

Notes from 8-8-02 WG4 Telecon

Participants - check list with Jonathan

Jonathan Hammer (CAASD)
Rose Ashford (NASA)
Bob Hilb (UPS)
Stan Jones (CAASD)
Greg Stayton (ACSS)
Steve Koczo (Collins)
Lee Etnyre (UPS-AT)
Dave Spencer (MIT LL)
Jerry Anderson (FAA)
Bob Manning
Michael Petri (FAA)
Ganghuai Wang (CAASD)
Bob Morris (Raytheon)

Action Items in RED.

Future Meetings Schedule

August Meeting Schedule – August 27-29 at Rosslyn – Rockwell Collins offices.

September Meeting – September

October Meeting at NASA Ames following the TIM for 2 ½ days. DASC follows the next week at Irvine, CA.

Telecon Agenda Overview

Greg Stayton's issue paper

Rose Ashford's paper

Ganghuai Wang on Fault Trees

Lee Etnyre's CD Safety Analysis

I) Rose Ashford on Error Sources due to Comm and Input Errors

This is in response to Action Items from Cedar Rapids meeting to address 'Communication and Input Errors for Spacing Applications' for putting numbers to our fault trees. Read back errors due to ATC call outs provide a good example. Since CDTI displays same information, it should reduce the probability of read back errors. 1% number for read back error rate seems reasonable.

Greg Stayton – if 1% is for one message, don't we need to multiply it by the number of messages due to multiple opportunities to make errors.

Bob Hilb – can we caveat the 1% number. Jonathan – yes, it is very conservative number and has minimal impact on the application. (Bob has the concern that these numbers will take on a life on their own, with people perhaps quoting numbers

Stan Jones found an ICAO reference concerning ‘frequency of incorrect information’ that Jonathan had sent to Rose (Australia study). Concluded that VFR pilot not as trained as IFR pilot. Stan to discuss this with Rose offline.

Rose – her numbers make sense with those used by Jonathan on ASIA. After Stan and Rose discuss this further, then action item is complete. Rose will send an electronic copy with references to Jonathan.

Opportunity for crosschecking by flight crew makes 1% into .0001 (10⁻⁴).

II) Lee Etnyre on EVA and CD Fault Trees

Starting with EVAcq fault tree, Lee discussed fault tree generated based on previous inputs from Dave Spencer’s work. On left hand side (Event C3), “reduced spacing increases collision threat” of $Q=0.6$ can be supported and still achieve 10⁻⁹. C3 represents how often an aircraft gets close enough to where you could hit it. This may be very frequent in VFR, and infrequent in IFR will result in 10⁻⁹ at top of tree for Collision ops consequence.

Interpretation of C3 was discussed. C3 is the environmental factor of aircraft that are “close enough” to be a collision risk.

Setting the numbers from top-down to determine what is required below.

We need to make it very clear that the context of the diagrams are well understood to avoid confusion and misuse of the numbers. Dave’s approach basically says that to achieve the top number of the fault tree, relatively modest performance can be tolerated by subsystems.

Dave thanked Lee for his efforts in putting this into the Fault Tree program.

Some discussion about fault tree parameters.

Ganghuai Wang on the parameters:

Failure rate is a conditional rate (r) – this is found at the bottom of the tree.

Frequency is an unconditional rate (ω or w) – this is found at top of the tree (Ω or w is always less than r)

W is the inverse of the system cycle time.

λ is the inverse of the cycle time of the state being successful???

Catastrophic failure – 10⁻⁸ for all catastrophic failures. 10⁻⁹ for a particular operation.

Lee continued with the CD fault tree.

Jonathan queried Lee and Dave on the documentation for the appendices. Lee will try to get a requirements summary completed in the next couple of days for CD. Dave will try to have something for the August meeting on the EVA applications.

Break

III) Greg Stayton's Issue Paper on TCAS / ADS-B Hybrid Surveillance

Greg's response to the mail out of the ASA MASPS on Hybrid Surveillance. This is in the ICAO SARPS. Greg thinks we should consider when do you use ADS-B for TCAS and when do you use active surveillance. Need to deal with the issue of independence. This should be addressed in SC-186. Greg noted the prior attempts by Jerry Anderson to get SC-147 to look into this, but was rejected by the users.

ACSS is going to implement hybrid surveillance in one of their products, and would like to find a way to get this into one of the US standards.

Jonathan – we need to look at the SC-186 Terms of Reference. Also should it be in ASA, or where?

Jonathan – concerning CDTI / integrated traffic displays, this clearly needs to be addressed by WG4. With respect to TCAS surveillance, this appears to be more of a TCAS issue and needs to be addressed in a TCAS diagram. Our context diagrams reflects the interfaces we are addressing. Perhaps TCAS MOPS should be addressed again in SC-147?

Stan – we need to address the compatibilities with TCAS, but Hybrid Surveillance is a SARPS issue (referred to Figure 1-3 as identifying what parameters need to be exchanged).

Jerry Anderson – Hybrid surveillance from surveillance processing perspective is an SC-147 issue. Display issue is a WG4 issue.

Interoperability issue. Blurring of surveillance processing may be an issue.

Jonathan – One way to handle the lack of a home for Hybrid Surveillance could be for a small subgroup to write this as a separate document. And later to put it either in the ASA MASPS if warranted or pursue adding it to the TCAS MOPS (SC-147). Jonathan asked Greg if he would want to lead such an effort or put out a call to the vendors for interest in pursuing this. Greg does not have a problem with this and noted that starting with the SARPS in a subgroup would be a way to go.

Stan - the integration of ADS-B into TCAS is a TCAS issue.

Bob Manning – TCAS is not surveillance.

Greg – TCAS function must remain independent. The TCAS platform can perform other functions, such as ADS-B receive, and also other applications such as an airport map.

Jonathan – Does anyone have an objection to work this as a separate subgroup as a white paper in WG4? May get our wrists slapped?

Bob Manning – should this be addressed at plenary?

Jonathan – bring this up at the SC-186 plenary or in an earlier SC-186 leadership telecom?

Stan – need a small effort to put together a few slides to frame the issue before presenting this to the leadership group in August.

Action items – Greg to write up the rationale to address Hybrid Surveillance.

Action item – Jonathan to forward Greg's rationale to SC-186 leadership.

IV) Ganghuai Wang on Fault Tree

Exponential model is a time dependent model.

Failure frequency and unavailability are all a function of time at the component level.

Exponential model unavailability goes to 1 at time – infinity for a repairable system.

But we are interested in the transient behavior of the system (a non-repairable system).

Must consider the lifetime that we must use (we cannot use the asymptotic values used in repairable systems at $t = \text{infinity}$).

We need to select a time period.

Jonathan – we were using the unavailability at the top of our fault trees. (for short operations should we be using w or Q ?). For an hour long or more should we be using w or Q ?)

Stan – what we really have here is some of each (long time and short time applications). Operator responses are more events with probabilities.

Ganghuai – even for a few hour operation we do not achieve the asymptotic state, so we can use both long and short time frames since they fall into the same non-asymptotic state.

Greg asked about MTBF. This is the inverse of the rate.

Ganghuai: Unavailability – prob of failure in 1 hour. Should we be calculating w or Q ?

Continuity is $1-Q$. Inverse of w is the average system cycle

Ganghuai will take the action to do a small write-up to better define the terms and system lifetime.

Next telecom is Wednesday Aug 14.

End of Notes from 8/8/02 Telecon