CSDL-R-2098
(Rev. 1)

SAFETY ANALYSIS OF THE ATCS

by

William W. Weinstein
Andrei L. Schor

April 1990

The Charles Stark Draper Laboratory, Inc.
555 Technology Square
Cambridge, Massachusetts 02139

CSDL-R-2098
(Rev. 1)

SAFETY ANALYSIS OF THE ATCS

by

William W. Weinstein
Andrei L. Schor

April 1990

The Charles Stark Draper Laboratory, Inc.
555 Technology Square
Cambridge, Massachusetts 02139

CSDL – R – 2098

SAFETY ANALYSIS OF THE ATCS

by

William W. Weinstein

Andrei L. Schor

Original release: October 1988

Revised: April 1990

The Charles Stark Draper Laboratory, Inc.

Cambridge, Massachusetts 02139

TABLE OF CONTENTS

1 Introduction

There are two reasons to model Advanced Train Control System (ATCS) safety. The first is to provide a general sense of how well the ATCS performs, from the viewpoint of safety, with respect to the current signalling and control systems. The second is to examine the relative contribution to the overall accident rate of the various elements of the ATCS. This knowledge provides the ATCS designers with the ability to apply resources where they will do the most good.

In the spring of 1987 the ATCS organization contracted with the Charles Stark Draper Laboratory (CSDL) to develop a model for the safety of railroad operation under the ATCS. CSDL had previously conducted such an analysis for the Advanced Railroad Electronics System (ARES), and as a result of this prior effort had developed techniques for reducing the model of a railroad operating region to a problem of tractable dimension. Since ATCS and ARES address the same control problem and happen to share structural similarities, these techniques could be applied to ATCS as well. In order to address the specific needs of the ATCS organization, significant enhancements were made to the modeling approach. The result was a spreadsheet-based model that provides improved modeling precision, allows a great deal of flexibility in specifying the characteristics of the operating region being modelled and provides a detailed breakdown of how well the ATCS addresses the hazards that produce accidents under current control system operation.

1.1 Goals of the Analysis

There are two objectives of this modeling effort: (1) to compare the safety of operation under ATCS Level 30 with the safety of operation under the various train control systems currently in use, and (2) to determine the relative contribution of the various ATCS elements to the overall accident rate under ATCS Level 30 operation.

Accident rate over an operating region is used as a safety measure because a region is the smallest entity that comprises a complete control system for ATCS[1], and because it is the smallest entity for which accident statistics are currently kept. In order to provide an apples-to-apples comparison of control system safety, one must compare the current accident rate for a *particular* region with the predicted accident rate for that *same* region operated under ATCS.

It suffices to model relative and not absolute accident rate. Human errors must be an input to any ATCS accident model (and, in fact, turn out to be the prime cause of accidents in both ATCS and conventional systems). The most objective value of human error rate is the measurable result of human errors, namely human-caused accidents under current control systems operation. Because human error rate in an ATCS model is derived from

[1] Under some conventional control and signalling systems, dispatchers work essentially independent of each other off of separate boards. ATCS cannot be broken down that finely because all dispatcher stations in an ATCS Central Dispatch Center share a common computer system.

current system accident statistics, any ATCS accident rate prediction is necessarily relative to current system operation.[1] A prediction of the actual accident rate for a particular region operated under ATCS is easily derived.

The relative contribution to the ATCS accident rate by failures of the various hardware elements indicates which of those elements drive the unreliability of the system. This provides a metric by which the system designers can determine where reliability or coverage[2] improvements are most needed. Balancing the reliability of the various system elements provides the best use of system resources.

1.2 Methodology

The basic approach to modeling ATCS accident rate is to generate reliability and availability models for the different types of hardware elements in an ATCS region. The reliability models address those situations of undetected hardware failures that can lead directly to an accident without operator participation. The availability models address those situations of detected failures where some trains in the ATCS region are operating in a mode without automatic authority enforcement and are therefore subject to the possibility of operator error. Human error transitions are spliced onto the availability models, and the results of all the models are combined to generate a prediction of regional accident rate.

The reliability and availability models are generated using Markov modeling techniques. The models are generated by first developing a failure modes and effects analysis at the appropriate level of modularization of hardware elements. This level of modularization is determined by examining the ATCS architecture and operating philosophy.

The model employs certain approximations in order to make it computationally tractable. In all cases these approximations are chosen to be conservative from the safety point of view, thus the model will tend to predict a higher ATCS accident rate than may actually be the case. Over the range of meaningful input values (i.e., the regional complement of hardware elements and human operators, and the various hardware failure and repair rates) the errors are insignificant. In order to facilitate easy and meaningful application to a variety of different ATCS configurations by ATCS personnel, the model has been designed to produce reasonable results even for extreme configurations, hardware failure rates and repair times.

---

[1] It is assumed that the probability of critical human error per operator per unit time will be essentially unchanged in the ATCS environment. This is not an unreasonable assumption, since exposure to human errors under ATCS will be seen to occur in just those cases where, due to ATCS equipment failure, certain operations between dispatchers and engineers will be conducted in a backup mode, via voice radio dispatching techniques, much as they are now.

[2] A measure of the fail–safeness of the system.

Two approaches are taken. The first develops an aggregate human error rate from the current system accident statistics and applies it to the combined Markov chains. The second reverses the process by breaking down the current accident statistics by hazard and scaling each of them by the output of the appropriate Markov chain.

1.3 Summary of the Results

Since the model developed is a tool for use by anyone implementing ATCS, the analysis did not use current accident data from any specific railroad. Instead, it was tested for correct logical operation and then executed for three distinctly different scenarios, using as inputs conservative hardware failure rates, mean times-to-repair and three significantly different current accident groups. As expected, the ATCS Level 30 shows a significant improvement in safety over current control systems. The level of improvement depends chiefly upon the distribution of current accidents by cause, and which of those cause categories are included under the scope of "current control system related accidents".

A qualitative understanding of why ATCS improves safety can be gained by understanding that human error is the overwhelming cause of current control system related accidents. Human errors are covered by the ATCS Level 30 enforcement mechanisms except when ATCS hardware has failed, or when operating under joint authority where there is no enforcement *among the entities operating jointly*. Generally, the lack of a fully functioning, fully vital complement of ATCS equipment to support a particular dispatcher / engineer / wayside unit scenario will result in the use of a voice radio backup control mode for that particular situation. This results in an exposure to two human error sources for the duration of the localized backup mode operation. The analysis shows that this residual exposure to human error under these backup cases is a small fraction of the total exposure to human error under current control system operation. Thus, this major source or accidents is greatly reduced under ATCS.

There is no quantitative analysis of the risk associated with undetected system logic or firmware failures, just as accidents due to hardware failures of the current system are not analyzed. The exhaustive technical analysis of the ATCS system logic and the development of engineering tools to control the implementation of the system logic will serve to reduce the risk of this as an accident cause.

