NATIONAL TRANSPORTATION SAFETY BOARD

Office of Aviation Safety
Washington, D.C. 20594

March 09, 2015

Attachment 18

Methodology Section of Scaled's document T1B-90E033

SYSTEM SAFETY

DCA15MA019

3.0 METHODOLOGY*

Scale Composites is an Aerospace company that has built over 40 aircraft using standard Part 25 risk analysis. The typical Scaled Composites systems risk analysis is easily adapted to conform to AST Hazard Analysis requirements.

This qualitative analysis was performed to provide an initial system safety assessment. The will be the ground work for future permitting or licensing application requirements. This is an evaluation of the critical system to affirm that no large scale system failures are present in the aircraft and to identify systems that require further testing and validation.

For the flight test phase of this program only the high risk functions are analyzed beyond the FHA. Functions with a class of Major or Minor as not analyzed beyond the FHA because the issue is controllable and does not endanger the passenger, crew, or vehicle. It should be understood that multiple major events could couple to yield a catastrophic failure. Post flight test, further analysis is recommended to determine dispatch reliability.

Because of the R&D nature of the program, the aircraft systems are designed with the mentality that redundancy is essential. I.e. we don't or won't be able to verify the PF for many components in the R&D program. Therefore, where possible in Safety Critical systems single POF hardware are duplicated for redundancy. Safety, consistent with overall system objectives and requirements, is designed into the system. Design changes required to meet specified levels of risk are minimized through the efficient and effective application of safety features during the R&D phase of the system. System safety data, including lessons learned from similar systems and past projects, are applied. Safety assessments and analytical practices are chosen and employed to new designs, materials, processes, and procedures to minimize the associated risk, through the Materials and Processes, and Quality Assurance documentations. Data banks are established to ensure that current aircraft related documents are retained and readily available for trend analysis, through Scaled's revision controlled Released Documents System. Changes in system design, configuration, or application are evaluated and analyzed for impacts to overall system safety. Changes will be made and analyzed to compensate for anomalies or improvements. This is how the corrective action and anomaly reporting will be controlled.

Because of the R&D nature of the program a Program wide a 1.00e-3 failure rate is use as base for all events. This rate is conservative based on standard aerospace industry methodology. Also known to be conservative, the Non-Electrical Parts Reliability Database NPRD and MIL-HDBK-217 were sometimes used for more realistic failure rates. The NPRD shows a highest (worst) probably of failure of any part as 10^{-3} also proving that our program wide 1.00e-3 as conservative. Also note: where NPRD was used as a basis for PF, the highest, worst case failure rate for that component was used (conservative).

The following is the process with which this analysis was performed.

FHA

1. Identify the aircraft functions to be evaluated.
2. Identify safety-critical failure modes and their consequences for the functions.

3. Identify the effects the failure mode can impose on the crew/passenger and the aircraft.
4. Identify and apply a Class to the failure mode based on the effect on the crew/passenger and the aircraft.
5. Identify mitigation and control measures to reduce or minimize risk.

FTA

6. Perform a Fault Tree Analysis (FTA) for failure modes with Hazardous and Catastrophic Classes using a qualitatively conservative failure probability for each event ($1.00e^{-3}$). This will identify addition mitigations and control measures, and provide evidence that validates and verifies the system safety analysis.
7. Indentify failure modes with failure probabilities greater than the required value.
8. Improve the system if possible where possible.
9. Update FTAs that include the improved systems.
10. Indentify failure modes continuing to possess failure probabilities greater than the required value.
11. Apply failure rates to controlling events using NPRD, MIL-HDLK-217F, or rates provided by the manufacturer or design engineer.
12. Identify the failure modes continuing to fail to meet the requirements. Note that system and/or controlling event need further testing and/or evaluation prior to commercial implementation.
13. The install system is check against the schematic to insure the FTA is correct to the flight configuration.
14. As changes are required or requested, the FTA is updated to prior to the change to determine the change will be acceptable and reliable.
15. Throughout Flight Test the FTA is revised as issues arise. If the classification of a failure condition changes do to flight test the FTA will be revised.

CMA

16. Identify repeated events and branches in the FTA and develop the Common Mode Analysis (CMA). This show the sub systems that affect more than one function.

ZSA

17. Perform a Zonal Analysis to show how system in the same zone of the vehicle are installed and maintained to reduce interaction or failure.

The steps are repeated/updated as the development life cycle progresses. The fault trees are updated to account for improvements in the systems design as a result of testing, and evaluation data as it becomes available during development. Hazards associated with the form, fit, function, operation, and support of the system are identified, evaluated, and eliminated, or the associated risk is reduced to acceptable levels throughout its entire life cycle.

The outcome of the FTA will provide qualitative validation of the failure mode, and verify the probability of the failure to be acceptable remote give the class.

[redacted]