Commercial Space Transportation Advisory Committee (COMSTAC)
Systems Working Group Minutes
January, 15, 2013, 1:00 – 2:00 pm EST

I. Introductions

a. Randy Repcheck, FAA, welcomed participants to the sixth telecon on human space flight, and announced the topic for this meeting was Fault Tolerance, Margin, and Reliability.

b. Randy also noted that Pam Melroy, formerly FAA, had taken a job at DARPA, and all comments on this meeting usually sent to her should be sent to Randy.

c. Randy then introduced the presenters, Mike Machula and Tom Martin, FAA.

d. Mike reminded participants that the FAA cannot propose new regulations for spaceflight participant safety until 2015, so the telecon is just background research to hear opinions.

e. Mike also noted that minutes of the meeting will be published on the AST website. And the next telecon is scheduled for March 12th, after the AST conference on February 6th and 7th.

II. Presentation

a. Mike summarized last month's telecon, in which Henry Lampazzi lead a discussion on aborts and abort systems, and how they play a part in fault tolerance. He then connected it to this telecon's goal of discussing how to balance fault-tolerance, design margin and reliability, to achieve occupant safety.

b. Mike also stated key questions asked from a guidance perspective:

   i. What would be appropriate rationale at a functional level for a choice of fault tolerance, design margin, or high reliability to protect the safety of the occupants?

   ii. What is the minimum recommended level of fault tolerance? Is it different for orbital vs. suborbital?

   iii. When is risk high enough to justify additional fault tolerance?

   iv. What determines whether fault tolerance should be handled at the function level or system level?

c. Appropriate Rationale

   i. Mike started the discussion by asking: When would redundancy be recommended?

   ii. Randy Riley, Sunshine Aerospace, was familiar with the NASA system, of deciding the criticality of the major systems, which should not be exceeded by the criticality of its components.

   iii. Randy Riley also described three categories of criticality: in the first, a single failure could result in loss of life or vehicle; the second, loss of

mission or flight; and the third, failures which don't affect the mission or cause loss.

iv. Randy Riley clarified that redundancy is only required in the first category of criticality, in cases of loss of life or mission; though redundancies are not always possible. When they are, they should be separated.

v. Tom Martin asked whether the FAA would regulate redundancies for both mission assurance as well as human safety. To which Randy responded that it is something that would be categorized, and may not be regulated.

vi. Mike reiterated that the goal of the telecon was to examine reliability for occupant safety, while acknowledging that mission assurance is an important factor for participants. He also asked whether redundancy should be required if its achievable.

vii. Jim Hudson, Hector Inc., responded that multiple factors should be considered before requiring achievable redundancies, like weight.

viii. Dave Klaus, Colorado, also suggested that achievable redundancies should also be demonstrated beneficial.

d. High Reliability

i. Mike then moved the discussion by asking: What differentiates redundancy from high reliability, and how do you measure and demonstrate that?

ii. Randy Riley described high reliability as a system level or component level test. It may be possible to expose components to extreme environments to test them, but it's almost never possible to do with a fully integrated vehicle.

iii. Jim Hudson stated that there are many ways to do analysis, including historical evidence.

iv. Mary Ellen Vojtek, SMC Aerospace, asked for a definition of functional level versus system level. Tom Martin briefly described function as accomplishing a task, including the multiple systems that may involve. Tom also stated this was not a formal definition.

v. Dave Klaus stated that there can be dissimilar redundancies, different ways of meeting a function.

vi. Mark Sander, Cleveland State University, agreed, stating that unlike redundancies are recommended as a best practice. As in the Apollo capsule that had both a digital flight system as well as analogue.

vii. John Dicks, L3 Communications, noted that dissimilar redundancies, while useful, do drive up design and development costs. He also noted that hardware reliability is probably easier to demonstrate than software reliability, due to lack of tests.

e. Design Margin

i. Mike moved the discussion again, by asking: When would it be appropriate to solely rely on design margin, and what determines how much margin is recommended?

ii. Randy Riley responded that it depends on knowledge base. The more experience there is with structures, and the materials they are made of, the larger the database, the more we know about their limits.

iii. Randy Riley compared it to the Shuttle Program. With each flight, they would learned more about the changes to the structures, and became more comfortable with predictions in engineering reviews. In the commercial sector, everyone may benefit from sharing data like this.

iv. Dave Klaus noted that the term Factor of Safety is usually used increasing structural strength, whereas design margin can also include things like additional fuel, oxygen, things that are aimed at addressing potential uncertainties and extending missions.

v. John Dicks responded to the previous discussion on criticality, to mention that time is an important factor. For example, in a short ascent phase, automatic redundancies would be very important.

