SC186 WG4 August 22, 2001
Teleconference Minutes

Attendees:

Phillipe Caisso, STNA
Bob Darby, EUROCONTROL
Lee Etnyre, UPS AT
Steve Koczo, Rockwell-Collins
Bill Lee, Boeing
Dave Spencer, MIT LL
Mike Ulrey, Boeing
Ganguai Wang, MITRE CAASD

1. Review of ED78A-DO264A Process Document – WG51 / SC-186 Coordination

The group reviewed the ED78A-DO264A coordination document provided by Bob Darby at the recent WG4 meeting at RTCA Hdqtrs on behalf of WG51. The goal is to identify a common process of developing, documenting and analyzing ASAS applications between WG51 and SC-186 WG4 in developing the ASA MASPS. Steve Koczo led the group through a walk-through of the document. It was noted repeatedly that the process identified in the paper is in considerable alignment with the process being followed by WG4 in development of the ASA MASPS. The following areas of agreement in process were identified:

a) The OSED (Operational Service and Environment Description) by WG51 and the Application Descriptions and State Diagrams being developed by SC-186 WG1 for WG4 serve as the input to the process. Using these descriptions, a Safety Analysis is conducted. WG51 refers to this analysis as the Operational Safety Analysis (OSA) which consists of an Operational Hazard Analysis (OSA) and a subsequent Allocation of Safety Objectives and Requirements (ASOR) to the airborne and ground segments. WG4 also refers to this as a Safety Analysis, which develops Safety Tables and Fault Trees in identifying system criticality and making allocations to the airborne and ground segments. Both groups are generally following the same process.
b) While the full WG4 was not represented in the telecon, it was agreed by those present that adoption of two new terms / definitions are in order: 1) WG4's previous use of "Operational Hazard" in its safety tables will be called "Operational Consequence" from now on. Similarly, WG4's previously use of the "Contributing Event" column in the safety tables will be referred to as "Operational Hazard". The meanings are unchanged in how these terms were used, but it was felt that the newly adopted terms provide a more concise (i.e., less confusing) description. This change provides a common set of definitions used by both WG51 and WG4.
c) The paper also describes analytic and qualitative processes in determining safety. WG4 also shares this view of performing the safety analysis. Quantitative analysis is preferred, but for complex systems, one may have to resort to a more qualitative assessment of safety.
d) The reference to "phases" in the paper was discussed. It is noted that particular applications may consist of several "phases", e.g., traffic detection, visual acquisition, situational awareness, maneuver, etc (for EVA example). The group discussed the relationship between "phases" and "states". The general consensus of the group was

that while the two terms are somewhat related, "phases" represent a higher-level description of application modes and thus represent "high-level states," while WG4's use of "states" is for more detailed interactions between the various "agents." State diagrams provide a more detailed (i.e., lower level description) of the interactions by agents, e.g., flight crew or air traffic control. It was agreed that the concept of application phases should be used / retained for identifying the high-level processes of an application. Individual state diagrams can be used to supplement these higher level views / application phases by providing more detailed representations of the various states of the various agents / system views (i.e., flight crew view, air traffic control view, equipment view). A multi-view approach is likely needed to capture an application, using more detailed activity diagrams and states to capture the lower-level details. Mike Ulrey noted that the approach of phases in the ED78A/DO264A paper is consistent with the diagrams provided by Bill Lee. Mike took the action to continue to work an example of an application in more detail for further discussion. He also offered to provide a definition of the terminology that we discussed (e.g., phases, states, activity diagram, etc.).

Ganghuai also made reference to the Object Process Method (OPM), a superset of the Universal Modeling Language approach noted earlier by Mike Ulrey. Ganghuai noted that phases are depicted as processes in OPM and that states are the components of the system. Ganghuai will discuss this representation with Mike to factor in the two viewpoints.

Regardless of the outcome of these descriptions, the purpose is to use them to identify areas of exceptions / non-normal operations.

Bob Darby noted that so far he likes what he sees in terms of a common process in developing and analyzing the applications for the ASA MASPS. Phillipe Caisso also noted that "phases" address the upper level description of applications. As one takes a more detailed look, we will need to look at states for lower-level descriptions. Phillipe noted that WG51 and WG4 are addressing applications at different levels (top-down versus lower level view) and that our approaches are not far apart.

e) Dave Spencer noted that he liked the mechanical process of defining/identifying hazards by WG51 in the paper. Using "no detection" and "misleading detection" as general hazard categories allows one to identify potential hazards at the level of each application "phase".

2. OSED versus WG4's Application Description

Steve provided a comparison of the outlines of a typical Operational Case Studies (OSC) in the OSED compared to WG4's Application Description outline. While an Application Description focus on a specific application, OSCs and the OSED identify a set of related applications for a particular airspace environment and traffic characteristics. Currently these two outlines are considerably more divergent then the process identified above for ED78A/DO264A. Phillipe noted that of primary importance is that WG51 and WG4

agree on the specifics of the application "phases" and steps. How the OSED and Application Description capture this information is secondary in importance.

Bob Darby briefly reiterated the application of interest to WG51. These are the Enhanced Aid to Visual Acquisition, Enhanced Aid to Visual Approach, ACM / CD&R, and Approach Spacing (while not identical, they are similar). Bob has the action item to discuss with WG51 if there are any additional application of interest for the ASA MASPS.

Mike Ulrey noted that the Figure on page F-10 in the OSED aligns well with Bill Lee's approach and is a good way to capture the top-level of an application.

3. Review of Bill Lee's EVA Flow Diagram

The group review the EVA flow diagram developed by Bill Lee (refer to EVA-flow.ppt file sent out by Mike Ulrey prior to the telecon). This approach takes a look at each mini-phases and identifies a methodology of what can go wrong at each step. It was noted that agreement on the diagram is important and that perhaps this level of representation of an application may be sufficient. Mike noted that the level of detail needed depends on the application, i.e., how far we go into states using state and activity charts. Page 1 and 2 of the above file depict flow diagrams and show hazards. Mike will continue working the EVA and IMC Approach Spacing Applications phase and state diagrams to provide the group with an example for further review.

4. Mike's review of Fault Tree Plus Software Tool

Mike gave a brief review of his evaluation of the Fault Tree Plus tool for developing and capturing fault trees for the various ASA applications. Mike gave the tool a favorable review and saw no limitations. The tool allows capture of common hazards at different branches of the fault tree. The tool automatically accounts for these common hazards in the numerical calculations. Mike and Jonathan Hammer continue to look at the fault tree programs, and plan a look at the Relex fault tree tool before a determination is made on which tool is most suitable for development of the ASA application fault trees and safety analysis.

End of Minutes.