2nd USA/EUROPE AIR TRAFFIC MANAGEMENT R&D SEMINAR Orlando,1st - 4th December 1998

AN INTEGRATED SAFETY AND OPERATIONAL AVAILABILITY ANALYSIS SYSTEM FOR AIR TRAFFIC SYSTEMS

Peter F. Kostiuk
Logistics Management Institute
2000 Corporate Ridge Drive
Mc Lean, VA 22102-7805
(703) 917-7427

Stephan Kolitz
Draper Laboratory
555 Technology Square
Cambridge, MA 02139
Telephone: (617) 258-3885

Abstract

This paper develops and demonstrates an integrated safety analysis methodology, one of the key elements of an integrated system analysis capability. The work builds on several years of experience in analyzing the safety of air traffic management systems. This methodology is distinguished by its ability to merge system design and functionality information with the dynamic parameterization of a system's response to measure accident statistics and reliable system operation. The methodology can include both air and ground subsystems within the analysis framework. In addition, it can perform sensitivity analyses to identify weak points in the system's operation and design.

The approach starts with requirements derived for an operational concept and continues with the development of a Reliability Model of the system architecture that is proposed to meet those requirements. This represents a traditional reliability/safety modeling process. The reliability models are coupled with an Interaction-Response model that captures the environment in which the system is to operate, as well as the interaction of those environmental models with response models representing the execution of the rules and procedures that have been developed for the candidate concept. This represents a modeling process for the dynamic analysis of the system's situation.

Our approach to system safety analysis integrates the Reliability Model and an Interaction-Response Model. The Interaction-Response Model provides information regarding the frequency of encounters and the predicted outcome of those encounters as a function of the system's alerting system and ability to resolve encounters. The Reliability Model provides, as a function of time, probabilities associated with the availability and failure states of the critical systems. Scaling the operations safety metrics from the Interaction-Response Model by the system state probabilities from the Reliability Model creates system-level safety statistics.

The approach has been applied to the Center-TRACON Automation System and an assessment of cockpit-based approaches for independent approaches on closely-spaced parallel runways. The approach is now being incorporated into a terminal area safety model for further application and development.

Problem Definition

The continuing growth of air traffic will place demands on the worldwide air transportation system that cannot be accommodated without generating significant delays and economic impacts. To deal with this situation, work has begun to develop new approaches to provide a safe and economical air transportation infrastructure. Many of these emerging air transport technologies will represent radically new approaches to Air Traffic Management (ATM), for both ground and air operations. In recent years, LMI and Draper have developed an integrated methodology for analyzing the safety and operational impacts of emerging air traffic technologies. This report describes the safety analysis approach and shows how it is incorporated into the integrated system analysis framework. We have applied the methodology to a number of air traffic technologies including independent approaches to parallel runways, and the Center-TRACON Automation System.

Essential questions that must be answered before adopting a new approach to ATM include:

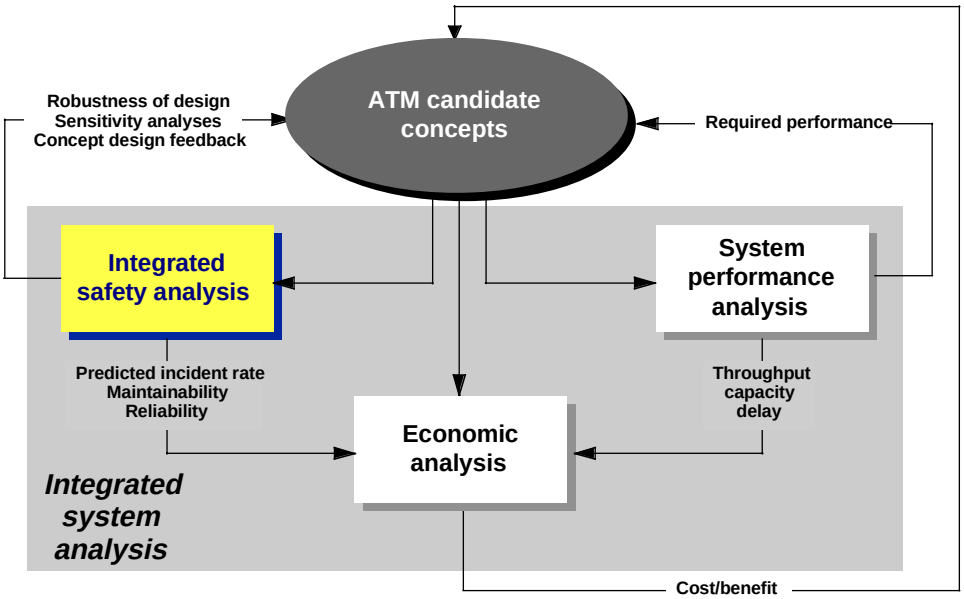
- Is the new system safe?
- What are the costs of implementing the new system?
- What are the direct economic benefits of the new system with respect to reduced delays or reduced airline costs?
- What is the optimal transitioning process from the current system to the new system to ensure safety?

