

Notes from 5-30-02 WG4 Telecon

Participants check with Jonathan

Lee Etnyre (UPSAT)
Dave Spencer (MIT LL)
Tim Rand (Collins)
Andy Zeitlin (CAASD)
Michael Petri (FAA)
Lee Etnyre (UPS-AT)
Steve Koczo (Collins)
Jonathan Hammer (CAASD)
Ganghuai Wang (CAASD)
Mark Cato (ALPA)
Stan Jones (CAASD)
Bob Hilb (UPS)
Shahar Ladecky (FAA OK City)
Martin Eby (Source Code Systems)

Action Items in RED.

Discussion

1) Conflict Detection Presentation by Lee Etnyre

Several Files were included in the review:

Fault Trees

Operational Event Diagram from Bob Hilb

Conflict Detection Safety and Hazard Analysis document from Lee

a) Fault Tree Discussion

Fault Tree Page 1-

Page 6 (unsuccessful avoidance) Fault Tree

Shahar Q about the “unsuccessful maneuver”, concerning Q value

- Shahar used 10-5 for AILS

Martin Eby: CD has no prescribed maneuver. Crew could make a wrong maneuver decision

The two cases of maneuvers are different.

Andy: Suggested CD fails and Crew loses CSA while threat persists : AND?

Dave: Lee depicting time phased sequence, thus OR

Andy: Leave as OR for two events CD Fails and Unsuccessful Maneuver; Feed Crew loses CSA while threat persists as an AND under Unsuccessful Maneuver - ??

Jonathan wants the bottom level of fault trees to include the subsystems to allow allocation of requirements to subsystem.

Jonathan – use of common fault tree modules should be used by all applications (Nav/GPS fail, ADS-B)

Steve K. and Jonathan Action - Common modules to be documented, and sent out as fault tree files to be of use to others.

Jonathan - Can use sufficiency argument. Use number that people agree are reasonable and meet the top level number.

Jonathan – should not use “unauthorized use of the system” in our fault trees

Jonathan – put a bound on the misleading information, which then contributes to the fault tree. If we figure in how people react, then this becomes difficult to quantify.

Comparing the various fault trees: (~10:1 improvements for each CD and ATC being available):

- CD no ATC (page 1: 1.1e-10), CD and ATC (page 2: 1.1e-11), No CD no ATC (page 5: 1.2e-9), ATC no CD (page 7: 1.6e-10)

Martin: CD is EVAcq with alerting, similar fault trees

Andy: Is collision the top, or critical NMAC? Recommends critical NMAC to remove aircraft size factor.

Shahar: Usually use 500 ft for Test Criteria Violation (TCV), but is application dependent.

Critical NMACs are more frequent than collisions. What are the TLS numbers.

Bob H.: They don't have to certify to TCVs, but to frequency of accidents. Concern that using TCVs makes the certification unnecessarily stringent.

Lengthy discussion on Collision versus NMAC: Jonathan recommended to a ratio between the two and apply it to the fault tree analysis.

- **Sahar took action to investigate data on Collision versus NMAC.**

b) Operational Event Diagram Discussion

Discussing Bob Hilbs diagram (from WG1 discussions). Lee has his own diagram.

Jonathan: We need to label the arrows between blocks, otherwise the diagrams are

Dave Spencer (and Lee) took the action to modify their diagrams based on the new WG1 inputs.

Jonathan question: CD and EVAcq become the same figure (except for the alert?). Bob H. Yes.

Lee: Are we assuming that everyone has CDTI for CD and EVAcq? Mike, ASA assumes a CDTI, so the answer is yes. Bob H. indicated that they were not going to preclude non CDTI CD, but those folks are on their own in terms of guidance from the ASA MASPS.

Review of Lee's document:

Jonathan – make sure safety tables are consistent with the diagrams.

Jonathan – Need to set and account for integrity of altitude reporting. Dave S. suggested checking into how RVSM dealt with altitude reporting integrity.

Jonathan on OH 3.1 – concerning PAZ (?)

Tim Rand – Concerning the Fault Tree on last page of Lee’s 5-15-02 document, that was reviewed by WG1 at NASA Langley: 2 items

- page 1 of fault tree, lacks the “debit” of CD
- referred to Lin Martin (NASA Ames) comment at WG1 meeting that things have to go bad on both aircraft for an accident to occur. Could result in significant credit in fault tree.

Andy – in visual conditions, one aircraft may not see the other. But with ADS-B, both should see it, thus additional credit. **Lee took action to look into incorporating the benefit of both aircraft having to fail.**

Next weeks telecom plan to go over Dave Spencer’s EVAcquisition and EVApproach – June 6.

ACM is up on June 13 (still TBD)

End of Notes from 5/30/02 Telecon