires great attention. Title 14 CFR XX.1309 Equipment, systems, and Installations regulatory requirements requires systems to operate and fail safely in all foreseeable operating conditions, with emphasis on those failure conditions that would
contribute to a hazardous or catastrophic condition on the aircraft. This is the regulatory requirement that best supports aircraft and systems safety assurance and a focus point for certification programs that incorporate new and emerging technologies.

**Airborne Systems Advisory Team (ASAT)**

Currently the ASAT team acts as the FAA engineering division’s technical resource for policy and guidance as it is related to systems integration and safety assurance. We provide technical advice and oversight to the Aircraft and Engine Certification Offices (ACO) that manage the approval and oversight of applications for type certification (TC), supplemental type certification (STC), and Technical Standard Order Authorization (TSOA) of systems and equipment.

Our review of published industry standards and best practices that address systems integration and safety assurance has identified SAE Aerospace, ARP 4754A, Development of Civil Aircraft and Systems as an industry practice that addresses the development life cycle processes used to implement aircraft functions. It uses a development assurance process to verify and validate aircraft and systems level design requirements and establishes traceability to the safety objectives at the aircraft and systems levels. It provides a rigorous and iterative approach to the development, verification and validation of design requirements and how they relate to lower level processes such as RTCA/DO-178B, Software Considerations in Airborne Systems and Equipment Certification and the safety analysis process.

To formally recognize the ARP we have developed an FAA Advisory Circular (AC) that identifies the ARP as an acceptable means for developing a compliance framework for aircraft and systems certification of software intensive, highly integrated and complex systems. When used in conjunction with other applicable FAA AC’s and industry standards, it supports compliance with the Title 14 CFR framework. The AC is scheduled to be published by September 30, 2011.

**Other FAA Engineering Activities**

Other teams within the FAA Engineering Division are also working on filling in the gaps for existing policy and guidance, such as the Technical Standard Order (TSO) core team. The TSO core team has recently published two ACs. One, AC 21-46 “Technical Standard Order Program” explains the TSO process and how it applies to TSO authorization (TSOA) and letter of TSO design approval (LODA). It provides general guidance and addresses subjects such as Non-TSO functions as part of a TSOA. Two, AC 21-50 “Installation of TSOA Articles and LODA Appliances”, which describes the appropriate use of data approved by the FAA, through the TSOA or LODA, by applicants seeking a type certificate or approval of change to type design.

The ASAT is working closely with these teams to identify the relationship of these processes how they can be used to support various aircraft and systems certification programs.

In 2012 the ASAT will be working on an implementation plan for the AC. We will continue to support the systems integration and safety assurance aspects of on-going certification programs and monitor how the ARP is applied.

**Conclusion**

The FAA’s engineering division continues to look for new and innovative ways to fill the policy and guidance gaps through our desire for continuous improvement. We recognize industries need to remain flexible and competitive in today’s aviation markets and focus our efforts on the relationships and transition points between the various stages in the development and certification of aircraft and their systems as we move to the next level of safety and NexGen.

**References**
