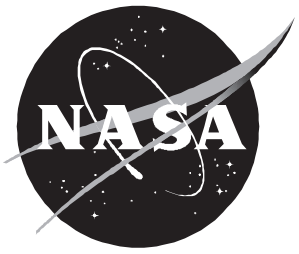
NASA / CR-1998-207673



A Method for Evaluating the Safety Impacts of Air Traffic Automation

Peter Kostiuk and Gerald Shapiro
Logistics Management Institute, McLean, Virginia

Dave Hanson, Stephan Kolitz, Frank Leong, and Gene Rosch
The Charles Stark Draper Laboratory, Cambridge, Massachusetts

Charles Bonesteel
Chava Group, Boston, Massachusetts

May 1998

The NASA STI Program Office . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA Scientific and Technical Information (STI) Program Office plays a key part in helping NASA maintain this important role.

The NASA STI Program Office is operated by Langley Research Center, the lead center for NASA's scientific and technical information. The NASA STI Program Office provides access to the NASA STI Database, the largest collection of aeronautical and space science STI in the world. The Program Office is also NASA's institutional mechanism for disseminating the results of its research and development activities. These results are published by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counter-part or peer-reviewed formal professional papers, but having less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services that help round out the STI Program Office's diverse offerings include creating custom thesauri, building customized databases, organizing and publishing research results . . . even providing videos.

For more information about the NASA STI Program Office, see the following:

- Access the NASA STI Program Home Page at ***http://www.sti.nasa.gov***

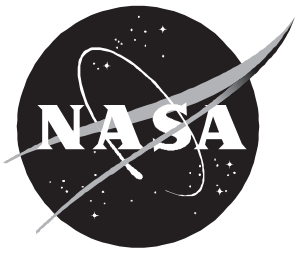
- Email your question via the Internet to help@sti.nasa.gov

- Fax your question to the NASA Access Help Desk at (301) 621-0134

- Phone the NASA Access Help Desk at (301) 621-0390

- Write to:
  NASA Access Help Desk
  NASA Center for AeroSpace Information
  7121 Standard Drive
  Hanover, MD 21076-1320

NASA / CR-1998-207673



A Method for Evaluating the Safety Impacts of Air Traffic Automation

Peter Kostiuk and Gerald Shapiro
Logistics Management Institute, McLean, Virginia

Dave Hanson, Stephan Kolitz, Frank Leong, and Gene Rosch
The Charles Stark Draper Laboratory, Cambridge, Massachusetts

Charles Bonesteel
Chava Group, Boston, Massachusetts

National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23681-2199

Prepared for Langley Research Center
under Contract NAS2-14361

May 1998

Available from the following:

NASA Center for AeroSpace Information (CASI)
7121 Standard Drive
Hanover, MD 21076-1320
(301) 621-0390

National Technical Information Service (NTIS)
5285 Port Royal Road
Springfield, VA 22161-2171
(703) 487-4650

Contents

FIGURES

TABLES

Chapter 1
Introduction and Summary

PROBLEM DEFINITION

The continuing growth of air traffic will place demands on the worldwide Air Traffic Management (ATM) 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 providing a safe and economical air transportation infrastructure. Many of these emerging air transport technologies will represent radically new approaches to ATM, both for ground and air operations.

The following are essential questions that must be answered before adopting a new approach to air traffic management.

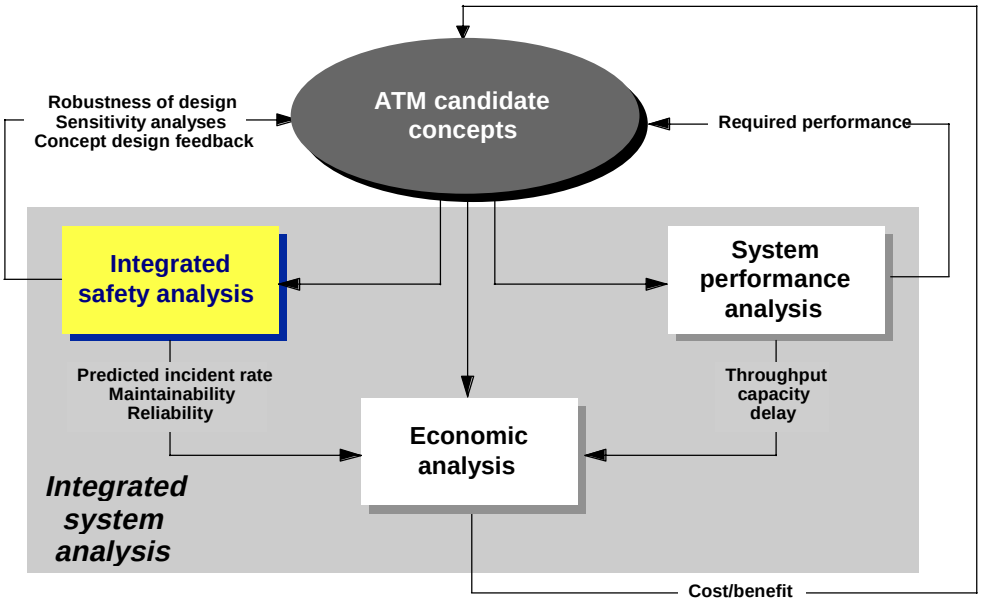
- Is the new system safe?
- What are the costs of implementing the new system?
- What are the direct economic benefits of the new system in reduced delays or lower airline costs?
- What is the optimal transitioning process from the current system to the new system to ensure safety?

To answer these questions and select a viable ATM concept, analysis will contain

- 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 1-1, 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 Air Traffic Management 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 1-1. 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.

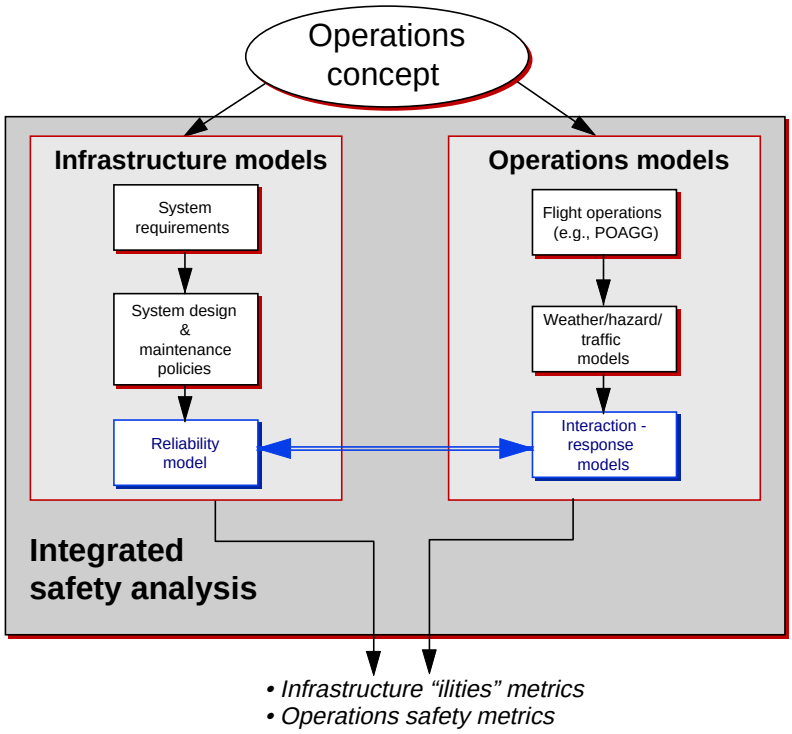
Products of this analysis include

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

INTEGRATED SYSTEM SAFETY ANALYSIS: CONCEPT, APPROACH, AND PRODUCTS

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/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 1-2.

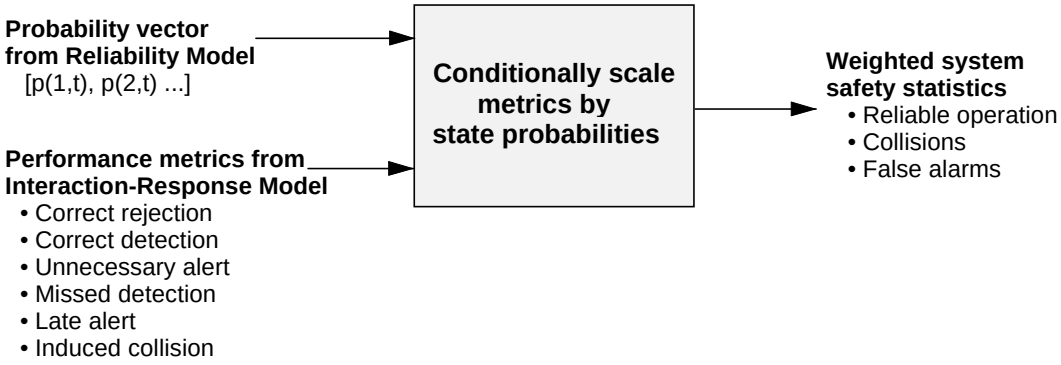
Figure 1-2. Integrated Safety and Reliability Modeling and Evaluation



On the left side of Figure 1-2 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 1-3.

Figure 1-3. 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 1-2 makes it clear that system safety is being addressed from a variety of perspectives, each of which affects safety. These include

- system functionality, the analysis of how reliably the system components perform;
- rules and procedures, the analysis of how the system is designed to respond in both safe and unsafe situations; and
- operational scenario, the analysis of the environment in which the system is expected to operate.

Integrating models that quantify each one of these three elements creates an analysis capability that is now system-wide and responsive to ongoing changes in the definition and requirements of the operational concept.

APPLICATION TO CENTER-TERMINALRADAR APPROACH CONTROL AUTOMATION SYSTEM AT DALLAS FORT-WORTH INTERNATIONAL AIRPORT

To illustrate this method, we analyzed the operation of the Center-Terminal Radar Approach Control (TRACON) Automation System (CTAS) at Dallas-Fort Worth International Airport (DFW). CTAS is a automation aid that provides suggested aircraft sequencing and runway assignments to controllers working approach positions. Recent field tests of the CTAS Passive Final Approach Spacing Tool (P-FAST) at DFW suggest significant improvements in airport arrival capacity through the use of this automation aid.

To perform the safety analysis application, we developed functional models of key components of the Dallas TRACON and tower, along with relevant aircraft functions. With limited time and resources, we were unable to obtain complete data on all the systems included in the functional models. Consequently, the conclusions of the study do not necessarily represent a complete evaluation of the safety impacts of CTAS at DFW, or the overall safety of the airport operation. The estimates should only be used to indicate how the method can be used to evaluate such operations, if complete data become available.

The operational analysis guided the construction of a simulation of airport arrivals over a two-hour period. We then 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. The results are shown in Table 1-1.

As can be seen in Table 1-1, the results showed that in comparing two Baseline cases, more aircraft 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.

Table 1-1. 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

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 hazard indicator presented is that of minimum in-trail separation. 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 does not increase the likelihood of a specific hazardous condition, but does reduce controller workload, thus decreasing the likelihood of a hazardous condition resulting from controller overload.

Chapter 2
Safety Analysis Methodology

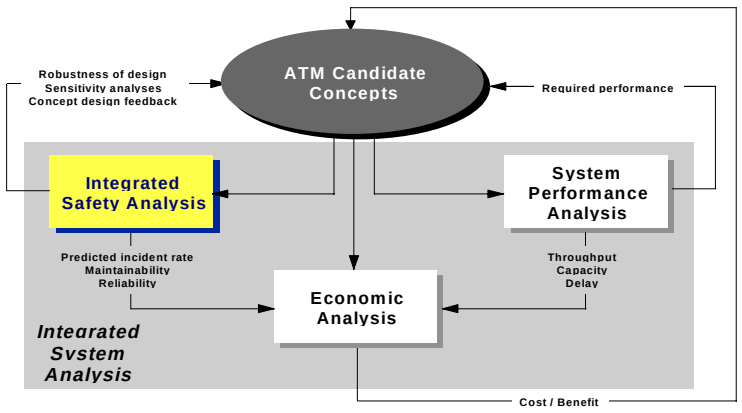
OVERVIEW

This chapter presents a brief overview and perspective of approaches and methodologies for performing safety analyses for complex systems. Ensuing chapters provide the technical details that underlie our methodology for Integrated Safety Analysis, as applied to CTAS at DFW.

The key feature of our approach is that it aims to provide a comprehensive analysis perspective for all the important aspects of system design and development. Within this perspective, the safety analysis is part of an overall integrated analysis that also addresses operational performance and the economic impacts (including the cost-benefit analysis) of the system under investigation.

As shown in Figure 2-1, the analysis begins with a definition of the system concept under investigation. Concept data are then used as inputs to safety, performance, and economic models to evaluate the utility of the concept. As shown in Figure 2-1, we treat the design, analysis, and evaluation of Air Traffic Management concepts as part of an interactive process in which the analysis provides crucial feedback to system developers, as well as the benefits and safety metrics required to support program advocacy.

Figure 2-1. Integrated System Analysis



The methodology includes interactions among: performance models, safety models (including “ilities”), and economic models. It 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, distinguish 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.

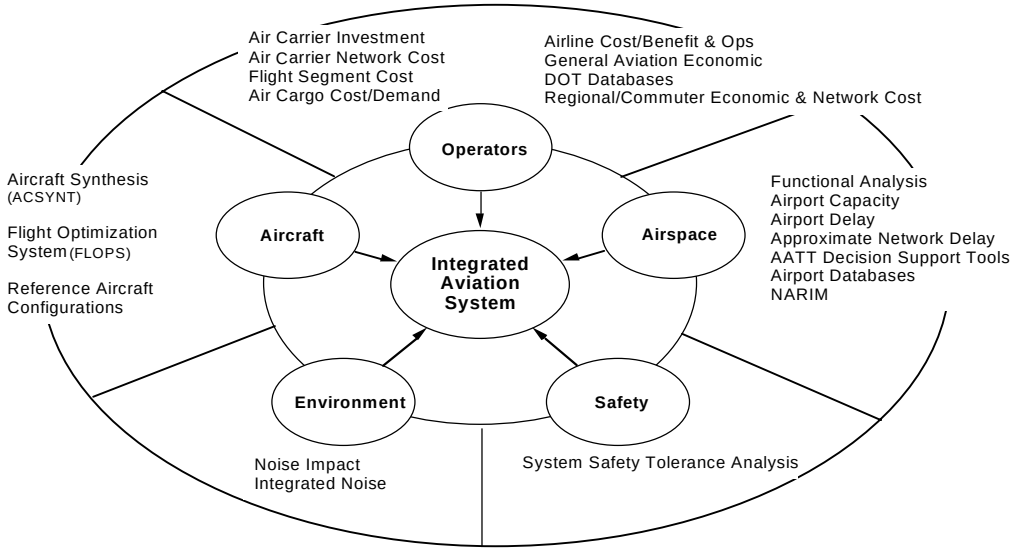
SAFETY ANALYSIS: PART OF A SYSTEM CONCEPT EVALUATION

The integrated safety analysis portion of Figure 2-1 comprises a crucial part of the comprehensive system evaluation. It can include all aspects (or subsets) of the system: gate, runway, terminal area, and en route operations.

AVIATION SYSTEM ANALYSIS CAPABILITY

Much of this integrated analysis approach is being implemented in the Aviation System Analysis Capability (ASAC), a suite of integrated models and databases designed to analyze the impact of advanced aviation technologies on the air transport system. ASAC is sponsored by NASA through the Technology Integration element of the Advanced Subsonic Technology (AST) program, and it is being applied to analyses of AST and Advanced Air Transportation Technologies (AATT) program elements. As shown in Figure 2-2, ASAC contains models of major components of the aviation system, including a safety analysis component. Through ASAC, the safety analysis approach developed and applied in this study can be integrated with the cost-benefit analyses that support the AATT program.

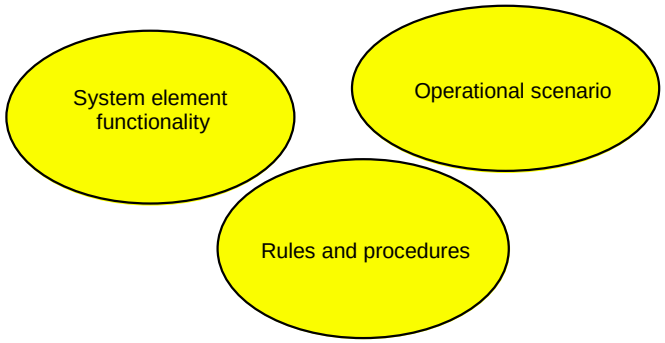
Figure 2-2. Aviation System Analysis Capability



SAFETY ANALYSIS: PERSPECTIVES

A thorough analysis of system safety must address the problem from a variety of perspectives—each impacting safety in different ways. One perspective relates to the operational environments or operational scenarios within which the system is expected to function. Those environments or scenarios that, by their nature, provide opportunities for unsafe operating conditions, have an adverse impact on system safety should be identified. Then, approaches to modeling and on understanding those impacts must be developed. Another safety perspective relates to the reliability and availability of the functions performed by the hardware, software, and human components of the system. Failures or degradation in the performance of elements of safety-critical system components have an impact on safety; models of the reliability of those elements must be developed to determine the impact on system safety. Finally, the rules and procedures under which a system operates can have a significant impact on a system's safety; approaches must be developed to analyze the impact of those rules and procedures on safety for all modes of operation of the system.