To answer these questions and, thus, select a viable ATM concept, the integrated methodology contains:

- performance models to measure delays, throughput, and aircraft density;
- safety models to measure aircraft interactions and predict accident statistics; and
- economic models to measure system costs and associated benefits.

As shown in Figure 1, each of these three classes of analysis models rely on the others for some of their inputs. In other words, the design, analysis, and evaluation of ATM concepts must be treated as an interactive process in which the analyses provide crucial feedback to system developers, as well as the benefits and safety metrics required to support program advocacy.

Figure 1. Integrated System Analysis and Development



Thus, the primary focus in developing a methodology for integrated system analysis must be to understand and model the *interactions* among performance models, safety models, and economic models. By doing so, the methodology can be used to

- identify the drivers or weak links in the current system;
- provide guidance in selecting topics for improvement studies;
- measure net improvement in a proposed concept, distinguishing candidate concepts that represent global gains from those that solve one problem by creating another; and
- provide a foundation for cost/benefit analyses that can measure true system-wide impacts.

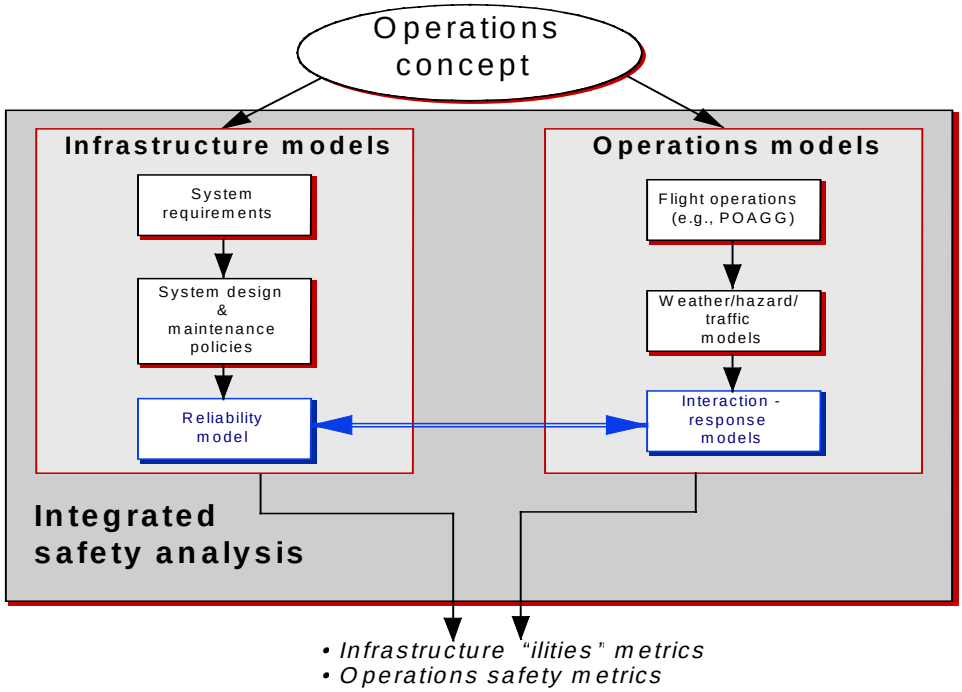
Products of this safety analysis can include

- predicted incident (encounter) statistics;
- predicted accident statistics;
- predicted false alarm statistics; and
- system availability and reliability.

Integrated System Safety Analysis: Concept, Approach, and Products

In this paper, we develop and demonstrate an *integrated safety analysis methodology*, one of the key elements of an integrated system analysis capability. This methodology is distinguished by its ability to merge system design and functionality information with the dynamic parameterization of a system's situation to measure accident statistics and reliable system operation. The "system" may include both air and ground subsystems within this analysis framework. In addition, it can perform sensitivity analyses to identify weak points in the system's operation and design. This is illustrated in Figure 2.

Figure 2. Integrated Safety and Reliability Modeling and Evaluation



On the left side of Figure 2 are the steps leading from requirements derived for an operational concept to the development of a Reliability Model of the system architecture, which has been proposed to meet those requirements. This represents a traditional reliability/safety modeling process. On the right, are the models required to capture the environment in which the system is to operate, as well as the