f. Minimum level of recommended fault-tolerance

i. Mike asked whether single fault-tolerance for critical functions, with abort capability for orbital flights, is generally acceptable.

ii. Jim Hudson commented that it may be acceptable for a highly reliable system; however, the time to complete complex intervening actions should also be considered.

iii. Randy Riley agreed there is a timing factor. Aborts require a lot of safeguards to prevent false positives, for example in momentary dips in flight data. Also, aborts cannot take care of everything, and sometimes it's a fact of the overall reliability of the system.

iv. Randy Riley clarified that depending on the design, one has to accept single-fault or no-fault tolerance for critical functions, and be increasingly aware of process control and system reliability.

v. Mike asked whether human errors should "stack," or whether fault tolerance should protect for a single system failure combined with a single human error.

vi. George Tyson, Orbital Commerce Project, noted that human error is part of the chain of events in an accident, and should be considered with engineering limitations. The goal is to break the chain before an accident.

vii. George added that whether a human is on the ground or in the vehicle, they are part of the safety system.

viii. There was a question about whether regulation would go into the manufacturing and then aggregation of a vehicle. For critical processes that cannot be inspected once they are completed, samples can be tested to mitigate the risk. And as in airlines, certified training can be offered for critical processes.

ix. Mike then asked what the rationale would be for having different recommended levels of fault-tolerance, between orbital and sub-orbital?

x. Jon Turnipseed, Virgin Galactic, indicated a preference for different levels, citing the reasons in the presentation slide, factors of exposure time and severity of the environment.

xi. Dave Klaus agreed with another participant that the overall risk factor of a given mission profile should be taken into account.

xii. One participant suggested assessing fault tolerance by phase of flight, for example in powered ascent versus gliding descent, where different kinds of energy are involved.

g. Additional Fault Tolerance

i. In the interest of time, Mike moved on by asking: when is risk high enough to justify additional fault tolerance?

ii. Jim Hudson characterized the question as: what is acceptable risk?

iii. Dave Klaus noted that the current NASA commercial crew requirements are no more than one in 270 catastrophic failure loss of life.

iv. Randy Riley stated that critical systems are usually propulsion, communication, both exterior and interior, and life support. All are analyzed down to a component level. Things that cause interactive failures or a chain of events are identified as high risk.

h. Function level or System level

i. Mike asked finally: what determines whether fault tolerance should be handled at the function level or system level?

ii. Dave Klaus argued that meeting a function was the primary concern.

iii. Geoff McCarthy asked for a definition of function versus system, to which Mike responded with the previous example, and reiterated that a clear definition was clearly needed.

iv. Dave Klaus also used the space suit requirement to provide breathable air as an example of function over system. If the carbon-dioxide scrubber failed, then oxygen would need to be continuously pumped while venting the waste gas. The function of providing air was achieved over the failure of the carbon-dioxide system.

v. John Dicks suggested that analysis will build upwards from the sub systems and component to the higher level requirements.

vi. Randy Riley reiterated the point that time is a factor.

vii. Jim Hudson suggested that the impact of common mode failure should really be considered.

viii. Jon Turnipseed also expressed concern that any information collected from different sources will be difficult to compare to the drastically different vehicle and mission profiles being designed.

III. Conclusion

a. Randy Repcheck concluded the call by thanking all the participants, and inviting comments to be sent to his email. He reminded participants that after the AST conference in February, there will likely be two more telecons, in March and April, before the May COMSTAC meeting.

Teleconference Participants:

David Allen (Black Sky Training), Sirisha Bandla (Commercial Spaceflight Federation), Michael Beavin (Commerce Department), Giugi Carminati (Weil), John Dicks (L3 Communications), Pete Fahrenthold (Northrop Grumman), Christine Fanchiang (Colorado), Oscar Garcia (Interflight Global), Brienna Henwood (NASTAR), Ruth Hunter (DoT), Robert Johnson (FAA), Steven Kane (SpaceTEC), David Klaus (Colorado), Charles Larsen (FAA-retired). Michael Lopez Alegria (Commercial Spaceflight Federation), Gaspare Maggio (SpaceX), Kate Maliga (Tauri Group), Geoff McCarthy (Aerospace Medical Association), Stokes McMillan (Sierra Nevada Corp), Robert Millman (Blue Origin), Michael Murray (ULA), Aaron Oesterle (PoliSpace), Michelle Peters (Go Zero-G), Mark Purcell (Lockheed Martin), Alex Saltman (Commercial Spaceflight Federation), Mark Sundahl (Cleveland State University), George Tyson (Orbital Commerce Project), Mary Ellen Vojtek (SMC Aerospace), Thomas Wiener (private practice)

Participants from the FAA Office of Commercial Space Transportation (AST) included: Randy Repcheck, Mike Machula, Tom Martin