Figure 2-3. Perspectives of a System-Level Safety Analysis



The three perspectives are illustrated in Figure 2-3 and can be summarized simply as follows:

- System element functionality involves the analysis of how well and reliably the system elements work and the attendant impact on safety.
- Rules and procedures involve the analysis of how the system rules and procedures have been designed to respond in both safe and unsafe situations.
- Operational scenario involves the analysis of the environment in which the system is expected to operate and its attendant impact on system safety.

APPROACHES AND TOOLS FOR EVALUATING SYSTEM SAFETY

Several approaches have been developed to address the three perspectives of system safety analysis described in the preceding section. Some of those approaches are outlined below.

Statistical Analysis of Existing Systems (Descriptive Approaches)

These approaches are based on statistical analyses of data that are collected over long periods of time. The work of Professor Arnold Barnett of the Massachusetts Institute of Technology (MIT) is an example of this kind of effort. These approaches to safety analysis are "after the fact" and useful in identifying shortcomings in existing systems, but they have limited utility in predicting the safety consequences of proposed system concepts. Since our interest is in evaluation and analysis of the safety of new system concepts, we will not dwell on these approaches.

Analysis of Candidate Designs that Model Human, Technical (Hardware and Software), and Procedural Aspects of the System (Predictive Approaches)

Evaluation tools here include the following:

- "ility" analytical modeling

  These are Markov, Semi-Markov, combinatorial, and fault-tree models used to determine system reliability, availability, maintainability, etc. These approaches have matured over time and the Markov reliability modeling approach is the one that we have chosen and that is elaborated upon in later chapters.

- Simulation

  A variety of statistical event simulation approaches—including discrete–event simulation, importance–sampled Monte Carlo simulation, and hybrid simulations with both human operators and hardware in the loop-have been used to predict the safety of proposed system concepts. The advantage of simulations is that they typically are easier to design and implement than the analytical "ility" models just described. The disadvantage is that, in order to obtain statistically significant results for very low–probability events, many simulations must be performed.

The approach that we have taken in this study is to use a Markov model to determine the probabilities of being in potentially unsafe system states and to employ a deterministic simulation of the system operating in those states. The hazard indicator metrics generated by the TRACON simulation are then weighted by the Markov state probabilities to obtain the total expected values of those metrics.

- Human performance modeling

  The development of models to predict the effect of workload and task design on human error rates and human response times was considered beyond the scope of the effort for this task. Indeed, good models of human performance are critical to the complete analysis of a system. Due to constraints on time and budget, we chose to use simple models of human performance and to embed those in our system Markov models. Thus, at the level of failure and performance degradation, the function of the human is characterized no differently than that of other system components.

- Formal methods

  These are mathematical, logic-based approaches for specifying and implementing safety-critical hardware and software systems and for verifying correctness and completeness of their design and implementation. Typical of these approaches are those taken by Professor Nancy Lynch at MIT and Professor Nancy Leveson at the University of Oregon.

- Information security

  For safety–critical information exchanges (e.g., ADS-B for local air traffic status between aircraft when air separation responsibility is transferred to pilots), the security and integrity of the exchanged information are clearly critical. One way to view information security is in terms of protecting the computers and communications assets of the system. Several protection mechanisms exist: protection against unauthorized alterations of the data and protection against denial of exchange of data. To date, little has been done in the development of models of information security and its impact on safety–critical functions. This is an area for research and is not addressed further here.

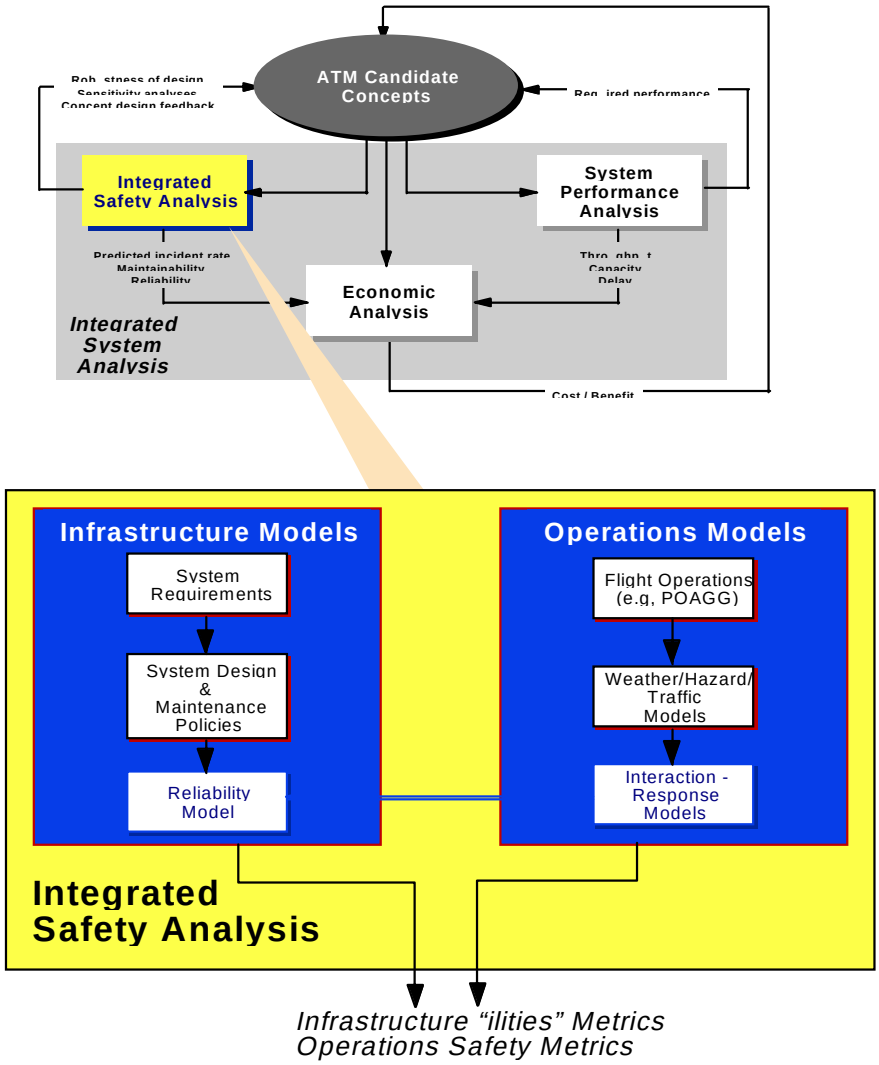
OBJECTIVE: A UNIFIED FRAMEWORK FOR INTEGRATED SAFETY ANALYSES

What is the best way to combine the many evaluation approaches into a unified framework for safety analysis? We seek to draw the three perspectives shown in

Figure 2-3 into a unifying framework that directly addresses the interactions and coupling among those perspectives. Our first step toward such a unification is described in the following sections and has been applied in evaluating the IAPR concept. As time and experience in applying this unified approach evolve, we anticipate further refinements will be made.

The *integrated safety analysis* that we employ is distinguished by its ability to merge system design or functionality information with a parameterization of a system's situation. This is illustrated in Figure 2-4. The "system" may include both air and ground subsystems.

Figure 2-4. Integrated Safety and Reliability Modeling and Evaluation



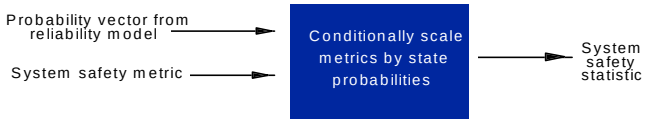
The steps leading from requirements derived for an operational concept to the development of a reliability model of the system architecture that has been proposed

to meet those requirements are shown on the (lower portion of the) left side of Figure 2-4. This represents a *traditional* reliability/safety modeling process. On the right are the models required to capture the environment in which the system will operate as well as the interaction of those environmental models with response models that represent 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 system safety metrics from the Interaction-Response model by the system state probabilities from the Reliability model creates system-level safety statistics. This process is illustrated in Figure 2-5.

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 2-5. Combining Model Outputs



From Figure 2-4, we see that system safety is being addressed from several perspectives, each of which impacts safety. These include

- system functionality (the analysis of how reliably the system components perform);
- rules and procedures (the analysis of how the system is designed to respond in both safe and unsafe situations); and
- operational scenario (the analysis of the external environment in which the system is expected to operate).

The integration of models that quantify each one of these three elements creates an analysis capability that is now system-wide and responsive to ongoing changes in the definition and requirements of the operational concept.

KEY FEATURES OF AN APPROACH TO ANALYZE SAFETY IMPACTS

The approach we developed focuses on the analyses required to support the system design process and concept evaluation. Most significantly, the analytical results supply feedback throughout design and development and can accommodate the varying levels of system detail that are available at different stages of the development process, from early exploration through production. For example, the approach can be used to identify deficiencies in the initial high-level analysis and then progressively provide more detailed information as the design solidifies and evolves over time. The breadth and depth of the analysis can be readily modified to meet varying requirements at different stages in development or to support selection of alternative concepts.

Through integration with the performance and economic models, design tradeoffs can be informed by cost and performance measurement.

DALLAS-FORT WORTH STUDY

For this study, a primary objective is to demonstrate the usefulness of the safety approach for practical applications of concepts early in the development process. We meet this objective by analyzing one of the tools under development within NASA, the Center-TRACON Automation System. While performing that analysis, we also aimed to formulate the model so that it can be enhanced to accommodate future system analyses at key NASA test sites. NASA selected Dallas-Fort Worth International Airport, in particular, to be the primary test-bed for ATM systems. The model we present in this report provides a significant starting point for analyses of terminal area technologies.

To meet tight time and resource constraints, we needed to select a portion of CTAS to analyze. Consequently, we chose the approach phase of flight that uses the CTAS Passive Final Approach Spacing Tool (P-FAST) to show a useful level of detail within the limited time and resources available. Within P-FAST, the study concentrates on aircraft operations from the meter gate through to the runway.

SUMMARY OF APPROACH TO SAFETY IMPACTS

Our approach to analyzing the safety impacts of CTAS at DFW is straightforward. The steps can be categorized into four phases.

1. Build a *model framework* for approach operations at DFW.

- The first phase focuses on constructing the modeling framework for analyzing approach operations at DFW. This phase consists of three steps:
- Build functional models of key components.
- Construct flow diagrams of system interactions.
- Define operational states by function.

2. Develop *operational scenarios.*

   - In the second phase, we develop operational scenarios that describe realistic indicators of DFW approach operations. The steps in building the operational scenarios are as follows:
     - Collect operational data.
     - Meet with controllers to identify useful problems to analyze.

3. Identify *operational differences* due to CTAS.

   The next step in the analysis requires us to define the operational difference attributable to the use of CTAS by controllers at DFW. Among the differences we examine are

   - changes in roles and responsibilities,
   - changes in system or equipment performance, and
   - variations in traffic flows.

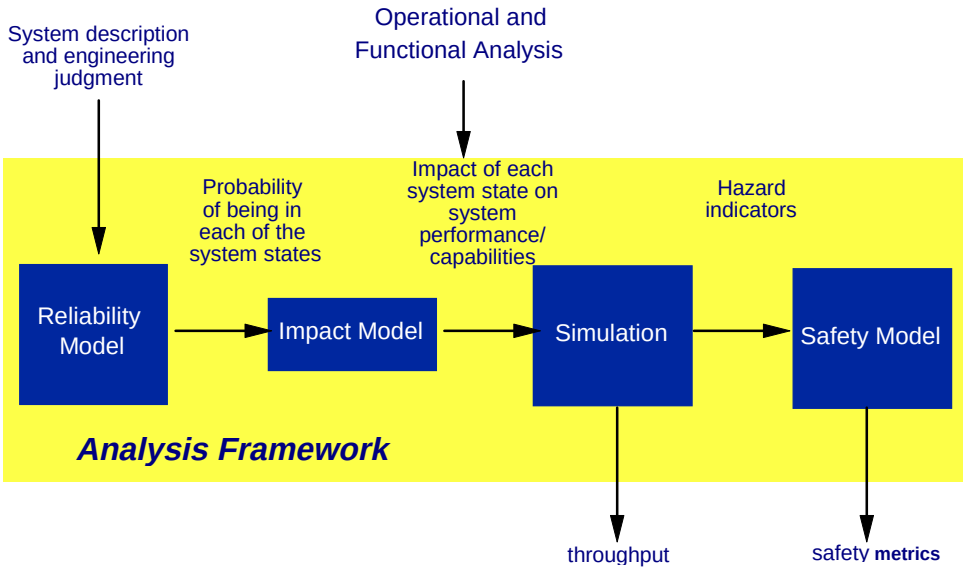
4. Develop system safety *performance measures*.

   The final phase of analysis generates the performance measures that can be used to track system safety. Performed in parallel with the model development, this phase aims to ensure that the analysis generates meaningful measures of system hazards that can be used to compare safety under different systems.

Figure 2-6 summarizes the key components of the analysis. Using the results of the system descriptions generated in the first phase, we build reliability models 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.

Figure 2-6. Analysis Framework



Chapter 3
Safety Analysis Methodology Applied to Dallas-Fort Worth Airport

This chapter describes in detail how we applied the safety analysis methodology to evaluate the safety impacts of CTAS at DFW.

FUNCTIONAL ANALYSIS AND ELEMENTS

The first step in our analysis was to develop the functional model of operations at DFW. The functional model represents *what* must be done to operate DFW, not *how* it is done. There were three sources of information for developing the functional model. The first was the extensive work done previously by the team. The second was general documentation regarding the systems and operations within the TRACON airspace and the U.S. NAS and more specific documentation relating to the TRACON at DFW. The third was visits to the TRACON facilities at DFW and the TRACON and Tower facilities at Logan Airport, Boston, Massachusetts for technical discussions with controllers and traffic management specialists.

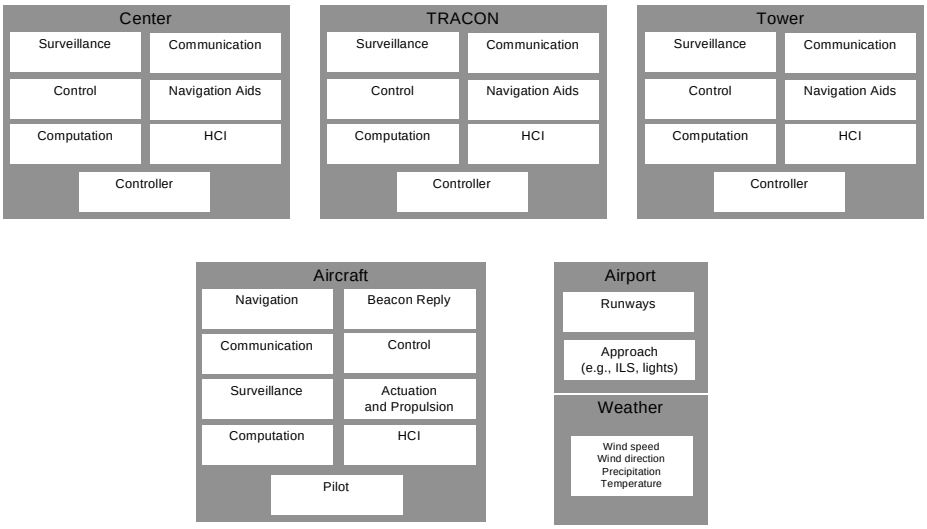
We examined information on DFW layout and approach topology, using the runway configuration and corner posts from the time of the CTAS field tests. We also examined information on equipment at DFW, including navigation aids at the airport and in the TRACON, surveillance equipment, communication equipment, and other equipment controllers utilize. We also examined operational procedures followed by controllers and pilots, both for normal operations and for contingencies, such as equipment failures at the airport, adverse weather, equipment failures on aircraft, etc. Traffic patterns in the TRACON, including distribution of routes and the density of traffic along the routes, were taken from Official Airline Guide (OAG) and Enhanced Traffic Management System (ETMS) data.

Overall, we found that most important effect of P-FAST is to balance runway utilization, resulting in higher throughput and fewer changes of runway assignments. A major effect is reduced workload for both controllers and pilots, with fewer communications needed. P-FAST enables controllers to issue some commands early, eliminating the need to make them later when things may be getting tight, causing less distraction for controllers and allowing them more time to spend on the fundamental job of separation. There is a reduction in the likelihood of hazards that occur from a sequence of events, when controllers and/or pilots focus on one thing—and then a hazardous situation arises.

The major impact of Center-TRACON Automation System (CTAS) on operations in TRACON is from the improved prediction of incoming traffic, which facilitates better decision-making by traffic managers and controllers. It helps traffic managers in deciding what positions to combine and de-combine so that the "right" number of planes is available for a controller to handle, so that the controller is neither bored nor overloaded. It also helps traffic managers to provide the right number of planes for a trainee to handle.

Figure 3-1 illustrates the high-level functional elements of the Center, TRACON, Towers, and Aircraft—that interact with the Airport functional element. At this high level, Center, TRACON, and Tower have the same functional elements.

Figure 3-1. Functional Elements of Dallas-Fort Worth



In order to demonstrate the methodology within the constraints of the project, we examined the subset of functional elements described in Tables 3-1 through 3-3 in the TRACON aircraft and airport.