The value of the improvement factor will vary depending upon the current accident rates. Improvements of as much as two orders of magnitude are not unreasonable. Caution must be exercised in using these improvement factors as absolute numbers because of the link to railroad specific current accident causes. Also, the improvement factor does not provide a clear picture of the absolute improvement in the number of accidents. For this analysis, the accident causes were evaluated individually, which clearly shows where the greatest absolute improvement can be gained.

Both the requisite hardware reliabilities and coverage values are comfortably achievable with available hardware components and proven fault-tolerant electronic design techniques. However, since the predicted ATCS accident rate exhibits a first order sensitivity to the coverage of vital hardware elements, adequate coverage must be obtained by the use of fault-tolerant design techniques, in order to assure that the necessary level of coverage has actually been attained.

1.4 Organization of the Report

Section 2 presents a brief overview of the relevant aspects of the ATCS architecture and operation.

Section 3 provides an introduction to Markov analysis and discusses the issue of model decomposition.

Section 4 describes the application of Markov techniques to the ATCS problem and develops the ATCS model.

Section 5 discusses application of the model and interpretation of the outputs.

The Appendix presents the details of the Excel spreadsheet implementation, including the specific formulas that are used and a description of the accident hazard categorization.

2 Overview of the ATCS

This section presents a cursory overview of the ATCS. It addresses those characteristics and features of the ATCS that provide the basis for safety modeling. In actuality, the system is much more complex than this, but the plethora of possible failure modes map into a limited set of effects in a reasonably straightforward manner.

2.1 Architecture and Operation

The ATCS is a system for centrally controlling the movement of trains, and for effecting positive, enforceable separation between trains, in a fail-safe manner[1]. To do this, it provides:

- A means of communicating data among a central dispatch facility, trains, wayside devices and track forces
- Accurate train location information
- A means of generating conflict-free movement authorities and track occupancy permits
- A means of positively enforcing movement authorities
- The ability to detect hardware failures and data transmission errors in a manner that prevents corrupted information from being unknowingly employed by the system, thus possibly resulting in an accident.

Figure 2.1 depicts the interrelationships of the various ATCS elements described in the ATCS system specification. A baseline central dispatching facility consisting of a Central Data Computer (CDC), a Front-End Communications Processor (FEP) and a Cluster Controller (CC) communicates over a groundline and microwave network to Base Stations in the field. These Base Stations consist of a Base Station Controller (BSC) and a Base Radio (BR) and are located so as to provide radio coverage of the appropriate sections of track.

Trains and track forces communicate with the CDC via the base stations. They each consist of a Mobile Radio (MR) a Communications Management Unit (CMU), and some version of a keyboard/display. In addition, trains have an On-board Computer (OBC), an interrogator unit for obtaining location fixes from embedded track transponders, and tachometers for extrapolating train location between transponder fixes.

[1]The engineer still controls the operation of the train, but the ATCS prevents him from exceeding speed and position limitations.

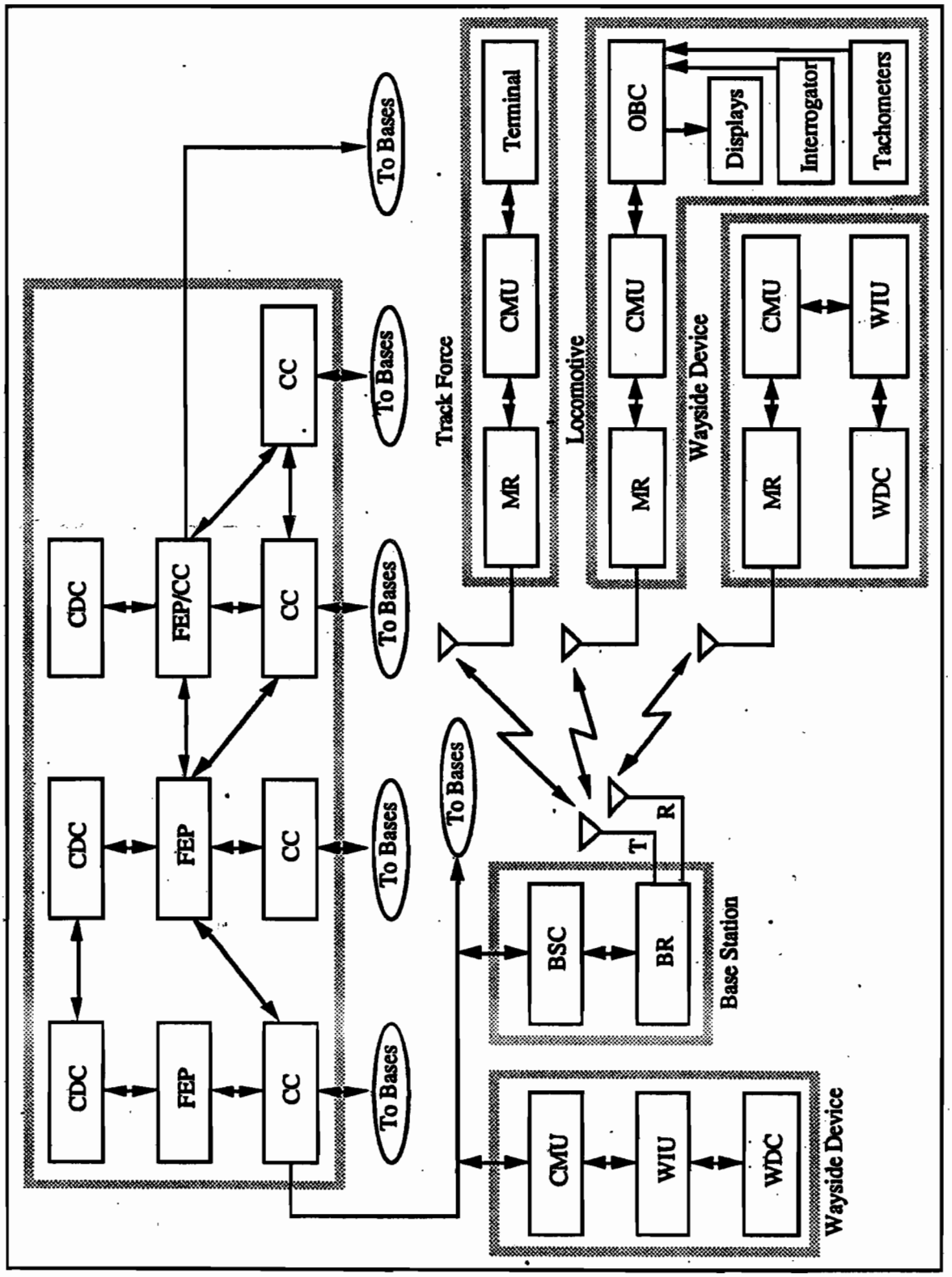

Figure 2.1 Organization of ATCS Elements

Wayside units provide the ATCS interface to trackside sensors and switches. They consist of a Communications Management Unit (CMU), a Wayside Interface Unit and a set of device-specific Wayside Device Controllers (WDC). A wayside unit may be directly connected to the network or it may interface via a base station, in which case it also contains a radio[1].

The major ATCS elements (central dispatch facility, communications network, trains, track forces and wayside devices) provide the aforementioned capabilities in the following ways.