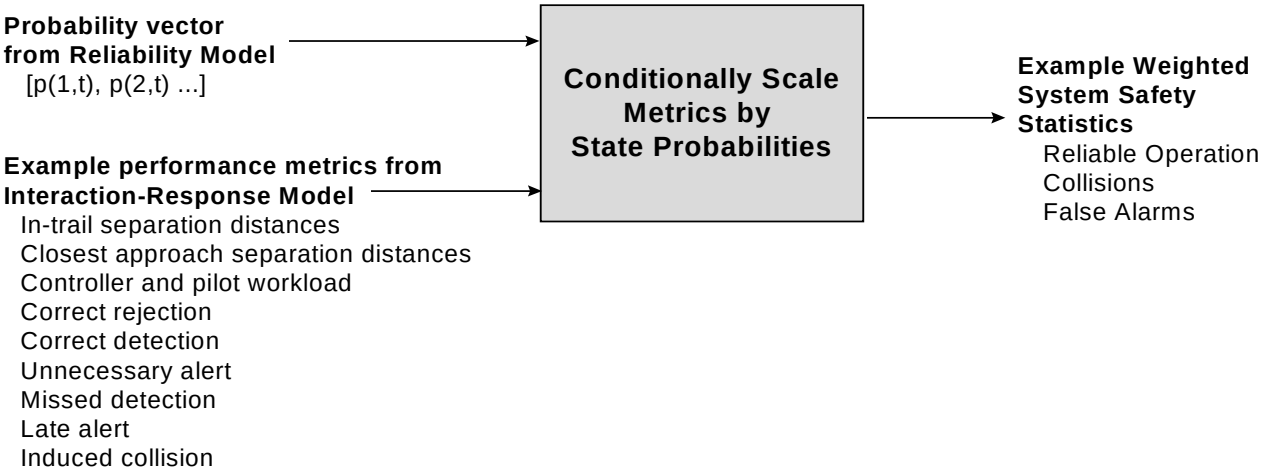
interaction of those environmental models with response models representing the execution of the rules and procedures that have been developed for the candidate concept. This represents a modeling process for the dynamic analysis of the system's situation.

Our approach to system safety analysis results from the integration of the Reliability Model and the

Interaction-Response Model. The Interaction-Response Model provides information regarding the frequency of encounters and the predicted outcome of those encounters as a function of the system's alerting system and ability to resolve encounters. The Reliability Model provides, as a function of time, probabilities associated with the critical systems' availability and failure states. Scaling the operations safety metrics from the Interaction-Response Model by the system state probabilities from the Reliability Model creates the system-level safety statistics.

This process is illustrated in Figure 3.

Figure 3. Combining Model Outputs

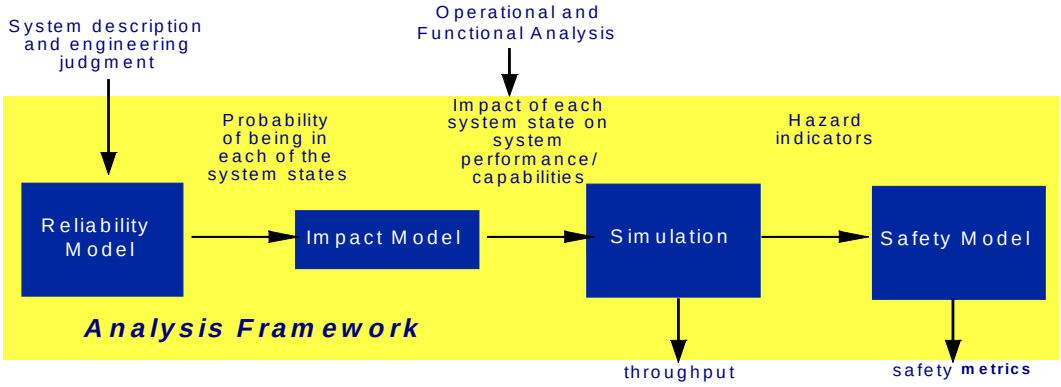


Moreover, as the operational concept evolves, the impact of changes in system architecture, rules and procedures, and operational scenarios can be easily re-evaluated with this methodology.

Figure 4 summarizes the key components of the analysis. Using the results of the system descriptions generated in the first phase, we build reliability models[1] of the basic parts of the system. From these reliability models, we calculate the probability of being in each state. Depending on the level of detail, the number of states can be very large. For each state, we determine what the impact on the system will be. For selected states, we build a simulation model to analyze the response of the system to specific events. The simulation model produces estimates of hazard probabilities, which then are weighted by the state probabilities to estimate the overall system probability of the hazards.

