NATIONAL TRANSPORTATION SAFETY BOARD

Office of Aviation Safety
Washington, D.C. 20594

March 09, 2015

Attachment 24

Scaled's Formal Response to the NTSB Regarding the Waiver

SYSTEM SAFETY

DCA15MA019

Response to NTSB Request for Information

Corrected, March 4, 2015

The NTSB System Safety group requested that Scaled explain its understanding of the issues related to the waiver under 14 CFR 437.55 issued by the FAA in July 2013.

Scaled extensively consulted with the Office of Commercial Space Transportation (AST) regarding its system safety analysis (SSA) throughout the permitting process. Scaled's permit application included its "System Safety Analysis Approach" (Document: T1B-90E060 Appendix G R A.2), which detailed Scaled's position as to how its SSA complied with 14 CFR 437.55. Specifically, that document noted that Scaled's approach was "derived from industry practice for certificated aircraft, which have higher standards than experimental aircraft."

Scaled considered human error carefully in accordance with FAA guidance. As set forth in FAA AC 23.1309 ("System Safety Analysis and Assessment for Part 23 Airplanes," which is referenced in AC 437.55-1 as one of the government standards used by the FAA to develop criteria to reasonable by virtue of those tasks being included in training, documented in the Pilot's Operating Handbook, successfully performed in prior flights and simulations, and discussed among pilots and engineers in connection with design of the vehicle and development of flight procedures. This approach was made clear in Scaled's SSA (3.0 - "METHODOLOGY"):

> Human error is reduced by testing processe[s] and procedures. The flight crew and control room crew run through many SIM drills. These drills involve every kind of failure through the entire mission. These SIM sessions are designed to teach and prepare all crew involved on how to handle all kind[s] of situation[s]. Ground crew and Maintenance crews follow strict process and procedures for every change, test and pre/post flight operations, ERs, TRDs, Checklists and signoffs are required. SS2-90E08, SS2 Mission Procedures, and WK2-60P080 Pre-Flight Checklist are some of the documents that must be followed to make a change, test a system and\or fly a mission. Given all the checks and balances, Human error is not part of the FHA [functional hazard assessment].[1] In the FTA [fault tree analysis] under high workload and very time sensitive events human error is a factor in the fault tree.

Scaled similarly considered software error in accordance with applicable guidance and regulations. In section 1.4.12 of its permit application, Scaled identified the software-controlled systems in SS2. As set forth in that section, all but one of those systems are not considered safety critical, or have non-software-controlled backups or other devices such that the failure of the software does not cause hazardous or catastrophic consequences. Scaled identified the

[1] Scaled's SSA for SS2 includes a functional hazard assessment, fault tree analysis, zonal safety analysis, and common mode analysis. AC 437.55-1 explicitly identifies functional hazard analysis as an acceptable analytical approach to identifying and characterizing hazards and risks. AC 23.1309 recommends functional hazard assessments, and also identifies fault tree analysis, zonal safety analysis, and common mode analysis as appropriate assessment methods.

[redacted] [redacted]

Rocket Motor Controller as the one safety critical software controlled device, and that device received the appropriate additional analysis in the SSA.

In light of this, and its discussions with AST, Scaled understood it was in compliance with 14 CFR 437.55, as set forth in its permit application. After further consultation with Scaled, AST issued conditional Experimental Permit 12-007 in May 2012. [2] In May 2013, AST unconditionally renewed Scaled's permit. Under these circumstances, Scaled understood it was in full compliance with FAA requirements.

Scaled did not request a waiver. Scaled became aware of FAA's intent to issue a waiver towards the end of June 2013.

[2] One condition of the permit (Order A, condition 8) was that Scaled's hazard analysis must be updated before any launch could occur. Scaled updated its hazard analysis to include rocket motor analysis and qualitative mitigations for certain recognized hazards unrelated to human or software error, and received written confirmation from AST in April 2013 (prior to SS2's first powered flight) that its submission satisfied the referenced condition.