The functional elements defined in Table 3-1 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 of surveillance information to the TRACON controllers. The states of the communication and control functions will reflect the availability 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 function will indicate the availability of the signals that radiate into the TRACON airspace, which aircraft can use to navigate in the TRACON airspace.

Table 3-1. Functional Elements for Terminal Radar Approach Control

Surveillance	The capability of TRACON to detect and interrogate aircraft for surveillance data in TRACON and adjacent airspace and provide this information to TRACON controllers
Communication	The capability of TRACON to allow TRACON controllers to transmit and receive voice communications with aircraft in or about to enter TRACON and with controllers in the adjacent tower and the adjacent center
Control	The capability of 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 TRACON
Navigation aids	The capability of 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

In Table 3-2, the function definitions are the capabilities for a single aircraft. The level of capability, or accuracy, of these functions can be different for each type of aircraft. Some aircraft may not have the beacon reply function. When reliability models are developed, each aircraft type may need a unique reliability model to capture the reliability of equipment particular to that aircraft type. The impact to the TRACON simulation may be different for each aircraft type.

Table 3-2. 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 3-3 defines the functional elements for the airport category. The airport, tower and center airspaces are not part of the TRACON airspace, but failure events of systems in these facilities can affect the flow of traffic through TRACON 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 TRACON simulation are defined in Table 3-3.

Table 3-3. 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

OPERATIONAL ANALYSIS

In the remainder of this chapter, we describe the operational interactions between the various elements of the air traffic control system that are involved in aircraft approaching and landing at DFW. In particular, this includes the following:

- Center/TRACON interfaces
- TRACON/tower interfaces
- Handover of aircraft from Center, to TRACON, to tower
- Role of navigation aids
- Role of approach clearances, Standard Terminal Arrival Routes (STAR), and vectoring
- Impact of missed approaches
- Impact of reliability failures, accidents, etc.
- How weather affects operations.

The analysis presented provides the basis for understanding the relative importance of the functional elements and an overall framework for system simulations, including the current simulation capability, and future simulations with more fidelity in modeling system elements and the dynamic decision-making process.

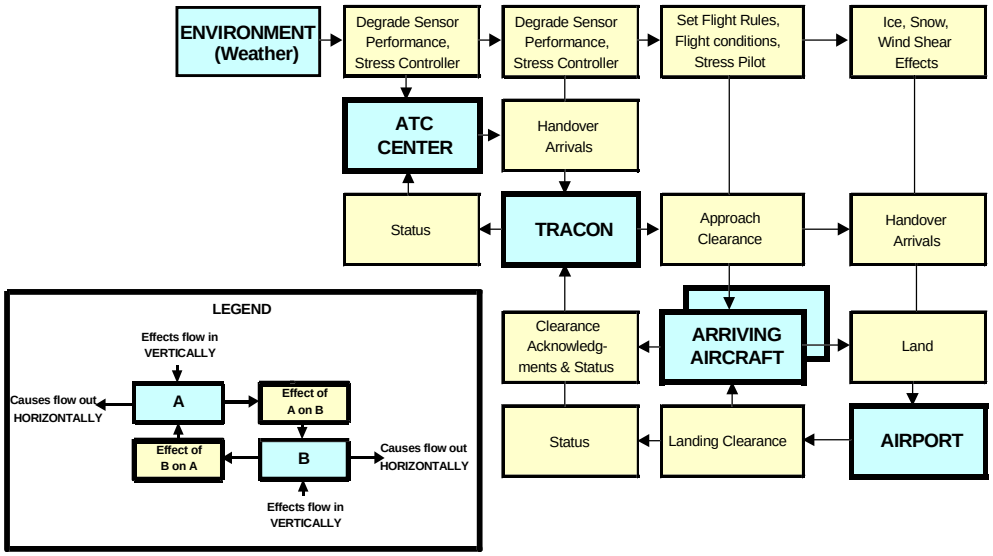
N^2 System Interaction Diagrams

A proper analysis of the operations involved in bringing large volumes of air traffic into a single high-density airport requires consideration of many types of interactions. Although we have deliberately excluded departing traffic in order to simplify the analysis to a point consistent with the scope of work of this task, the interactions involved with arriving traffic alone are quite complex. To clarify these interactions, we have adopted a graphical analysis technique particularly well-suited for showing interactions among elements of complex systems. This technique uses specially formatted diagrams known as "N^2 System Interaction Diagrams," so-called because they arrange the "N" elements of the system under consideration in a square $N \times N$ matrix with the elements themselves occupying

the diagonal positions in the matrix and the interactions among elements lying in the off-diagonal positions. Diagrams of this type can potentially show interactions down to any desired level of detail, while still retaining a system-wide overview.

Figure 3-2 is a top-level N^2 system interaction diagram that shows the major elements of the air traffic system and its operating environment that are applicable to the employment of P-FAST in the DFW TRACON. Because it is relatively simple, this figure also is useful for explaining the syntax of N^2 system interaction diagrams. At this level, we identified five major elements applicable to the analysis of P-FAST. These elements occupy the diagonal positions (i.e., top left bold framed flow box to bottom right box), in the flow matrix. In general, the major drivers of the system are placed near the upper left of the diagram, and the major impacted elements towards the lower right (this arrangement is, however, often altered to avoid too many overly long "reaches" between elements sharing many interfaces). Such an arrangement allows the Figure 3-2 to be read from left to right and top to bottom. When an element can have multiple instances, such as "arriving aircraft" here, that multiplicity is shown by simply adding an extra hidden box behind the main element.

Figure 3-2. Top-Level System Interactions



The off-diagonal elements of an N^2 system interaction diagram identify, in summary form, how the system element on that *row* interacts with the system element in that *column.* A complete N^2 diagram is accompanied by documentation that elaborates on each off-diagonal entry in the diagram. Thus, where we show that the "Environment (Weather)" element interacts with the "Arriving Aircraft" element by "Set flight rules, flight conditions, Stress pilot," we could augment that interaction summary with a separate detailed discussion of Visual Flight Rules

(VFR) versus Instrument Flight Rules (IFR); how turbulence, storms and icing conditions affect the flight; and how severe weather causes increased stress in the flight crew.

The basic syntactical rule for the flow of cause and effect in an N^2 system interaction diagram is shown in the legend of Figure 3-2. When one element is the source of the influence, then that interaction flows outward *horizontally* from that element. When an element is influenced by another, that influence flows inward *vertically* to the influenced element. When influence is mutual, then the influence is show twice in symmetrically located, off-diagonal boxes on the diagram.

The major elements of the system under analyses are

- the Environment (Weather),
- the Center,
- the TRACON,
- the Arriving Aircraft, and
- the Airport.

The diagram indicates that element # 1 (the weather) influences all other elements as follows. It affects the Center (element # 2) by possibly degrading the performance of its radar systems and possibly stressing the Center controllers. It affects the TRACON (element # 3) similarly by possibly degrading the performance of its radar systems and possibly stressing the TRACON controllers. It affects the arriving aircraft (element # 4) by determining whether or not IFR flight rules are required, causing the flight conditions of the aircraft (e.g., in the form of turbulence, icing, and lightning). And, partly as a result of the first two effects, it may cause the flight crew to become stressed. Finally, it affects the airport (element # 5) by possibly causing one or more runways to be degraded or closed because of ice or snow on the runway or wind shear in the approach path to the runway. The weather (being part of nature) is unaffected by any other system element.

Element # 2 (the Center) interacts with TRACON (element # 3). It affects TRACON by handing over control responsibility for arriving aircraft to it. It also is affected by TRACON by receiving status information on the overall state of the TRACON environment and the airport. This interaction is dynamic. If TRACON or the airport becomes saturated, appropriate status messages might cause the Center to hold aircraft outside the TRACON area and/or meter them into the area at a slower rate. The weather (element # 1) can affect Center operations as described above. As far as the system being analyzed is concerned (P-FAST at DFW), the Center has no direct interactions with any other system element. Its direct interaction with the arriving aircraft, for example, occurs prior to their

entering the P-FAST environment and need not be addressed explicitly within the TRACON system.

Element # 3 (TRACON) interacts with the Center (element # 2) by issuing status information to it. It affects the arriving aircraft (element # 4) by issuing approach clearances to them, and it affects the airport (element # 5) by handing over control responsibility for landing aircraft to it. It is affected by the arriving aircraft (element # 4) by receiving clearance acknowledgments and status information from them, and it is affected by the airport (element # 5) by receiving status information from it. It is affected by the weather (element # 1) as described above.

Element # 4 (Arriving Aircraft) affect TRACON (element # 3) by issuing clearance acknowledgments and status information to it. It affects the airport (element # 5) by approaching it and landing thereon. It is affected by TRACON (element # 3) by receiving approach clearances from it and by the airport (element # 5, more specifically the tower, which is part of the airport) by receiving landing clearances from it. It is also affected by the weather (element # 1) as described above.

Element #5 (Airport) affects the arriving aircraft (element # 4) by issuing landing clearances to them and the TRACON (element #3) by issuing status information. It is affected by the arriving aircraft (element # 4) by having them approach and land upon it, and by the TRACON (element # 5) by receiving aircraft handovers from it. It also is affected by the weather (element # 1) as described above.

At this level, the interactions described above are rather basic. As we expand the interactions to lower levels we will see each interaction shown on this chart become, in general, several interactions with specific subelements of the major elements shown here.

Note again that throughout this discussion, departure air traffic is ignored. Since the main purpose of the present effort has been to demonstrate our analysis methodology, this simplification appears justified. Obviously a more thorough analysis of this problem will require departure aircraft to be included in the overall system interaction diagrams as important entities that could interact with arriving aircraft and require accommodation by TRACON controllers.

This analysis approach serves three purposes. First, a complete N^2 system interaction diagram shows the entire system, all of its critical parts, and all of the critical interactions among those parts as a single entity. The collection of these interactions is the “big picture” view of the system (i.e., the “forest”) while the interactions themselves provide detailed knowledge about how each part of the system works with the other parts (i.e., the “trees”). A complete N^2 system interaction diagram can become quite large. In most cases, however, such a diagram can “capture” the essence of a complex system down to a fairly low level on a single (large) sheet of paper. Such a large diagram is not suited for inclusion in a report such as this one, however, and the charts that follow only show selected parts of

such a diagram expanded and enlarged for clarity. (A miniaturized version of the entire diagram for this system is shown, for comparison purposes only, at the end of this section.)

The second purpose served by this approach is to establish a systematic analytic method for defining and understanding very complex systems such as that considered here. The process of creating such diagrams forces the analyst to address all system issues, often exposing initial gaps in understanding that must be filled in for logical completeness. Each interaction between any two elements becomes unambiguously isolated and must be understood and rigorously defined for logical completeness. All loose ends should be tied down.

The third purpose served by this approach is to provide a logical *qualitative* basis for *quantitative* analysis. The components and interactions of the computer models and simulations used in the analysis are identified and linked to the highest system level. Our current simulation, described below, incorporates many of the elements and interactions described in this section. The reliability modeling described in the Reliability Modeling and Analysis section draws upon the interactions described in this section. The N^2 format is readily adaptable to the definition of Markov Process states and transitions used in our reliability model. Future higher fidelity models and simulations could incorporate more of the system elements and element-to-element interactions described here.

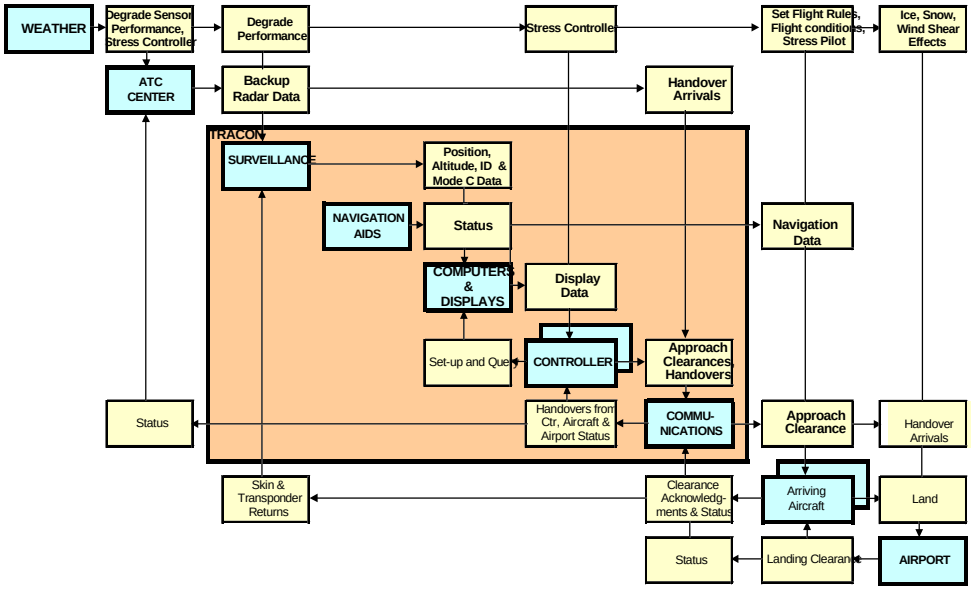
Major Operational Interactions Affecting P-FAST

The following three subsections expand upon three of the major system elements discussed above. These include (1) the TRACON and some of its subelements, (2) the Arriving Aircraft, and (3) the Airport.

INTERACTIONS WITHIN THE TRACON

We have identified five major subelements within the TRACON. These are shown in Figure 3-3 (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 3-3. TRACON



As an indication of the greater level of detail depicted on Figure 3-3 when compared with Figure 3-2, note that the input interactions from the Weather, the Center, the Arriving Aircraft, and the Airport are broken down into more detail.

The weather, for example, affects surveillance by possibly degrading sensor performance, and the controllers by possibly adding stress. All communications between the controllers and either the Aircraft, the Tower, or Center pass through the communications system (which will be broken down into more detail in a later chart).

Notice also that the controllers interact exclusively with the computer and display system and the communications system. Operationally, we are now beginning to see detail where hardware reliability or human error could begin to affect overall operations. Interactions shown at this level show that the controller can only act upon the information presented to him by the display and communicated to him by the communications system. The display, in turn, is fed by the surveillance system and the computers. The controller interacts with the computers and displays by setting them up for her particular needs and querying them for information. Lack of data, hardware or software errors, equipment failure, or human error in any of these interacting elements could affect the controller's decision-making process. In addition, the intangible effects of stress, whether induced by dense traffic dynamics, the advent of severe weather, or some other factor, could likely affect his decision-making process as well. Less than perfect decision-making on the controller's part, however, is not necessarily adverse to the overall operation of the system. While, in the worst case, poor decisions could lead to hazardous conditions; more typically, they merely lead to less than maximally efficient traffic flow. The specific influence of P-FAST functionality occurs primarily in this

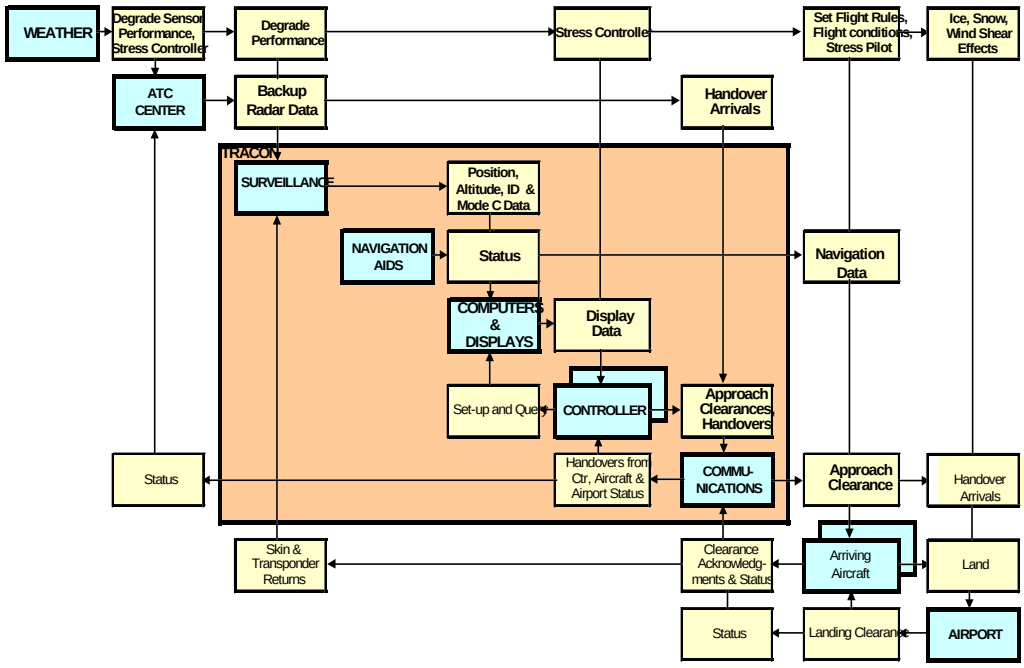
portion of the overall system. As a decision-making aid, P-FAST may help the controller in many ways. It may delay or avoid the onset of stress in dense traffic or adverse weather conditions; it may reduce the controller's need to input new queries into the computer/display system; and, finally, it may reduce his need to communicate with inbound aircraft or the tower. The N^2 diagram format of this figure shows traceability upward from these specific subelement interactions to overall operation of the system.