Communications

At its core, ATCS provides a digital communications environment for the exchange of data among trains, trackside devices and a central dispatch facility. Figure 2.2 depicts the data flow among these ATCS elements. The following categories of information are exchanged:

Status

- Status information from trains, which includes: train position, speed and the health of all on-board systems
- Status information from trackside devices, which includes switch position information; sensor information from devices such as hot box detectors, slide fences and track circuits; and the health of all such trackside devices
- Status of track force activities

Movement and Track Occupancy Authorization

- Movement authorities from the central dispatch center to trains
- Track occupancy authorities from the central dispatch center to track forces
- "Proceed through" clearances from track forces to trains[2]

Commands to Wayside Devices

- Position commands to powered switches, drawbridges, etc.

---

[1] This radio is configured as a mobile radio if the wayside device is within base station radio coverage and therefore talking to a base station. It is configured as a base radio when the wayside device is out of radio coverage and therefore communicates directly with trains (which all have mobile configured radios).

[2] This may take the form of track force status to the central dispatch center followed by a movement authority to the train.

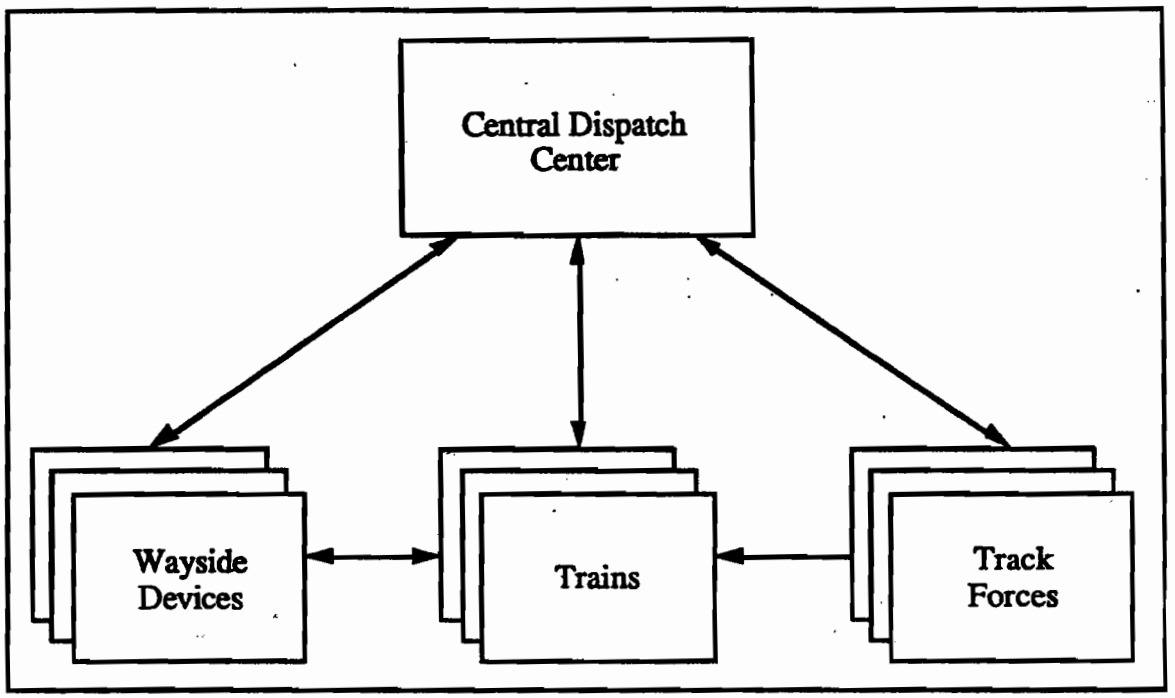

Figure 2.2 Data Communication Among ATCS Elements

Train Location

This information is determined on-board the train. Train location fixes are obtained when the train passes over transponders located between the rails. Location between transponders is extrapolated by dead reckoning (integrating train speed obtained from the tachometers, or directly from an odometer package, depending on the implementation). The transponders are spaced so that the dead reckoning error should never exceed a specified amount. Transponders are also placed on all three branches of switches, so that positive feedback is obtained about which branch the train takes.

Authority Generation and Conflict Resolution

The central dispatch facility houses the train dispatchers. When a dispatcher enters a new request for a movement authority, the system determines whether that authority can be issued based upon the current positions of all the trains and all other currently active movement authorities.

Authority Enforcement

The On-Board Computer is programmed to apply braking automatically, if necessary, so as to keep the speed and position of the train within the envelope of the current authority limits. The enforcement is predictive, based upon the current train speed, upcoming track profile, speed limits over that profile and authority limits for the train.

Failure Detection

The system is designed so that those elements that generate or consume vital information are themselves vital. These elements are the Central Dispatch Computer (CDC) which performs conflict checking and forwards authorities to the trains, the On-Board Computer (OBC) on the train which generates train location data and performs enforcement, and the Wayside Interface Unit (WIU) which monitors switch positions and the status of the track. The vitality of data transmissions is provided by two layers of error detection coding, one applied and decoded within vital elements, and the second applied on top of the already encoded data by the data transmission hardware.

2.2 ATCS Safety Considerations

The ATCS achieves safety by (1) checking that all movement authorities are conflict-free (2) by positive enforcement of those movement authorities to cover any operating errors made by an engineer, and (3) by preventing corrupted or otherwise improper information from propagating to the point where it can adversely affect train operation. These things are accomplished with a combination of vital hardware and special operating procedures called control flows.

The control flows are a set of protocols for managing train movement and for communicating information among the CDC, the trains and the WIUs. Protocols are provided for such actions as issuing a movement authority, approaching a switch, etc. These protocols allow the status of relevant items (e.g., switch position) to be verified before any action is taken (e.g., the train commits itself to traverse the switch).

Vital hardware, in the context of ATCS, is hardware whose failure must be detectable by the system with a sufficiently high probability within a defined time frame. This does not mean that the hardware must never fail, or even that it must be particularly reliable. But the system must have *accurate and timely knowledge of whether a particular piece of hardware is working properly* so that it does not act upon false information.

When contrasted with the current control systems in use, the salient characteristics of the ATCS emerge. (1) When all of the ATCS hardware is operational, it covers most of the human errors that currently result in accidents. (2) When selected items of ATCS hardware are not working (and are known not to be working), the system is exposed to those possible human errors which that hardware was supposed to cover. (3) The ATCS introduces new hardware items not found in the current control systems. If one of these items fails undetected, then it could lead to an accident. In fact, the analysis conservatively assumes that an accident will always result in this case.

The analysis will show that for hardware of moderate reliability configured to employ proven failure detection methods, far more human errors are prevented by ATCS operation that are introduced by undetected hardware failure modes.