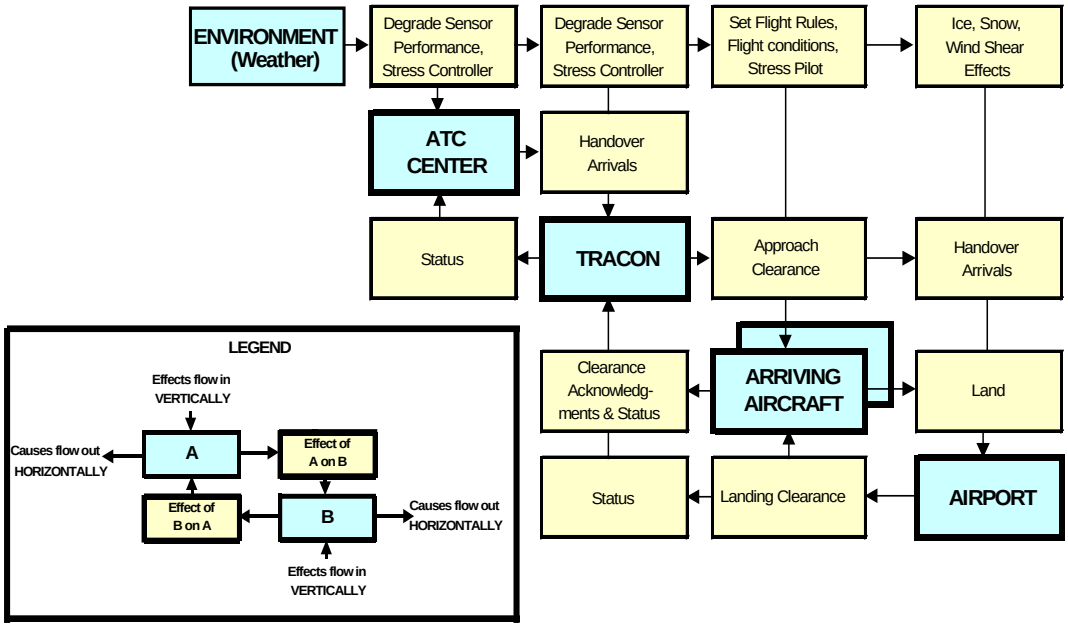
[1] Typically, we use a Markov reliability model to capture the dynamic nature of the system.

Figure 4. Analysis Framework



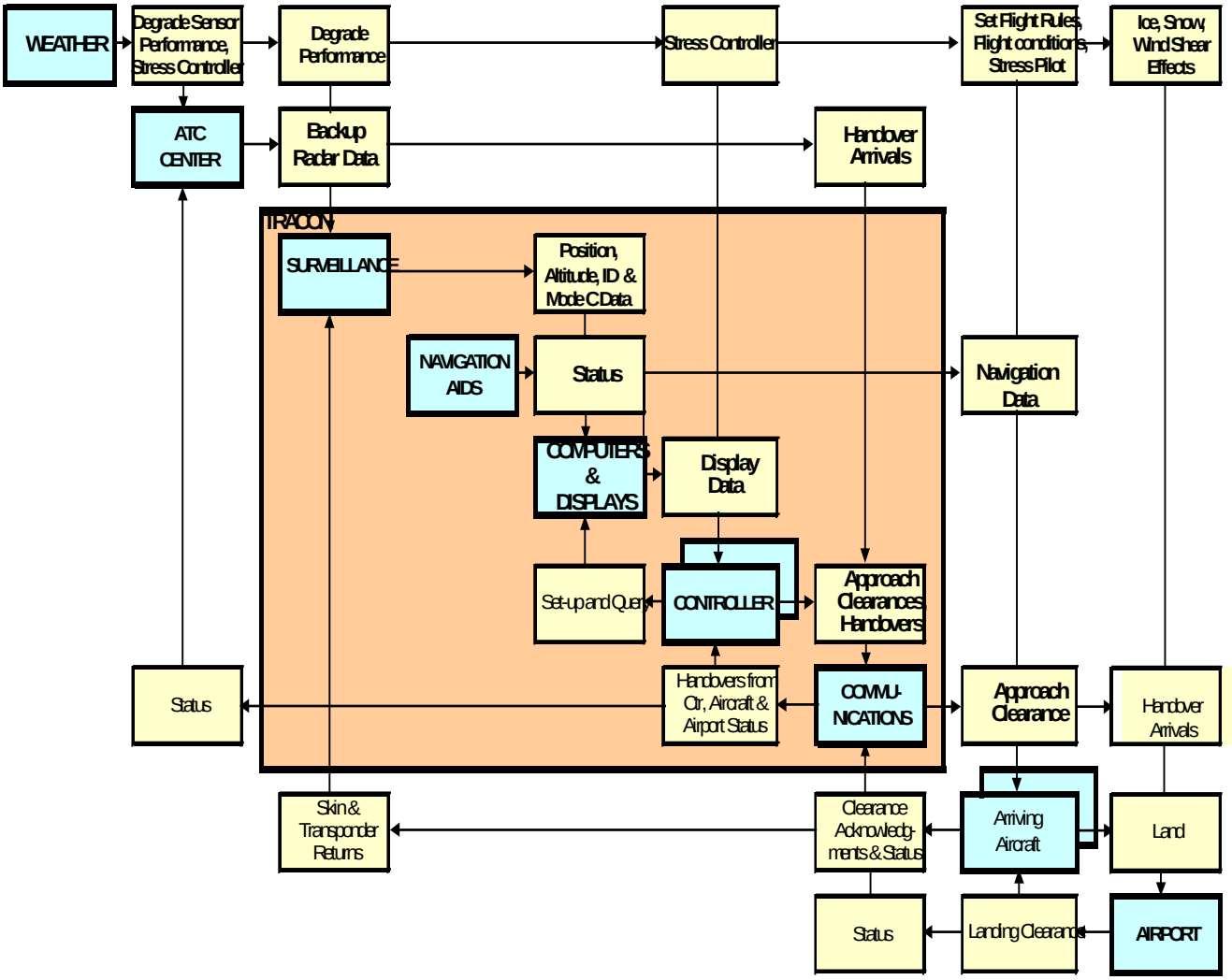
In order to illustrate more details of the approach, we now discuss the application of the methodology to an analysis of proposed CTAS operation at DFW. The hierarchical nature of the analysis approach can be seen in the example illustrated in Figures 5 and 6; the system modeled is near-terminal airspace. To build the reliability models, we first construct an N×N diagram of the functional interactions within the system. Figure 5 shows these functions and interactions at the top-level. Figure 6 expands the TRACON portion to show the functional components and interactions in greater detail. In the reliability study, models for each component are constructed and the interactions defined explicitly.