The next three subsections carry the analysis down to still another level of detail for three of the major TRACON elements.

TRACON Surveillance

Figure 3-4 expands the TRACON surveillance element. It consists of two elements: a radar system (in the case of DFW there are multiple instances of this system) and a backup capability supplied by the Center radar. The radar itself consists of two parts, the primary radar and the beacon system. Note that we can now isolate on the chart-specific interactions among equipment items and show their impact on other elements. For example, the primary radar supplies range information only to the controller via a skin track of the aircraft. The beacon system (interacting with Mode C transponders in the arriving aircraft) supplies altitude and ID information. The backup system, when required, can supply similar data obtained from the Center radar (although possibly missing coverage of some portion of the airspace).

Figure 3-4. TRACON Surveillance

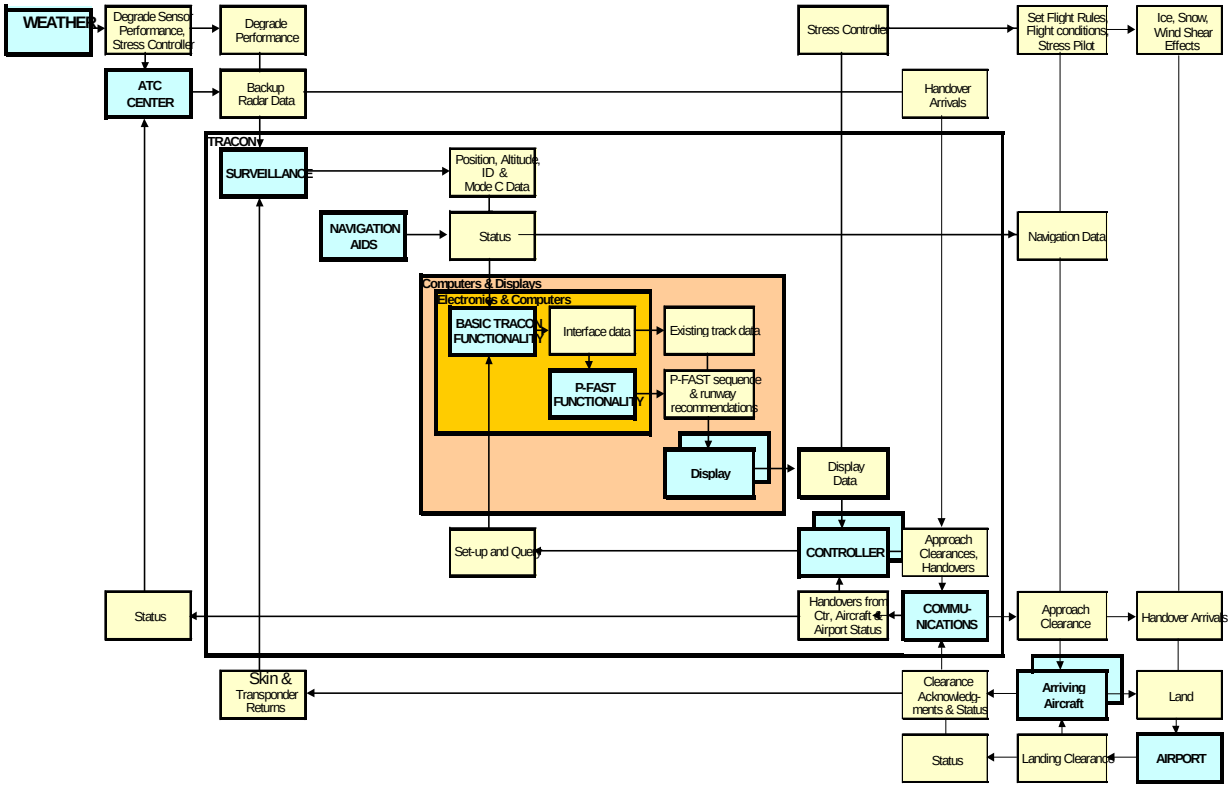


TRACON Computers and Displays

Skipping over the Navigation Aids element (which consists of the Very High Frequency Omni Range/Tactical Air Navigation (VORTACS) and other navigation aids within the jurisdiction of the TRACON), Figure 3-5 expands the interactions involving the computer and display subelements of the TRACON. The computer element is actually composed of a basic capability and the additional capability supplied by the P-FAST system. At this level, we have chosen to break the computer system down into its major functional elements. By splitting the functionality of the computer system this way, when we compare scenarios with and without P-FAST functionality, this diagram helps us recognize the appropriate interactions for both cases.

Note, also, that there are multiple instances of displays, just as there are multiple controllers. Another level of detail would enable us to look at the interactions between individual controllers within the TRACON.

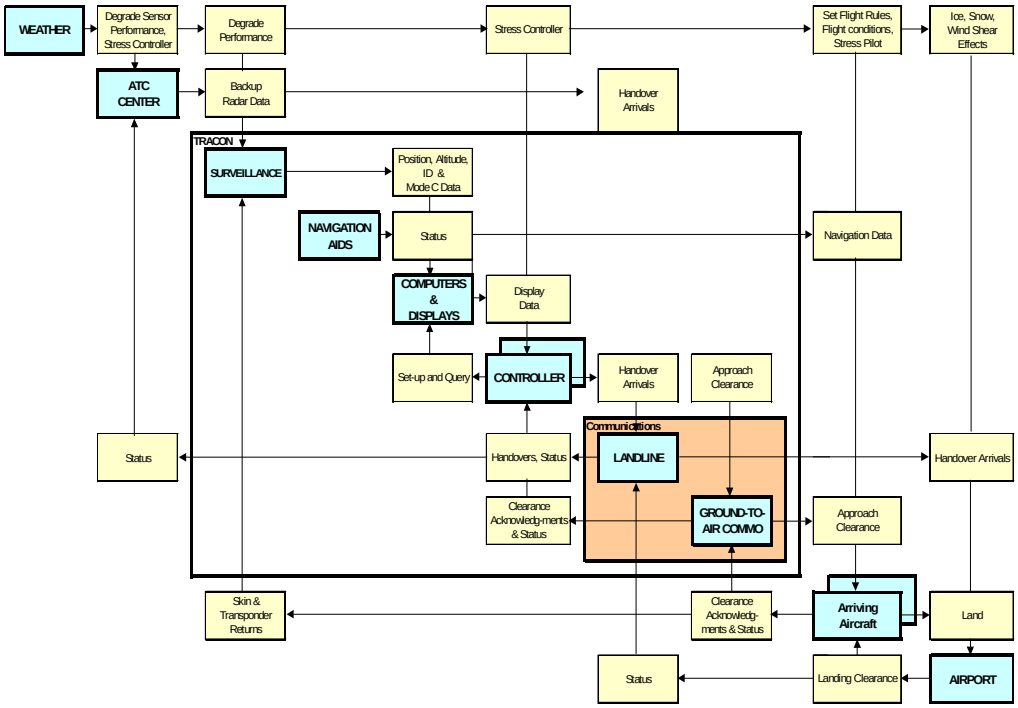
Figure 3-5. TRACON Computers and Displays



TRACON Communications

Figure 3-6 breaks the Communications system into its landline and ground-to-air components. This determines the paths that different types of communication will take and enables us to isolate the effect of, for example, failure of transceivers, frequency congestion, and radio-out aircraft.

Figure 3-6. TRACON Communications



ARRIVING AIRCRAFT

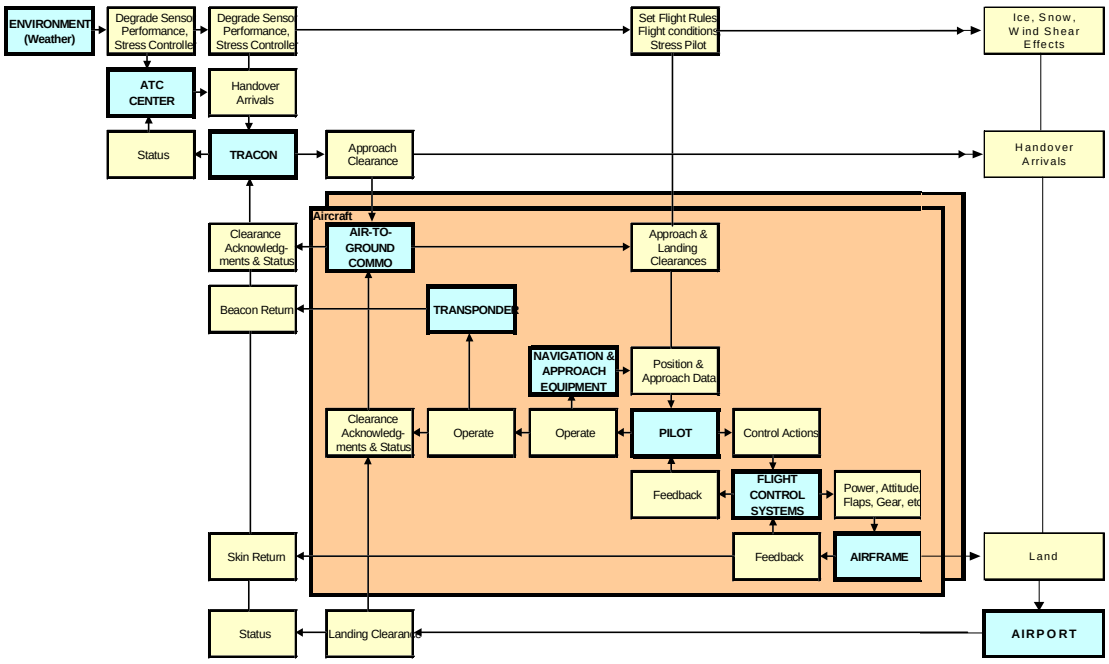
As indicated in Figure 3-7, each aircraft is a complex system in itself. Furthermore, most aircraft in the system will differ from one another in many respects. In addition to size and speed differences, some may have larger or smaller crews, some may have more or less navigation equipment, and some may be more capable in bad weather than others. Appropriate expansion of the major aircraft elements shown here allows for accommodation of these differences.

The major elements of an aircraft are identified here as

- communications (shown in the upper left to conform to the “readability” rule described earlier—the major driver of the aircraft’s interaction with the rest of the system comes via clearance from ground controllers, which comes through the communications system—an indication of how critical communications failure can be);
- the aircraft beacon or transponder (which interacts exclusively with the TRACON secondary radar);
- the navigation and approach equipment;
- the pilot (and other crew members, if any);

- the flight control system (including autopilot, engine and engine controls, flight control surfaces and their controls, etc.); and
- the airframe itself.

Figure 3-7. Aircraft



The airframe is included here as the physical "container" in which everything else in the "Arriving Aircraft" system element resides. It is this "container" that moves through the sky in response to pilot actions which, in turn, are in response to controller-issued clearances and navigation and approach equipment indications. It is also this "container" that must ultimately land successfully on an airport runway.

AIRPORT

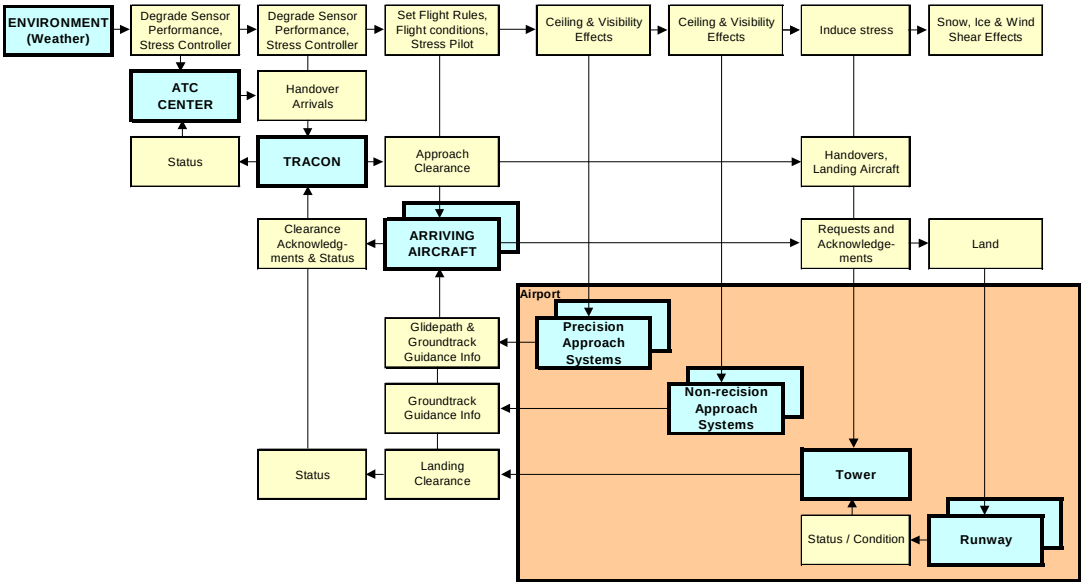
The final expansion of system elements considered here is the airport. As shown in Figure 3-8 the airport consists of

- Precision Approach Systems (i.e., ILS systems) in multiple instances;
- Nonprecision Approach Systems, also in multiple instances;
- the Tower; and
- the Runways (in multiple instances).

This breakdown of the airport enables us to isolate weather effects—bad weather can preclude the use of nonprecision approaches while allowing precision

approaches, for example. We also can isolate the functionality of the approach systems as they affect the arriving aircraft. Failure of a glideslope, for example, denies independent descent path information to the pilot, converting a precision approach system into a nonprecision approach system. Depending on current ceiling and visibility, this may effectively eliminate one runway for arrivals.

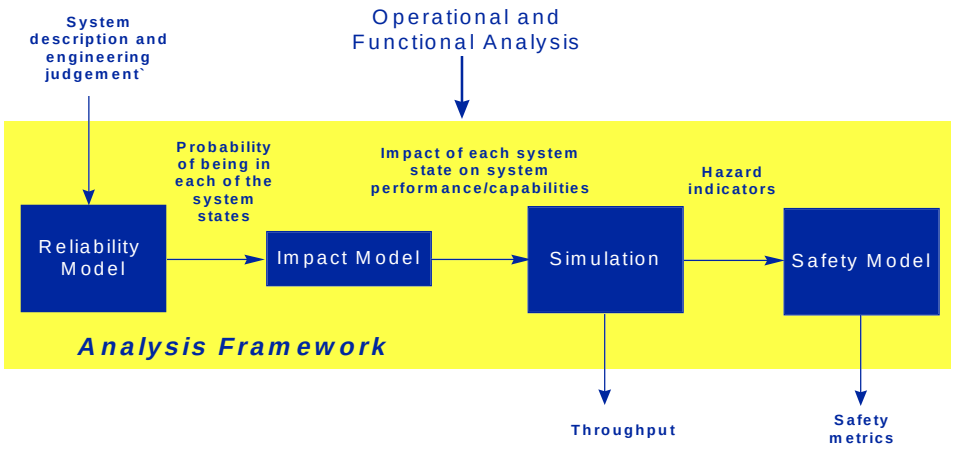
Figure 3-8. Airport



ANALYSIS FRAMEWORK

We implemented the analysis framework illustrated in Figure 3-9 and described in this chapter. We discussed the overall methodology earlier under Objective: A Unified Framework for Safety Analysis.

Figure 3-9. The Analysis Framework



Reliability Modeling and Analysis

In this section, we discuss several reliability modeling techniques and present Markov reliability models of two critical components of the DFW TRACON: (1) a surveillance radar system and (2) an ILS approach system.

RELIABILITY MODELING TECHNIQUES

Three classes of standard reliability modeling techniques are simulation, combinatorial models, and Markov modeling.

Using simulation (e.g., Monte Carlo simulation), system reliability is determined by generating failure and repair events at times distributed according to the component failure and repair rates. Simulations are repeated until statistically significant reliability measures are accumulated. A major strength is the ability to analyze complicated repair and reconfiguration scenarios. A disadvantage is that for highly reliable systems, the failure rate is so low that a very large number of simulations must be run to accumulate a statistically meaningful number of events.

Combinatorial models (e.g., Fault-Tree Analysis) are based on a system architecture and redundancy management approach, in which component failure probabilities are combined to determine system reliability. Limitations include difficulty including events that have order dependencies, such as repairs and explicit modeling of reconfiguration strategies. Also, because all combinations of events for the entire time period must be included, for complex systems this results in a complicated fault tree that is difficult to construct and validate.

Markov modeling techniques calculate the probability of the system being in its various states as a function of time. A state represents the system status with respect to component failures and the behavior of the system's redundancy management strategy. Transitions from one state to another occur at given transition rates that reflect component failure and repair rates and redundancy management performance. Advantages of Markov modeling include these (1) model construction does not require *explicit* generation of all possible combinations of events that can occur over the entire time period; 2) order dependent events are included naturally; and 3) the model is solved analytically (or numerically), avoiding simulation. A disadvantage is that the state space can grow exponentially with the number of components. However, in many situations of interest techniques have been developed to render this problem tractable, including model truncation, state aggregation, and behavioral decomposition.

Figure 3-10 summarizes the steps required to reduce a complex real-world system into an analyzable scientific abstraction from which its reliability can be calculated.