3 MODELING METHODOLOGY

3.1 Need for Safety Modeling

In this report, the terms reliability and safety will be used more or less interchangeably, since the aspects of system reliability being investigated here are exactly those that impact the safe operation of the system. Establishing that a complex, highly reliable system satisfies certain reliability requirements raises an interesting dilemma. On the one hand, since such a system is designed so as to experience only very infrequent failures, a prohibitively long testing period would be required, making the traditional approach of prototype testing clearly not feasible. Constructing many copies of the system and testing them for a shorter time is not a practical solution either, due to cost limitations. On the other hand, since the system reliability corresponds directly to its safety, then measures of the system safety should be obtained before operational testing of the system can be permitted.

ATCS is a large and complex system. In common with other modern control system designed for safety-critical applications, it addresses the problem of achieving high reliability at the system level by employing an appropriate configuration of redundant components which themselves need only be moderately reliable. The reliability (hence the safety) of such a system can be assessed by the application of mathematical reliability modeling techniques. ATCS components (radios, computers, sensors, etc.) are such that their failure rates can be determined by measurement.[1] These rates serve as inputs to an analytical model, which is based on architectural structure and operational rules, to obtain the overall accident rate for ATCS. Specifically, the analytical model employs information about the system architecture (how the system's components are interconnected), system operating mode descriptions (what equipment and abilities are needed for the system to be operational in its various modes), and the redundancy management approach (how component failures are detected and identified, and how the system is reconfigured to accommodate these failures).

3.2 Selection of an Analytical Reliability Modeling Technique

The analytic approaches to quantifying system reliability fall into three classes: Monte Carlo simulations, combinatorial methods and Markov models. The strengths and weaknesses of these three approaches are briefly described in this subsection.

Simulation can be used to determine reliability by generating failure and repair events at times distributed according to the component failure and repair rates. These simulations are repeated until statistically significant reliability measures are accumulated. A major strength of the simulation approach is its ability to analyze very complicated repair and

[1] The error rate of the human operators, which are components of the train control system, is also obtained by empirical observation, i.e., statistical data about human caused accidents.

reconfiguration scenarios, with relatively little knowledge required beyond a description of the system to be analyzed. However, a key difficulty of this method is that for highly reliable systems the failure rate is so low that, in order to accumulate a statistically meaningful number of events, a very large number of simulations must be run. While there are means (collectively known as variance reduction techniques) of increasing the efficiency of the basic method, the underlying difficulty remains a drawback.

Historically, *combinatorial reliability models* have been widely used. Fault-tree analysis , for example, has become a standard analytical method for reliability prediction in a wide variety of applications. This analytical technique statistically combines component failure probabilities, based on the system architecture and redundancy management approach, to determine the system reliability. Since there is no explicit simulation of system operation, the combinatorial technique avoids the deficiencies of the Monte Carlo simulation. There are, however, three limitations to this approach. First, the fault tree is constructed to predict the probability of the system being in a *particular* operating condition (for example, a working condition or a failed condition). If it is desired to investigate the probability of being in other conditions, such as a variety of different operating modes, then new fault trees have to be constructed. Secondly, it is difficult to include events that have order dependencies, such as repairs and explicit modeling of reconfiguration strategies. Even in simple systems, there are often sequence dependencies which are quite subtle. Finally, the nature of the combinatorial analysis requires that 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 validate.

More recently, *Markov modeling* techniques have been increasingly used for reliability prediction. These techniques have also been used successfully to aid in the design of fault-tolerant systems. A Markov reliability model calculates the probability of the system being in various states as a function of time. A state in the model 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 transitions rates which reflect component failure and repair rates and redundancy management performance. Each components in the model's state vector represents the time-dependent probability of being in a specific state. Since the Markov model traces the evolution of state probabilities based on the above mentioned transition rates, it is not explicitly simulating the system and therefore does not have the deficiencies associated with the Monte Carlo technique. The Markov model is cast into a system of differential equations. Sequence dependencies, such as repairs and redundancy management decisions, are included naturally. Furthermore, the differential nature of the model means that it is not necessary to generate *explicitly* all possible combinations of events that can occur over the time period in question; rather, it is only necessary to model events that can occur during an infinitesimal time step. Of course, there are also some drawbacks to this method. First, the state space grows exponentially with the number of components. However, techniques have been developed to render this problem tractable in many situations of interest. Second,

treatment of complex mission scenarios and repair strategies, although possible, are generally cumbersome.

It should be emphasized that the reliability of a system does not depend on the analytical method used to evaluate it, as long as any approximations and simplifications are consistently applied or interpreted.

The Markov modeling technique has been selected to examine the safety (reliability) of ATCS. ATCS is a complex system comprising thousands of components, undergoing failures and repairs. The repair strategy however is quite simple, at least under the (very reasonable) assumptions described later in the report. Moreover, even though the number of components is large, there are only a few distinct types of components, i.e., there is a high degree of replication, which will be seen to play a key role in solving the state space proliferation problem. An additional important aspect of the required analysis is the need to model the entire system only in a steady state mode. Indeed the size and the inherent dynamics of this system combine to settle it rapidly into a time-invariant behavior. For a system with these characteristics, Monte Carlo simulations are ruled out due to their inefficiency. The combinatorial approach is not easily used either, because of the system's large size and the existence of sequence dependencies such as repairs. However it will be seen that some combinatorial aspects are used to cast our model in a very efficient form, taking advantage of the basic independence of the subsystems involved. The methodology described in this report indicates that indeed the Markov modeling technique is particularly suited to the problem under consideration.

3.3 Overview of ATCS Modeling Techniques

The key difficulty in using Markov models is the problem of state proliferation. In fact, appropriate means must be found to reduce the state space or the Markov model will be intractable even for moderately sized systems. Further, an appropriate model must be found for the humans which are integral elements of the system.

As an example of the problem of state proliferation, consider a system composed of 20 components. To model all (sequence independent) failure combinations requires 2^{20} (approximately 10^{6}) states. However, 10^{12} states are needed to model a system with 40 components. Hence, the number of states grows exponentially with the number of components. A brute force generation of an exact Markov model for an ATCS control region, with its approximately 1000 components, is clearly an intractable problem.

Two techniques are used to alleviate this state space explosion. First, it is noted that in many cases failures of different component types do not interact in such a way as to cause an accident. Thus, there are certain sets of equipment whose interactions in the safety analysis are easily understood. The failure of a switch does not impact the failure of any locomotive equipment, for example. This permits the analysis of switch failures and repairs and their impact on system safety independently of the investigation of the impact of

locomotive equipment failures. The result is a set of essentially independent Markov models for each set of components, the outputs of which are merged using a combinatorial technique.

The second technique applied to reduce the state space deals with the problems associated with the submodels. For example, the submodel for the switches may have hundreds of switches to keep track of. If all switches are assumed to fail in such a way as to have the same impact on safety, then there is no need to distinguish among the individuals. This property is known as symmetry. The resulting model has one state for "no switches failed", one state for "one switch failed", one state for "two switches failed", etc. However, this still results in a model with hundreds of states, an undesirable situation when a numerical solution is envisaged. In general, this aspect is dealt with by noting that clearly some states are more likely than others. For example, the state where all switches are failed is very unlikely, as is the state where all but one have failed. Due to its flexibility, Markov modeling permits focusing on the failure modes that have significant impacts on the solution. Essentially, one can construct a model containing significantly fewer states, but practically retaining the accuracy of the complete model, by not considering negligable contributions.This technique is called model truncation.