Figure 5. Top-Level System Interactions



We have identified five major subelements within the TRACON. These are shown in Figure 6 (diagonally in the grey area, top left to bottom right) and include (1) the Surveillance system, (2) the Navigation Aids for which the TRACON has responsibility, (3) the various Computers and Displays within the TRACON, (4) the TRACON air traffic Controllers themselves, and (5) the communications systems used by the TRACON.

Figure 6. Terminal Radar Approach Control



These diagrams are necessarily abstract. To perform analyses, each function must be defined and its possible states enumerated. Each state is then evaluated for its possible impact on overall system performance. The following sections describe examples of how functions are treated within this analytical approach.

The functional elements defined in Table 1 differentiate the capabilities of the TRACON systems that directly impact the inputs of the TRACON simulation described later. The TRACON controllers are ultimately responsible for maintaining the separation of aircraft within the TRACON. However, the controller's concept of where the aircraft are at any given time depends on the information they receive. The state of the surveillance function will model the availability and quality of surveillance information to the TRACON controllers. The states of the communication and control functions will reflect the availability and quality of the information the controllers would receive through these channels. The status of the communications function will also model whether or not this channel is available to the controllers to direct aircraft. The state of the navigation aids func-tion will indicate the availability of the signals that radiate into the TRACON airspace, which aircraft can use to navigate in the TRACON airspace.

Table 1. Functional Elements for Terminal Radar Approach Control

Surveillance	The capability of the TRACON to detect and interrogate aircraft for surveillance data in the TRACON and adjacent airspace and provide this information to TRACON controllers
Communication	The capability of the TRACON to allow TRACON controllers to transmit and receive voice communications with aircraft in or about to enter theTRACON and with controllers in the adjacent tower and the adjacent center
Control	The capability of the TRACON to process surveillance information, flight plan information, equipment status information and inputs from TRACON controllers to produce display information to assist TRACON controllers and pilots in assuring the safe flow of air traffic through the TRACON
Navigation aids	The capability of the TRACON to provide electronic or visual information that aircraft may use to navigate within TRACON (The source of the aid may be outside TRACON)
Controller	The capability TRACON controllers provide in the safe operation of the TRACON

Tables 2 and 3 define the functional elements for aircraft and the airport. The airport, tower, and center airspaces are not part of the near-terminal airspace, but failure events of systems in these facilities can affect the flow of traffic through near-terminal airspace. For this sample study, the failure events in the systems of the tower and center facilities are ignored. However, the failure events of systems at the airport are included and the capabilities of interest to the near-terminal simulation are defined in Table 2.

Tables 4 and 5 describe how operational states for the functional elements are defined and assessed for their impact on the system, as well as the impact on the component simulation in the model.

Table 2. Functional Elements for Aircraft

Navigation	The capability of the aircraft to monitor its position and velocity and its adherence to the desired flight path
Beacon Reply	The capability of the aircraft to receive and respond to interrogation from TRACON surveillance radar
Communication	The capability of the aircraft to allow the pilot (and crew) to transmit and receive voice communications with TRACON Controllers
Control	The capability of the aircraft to adhere to the flight path desired by its pilot
Pilot	The capability the pilot and crew provide in the safe operation the aircraft

Table 3. Functional Elements for Airport

Approach Facilities	The capability of the airport to provide electronic or visual aids to guide an approaching aircraft to a runway
Landing Facilities	The capability of the airport to provide clear runways to land approaching aircraft

Table 4. Terminal Radar Approach Control Surveillance Operational States

State of Function	State Definition	System Impact	Simulation Impact
Fully Operational	Primary Radar indication of all aircraft in TRACON; Secondary Radar data available for all aircraft equipped with functioning Transponders	Position estimate of all aircraft in TRACON presented to controller is sufficient to control normal approach	Normal position errors and flight paths for all aircraft
Primary Only	Loss of Secondary Radar	Position estimate of all aircraft in TRACON presented to controller is limited to accuracy provided by Primary Radar	Vertical position error of all aircraft with functioning Transponders increased from normal to reflect loss of Secondary Radar information
Secondary Only	Loss of Primary Radar	Position estimate available for only aircraft with functioning Transponders	Position error of all aircraft without functioning Transponder increased from normal to reflect loss of Primary Radar
Failed	Primary and Secondary Radar not functioning	Aircraft permitted to land but under contingency procedures	Position error of all aircraft increased from normal to reflect loss of Primary and Secondary Radar information