Figure 3-10. Markov Modeling

- Understand the system
  - Must understand both the “forest” and the “ trees”
- Identify groups of system components at the same level of aggregation
  - At any level of detail, must be sure that we are comparing “apples” with “apples”
- Define failure modes
  - Which components are “critical”?
  - Which “trees” or “groups of trees” are essential to the survival of the “forest”
- Define Markov states
  - Cast our understanding of the system in terms of well-defined “states” that interact with one another by well-defined “transitions”
- Create state transition matrix
  - Create a transition diagram showing paths that lead from one state to another state
  - Associate the paths in the diagram with the off-diagonal elements in the Markov transition matrix
- Obtain failure rate (or MTBF) data
  - Beware of GIGO
- Identify levels of functionality
  - Associate selected Markov states with common levels of overall system functionality
- Calculate functionality probability state vector
  - Straightforward mathematical exercise

In the case of the components at DFW for which we constructed reliability models, the first bullet in the figure means that we must understand the complete environment—both the natural environment and the larger Air Traffic Control System within which the DFW TRACON is imbedded. The Operational Analysis methodology described in this chapter is directly applicable to this process.

From a reliability point of view, the real-world radar and ILS systems to be analyzed are far too complex to be simulated in detail within the scope of this task. Instead, in order to illustrate the methodology involved, we selectively grouped entire areas of detail into single aggregates that can be characterized in our models as single objects. In doing so, care must be taken not to overemphasize some areas (just because they are better understood) while “glossing over” others (because of an initial lack of understanding). Again, the methodology ensures that the correct balance is achieved.

Having aggregated the details into manageable groups, we must define exactly what happens to the overall system when one or more of those aggregated groups fail, either totally, or partially. These are the formal “failure modes” of the system.

The next step is to define the failure modes as Markov states. This is the first point in the process where mathematical rigor must be strictly imposed. Some general comments of Markov Processes are in order before proceeding.

Complex systems often can be characterized as always being is some specific "state." All possible states of the system must be well-defined and complete, in the sense that the system must be in one of the defined states. If the system can change states at random intervals, then there is some probability that, at some arbitrary time, it will be in one of the states. The sum of the probabilities that it is in each of its possible states must always equal 1.0 (another way of saying that the set of states is complete). When the system changes from one state to another, we say that it "transitions" from the previous state to the new state. To satisfy the mathematical requirements of a Markov process, the probability that the system can transition from any one of its states to any other state must not depend on past history, but only on the two states involved (the previous state and the new state). Finally, a "stationary" Markov process is one in which the transition probabilities do not change with time.

Discrete Markov processes only can make transitions from one state to another at discretely specified intervals. They are completely defined if all of the transition probabilities are defined. Differential Markov processes can change states at any time. For these, instead of defining a transition probability, we define a transition "rate." Its units are "transitions per unit time" (whereas transition probabilities are just dimensionless numbers).

Reliability models of complex systems can be fit into the mathematical mold of differential Markov processes. In such models, each state of the system represents one of the ways in which some aggregated set of its components can fail. In redundant systems, some failures will not change the overall functionality of the system, some failures will result in degraded functionality, and some failures will result in no functionality or overall system failure. One of the states is the "no failures" state. We can think of the system as starting out in its "no failures" state. The rate at which it will transition from this state to another state is simply the failure rate of the aggregated components that define the new state.

Reliability models also include repairs. Given that the system is in one of its failed states, it can return to the "no failures" state at a rate equal to the repair rate (in units of repairs per unit time) for the aggregated components.

Given the states, the next logical step in the process is to define precisely exactly what can happen in the real world to force the system to transition from one state into another. This step is complete when a well-defined Markov transition matrix can be defined, at least symbolically.

Data specifying the quantitative failure rates or mean times between failures for each aggregate of components must be obtained, by actual observation, by

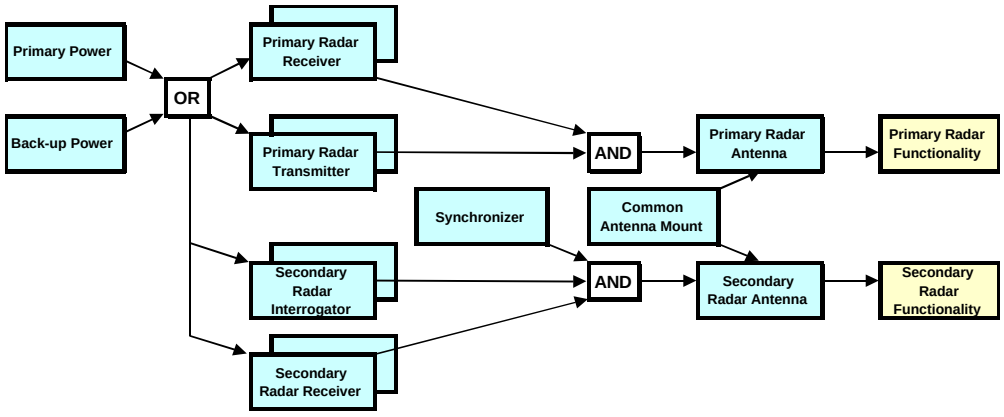
experiment, by off-line simulation, or by exercising good engineering judgment. We must avoid "garbage in, garbage out!"

Since we are interested in levels of operational functionality, there will be, in general, several Markov states that, collectively, result in the same level of functionality (to the level of detail that is important to our problem). These must be identified so that we can sum their probabilities of occurrence to determine the desired probabilities of having a given level of functionality.

SURVEILLANCE RADAR RELIABILITY MODEL

Figure 3-11 is a simplified top-level diagram of a surveillance radar system similar to those typically used in a TRACON (DFW actually had two [now four] of these radars at the time that the P-FAST experiments were conducted, either one of which would have been sufficient to conduct full TRACON operations). This is a generic diagram representing a system with dual redundant—critical components (as are the DFW radars). 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 3-11. Surveillance Radar Reliability Model

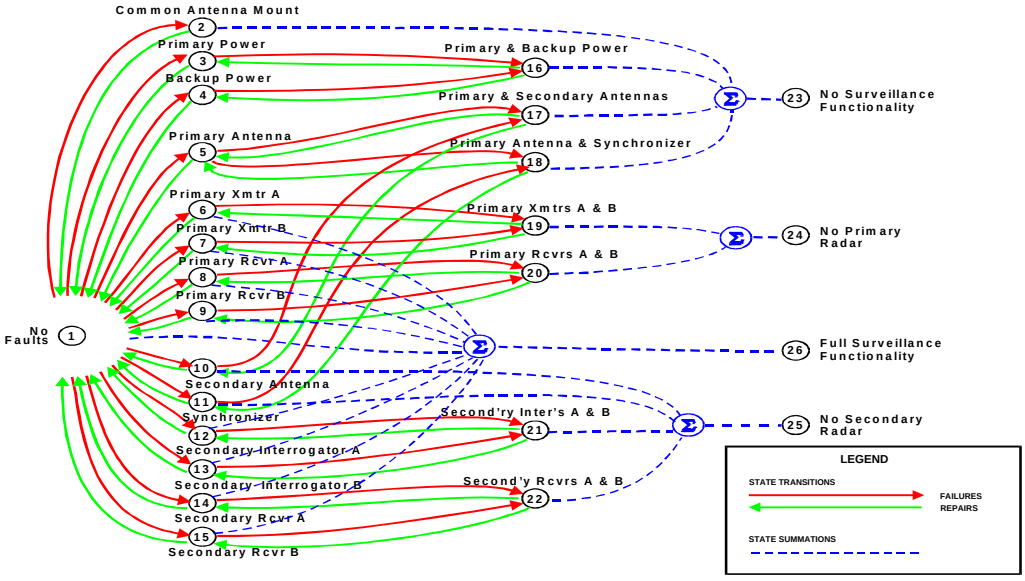


The primary and secondary antennas are rigidly connected, and share a common rotating antenna mount. Secondary (beacon) radar interrogations are synchronized to the pulses transmitted by the primary radar. The system is assumed to have both primary and backup power sources.

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 3-12 shows the 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.

Figure 3-12. Surveillance Radar State Transition Diagram



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 antenna mount,” results in total loss of the surveillance 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 3-13 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 3-13. 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				

Figure 3-14 shows the dynamic response of the reliability model as it approaches steady state. This figure shows the probability of being fully functional as a function of time, given that the system started in a state of full functionality.

Figure 3-14. Probability of Full Capability Over Time

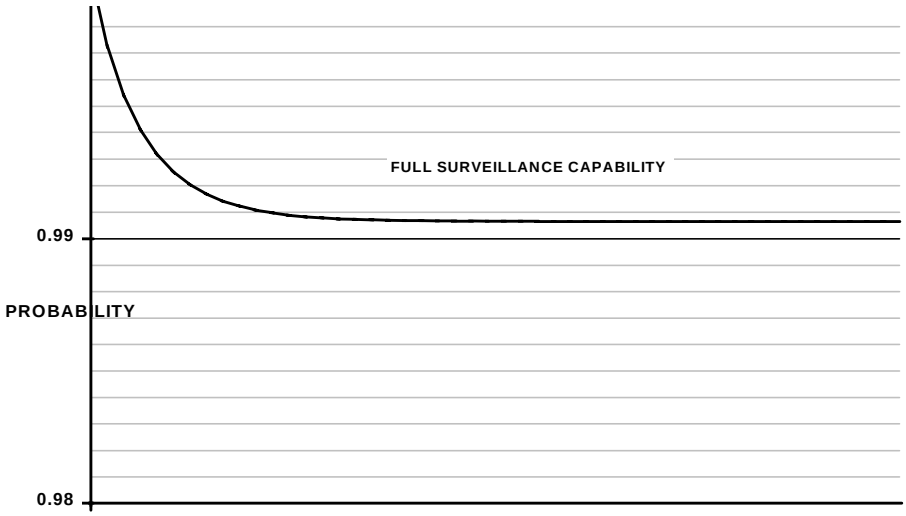
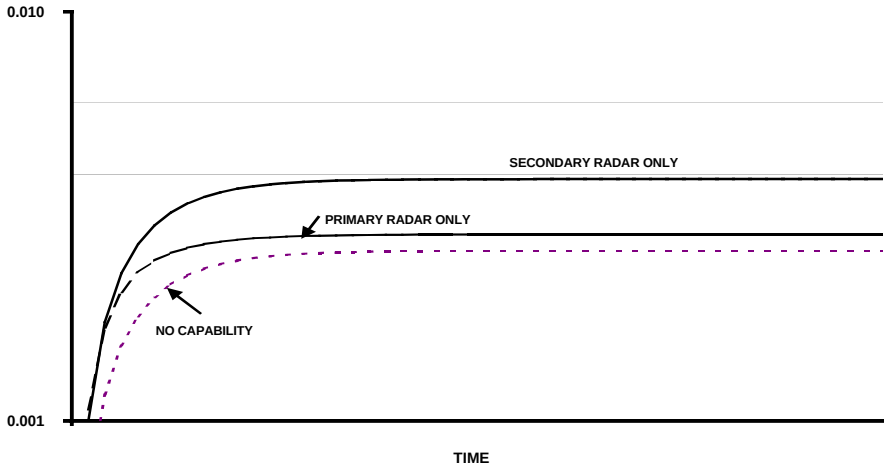


Figure 3-15 shows the probabilities of being in the other possible functional states as functions of time, given that the system started in a state of full functionality (note: this figure uses a logarithmic scale for its ordinate).

Figure 3-15. Probability of Failures Over Time



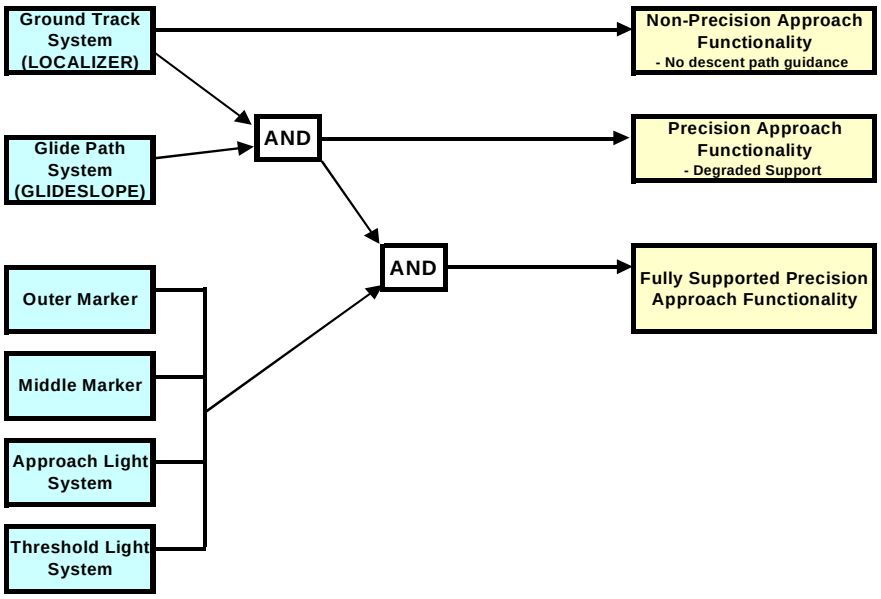
PRECISION APPROACH SYSTEM INSTRUMENT LANDING SYSTEM RELIABILITY MODEL

Figure 3-16 is a simplified top-level diagram of a precision approach system. It is modeled after a standard system, but it is sufficiently generic to represent any system that provides independent guidance in both the vertical and horizontal planes to aircraft approaching land. The system consists of two major subsystems, the ground track system (or, in the case of an ILS system, the localizer) and the

glide path system (or glideslope). In addition, it is supported by independent outer and middle markers (for systems utilizing an inner marker it would also be included in the support systems) and approach and threshold lighting systems.

For this system, it is assumed that failure of the localizer would result in total loss of approach functionality. If only the glideslope failed, non-precision localizer approach functionality would remain (requiring higher weather minimums for use). If any of the support systems failed, precision approach capability would remain with degraded support, probably requiring slightly higher weather minimums than with all systems functioning. (Since this particular model excludes two simultaneous failures as being of insignificantly low probability of occurrence, this logic diagram only requires that *all* support systems *not* be available to force the result into the degraded mode. If *all* support systems *are* available, full precision approach functionality is available.)

Figure 3-16. Instrument Landing System Reliability Model



This reliability model incorporates the ability to alter the repair strategy. If, for example, the glideslope were to fail, TRACON could elect to shut down the approach and have it repaired immediately, thereby taking the associated runway out of service in weather good enough for nonprecision approaches. Alternatively, they could continue to operate with the localizer only, delaying the repair until a future time when traffic could be expected to be lighter. This reliability model enables a user to select repair strategies for all components except the localizer.

Figure 3-17 is the state transition diagram for this model. While the model only allows for a single simultaneous failure, it enables the user to select repair strategies. It is assumed that the probability of two failures is sufficiently low to be insignificant. (Recognize, however, that two or more simultaneous failures could be accommodated by modeling the ILS as a system with more states than used here.)

When a failure occurs (in any subsystem other than the localizer) the strategy could be to repair it immediately or to delay initiation of the repair until a later time. In the first case, it is assumed that the entire approach system would have to be shut down while the repair was in process. In the second, the system could continue to operate with degraded functionality while awaiting start of the repair.

To accommodate the variable repair strategies two states are assigned to each failure (other than the localizer). These are "wait to start repair" and "start repair immediately." If the "wait" strategy is selected, then a mean wait time is introduced and an additional transition required before the repair can begin. If the "repair immediately" strategy is selected, the waiting state is skipped and the system goes directly into repair.