We mention the latter technique only for completeness and generality in discussing the repertoire at our disposal. In this analysis, however, we have been able to circumvent altogether the need to truncate the model This became possible because we have been successful in obtaining analytical solutions to the models, therefore removing the large actual number of states as an issue.

Thus, a large, complex system such as ATCS can be modeled using Markov techniques. The state space size is controlled through a "hybrid" approach that permits the separate solution of a set of submodels that are then combinatorially merged and the use of symmetry to drastically reduce the size of the submodels.

3.4 The Modeling Process

The process of generating a reliability or safety prediction for a system can be divided into three steps. First, the system needs to be investigated. The goal is to discover how the system operates and what are its critical aspects. This step results in a system description. Second, the impact of failures is explored. This step is often called a failure modes and effects analysis (FMEA). During this step the accident modes of the system are delineated. Third, the Markov model is constructed. Information on system operation from step one is used to guide modeling decisions such as the proper representation for the human elements. The model is a systematic representation of the FMEA from step two.

The actual process of generating a model requires information on: architecture, component characteristics, operational requirements and reconfiguration procedures. The system architecture provides information such as what components exist and how they are

connected, both physically and logically. The model also needs various component characteristics, such as failure and repair rates. The operational requirements provide a definition of what equipment or abilities are needed to achieve an operational state. There may be several operational modes, such as full ATCS or radio blocking rules. Further, these various modes may coexist at various locations within the system simultaneously. The reconfiguration procedures are the actions taken when a failure occurs so that system operation remains in the most desirable mode.

The notion of system reconfiguration is implicit in a redundant system. Having a redundant element for backup purposes is of no use if the system cannot detect the failure of the primary element, locate which element has failed, and take proper action to provide the system with access to the backup. All of this must take place in a time period such that system operation is not critically affected. If this process of fault detection, identification, and reconfiguration (FDIR) occurs in an acceptable time period, the component fault has been "covered". Thus, the performance of the system FDIR—the fraction of each component's faults that can be covered—must be included in the system model. Sometimes these coverage values are known; often they must be calculated using a Markov model to explore the performance of the FDIR process. A coverage model of the dualized vital elements of ATCS, such as the CDC and WIU, will be presented in the Section 4.

A variety of information can be obtained from the ATCS safety model. The main result is a prediction of the overall accident rate that can be expected when ATCS is put into operation over a given operating region. This value can be compared to the present measured accident rate for the region to determine the relative safety of ATCS. The model provides information about which components of the system contribute the most to the accident rate. This allows efforts directed towards the improvement of hardware reliability to be focused where they will be most beneficial. The model also indicates when certain operational decisions impact safety (such as whether to continue operation in a backup mode, or to wait until the primary mode hardware has been fixed). Finally, sensitivity analyses indicate how different modeling assumptions and uncertainties in inputs to the model affect the results.

3.5 Introduction to the Markov Modeling Method

3.5.1 Background

Markov modeling techniques provide a systematic means of investigating system reliability and safety for large, complex systems. They permit the inclusion of sequence dependent events such as repairs in a natural fashion. One of the most powerful aspects of Markov models is their ability to permit simplifying approximations to be made and to provide means to obtain bounds on these approximations. The basic concepts of Markov modeling are introduced via simple, but representative examples. These examples clearly point out the general flexibility as well as the main drawback of the method, particularly the rapidly proliferating state space. Two powerful techniques used to reduce the state

space to manageable proportions, without compromising the quality of the analysis, are then described.

3.5.2 Single-Component System

Figure 3.1a shows a single-component system. The first step in modeling the reliability of this system is to determine what is required for the system to be in an operational state. This single-component system has a trivial operational requirement: it is operational if the single component, A, has not failed. (Conversely, the system is failed if component A has failed). While this step is simple for this system, it is often one of the most complicated steps in modeling a complex system, characterized by many operational states and subtle interactions among components.

Given the system operational requirements, the next step is to construct Markov model states. A *state* represents a unique configuration of failed and operational elements, sometimes distinguished by the sequence of the failures that led to it. Figure 3.1b shows the Markov model for the one-element system. In general, a model is generated by first creating state 1, the state where there are no failed components in the system. The various transitions out of state 1 represent failures of the system components, accounted for individually or in groups. In this case there is only one component, thus a transition denoted a is created leading to state 2. This state represents this system when component A is failed. Noting the operational requirements for this system, state 2 is labeled as a system failure. Since there is only one component in the system and its failure has been accounted for, the Markov model is complete.

This system's reliability is just the probability, as a function of time, of being in state 1. Actually, there is a probability associated with each state. For example, at time zero the probability of being in state 1 (no failures) is 1 (or 100%) and the probability of being in state 2, or any other state, is 0. Parameter a on the transition in the model not only indicates that component A has failed along this transition, but that the component's failure rate is a failures per hour. Throughout our discussion, it will be assumed that all failure rates are constant in time. To obtain the system reliability as well as other state probabilities of interest as a function of time, we need to track the probability "flowing" out of state 1 into state 2. Probability flow is the product of the transition rate and the state probability for the state at the origin of the transition. Thus, a state with zero probability has no probability flowing out of it, a state with no exiting transitions has no flow out, and a state with probability equal to 1 and an exiting transition rate of a has an instantaneous flow out equal to a. The rate of change of each probability is then given by the net probability flow into the corresponding state. A Markov model is thus mathematically described by a set of differential equations governing the evolution in time of the probabilities of being in each state.