Table 5. Airport Approach Facilities Operational States

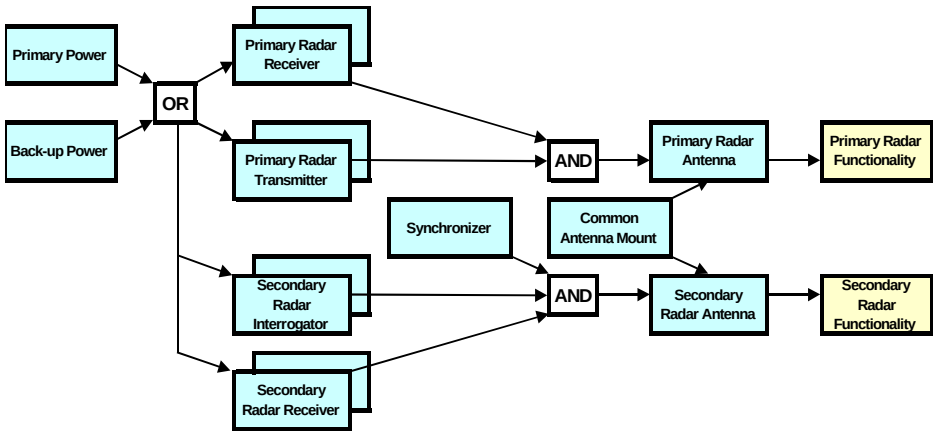
State of Function	State Definition	System Impact	Simulation Impact
Fully Operational	Full functionality is available for precision approach of aircraft to runway	Approaches permitted under Instrument Flight Rules (IFR) for lowest allowable minimum ceiling and visibility requirements	Aircraft follow normal flight paths to runway
Degraded - Loss of Markers or Lighting Systems	Failure of a Marker or Light; Descent path available with degraded support	Increased minimum ceiling and visibility requirements to conduct IFR approach and increased stress on pilot	Assuming low ceiling under IFR, aircraft precluded from approaching runway; desired flight paths changed to remaining available runways
Degraded - Loss of Descent Path	Loss of Descent Path (Glideslope)	Increased minimum ceiling and visibility requirements to conduct IFR approach and increased stress on pilot (Increases are greater than those for other Degraded State)	Assuming low ceiling under IFR, aircraft precluded from approaching runway; desired flight paths changed to remaining available runways
Failed	Loss of Localizer; Groundtrack not available for navigation to runway	Approaches to runway are no longer permitted under IFR	Assuming IFR, aircraft precluded from approaching runway; desired flight paths changed to remaining available runways

SURVEILLANCE RADAR RELIABILITY MODEL

As an example of how reliability modeling is done in the methodology, we briefly discuss a reliability model of surveillance radar. Figure 7 is a simplified top-level diagram of a surveillance radar system similar to those typically used in a TRACON. This is a generic diagram representing a system with dual redundant—critical components.

The system includes both a primary radar that can track the skin return from any target in its coverage area and a secondary radar, or beacon system, which sends out interrogations that trigger transponder responses in all transponder-equipped aircraft. The primary radar has dual redundant transmitters and receivers, and the secondary radar has dual redundant interrogators and receivers.

Figure 7. Surveillance Radar Reliability Model



The primary and secondary antennas are rigidly connected, and share a common rotating antenna mount. Secondary (beacon) radar interrogations are synchronized to the pulses transmitted by the primary radar. The system is assumed to have both primary and backup power sources.

For this system, it is assumed that a single failure in any transmitter, interrogator, or receiver leaves the overall system functional. A second failure in one of those components, however, results in the loss of the associated functionality (i.e., either the primary or secondary radar functionality is lost). Either power source can fail without bringing the system down; however, if both fail, the entire system is lost. If the common antenna mount fails, the antennas cannot rotate and the entire system is lost. Finally, if the secondary radar synchronizer fails, secondary radar functionality is lost.

Figure 8 shows the Markov state transition diagram for the TRACON surveillance radar system described in the previous figure. It provides for up to two consecutive failures leading to total loss of system functionality. Although more failures are theoretically possible, the probability that they might all occur while some functionality remains is very small compared with the probabilities that the system might be in one of the states that are defined here. This is a common assumption in reliability models of this type, and it serves as a bound to keep the number of states that must be considered manageable. The “no failures” state, state #1, is at the left of the diagram. The arrows leading away from state 1 show the various types of first failures considered. Of these first failure states, only state 2, “common an-tenna mount,” results in total loss of the surveil-lance system. States 6 through 9 and 12 through 15 leave the system fully functional. Because all of these states contribute to the probabilities of having certain common levels of functionality, they are “summed” by defining “pseudo states” that strictly speaking, are not part of the Markov process, but are convenient to calculate along with the probabilities of being in the “true” Markov states. The transitions to these pseudo states are shown by dashed lines.

