Minutes -- WG4 telecon 7-11-01

Participants:

Steve Koczo (Rockwell Collins)
Jonathan Hammer (CAASD)
Ganghuai Wang (CAASD)
Lee Etnyre (UPS AT)
Jerry Anderson (FAA Certification)
Michael Petri (FAA WJHTC)
Ann Drumm (MIT LL)
Ken Carpenter (DERA)
Randy Bone (CAASD)
Pio Blankas (Honeywell)
Mike Ulrey (Boeing)
Bill Lee (Boeing)
Andy Zeitlin (CAASD)
Bob Passman (FAA)

1. RXX, chapter 2, service level

Steve Koczo led a discussion on Rxx. The problem we're trying to attack has a definition of "service levels," is not just RSP, there are also external and environmental factors that affect Rxx and service levels.

The surveillance part of service levels should be the easiest part to identify. That is "RSP." Beyond that, it seems that the key attributes/metrics boil down to integrity and continuity.

Also we need to organize our fault trees such that we can draw a circle around what we call our "application." The mitigations should come into the fault tree above the application and the avoidances come in below.

Mike Ulrey -- liked the comment about mitigations above and avoidances below, and the potential depiction in the fault-trees of what is inside and outside.

Andy -- mitigations are outside the system. Andy raised the need to include as assumptions external factors so that there is a recognition that these system elements are necessary for the analysis to hold. E.g., if the procedure depends on ATC then we must say so; otherwise ATC may be thought to be superfluous and folks will get the impression that the application is supported without them.

Lee asked whether the mitigations become a component of the service level.

Andy -- we should stress the environment description as this includes the operational environment. Any mitigation that we expect to be there is included in the analysis. Anything else is a recommended control.

Mike -- mitigations & avoidances might not be put at the bottom & top of the fault-tree. Inside and outside the system is probably more clear.

Steve – it is difficult to talk further about service levels without going through the exercise of evaluating / analyzing the applications. Custom aspects of the applications will need to be discussed in the appendices and wouldn't be something that we can talk about in chapter 2. We need to define the requirements as something that can be allocated.

We could write a table with the applications as rows and the mitigations as the columns.

Andy -- We can come up with a few generic mitigations -- is the pilot expected to maneuver, is visual acquisition possible, is ATC expected to monitor the encounter, is the proximity close?

Jonathan submitted the thought that integrity was difficult to define at a high level, although continuity might be a reasonable metric. Michael Ulrey felt that undetected failures can combine in so many ways to create a hazard that it will be very difficult to define a high-level metric related to integrity.

2. Fault trees

Next we reviewed some analysis of approach spacing presented by Jonathan. We went through a safety table that was put together based on our last telecon's inputs. Randy Bone raised an issue on the item that indicated a potential loss of separation could occur due to a missed approach. Randy felt that the hazard is no different than it is today. Bob Passman, who had brought this up at the last telecon, later joined, and confirmed that the hazard is no different than today. On this basis, we will delete this from the safety table for approach spacing.

Jonathan went through a path through the fault tree that he had developed to try and attach the required integrity problem. Several comments were made on the fault tree that will be incorporated for the next revision.

Finally, Jonathan presented some Monte-Carlo analysis that indicates the required integrity at the bottom of one of the cuts through the fault tree. Jonathan asked if this methodology was one that the group could endorse, and the group answered in the affirmative.

3. Next telecon

Our next telecon will be held July 24th and the subject will be state diagrams. Steve agreed to contact the subgroup on state diagrams to make sure that some material will be available for discussion.