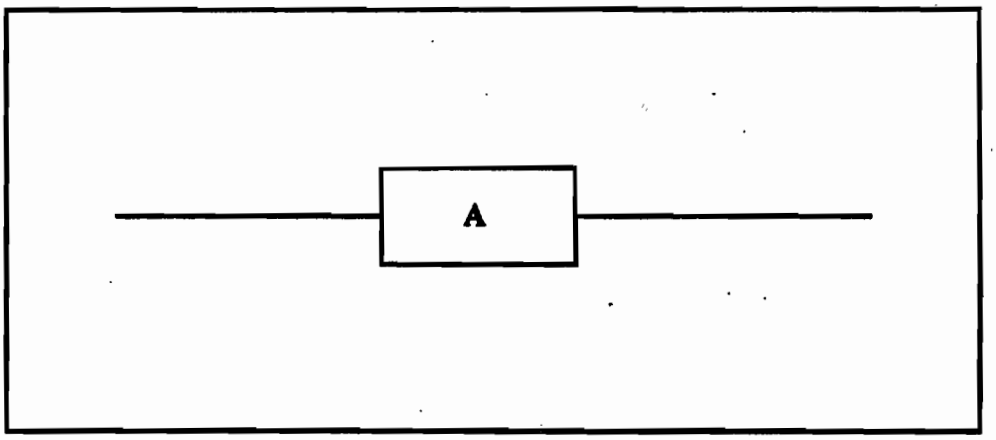

Figure 3.1a Single-Component System Block Diagram

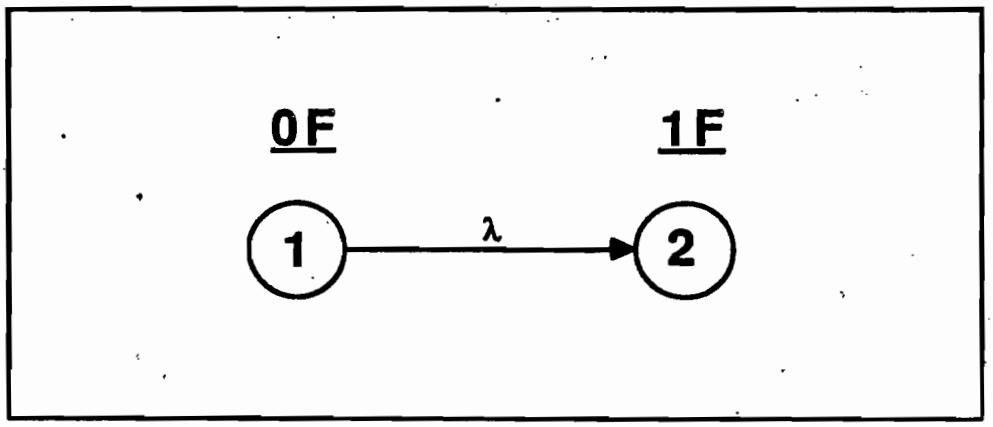

Figure 3.1b Single-Component System Markov Model

Using the definition of the probability flows, the following equations are obtained for the Markov model shown in Figure 3.1a:

$$dP_1(t) / dt = -\lambda P_1(t) \quad (1)$$

$$dP_2(t) / dt = \lambda P_1(t) \quad (2)$$

These equations, representing the rate of changes in each state variable (P_1 and P_2), are called state equations. Equation (1) shows that the rate of change in probability for state 1 is the exiting transition rate λ times the probability of being in state 1. The minus sign indicates that the transition is out of the state and, therefore, reduces the probability of being in state 1. Equation (2) is interpreted similarly. Note that the flow is *into* state 2; the positive term indicates an entering transition which increases the probability in state 2. Also, the flow into state 2 is the rate λ times the probability of *state 1*; the flow on this transition is due to state 1, the origin of the transition. Equations (1) and (2), along with the initial condition of the state probabilities, $P_1(0) = 1$ and $P_2(0) = 0$, provide a complete description of the system's reliability. Markov models have the property that a flow leaving one state enters another, as shown in Equations (1) and (2). Hence, the total system probability does not change as the system evolves. This property is called conservation of probability.

There are many ways of solving Equations (1) and (2) in closed form, such as standard integration or Laplace transform. Using any convenient technique and recalling that the failure rate λ is constant, yields the following solution:

$$P_1(t) = e^{-\lambda t} \quad (3)$$

$$P_2(t) = 1 - e^{-\lambda t} \quad (4)$$

State 1 starts with a probability of 1 and decays exponentially toward 0, while state 2 has a probability initially at 0 which grows toward 1. Notice that the sum of the two state probabilities is 1 at all times, thus indicating the conservation of probability.

3.5.3 Two-Component System with Repairs

Figure 3.2a shows a two-component system where the components are connected in parallel. The requirement for system operation is that at least one of the two components is working. These components can be repaired when they are failed.