The second failure states (16 through 22) are arranged in a column down the center of the chart. These states also are linked with the summary pseudo states, which indicate the level of overall functionality represented by their failure.

A Microsoft Excel spreadsheet was used to implement this reliability model. Figure 9 shows the input/output interface for this model. The user enters mean time between failures (MTBF) and mean time to repair (MTTR) values (in hours) and the model calculates and indicates the steady-state probabilities that the system is in any one of the indicated levels of functionality. The numerical data shown hear are purely arbitrary and fictitious. They were selected solely for the purpose of illustrating the methodology, and they provide output values that, while not representing any actual system reliabilities, can be interpreted as if they did.

Figure 8. Surveillance Radar State Transition Diagram

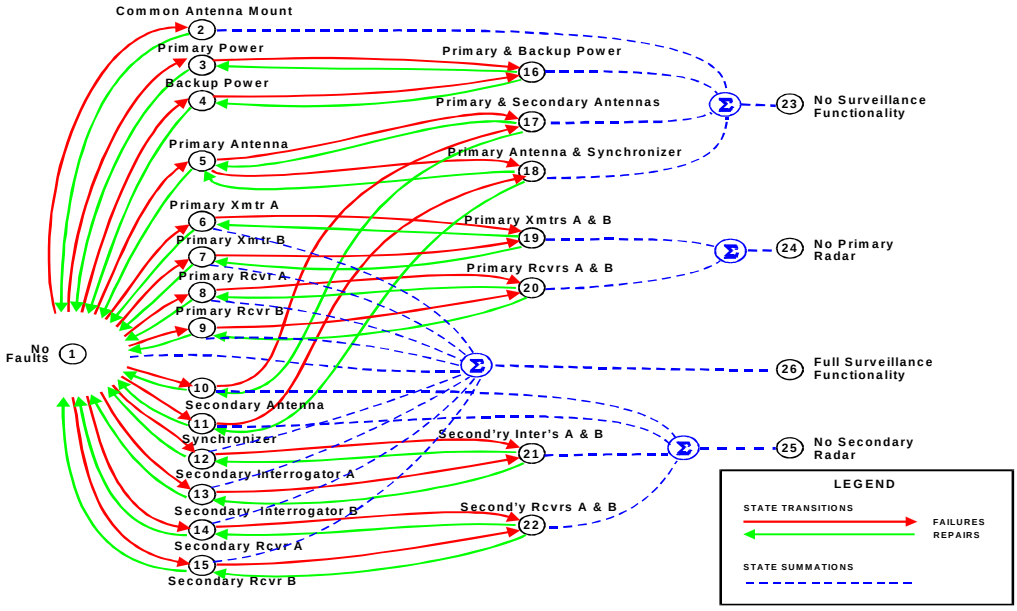


Figure 9. Input/Output for Surveillance Model

	INPUT Mean Time Between Failures MTBF in hours	INPUT Mean Time To Repair MTTR in hours	Functionality State Probability Vector			
Common Antenna Mount	1500	4	Functionality			
Primary Power Source	3000	2	Full	Primary Only	Secon-dary Only	None
Backup Power Source	2000	4				
Primary Radar Antenna	1000	4	0.99064	0.00286	0.00390	0.00260
Primary Radar Transmitter Channel A	750	2				
Primary Radar Transmitter Channel B	750	2				
Primary Radar Receiver Channel A	750	2				
Primary Radar Receiver Channel B	750	2				
Secondary Radar Antenna	2500	4				
Secondary Radar Synchronizer	1500	2				
Secondary Radar Interrogator Channel A	1000	2				
Secondary Radar Interrogator Channel B	1000	2				
Secondary Radar Receiver Channel A	2000	2				
Secondary Radar Receiver Channel B	2000	2				

In a similar fashion, the other functional components of the reliability model are modeled. The probabilities of the system being in each of the system states are calculated.

Simulation Input and Output

As shown in Figure 4, a simulation of the near-terminal area is then used as the basis for the Interaction-Response model. In particular, the near-terminal simulation simulates aircraft flying through TRACON-con-

trolled airspace, while calculating hazard metrics. The TRACON area simulated is based on the four corner posts at DFW in effect at the time of CTAS field tests in 1996.

The input to the simulation includes flight information for a specified time interval for each arriving aircraft in the scenario. This includes the aircraft ID; time of entering TRACON airspace; and a set of M waypoints, including the aircraft's entry point into TRACON-controlled airspace at a corner post.
Each waypoint contains the following information:

- Position (x, y, and z)
- Heading (heading, pitch, and velocity)
- Flight path ID
- Aircraft nominal and degraded position uncertainty.

Position uncertainty can be used to approximate faults within the reliability model. Weather is not captured explicitly in the simulation, but is modeled implicitly in the scenario data.