Figure 3-17. Instrument Landing System Transition Diagram

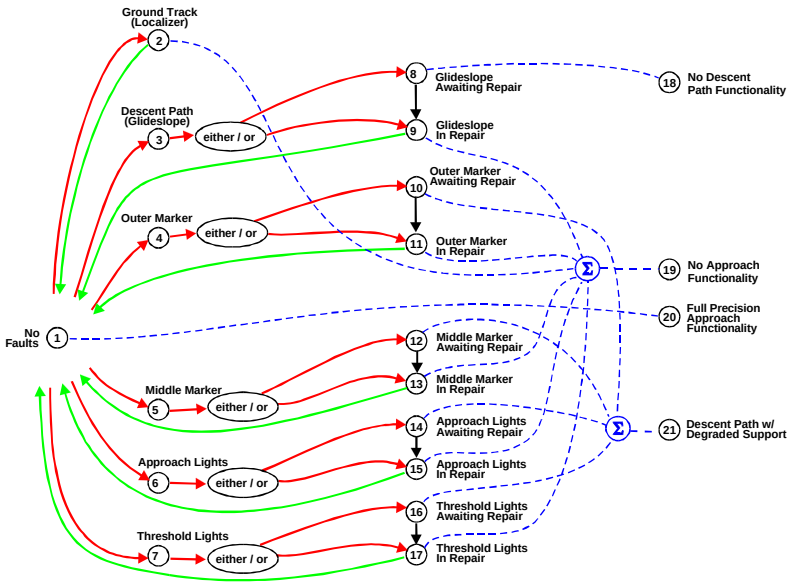


Figure 3-18 is the input/output interface for the ILS reliability model. In addition to the MTTF and MTTR inputs, the user has another set of inputs. He can select the repair strategy for each type of failure and, if "wait" is selected, enter the mean wait time (MWT). The output shows precision and nonprecision capabilities and breaks the precision capability down into fully supported or partially supported

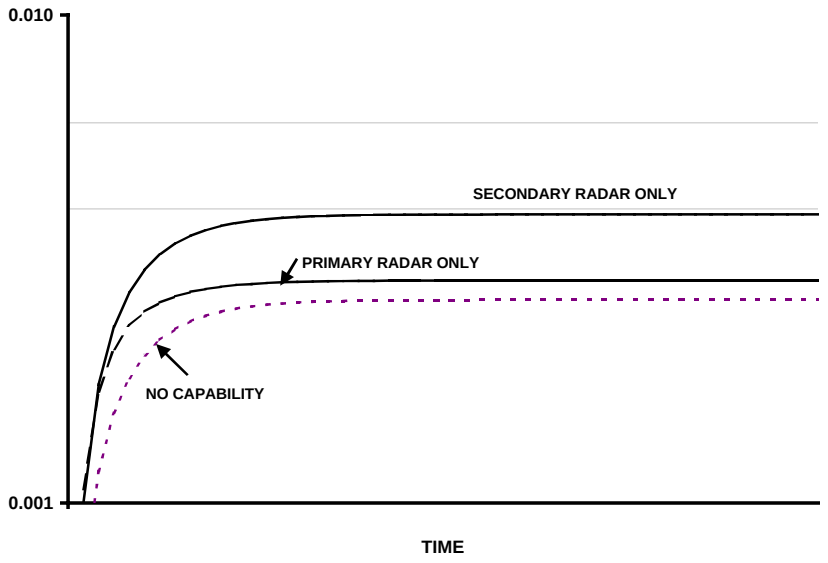
(meaning that one of the support systems—OM, MM, approach lights or threshold lights—has failed).

Figure 3-18. Input Output for Instrument Landing System Model

	INPUT Mean Time Between Failures MTBF in hours	INPUT Mean Time To Repair MTTR in hours	OUTPUT Functionality Probability State Vector		
Ground Track System (Localizer)	3000	4	Functionality		
Descent Path System (Glideslope)	2000	2	Precision Approach (incl. Glideslope)	Localizer Only	None
Outer Marker	2000	4	0.9925169	0.0063544	0.0011286
Middle Marker	2000	4			
Approach Lights	1000	2	Full Support	Degraded Support	
Threshold Lights	1000	2	0.8461599	0.1463570	
	ENTER 1 to Wait ENTER 2 to Repair	If Waiting ENTER Mean Wait Time MWT in hours			
Wait/Repair Glideslope	1	12			
Wait/Repair Outer Marker	1	48			
Wait/Repair Middle Marker	2	48			
Wait/Repair Approach Lights	1	72			
Wait/Repair Threshold Lights	1	72			

Figure 3-19 shows the dynamic response of the reliability model as it approaches steady state. The probability of having precision approach capability (with full or partial support) is shown here.

Figure 3-19. Probability of Failures Over Time

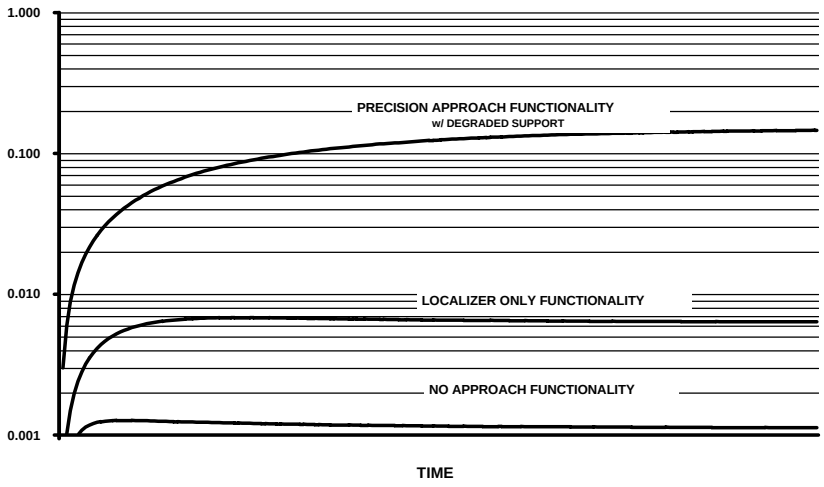


(Note that the transient behavior on this chart differs from that for the surveillance system. Here, the probability of full functionality drops to a low value, then

gradually increases to its steady-state value. This is because of the repair strategy. Because the glideslope and some of the support items are not repaired as soon as they fail, the system is actually in a lower state of functionality for a brief period while waiting for repairs to begin. Eventually, the repairs are made, however, and the final state of functionality is attained. By way of comparison, when the same MTBF and MTTR values were used with an immediate repair strategy for all components, the steady-state value of full functionality rises from 0.9925 to 0.9972, but the value of having some functionality, even nonprecision functionality, drops from 0.9988 to 0.9968. Presumably, the wait to repair strategy would be adopted because of the favorable trade-off of having at least some functionality during critical traffic situations rather than having full functionality at all times.)

Finally, Figure 3-20 shows the transient state probabilities for the other levels of system functionality: nonprecision functionality (i.e., no glideslope) and no approach functionality.

Figure 3-20. Probability of Degraded Capability Over Time



Impact

The Impact model shown in Figure 3-9 takes the unique and exhaustive listing of the failure configurations differentiated in the Reliability Model and provides, for each failure configuration, the input parameters to the TRACON simulation, which are determined by each failure configuration. To reduce the complexity, the states of the reliability model for each functional element defined in Tables 3-1 and 3-3 are each mapped to a limited number of operational states, which uniquely and exhaustively define the impact to the TRACON Simulation. Tables 3-4 and 3-5 present the operational states and impacts defined for the TRACON surveillance and airport approach facilities functions, respectively. Similar tables would need to be developed for each function in the system for a complete analysis.

Table 3-4. Terminal Radar Approach Control Surveillance Operational States

State of function	State definition	System impact	Simulation impact
Fulloperational	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 3-5. Airport Approach 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

Tables 3-4 and 3-5 both define four operational states for the TRACON surveillance function and the airport approach facilities function. Both include a fully operational state, which represents the state of the respective function when the systems that produce the function are performing as they were designed to, and a failed state, which represents the respective function when component fail failures prevent the function from being available. The operational states defined for both functions include two degraded states that will allow the safety implications of these degrade states to be explored. The system impact column in each table describes the impact each operational state will have on the TRACON system affecting safety. The simulation impact column indicates how inputs to the TRACON simulation are altered to account for the respective system impact.

TRACON Simulation

The TRACON simulation simulates aircraft flying through TRACON-controlled airspace, while calculating hazard metrics. The TRACON area simulated is based on the four corner posts at DFW in effect at the time of the CTAS field tests in 1996.

INPUT AND OUTPUT

The input to the simulation includes flight information for a specified time interval for each arriving aircraft in the scenario. It includes the plane 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. 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.
- Tower, includes runways.
- Controller
  - uses radar to determine location of airplanes;
  - tracks location of airplanes with respect to each other;
  - removes planes from airspace when land or crash;
  - 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.

HAZARD INDICATORS

The simulation evaluates hazard indicators for each aircraft at each time step. Hazard indicators for each aircraft can be output in two ways: (1) at each time step and (2) the worst violation. The hazard indicators include separation and workload metrics.

Separation metrics include

- absolute distance between each airplane in the airspace,
- in-trail separation distance between airplanes on common flight paths, and
- altitude separation between planes within the same cylinder of airspace.

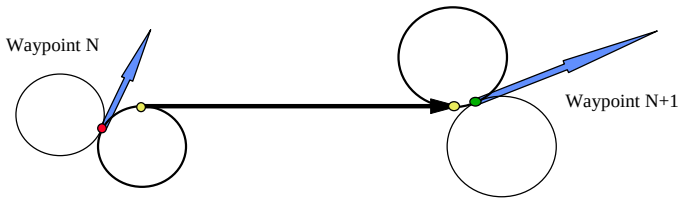
Workload metrics include

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

FLIGHT PATH BETWEEN WAYPOINTS

The airplanes fly between waypoints following simple trigonometry, as illustrated in Figure 3-21. Each waypoint includes the position, velocity, and heading constraints. The simulation determines the shortest path between waypoints while observing these constraints. The airplane can turn left or right with the given velocity and fixed turn rate. The airplane flies the tangent connecting the two closest circles. The airplane accelerates or decelerates between circles to arrive with desired velocity and then ascends or descends between circles to arrive with desired altitude.

Figure 3-21. Flight Path Between Waypoints



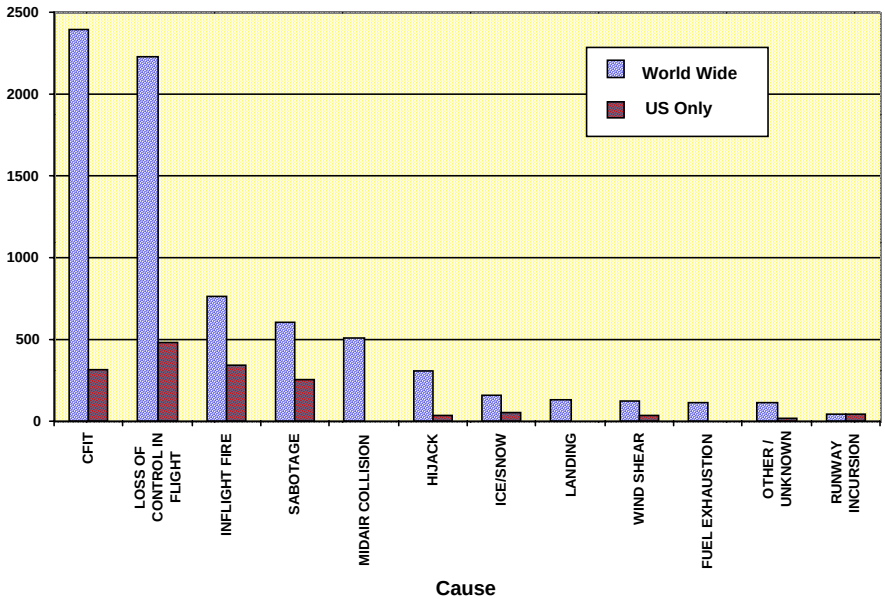
Safety Model

OBJECTIVE SAFETY DATA

Figure 3-22, derived from recently published data (*Aviation Week*, 8/18/97), shows worldwide and U.S. airline fatalities data for a 10-year period ending in 1996.[1] The data are for commercial jet transports over 60,000 pounds maximum gross weight and are categorized by type of accident. As can be seen, fatalities resulting from controlled flight into terrain (CFIT) are most common worldwide, with 25 percent of these occurring during approach. Several accident categories involve natural or human-caused failure of the aircraft in some form that cannot be prevented by either the pilot or controller (e.g., in-flight fire, sabotage and hijacking). These types of accidents are not directly pertinent to the analysis of P-FAST (although secondary effects, or hazards caused to other aircraft attributable to this type of accident, are of concern).

Categories that are directly applicable to the present task, however, include midair collisions, some instances of loss of control in flight, ice and snow, landing, wind shear, fuel exhaustion and runway incursion—collectively accounting for over 3,000 fatalities during the 10-year period. It is, primarily, these types of accidents that may be prevented, in part, by improved air traffic procedures such as those provided by P-FAST.

Figure 3-22. Worldwide and United States Airline Fatalities



[1]Data exclude the former USSR due to their unreliability.

SAFETY METHODOLOGY

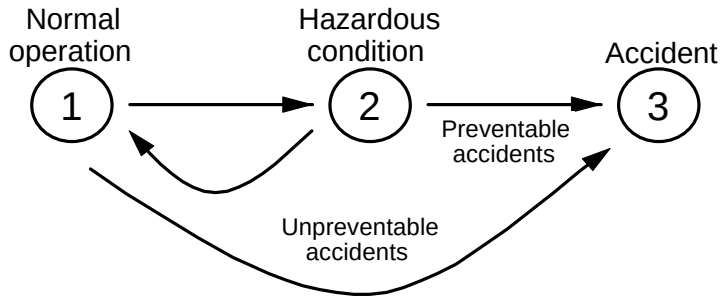
At least two approaches are available for predicting the likelihood of occurrence of accidents of the type mention above (1) explicit, based on dynamic modeling of aircraft flight trajectories and (2) inferential, based on modeling of generic causal situations. Our approach for this task has been the latter. Our simulation of air traffic arriving at a high-density TRACON, identifies "hazardous incidents" that could logically precede the types of accidents cited above and whose avoidance would preclude such accidents. While this approach does not predict actual accident probabilities, it does provide a direct measure of system safety appropriate to both the objectives and scope of this task.

Our simulation keeps track of a nominal position for each arriving aircraft. Because these positions are generated by kinematic rather than dynamic algorithms, the position data estimate, rather than simulate, true positions. This is appropriate for our methodology because, in reality, the only data available to either the pilot or the controller are estimates. Each acts to control the aircraft for which he is responsible by trying to adjust his estimate of its position to conform with some desired position. In each case, the individual's estimate of the position of the aircraft is based solely upon indirect evidence derived from navigation instruments, radar data, or verbal reports from each other or third parties. The notion that each has of where he or she wants the aircraft to be is likewise based on an indirect notion of true position. The pilot, for example, wants to reposition his aircraft, not to some specific point in space, but so as to cause an instrument indication on his panel to read a certain way. The controller, likewise, issues clearances to the pilot, not to move the aircraft to a specific point in space, but to cause one "volume" of reserved airspace to move toward a position where he can hand the aircraft over to the tower (or another controller) without having it conflict with other "volumes" or reserved airspace associated with other aircraft. The notion of position, for both pilot and controller, is an abstraction of the truth. They both believe that they are successfully carrying out their duties if their notions of desired position are met within acceptable limits–limits based on experience. If the navigation instruments give acceptable readings and if the "volumes" or reserved airspace seem to move in acceptable ways–based on experience–then both pilot and controller believe that the aircraft for which they are responsible is truly moving in a safe manner. In other words, they do not experience any "hazardous" incidents.

Whether or not hazardous conditions occur that do not result in accidents, but of which neither the pilot nor the controller are aware, is, to a certain extent, moot. On the other hand, preventable accidents can occur with apparent spontaneity—without either pilot or controller being aware of a preexisting hazardous condition. The types of accidents with which we are concerned in this study, however, can only occur from situations which, theoretically, given fully functioning support systems and error-free human performance, would be recognized as hazardous. We can, therefore, define, for the purposes of our analysis, the term "hazardous condition" as follows: "A hazardous condition is a state of the overall TRACON

system (which includes all hardware, software, aircraft, and people involved in primary TRACON operations) distinguishable from normal TRACON operations, which is necessary (but not sufficient) for the occurrence of a preventable accident." In Markovian terms, we can describe the overall system as being in one of three states: (1) normal; (2) hazardous or (3) accident (see Figure 3-23). For preventable accidents, the system *must* transition from state #1, to state #2, to state #3. Unpreventable accidents involve a transition directly from state #1 to state #3. Also, of course, state #2 can transition back to state #1 without the occurrence of an accident. This definition allows some latitude in defining the conditions that distinguish a "hazardous" condition from a "normal" condition. However, a preliminary distinction can be made based on experience and current FAA procedures.

Figure 3-23. TRACON Hazard States



At the present stage we have identified several preliminary "hazardous conditions". These include

- aircraft operating too close together in trail;
- aircraft at different altitudes crossing with insufficient vertical separation;
- any aircraft getting too close to other aircraft in flight; and
- aircraft getting too close to the ground before transitioning to the landing phase of flight.

The potential accidents to which these conditions can lead are

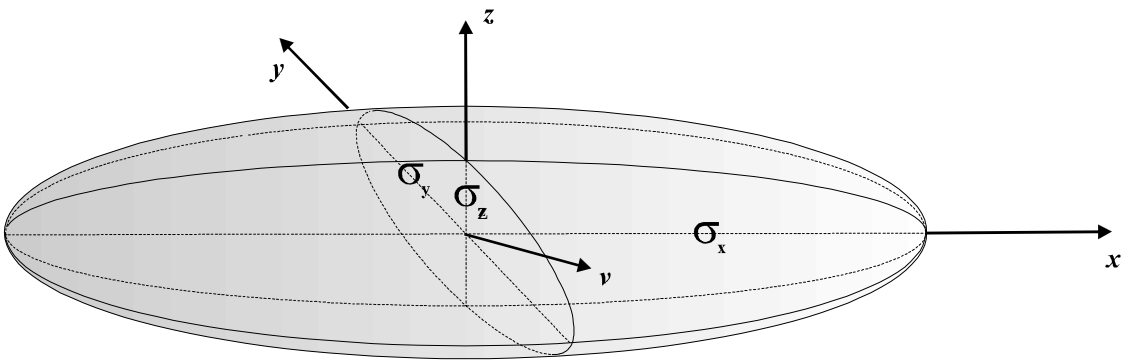
- loss of control due to wake turbulence;
- midair collision; and
- CFIT.

We developed a probabilistic approach to identifying hazardous incidents in our model, although this was not used in developing the earlier results, because we did not have time to acquire the data necessary to support the approach.