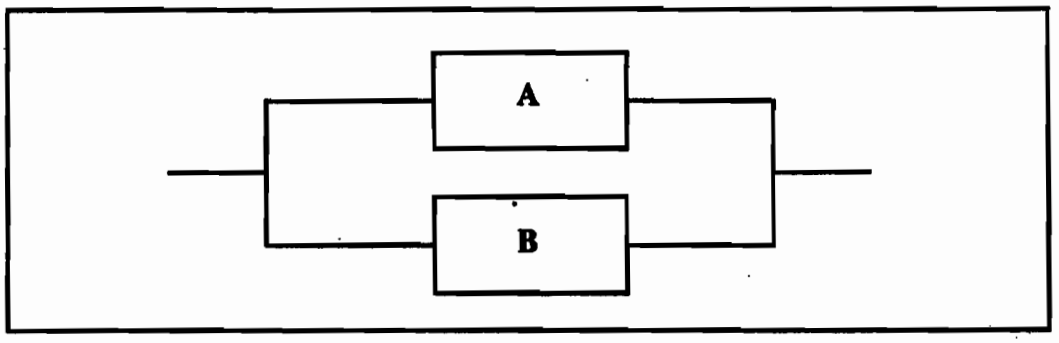

Figure 3.2a Two-Component System Block Diagram

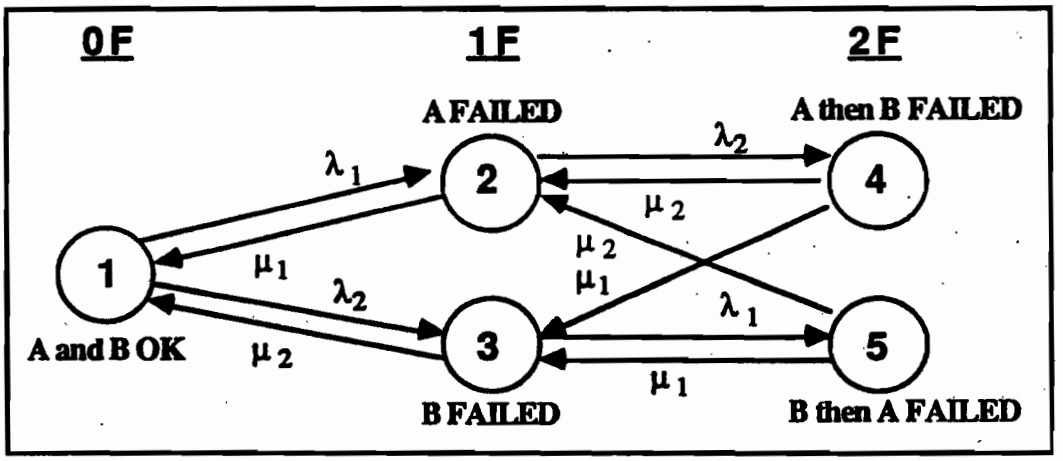

Figure 3.2b Two-Component System Markov Model

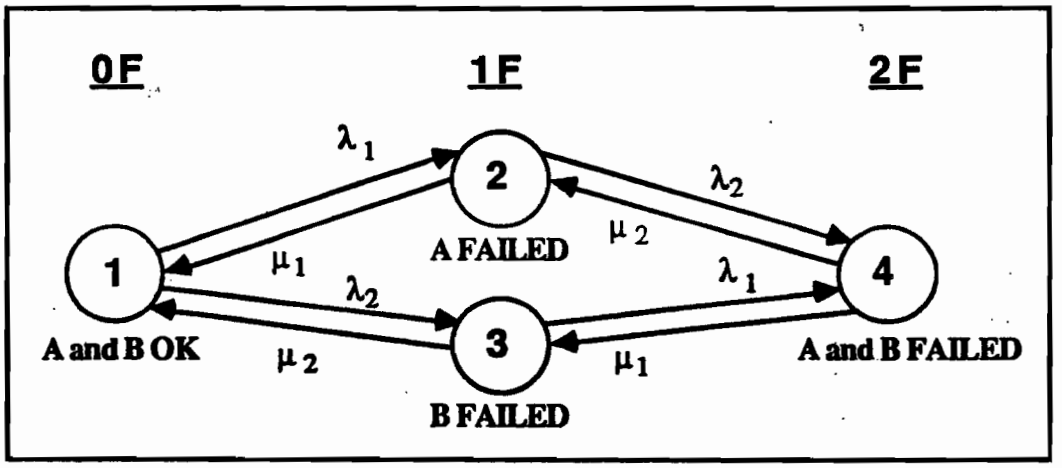

Figure 3.2c Aggregated Two-Component System Markov Model

The Markov model of this system is shown in Figure 3.2b. State 1 represents the no-failure configuration. Possible events when in this state are that component A can fail or component B can fail. These two possibilities are captured in the transitions leaving state 1 with the rates λ_1 and λ_2 respectively. State 2 represents component A failed and B working. Possible events leading out of state 2 are that component B may fail (exiting transition λ_2) or that component A may be repaired (exiting transition μ_1). Note that μ_1 stands for the repair rate for component A. The failure of component B leads to state 4, while the repair of component A leads back to state 1, returning the system to the no-failure state. Similarly, the exiting transitions for state 3, the B failed/A working state, are a failure of component A (transition λ_1 going to state 5) and a repair of component B (transition μ_2 going back to state 1). Notice that repairs, which are sequence-dependent events (since they can only be performed *after* a component has failed), are easily included in the model. States 4 and 5 represent system failure, being distinguished only by the sequence of events leading to the loss of both components. States 1, 2, and 3 represent the system in an operational configuration. If one was concerned with degraded operational modes, such as operating without a backup, then this model could also provide that information by giving the probability of states 2 and 3 independent of state 1.

States 4 and 5 both represent system configurations where components A and B are failed. However, in state 4 component A failed first and in state 5 component B failed first. In both of these states, the possible events are the repair of A (transition μ_1 leading to state 3) and the repair of B (transition μ_2 leading to state 2). Since the possible actions taken and their consequences, i.e., the destination states, are the same in states 4 and 5, these states may be lumped together if the order-of-failure distinction is not needed in the analysis. The resulting model is shown in Figure 3.2c. This simplification is referred to as exact aggregation of states and introduces no approximations. It is useful in systems where there are many identical components each with an identical impact on the system operation.

The state equations for the model in Figure 3.2c are obtained by inspection of the model diagram and applying the rule for determining flows. The state equations are:

$$dP_1(t)/dt = -(\lambda_1+\lambda_2)P_1(t) + \mu_1 P_2(t) + \mu_2 P_3(t) \quad (5)$$

$$dP_2(t)/dt = \lambda_1 P_1(t) - (\lambda_2+\mu_1)P_2(t) + \mu_2 P_4(t) \quad (6)$$

$$dP_3(t)/dt = \lambda_2 P_1(t) - (\lambda_1+\mu_2)P_3(t) + \mu_1 P_4(t) \quad (7)$$

$$dP_4(t)/dt = \lambda_2 P_2(t) + \lambda_1 P_3(t) - (\mu_1+\mu_2)P_4(t) \quad (8)$$

Note that all flows leaving a state (negative terms) appear as a flow entering a state (positive terms), thus indeed probability is conserved. Equations (5) through (8), together with the initial condition that state 1 has a probability of 1 and all other states have probabilities of 0 at time = 0, provide a complete description of the system.

All systems reach a point where the state probabilities are no longer changing. In the example of the single-component system this situation occurred when all of the probability was in state 2 and none was in state 1. This is common for systems without repair: after a long period of time most states have probabilities of 0 and only a few states, called trapping states, have probabilities that are between 0 and 1. Systems with repairs, however, have the property that when they get to this steady state all states may have probabilities that are between 0 and 1. This comes about because a balance is obtained between the flows leaving and those entering the states. For example, when the flow leaving state 1 in Figure 3.2c equals the flow entering state 1, its probability no longer changes. This occurs when the probabilities of states 1, 2, and 3 obtain values such that the flows are in balance. Equation (5) shows that this balance is obtained when $dP_1(t) / dt = 0$. Similarly, when the derivatives of all state probabilities are equal to 0, the system has come to its steady state. This steady state must still conserve probability such that the sum of the state probabilities is 1.

The steady state is an important condition in the ATCS analysis. ATCS comes to its steady state in a few days, yet it is a system that operates continuously over a much longer period of time. Although various components fail and are repaired as the system evolves, the probabilities of the various system states have come to steady state. Therefore, the analysis of ATCS is, in fact, an analysis of the system operating at steady state. For the completeness of this introduction however, we will briefly discuss the time-dependent problem.

The closed-form solution of Equations (5) through (8) for this two-component system, as is true of most systems with repairs, is rather complex and not particularly enlightening. It is more common to solve such system models numerically. First, the system equations (5) through (8) are written in matrix form:

$$\frac{dP(t)}{dt} = \begin{bmatrix} -(\lambda_1+\lambda_2) & \mu_1 & \mu_2 & 0 \\ \lambda_1 & -(\lambda_2+\mu_1) & 0 & \mu_2 \\ \lambda_2 & 0 & -(\lambda_1+\mu_2) & \mu_1 \\ 0 & \lambda_2 & \lambda_1 & -(\mu_1+\mu_2) \end{bmatrix} P(t) \qquad (9)$$

where the state vector is:

$$P(t) = [P_1(t), P_2(t), P_3(t), P_4(t)]^T$$

Notice that the columns of the matrix add to zero. This represents the flow conservation property in the system: all flows leaving a state must enter another state. The matrix equation may be written more concisely as:

$$dP(t) / dt = A\,P(t) \qquad (10)$$

Equation (10) is the continuous-time representation of the Markov model. Matrix A is the continuous-time transition matrix. While there are many ways of numerically integrating this equation, the one shown here is straightforward and adequate in many situations. The derivative is approximated over a discrete time step Δt by:

$$[P(t+\Delta t) - P(t)] / \Delta t = A\,P(t)$$

Multiplying each side by Δt and moving the state vector P(t) to the right-hand side gives:

$$P(t+\Delta t) = [I + A\,\Delta t]\,P(t)$$

where matrix I is the identity matrix. The term in brackets may be relabeled as matrix M:

$$P(t+\Delta t) = M\,P(t) \qquad (10)$$

M is the discrete-time transition matrix. The above approximation (Equation (10)) is called Forward (or Explicit) Euler integration.