Simulation outputs include hazard indicators in the form of separation and workload metrics. Separation metrics include

- minimum absolute distance between aircraft,
- minimum in-trail distances between aircraft on a common flight path, and
- minimum altitude separation between crossing aircraft.

Workload factors include

- number of aircraft in an airspace sector and
- average and variance in number of aircraft per runway.

ENTITIES MODELED

Most of the significant entities of the TRACON airspace are modeled, although the fidelity of each entity varies. The entities modeled include the Center, TRACON, the tower, the controller, and the aircraft. The pilot is not modeled independently from the aircraft. The functionality of each entity follows:

- Center
  - Controls airplanes entering into TRACON airspace.
- TRACON
  - ♦ accepts airplanes into TRACON airspace;
  - ♦ assigns controller to track each airplane (later hand-off between controllers is not implemented);
  - ♦ tracks location of each airplane with respect to the airport; and
  - ♦ sets flight path by reading waypoints.
- Controller
  - ♦ uses radar to determine location of airplanes;
  - ♦ tracks location of airplanes with respect to each other;
  - ♦ determines flight path between waypoints;
  - ♦ sends airplane the next waypoint position, heading, velocity; and
  - ♦ sends airplane the command to fly straight or turn left or right.
- Aircraft (and pilot)
  - ♦ flies between waypoints;
  - ♦ determines acceleration to arrive at next waypoint with desired velocity;
  - ♦ determines when arrived, near, or past desired waypoint; and
  - ♦ tracks own position uncertainty and hazard indicators.

RESULTS

To illustrate the methodology, we analyzed the operation of the P-FAST component of CTAS at Dallas-Fort Worth International Airport (DFW). P-FAST is an automation aid that provides sugggested aircraft sequencing and runway assignments to controllers working approach positions. To perform the safety analysis application, we developed functional models of key components of the Dallas TRACON and tower, along with relevant aircraft functions.

The operational analysis guided the construction of a simulation of airport arrivals over a two-hour period.

The basic scenario includes a "rush" from the East, with TRACON airspace empty at the beginning of the scenario. Two baseline cases were established; one baseline case without P-FAST and a second baseline case with P-FAST. A third and fourth case consisted of a runway outage 20 minutes into the scenario, with and without P-FAST. Any aircraft that are sequenced to land after the runway outage are diverted to another runway. Aircraft are metered into the TRACON corner posts[2] approximately every two minutes. Aircraft were assumed to be identical, with 2.5 nautical mile in-trail separation minimum requirements. Arrivals land on three runways, 13R, 18R, and 17L[3].

The simulated arrival pattern at the cornerposts was derived from the Official Airline Guide (OAG) and Enhanced Traffic Management System (ETMS) flight data (see Figure 3.4.1) into DFW. Flight paths were taken from data gathered at a site visit to DFW TRACON on August 27, 1997

In summary,we studied four cases:

- *Case 1*: Current baseline without P-FAST
- *Case 2*: Current baseline with P-FAST
- *Case 3*: Runway outage without P-FAST
- *Case 4*: Runway outage with P-FAST

The safety and performance metrics used in the study were total aircraft arrivals, average arrivals per runway, the standard deviation of arrivals per runway, and the percentage of separations less than 2.5 nautical miles. As can be seen in Table 6, the results showed that in comparing two Baseline cases, more aircraft

[2]The four corner posts defined for all of our cases are the cornerposts that were defined during 1996 when P-FAST was tested at DFW. In 1997, due to the addition of a fourth arrival runway, the DFW TRACON airspace was increased.

[3]The three arrivals runways are defined as the original three runways used during the testing of P-FAST during 1996. In 1997, when the fourth runway was added, arrival runway was added. Runway 17L was renamed 17C and a new runway was named 17L.

landed when P-FAST was in use and the arrivals per runway were more balanced. The workload, as measured by the standard deviation of arrivals per runway, was higher for Case 1, without P-FAST.

In Cases 3 and 4, with a runway outage, fewer aircraft have landed, and there is a significant increase in controller workload as measured by the standard deviation of arrivals per runway. The percentage of aircraft with less than 2.5 nautical mile in-trail separation is the same with and without P-FAST. The overall results imply that P-FAST reduces controller workload, which may decrease the likelihood of a hazardous condition resulting from controller workload.

Conclusion

This paper describes a promising approach for quantifying the operational availability and safety im-pacts of changes in the air traffic management system. The approach is both flexible and hierarchical, and therefore, can be applied to a wide variety of concepts at various stages in the concept exploration and development process. The approach has been applied to studies of final approach procedures, and has recently been implemented in a prototype version for terminal area aircraft operations.

Table 6. Summary of Results

	Total arrivals	Average arrivals per runway	Standard deviation arrivals per runway	Percent under 2.5nm (%)
Case 1	97	32.3	8.3	6
Case 2	112	37.3	0.5	5
Case 3	67	22.3	15.2	14
Case 4	76	25.3	13.8	14