Centered on the current position of each aircraft, a 3-dimensional normal probability distribution is defined by keeping track of its σ_x, σ_y, and σ_z values as the orthogonal axes of (ellipsoid [see Figure 3-24]).

The coordinates of this ellipsoid are maintained in alignment with the aircraft, σ_x and σ_y in the horizontal plane, while σ_z is vertical. The values of these σs, or standard deviations, are based upon the concepts described above. They represent the values relative to the nominal aircraft position in the simulation (which, as noted above, only approximates its true position) within which the presence of a "potentially hazardous object" would create a hazardous incident. This "potentially hazardous object" could be another aircraft, the wake of another aircraft, or the ground. The magnitude of the σs depends upon the flight conditions of the aircraft with respect to independent position-fixing sources. Thus, the σ_z value for an aircraft on an ILS glidepath or using a radar altimeter (within radar altimeter range of the ground) would be smaller than it would be with no source of altitude information other than its barometric altimeter. Whenever the aircraft is able to obtain a relatively accurate independent position fix, the σ_x, and σ_y values would be reduced to represent the accuracy of that fix (plus safety margin) but would, thereafter, grow steadily until another position fix could be obtained.

Figure 3-24. Aircraft Position Uncertainty Ellipsoid



To determine if a hazardous incident has occurred, it is possible to calculate metrics based upon the (values, e.g., the number of standard deviations by which the nominal in-trail separation between the two aircraft exceeds the minimum safe value. This number could be compared with some predefined minimum required threshold and, if exceeded, causes a "hazardous condition" flag to be set. Similar

calculations could be made to determine if vertical separation at crossing or absolute proximity are dangerously low, or by comparing σ_z with actual altitude above the ground, to determine the potential CFIT hazard.

$$N_{H_{i,j}} = \frac{s_{i,j} - s_{\min}}{\sqrt{\sigma_{x_i}^2 + \sigma_{x_j}^2}} \qquad \text{[Eq. 3-1]}$$

Using the similar criteria, many other potential hazards could be flagged. For example, suppose an aircraft is close to touching down on its designated landing runway. If the aircraft's altitude were low compared with σ_z, one might declare a potential for a hazardous undershoot. Likewise, if the altitude were too large, an overshoot condition might exist. Conflict on the runway with a previous landing that might not have cleared the runway would be indicated by both aircraft having values that might indicate that one landed late while the next landed early. These, and other hazard indicators could be added to future versions of the simulation.

For the current study, we used a deterministic hazard indicator, in-trail separation, and a deterministic controller workload metric, standard deviation of arrival aircraft (across arrival runways) to demonstrate the methodology.

SAFETY MODEL

The safety model takes hazard indicators from the simulation and produces a system safety metric (Figure 3-25).

Figure 3-25. Safety Model

The safety model could be developed at different levels of fidelity. In the next section, the hazard indicator presented is the percentage of aircraft violating minimum in-trail separation standards. The safety model could be a statistical model, based on historical records of accidents that occur when in-trail separation standards were violated. Or, it could be a high-fidelity physical model based on wake vortex transport, aircraft dynamics, etc. The overall system safety statistic can be calculated as shown in Figure 3-26. Figure 3-27 shows ETMS arrivals into DFW.

Figure 3-26. System Safety Statistic

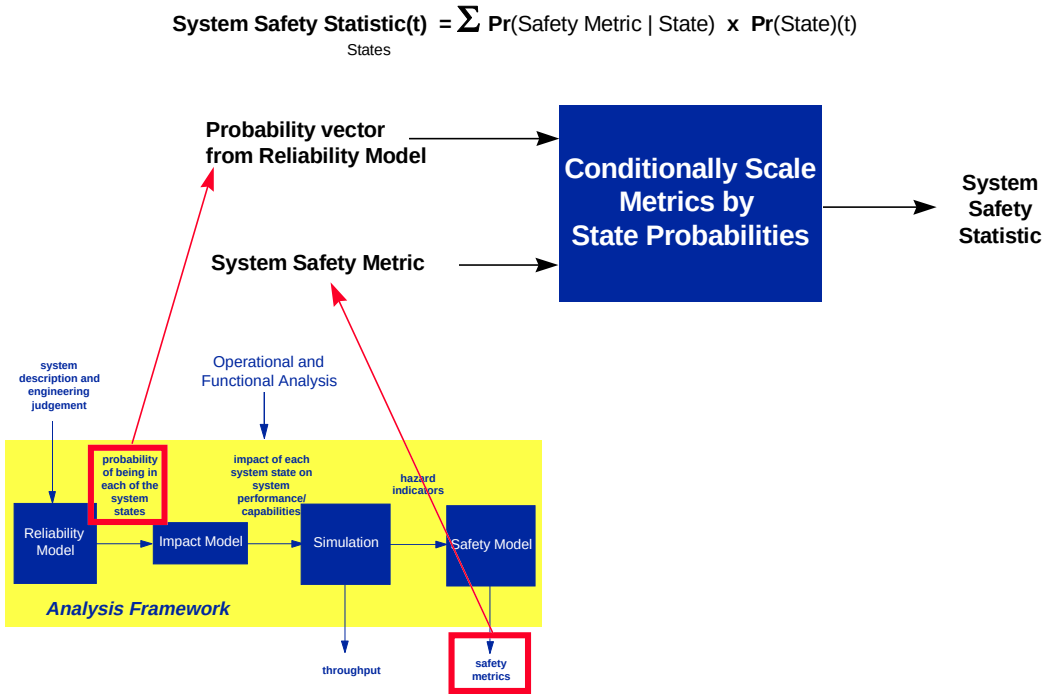
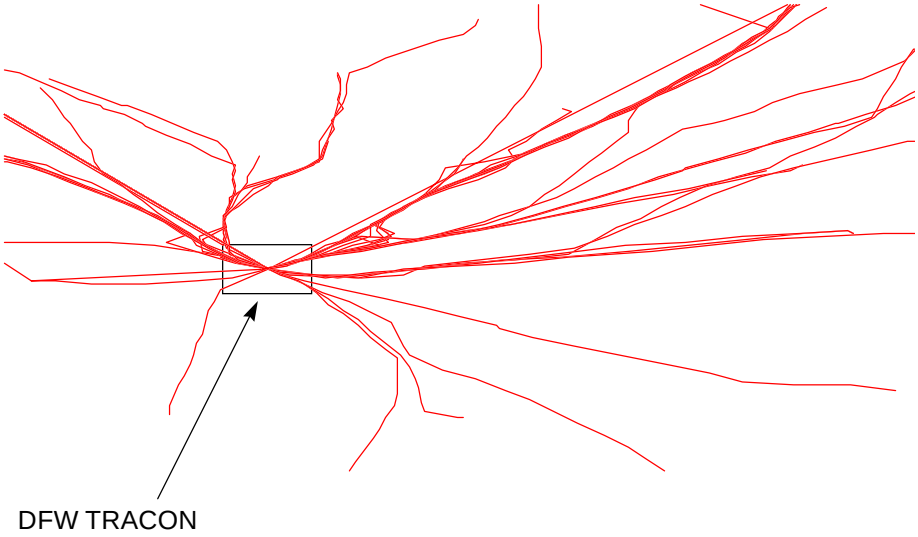


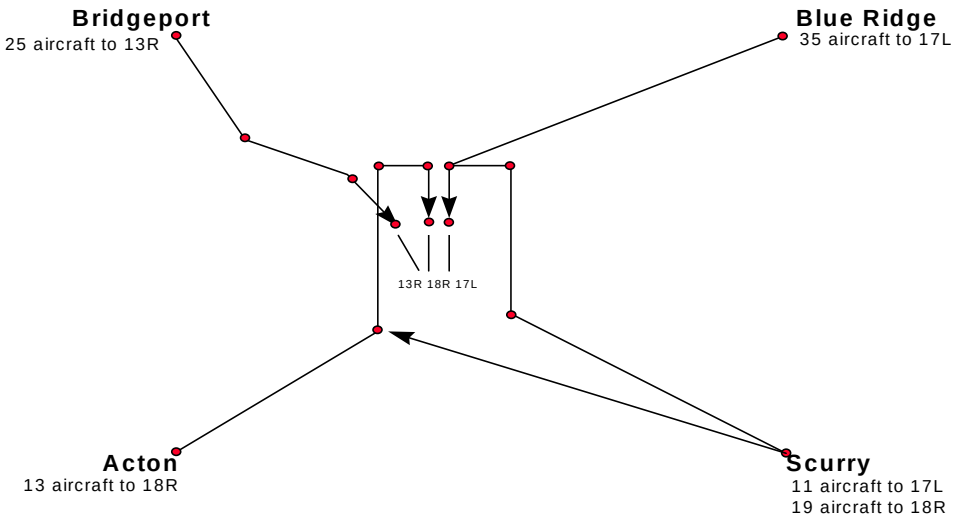
Figure 3-27. ETMS Data—Arrivals into DFW 14:00-15:00, April 6, 1996



Case 1: Baseline Without P-FAST

Figure 3-28 displays the simulated flight paths in TRACON airspace used in Case 1. Four cases of a scenario were run using the TRACON simulation program. The basic scenario is an 80-minute period that 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 2 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]

Figure 3-28. Baseline Without P-FAST Flight Paths



The simulated arrival pattern at the corner posts was derived from the OAG and ETMS flight data (see Figure 3-27) into DFW. Flight paths were taken from data gathered at a site visit to DFW TRACON on August 27, 1997. We present one of the hazard indicators (percentage of aircraft violating minimum in-trail separation standards of 2.5 nautical miles) generated by the TRACON simulation program. In addition, based on discussions with controllers, the standard deviation of the number of aircraft arriving on each runway is calculated as a controller workload met-

[2]The four corner posts defined for all of our cases are the corner posts 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.

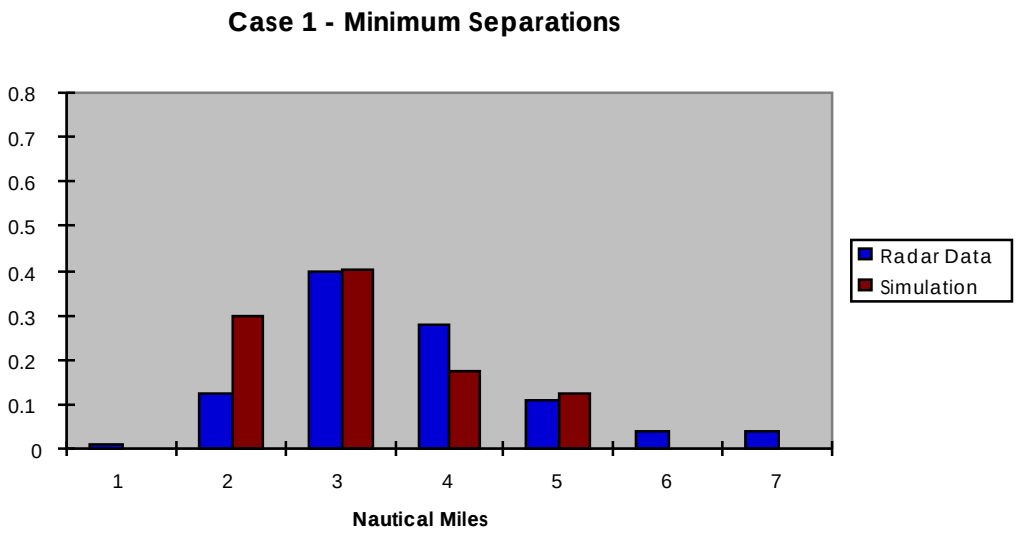
[3]The three arrivals runways are defined as the original three runways used during the testing of P-FAST during 1996. In 1997, a fourth arrival runway was added. Runway 17L was renamed 17C and a new runway was named 17L.

ric. That is, if the runways are balanced so that the same number of aircraft land on each runway, then the controller workload is less than if the runways are not balanced when there is not an equal number landing on each runway.

A total of 97 aircraft landed in the scenario. The distribution of arrivals on runways was 25 aircraft to runway 13R, 28 aircraft to runway 18R, and 44 aircraft to runway 17L.

In Figure 3-29, we see the aircraft in-trail minimum separation distances displayed in nautical miles. These are compared with the distribution from radar data.[4] The results show approximately 40 percent of the aircraft had a minimum separation of 3.0 to 4.0 nautical miles. Six percent of the separations were less than 2.5 nautical miles in both the radar data distribution and the simulated case.

Figure 3-29. Baseline Without P-FAST Minimum Separations

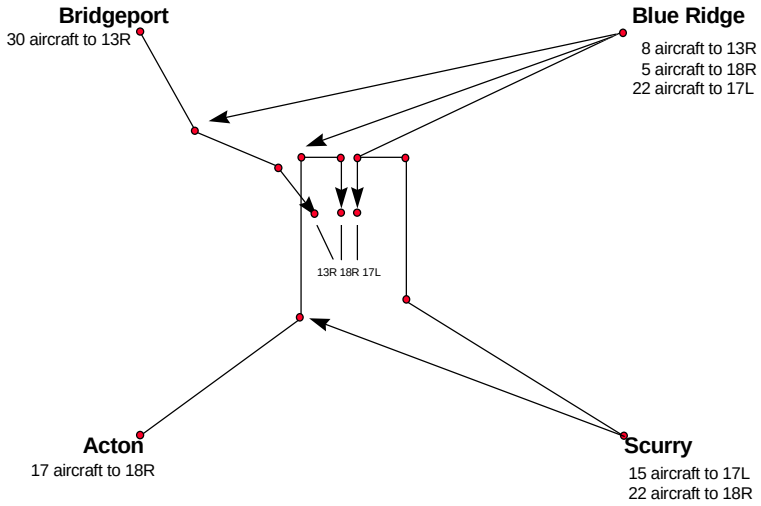


Case 2: Baseline with P-FAST

The second baseline case is similar to Case 1, above, except that P-FAST is now in use. Figure 3-30 displays the flight paths used for the simulation.

[4] The distribution from radar data was obtained from: "An Analysis of Landing Rates and Separations at the Dallas/Fort Worth International Airport," July, 1996, by Mark Ballin and Heinz Erzberger.

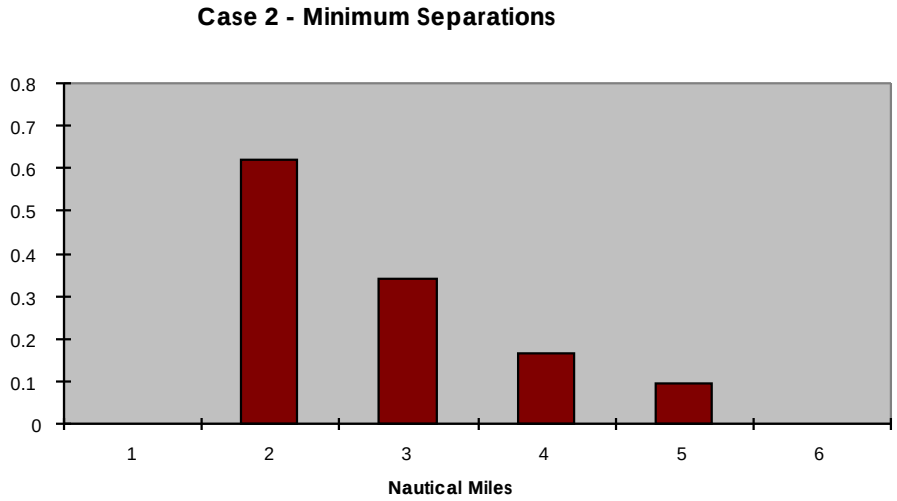
Figure 3-30. Baseline With P-FAST Flight Paths



For the baseline with P-FAST case, 112 aircraft landed. There was a rather even distribution of aircraft over the three runways (13R, 18R, and 17L) of 38, 37, and 37 aircraft landing, respectively.

Figure 3-31 shows the distribution of minimum in-trail separations. Five percent of the separations were less than 2.5 nautical miles.

Figure 3-31. Baseline with P-FAST Minimum In-Trail Separations



Case 3: Runway Outage Without P-FAST

For the third case, runway 13R becomes unavailable 20 minutes into the scenario. This could result from ILS failure when aircraft are operating under IFR or if the

runway was blocked by aircraft mechanical problems, among other causes. Remaining aircraft within the TRACON airspace that were scheduled to land on runway 13R must now execute a missed approach and be revectored to one of the two remaining runways, 18R, using the flight paths illustrated in Figure 3-32. The remaining aircraft scheduled to land on runway 13R must be resequenced by controllers to one of the two remaining runways available for landing.

