Notes from 8-14-02 WG4 Telecon

Participants - check list with Jonathan

Jonathan Hammer (CAASD)
Bob Hilb (UPS)
Stan Jones (CAASD)
Steve Koczo (Collins)
Stavan Parikh (Collins)
Tim Rand (Collins)
Michael Petri (FAA)
Ganghuai Wang (CAASD)
Bill Morris (Raytheon)
Richard Barhydt (NASA Langley)

Action Items in RED.

Introductory Material

Schedule

Telecon is next Friday.

I) ACM Review by Stavan Parikh

Process Diagram

Added "Crew Received LL alert – ignored" text.

Added "Conflict Prevention" processes to Process Diagram.

Bob Hilb – This should reduce the number of conflicts (get credit). Stavan has added this to fault trees (to be discussed later).

On Managed Airspace Process Diagram – split P3.10 into two (P3.10 and P3.15) to allow paths back to ATC monitor and ACM Analyze conflict, respectively.

Process Diagram

Figure 1: 3 components that need to occur to cause a collision.

Figure 2: Major changes here, for all the fault trees.

3 failures: 1) alerting, 2) maneuver, 3) human error

Alerting Failure

"Data Failure" – Common mode failure throughout fault trees.

Previously we had staggered the various alerting algorithms (shown detail of each algorithm).

Jonathan – Could we miss an advantage to multiple levels of alerting.

Stan Jones – There may be some merit in looking at longer term and shorter term alerting and the respective benefits.

Jonathan – Could expand "Crew flies contrary to guidance"? Use "Fails to follow (?)" – Action – Change Wording.

Action – Include impact of 'multi-level alerting' and 'conflict prevention' aspects in allocating the crew's contribution in "following / failing to follow ACM guidance"

Data versus algorithm discussion. Independence of data.

Discussing Data Failure sub-tree Figure 6. Jonathan - Looks consistent with previous examples.

Figure 3 – Mitigations (not many available for autonomous airspace). Conflict prevention is not shown as a mitigation here. It affects the failure numbers used later.

Concerning "managed airspace", ATC is a mitigation. Stavan – ACM will both help and hurt things for this airspace.

Jonathan - Gaining independence between both crews maneuvering, provides backup. It also says that one aircraft alone should be able to avoid a collision.

R=10-7, where did it come from? (Stan). Stavan – its an educated guess. Accounts for conflict prevention to help reduce this number.

Stan – why can't we make a relative case of benefit here, rather than having to make an absolute case? (because it is new)

Discussion of value of ACM in managed airspace:

Stavan – how useful is ACM in managed airspace. Situational awareness?

Richard – some autonomous operations – side-by-side with managed airspace.

Tim – could set threshold small in managed airspace. Helpful to catch separation failure by ATC.

Richard – ACM does provide redundancy in managed airspace.

Could TIS-B help? Any system that provides traffic reports could potentially be used by ACM.

Jonathan – Basic assumption is for autonomous airspace, everyone is equipped.

Q: What about parallel use – some autonomous in managed airspace.

Back to the issue on alerting levels.

Jonathan – add text that "alerting levels" are captured in one block. Even a perfect system doesn't make much difference. The common mode failures tend to dominate anyway.

Jonathan – When TCAS was analyzed, r=0 was used for this block. We could use a pretty low number here and still be OK due to TCAS. The two-level alerts will do better than TCAS in the first place. Stan – Ignoring things for 2-minutes is much different then TCAS type TA/RA.

Richard – In past experience at Boeing, crew actions never were given any credit (during occurrence of a situation)??

Jonathan – when we discussed CSPA, we assumed crew would follow breakout guidance. Some errors

Based on our May Meeting – we decided crew would always follow alerts properly. But we should add text that describes that ??

Probability of Collision Course should be kept separate from Conflict Prevention – Richard (time horizon issue)

Jonathan – Conflict Prevention has many of the same common failure modes as alerting; shouldn't be able to take credit for that.

Need to get Karl Bilimora's numbers on the Probability of Conflicting Airplanes (e.g., 10-7).

Make the sufficiency argument. May not need a risk ratio due to the good performance of ACM, for both Own and Target aircraft.

New numbers when crew is removed: 2.04 e-5 at top of Figure 2. Results in 1.9 e-6 at top of Figure 1.

We need one more Fault Tree module for "Failure to Receive ADS-B". (transmitter failure, receiver failure, link failure, antenna diversity?)

Jonathan – on Figure 5 numbers: Why isn't that at least 0.25, or does data time fold into that? Stavan to check.

If we want to take credit for Conflict Prevention, we need to include it in the fault trees to assure common mode failures are addressed (since they use the same data).

Figure 2 – How is alerting "missed detection" of the theoretical alerting algorithm accounted for?

Investigate impact of "tiered ACM alerting" in attaining the "missed detection" goal.

Action: "Investigate Missed Detection due to tiered ACM alerts". "ASSAP ACM alert failure" Gate. Also the number on ASSAP ACM maneuver failure Gate is too demanding.

Figure 6 and 7: 10-7 number on 'ADS-B receive failure' needs further evaluation.

UAT undetected failure of message data is 10-9. 1090 MHz integrity is ? JPL saw considerable data errors. Plan was for application to sort out the errors.

Next telecon is Friday, August 23.

End of Notes from 8/14/02 Telecon