Figure 3-32. Runway Outage: Flight Paths Without P-FAST

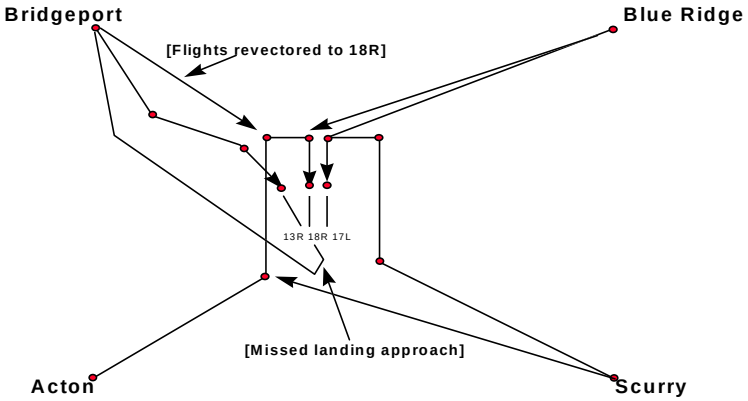
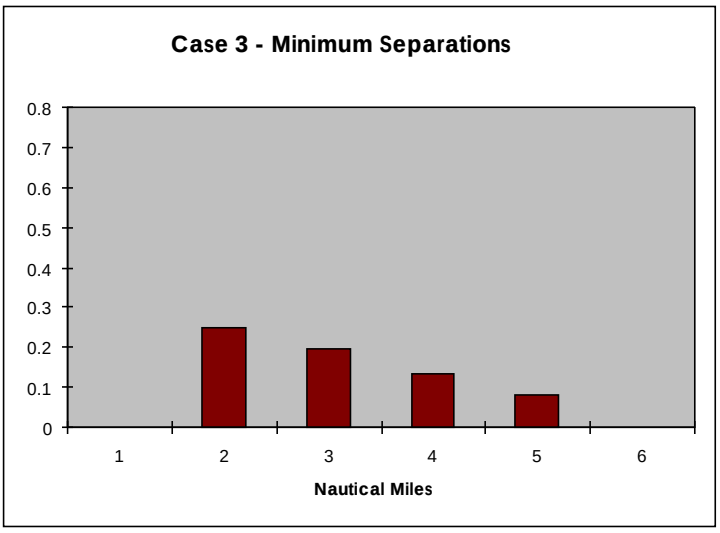


Figure 3-33 shows the minimum in-trail separation distribution. Fourteen percent of the separations were less than 2.5 nautical miles due to the complexity of the re-sequencing controllers performed in compensating for the loss of a runway.

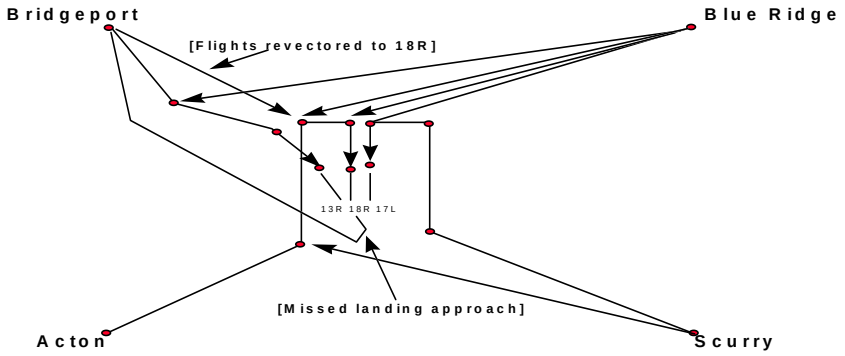
Figure 3-33. Runway Outage: Without P-FAST Minimum In-Trail Separations



Case 4: Runway Outage with P-FAST

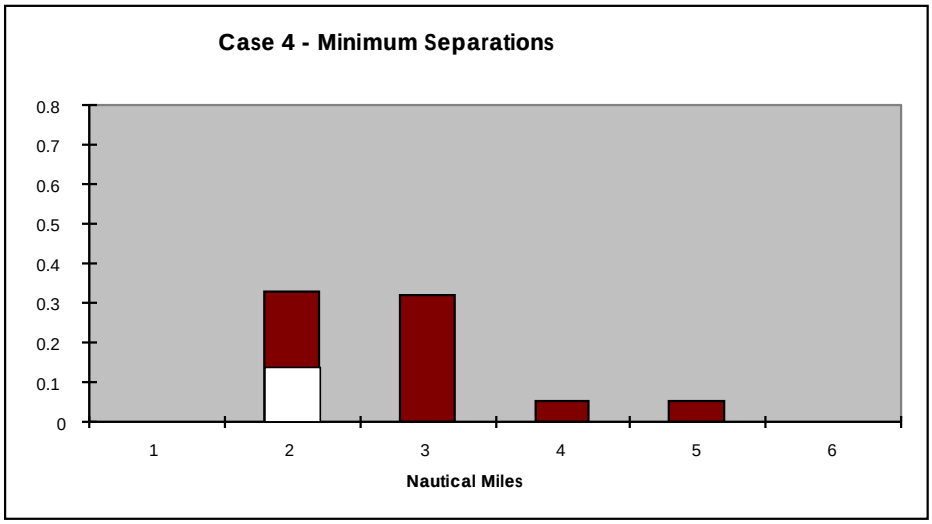
Case 4 is similar to Case 3 except that P-FAST is in use; hence, more aircraft are in the TRACON airspace. Figure 3-34 displays the flight paths used for this case.

Figure 3-34. Runway Outage: Flight Paths with P-FAST



In this case, 76 aircraft landed, with a decrease from Case 2 due to the loss of a runway and revectoring of aircraft in flight. Only 6 aircraft could land on runway 13R prior to the outage, with 37 aircraft landing on runway 18R, and 33 aircraft landing on 17L. Figure 3-35 shows the minimum in-trail separation distribution. Fourteen percent of the separations were less than 2.5 nautical miles due to the complexity of the re-sequencing controllers performed in compensating for the loss of a runway.

Figure 3-35. Runway Outage: Minimum Separations with P-FAST



Results Summary

As can be seen in Table 3-6 the results showed that in comparing two baseline cases, more aircraft 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.

Table 3-6. Summary of Results

Cases	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

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 hazard indicator presented is that of minimum in-trail separation. The percentage of aircraft with less than 2.5 nautical mile in-trail separation is the same with and without P-FAST.

Conclusion

The overall implication of the results is that P-FAST does not increase the likelihood of a specific hazardous condition, but it does reduce controller workload, thus decreasing the likelihood of a hazardous condition resulting from controller overload.

Chapter 4
Application of Safety Methodology to National Airspace System

In addition to the P-FAST analysis presented in this report, the essential elements of the safety methodology presented here also were previously applied to safety analyses of independent approaches to parallel runways, rail traffic flow control safety issues, and *Space Station Freedom*. This wide range of applications is evidence of the capability to use this methodology for analyzing other air traffic systems and the National Airspace System (NAS) as a whole.

The particular features of the methodology that make it a valuable tool are analytical flexibility and ability to model hierarchical systems.

Analytical flexibility is provided by the Impact Model concept. In the Impact Model, the states of the subsystems are defined in terms of their operational impact on the larger system. For hardware systems, some type of reliability analysis can be used to evaluate the probability of being in the fully operational or some degraded state. The specific technique used does not affect the Impact Model, and the best technique for each subsystem can be chosen independently. For systems where there is a human in the loop, the probability associated with the human's performance state must be generated by expert judgment or a human factors model.

In order to capture the effects of complex interactions among subsystems and their varying states of performance, a modelling technique more sophisticated than traditional reliability analysis may be required. This is the Response-Interaction Model. In our approach, we use a simulation model to capture these interactions; however, the framework is general, and any modelling technique may be used. It is quite possible to simulate some systems, while analyzing others with a deterministic technique.

A Response-Interaction simulation analysis can capitalize on the Impact Model state probabilities previously determined. Rather than run a full simulation of the system, a time-consuming process, the simulation can be constructed to introduce degraded states and see their impact. While such a simulation would not capture the long-run likelihood of such a failure occurring, in our approach this is not necessary, because the outcome of the simulation can be weighted by the previously determined Impact Model state probabilities to obtain the required likelihood.

For analysis of a system in isolation, the Response-Interaction model results, weighted by the probability of state occurrence, will provide the hazard factor

probabilities needed to compute a safety metric. For analysis of a system that is itself a component of a larger system, the weighted Response-Interaction model results can be used to determine the state probabilities for the Impact Model relating this system to the whole under consideration.

It is the generality of the Impact Model concept that allows our method to be used fruitfully in a hierarchical analysis. The Impact Model specifies how a subsystem performs in relation to the whole. The analysis of the whole can be built up from detailed analyses of the subsystems comprising that whole; each subsystem in turn has an Impact Model relating its components. Alternatively, the analysis approach may be from the whole to the components. Interaction-Response models of the state interactions among the gross-level subsystems may be used to identify those subsystems whose performance is most critical in the overall system's performance. The next stage of analysis would be to consider those subsystems in detail, by utilizing their Impact Models and Interaction-Response Models to determine the critical aspects at a finer level.

The system considered by our methodology can have components, described by Impact Models, that are as gross as TRACON's and ARTCC's, or as fine as hardware components of an electrical system.

Although the method offers great promise for hierarchical analysis, we must caution that it does not offer a turnkey solution to NAS safety analysis. Determination of appropriate system interactions is a task that requires strong engineering judgment. The N^2 system interaction diagrams are of great assistance in codifying this knowledge.

References

[1] G. A. Hocker and S. E. Kolitz, Airport Demand and Capacity Modeling for Flow Management Analysis; CSDL-T-1200; The Charles Stark Draper Laboratory, Inc.; Cambridge, Massachusetts; January 1994.

[2] M. T. Pozesky and M. K. Mann; "The U. S. Air Traffic Control System Architecture," Proceedings of the IEEE; Vol. 77, No. 11; November 1989; pp. 1605-1617.

[3] D. R. Isaacson, T. J. Davis, and J. E. Robinson III; "Knowledge-Based Runway Assignment for Arrival Aircraft in the Terminal Area," AIAA Guidance, Navigation, and Control Conference; New Orleans, LA; August 11-13, 1997.

[4] M. G. Ballin and H. Erzberger; An Analysis of Landing Rates and Separations at the Dallas/Fort Worth International Airport; NASA Technical Memorandum 110397; NASA Ames Research Center; Moffett Field, California; July 1996.

[5] Design and Operational Evaluation of the Traffic Management Advisor at the Fort Worth Air Route Traffic Control Center, Harry Swenson, Ty Hoang, Shawn Engelland, etc., presented at the 1st USA/Europe Air Traffic Management Research and Development Seminar at Saclay, France, June 17-20, 1997.

[6] Conflict Detection and Resolution In the Presence of Prediction Error. Heinz Erzberger, Russell Paielli, Douglas Isaacson, Michelle Eshow NASA Ames Research Center, Moffett Field, CA, presented at the 1st USA/Europe Air Traffic Management Research and Development Seminar at Saclay, France, June 17-20, 1997.

[7] Summary Overview and Status of AATT Program Development Activities (Draft), Mark Ballin, Richard Coppenbarger, and David Schleicher NASA Ames Research Center, Moffett Field, CA, May 27, 1997.

[8] Reduced Aircraft Separation Risk Assessment Model (RASRAM) Description, Rick Cassell, Roger Shepherd, Rajeev Thapa, and Derrick Lee, Rannoch Corporation, Feb. 24, 1997.

[9] Center/TRACON Automation System Passive Final Approach Spacing Tool (FAST) Assessment - Final Report, Crown Communications, Inc., Dec. 5, 1996.

[10] Center TRACON Automation System Build 2 System Specification, February 14, 1997.

[11] DFW 7110.65 Traffic Control Procedures, October 10, 1996.

[12] *An Analysis of Landing Rates and Separations at the Dallas-Fort Wort International Airport*, Mark Ballin and Heinz Erzberger
NASA Ames Research Center, Moffett Field, CA
NASA Technical Memorandum 110397 -July 1996.

[13] Reduced Aircraft Separation on Final - Approach - A Review of Separation Risk Models (Draft Report), Roger Shepherd, Rick Cassell, and Edwin Alphonso, Rannoch Corporation, June 5,1995.

[14] Conversion of the TRACON Operations Concepts Database Into a Formal Sentence Outline Job Task Taxonomy - Final Report, Mark Rodgers, Gena Drechsler, May 1995.

[15] Operational Test Results of the Passive Final Approach Spacing Tool, IFAC Symposium, T. Davis, D. Isaacson, J Robinson III, W. den Braven, K. Lee, and B. Sanford, June 1997.

[16] Conversion of the TRACON Operations Concepts Database Into a Formal Sentence Outline Job Task Taxonomy - Final Report, Mark Rodgers, Gena Drechsler, May 1995.

[17] *Reduced Aircraft Separation on Final - Approach - A Review of Separation Risk Models (Draft Report)*, Roger Shepherd, Rick Cassell, and Edwin Alphonso, Rannoch Corporation, June 5, 1996.

[18] *An Analysis of Landing Rates and Separations at the Dallas/Fort Worth International Airport*, Mark Ballin and Heinz Erzberger,
NASA Ames Research Center, Moffett Field, CA.
NASA Technical Memorandum 110397 -July 1996.

[19] DFW 7110.65 Traffic Control Procedures, October 10, 1996.

[20] Center/TRACON Automation System Passive Final Approach Spacing Tool (FAST) Assessment - Final Report, Crown Communications, Inc., December 5, 1996.

[21] Center TRACON Automation System Build 2 System Specification, February 14, 1997.

[22] Reduced Aircraft Separation Risk Assessment Model (RASRAM) Description, Rick Cassell, Roger Shepherd, Rajeev Thapa, and Derrick Lee, Rannoch Corporation, February 24, 1997.

[23] Summary Overview and Status of AATT Program Development Activities (Draft), Mark Ballin, Richard Coppenbarger, and David Schleicher, NASA Ames Research Center, Moffett Field, CA, May 27, 1997.

[24] Design and Operational Evaluation of the Traffic Management Advisor at the Fort Worth Air Route Traffic Control Center, Harry Swenson, Ty Hoang, Shawn Engelland, etc., presented at the 1st USA/Europe Air Traffic Management Research and Development Seminar at Saclay, France, June 17-20, 1997.

[25] Conflict Detection and Resolution In the Presence of Prediction Error, Heinz Erzberger, Russell Paielli, Douglas Isaacson, Michelle Eshow, NASA Ames Research Center, Moffett Field, CA. presented at the 1st USA/Europe Air Traffic Management Research and Development Seminar at Saclay, France, June 17-20, 1997.

Appendix A
Maps

[1] VFR Terminal Area Chart Dallas-Fort Worth, 49th edition, March 27, 1997.

[2] IFR Area Chart - Dallas-Fort Worth, July 17, 1997.

[3] IFR Enroute Low Altitude Chart - Dallas-Fort Worth, July 17, 1997.

Appendix B
Abbreviations

AATT	Advanced Air Transportation Technologies
ARTCC	Air Route Traffic Control Center
ASAC	Aviation Systems Analysis Capability
AST	Advanced Subsonic Technology
ATM	Air Traffic Management
CFIT	controlled flight into terrain
CTAS	Center-TRACON Automation System
DFW	Dallas-Fort Worth International Airport
ETMS	Enhanced Traffic Management System
FAA	Federal Aeronautics Administration
FAST	Final Approach Spacing Tool
IAPR	independent approaches on parallel runways
IFR	Instrument Flight Rules
ILS	Instrument Landing System
MIT	Massachusetts Institute of Technology
MM	middle marker
MTBF	mean time between failures
MTTF	mean time to failure
MTTR	mean time to repair
MWT	mean wait time
NAS	National Airspace System
NASA	National Aeronautics and Space Administration
OAG	Official Airline Guide
OM	outer marker
P-FAST	Passive Final Approach Spacing Tool
STAR	Standard Terminal Arrival Route
TRACON	Terminal Radar Approach Control
VFR	Visual Flight Rules
VORTAC	VOR/Tactical Air Navigation

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (*Leave blank*)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	May 1998	Contractor Report

4. TITLE AND SUBTITLE
A Method for Evaluating the Safety Impacts of Air Traffic Automation

5. FUNDING NUMBERS
C NAS2-14361
Task 97-11

WU 538-08-11-01

6. AUTHOR(S)
Peter Kostiuk, Gerald Shapiro, Dave Hanson, Stephan Kolitz, Frank Leong, Gene Rosch and Charles Bonesteel

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Logistics Management Institute
2000 Corporate Ridge
McLean, VA 22102-7805

8. PERFORMING ORGANIZATION REPORT NUMBER
NS711S1

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
Langley Research Center
Hampton, VA 23681-0001

10. SPONSORING / MONITORING AGENCY REPORT NUMBER
NASA/CR-1998-207673

11. SUPPLEMENTARY NOTES
Langley Technical Monitor: Robert E. Yackovetsky - Final Report
P. Kostiuk, G. Shapiro (LMI); D. Hanson, S. Kolitz, F. Leong, and G. Rosch (Draper Lab.); and C. Bonesteel (Chava Group)

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Unclassified - Unlimited

Subject Category 01 Distribution: Nonstandard

Avialability: NASA CASI (301) 621-0390

12b. DISTRIBUTION CODE

13. ABSTRACT (*Maximum 200 words*)

This report describes a methodology for analyzing the safety and operational impacts of emerging air traffic technologies. The approach integrates traditional reliability models of the system infrastructure with models that analyze the environment within which the system operates, and models of how the system responds to different scenarios. Products of the analysis include safety measures such as predicted incident rates, predicted accident statistics, and false alarm rates; and operational availability data. The report demonstrates the methodology with an analysis of the operation of the Center-TRACON Automation System at Dallas-Fort Worth International Airport.

14. SUBJECT TERMS
aviation safety, reliability analysis, operational availability analysis

15. NUMBER OF PAGES
74

16. PRICE CODE
04

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	Unlimited