Equation (11) represents a recursive solution for the Markov model. Given the system's initial condition, P(0), it is possible to use Equation (10) to propagate the state probability in time:

$$\begin{aligned} P(\Delta t) &= M\,P(0) \\ P(2\Delta t) &= M\,P(\Delta t) \\ P(3\Delta t) &= M\,P(2\Delta t) \\ P(4\Delta t) &= M\,P(3\Delta t) \\ &\bullet \\ &\bullet \\ &\bullet \\ P(n\Delta t) &= M\,P((n-1)\Delta t) \end{aligned}$$

The above procedure gives the state probabilities as a function of time from time = 0 to time = $n\Delta t$. It may also be viewed as an iterative solution of the steady-state problem, i.e., A P(t) = 0, if continued until the state probabilities no longer change.

A few remarks need to be made concerning this solution procedure. First, Δt must be judiciously selected such that the integration is stable, has the desired accuracy and

produces meaningful probabilities, i.e., between 0 and 1. Second, in performing these calculations on a computer, special care must be taken lest roundoff errors destroy the solution. Finally, a faster version of this integration scheme, taking advantage of the fact that M is time-invariant, may be constructed.

3.5.4 The State Space Explosion

It has already been mentioned that the major drawback of using Markov models to predict system reliability and safety is the problem of the growth of the state space. In this section we will discuss the rapid growth of the state space as a function of the number of components in the system. It is assumed that the systems considered do not have states that are distinguished only by failure sequences. That is, states which are only distinguished by the failure order are aggregated into one state. Each state is unique in that a specific list of components is failed; the order of these failures is not unique.

In Section 3.5.2 a single-component system was modeled. The model had 2 states. The two-component system modeled in Section 3.5.3 had 4 states when sequence dependencies were removed (Figure 3.2c). A 3-component system has 8 states, a 4-component system has 16 states, and a 5 component system has 32 states. Now consider a 20 component model. At the zero-failure level there is one state—no components have failed. At the first-failure level there are 20 states representing the single failure of each of the 20 components. Each of these 20 states has an exiting transition representing any of the other 19 components failing. Aggregating states with identical failed components gives 190 states at the second-failure level which describe the 190 combinations of dual failures. This pattern continues with 1140 states at the third-failure level, 4845 states at the fourth-failure level, etc., out to the 20^{th}-failure level where there is one state representing all components failed. The total number of states is about 10^6.

Repeating this exercise for a system with 40 components gives 1 state at the zero-failure level, 40 states at the first-failure level, 780 states at the second-failure level, 9880 states at the third-failure level, 91390 states at the fourth-failure level, etc., out to the 40^{th}-failure level. The total number of states is approximately 10^{12}. Storing this state vector requires one million megabytes of memory. Storage of the 10^{12} state equations would require much more memory. In general, a system with n components requires 2^n states to specify the model, if sequence dependencies are not of interest.

From these examples the exponential growth of the state space is apparent. However, these examples pale in the face of ATCS, which contains *hundreds* of components. Clearly, means of avoiding the state space explosion are needed to render the ATCS model tractable. In the following sections, various techniques are introduced to reduce the state space.

3.6 Techniques for State Space Reduction

Given the large number of components, the ATCS model has a potentially enormous number states. The use of techniques to reduce this intractable state space is clearly imperative. The primary technique employed is that of dividing the system into subsystems whose interactions are easily understood. These subsystems are modeled independently (submodels) and their results are merged combinatorially. This hierarchical approach is applicable only if the subsystems are independent, that is, a failure or repair event in one subsystem does not precipitate any event in another subsystem.

The division of the system into subsystems still leaves an intractably large state space for each submodel. Hence, further techniques are used to reduce the state space of these submodels. A major simplification is achieved by recognizing that, for our analysis, the identity of a failed component within a subsystem is not important. Rather, it is the number of failed components of a given type that we are interested in tracking, because any individual component has the same impact on the system. As already mentioned, this property is referred to as symmetry. A substantial reduction in the number of states is also accomplished by modeling separately the coverage process for dualized vital elements, obtaining a coverage value and using this coverage value to distinguish between covered and uncovered component failures. Finally, the use of virtual transitions to model the human- and hardware-induced transitions to accident states further contributes to reducing the state space.

The system model decomposition and the "chain" model are described in the next subsections. The model for the coverage of the dualized vital elements and the derivation of the virtual transitions are discussed in Section 4, along with the overall ATCS safety model.

3.6.1 Model Decomposition

The primary technique used to mitigate the state proliferation problem in the ATCS Markov model is the decomposition into submodels for each component type. The decomposition into submodels takes advantage of the relative independence of most of the component types. For example, the failure of a Base Station (composed of Communication Management Unit and Base Radio) results in a segment of track where trains are not in constant contact with the Central Dispatch Computer. Special operating rules must then be applied to get trains through this segment until a repair is made. Further, trains on this segment have lost the authority enforcement capability, thus exposing themselves to operator errors. This condition is true for this segment independent of failures of on-board train equipment such as the On-Board Computer. Notice, however, that the loss of two Base Stations means that there are now *two* segments where digital communication with the train is lost . This exposes the system to two places where operator errors cannot be corrected before an accident situation occurs.

Using the above scenario, the ATCS model is decomposed into submodels that contain all components of one type. There is one submodel for all of the Wayside Interface Units, one for the Base Stations, etc. The deciding factor in selecting submodels is the independence of the impact of failures on the system operation. Thus accident contributions will be accounted for in each submodel and the results merged to provide the composite accident rate for the complete model. This merging process will be described in Section 4.

3.6.2 The Chain Submodel

The most common submodel used in ATCS has a pictorial form that has led to its name of a "chain submodel". Consider the first failure level of a submodel of 3 components of the same type (Figure 3.3a). At the first failure level there are three states representing the single failure (at rate λ) of each of the three components. The exit transitions from each of these states shows the failure of the remaining two components or the repair of the single failed component (at repair rate μ).

The implication for the system in each of the single-failure states is that one location or train is missing a certain capability. Thus, if there is no concern for which *specific* location or train has lost this capability then these three states are equivalent and can be aggregated into one. This aggregation does not introduce any approximations (see Section 3.5.3).

The resulting model is shown in Figure 3.3b where the states at each failure level have been aggregated. State 1 contains the configuration where no components have failed. The failure of any one of the 3 components, a transition rate of 3λ, causes a transition into the state where one component has failed (state 2). In state 2 the failed component can be repaired (at rate μ or one of the remaining 2 components can fail, leading to state 3 at the rate 2λ. State 3 is the aggregate of all configurations where two components have failed. From this state, one of the two failed components may be repaired (rate 2μ) or the remaining component may fail (rate λ). State 4 represents the failure of all three components. Any of the three components may be repaired (rate 3μ) from state 4 causing a transition to state 3.

Figure 3.3b has the form of a chain. Notice that the failure of any of three components (the transition from state 1 to 2) is simply the sum of failing component 1 *or* component 2 *or* component 3. It is the uncertainty of precisely which component will fail that indicates the OR operation is needed, resulting in a sum of failure rates. The repair transition from state 4 to state 3 is 3μ. Similarly, this implies an uncertainty in exactly which component is being repaired. This could only be true if there were three repairmen all doing the repairs at the same time.

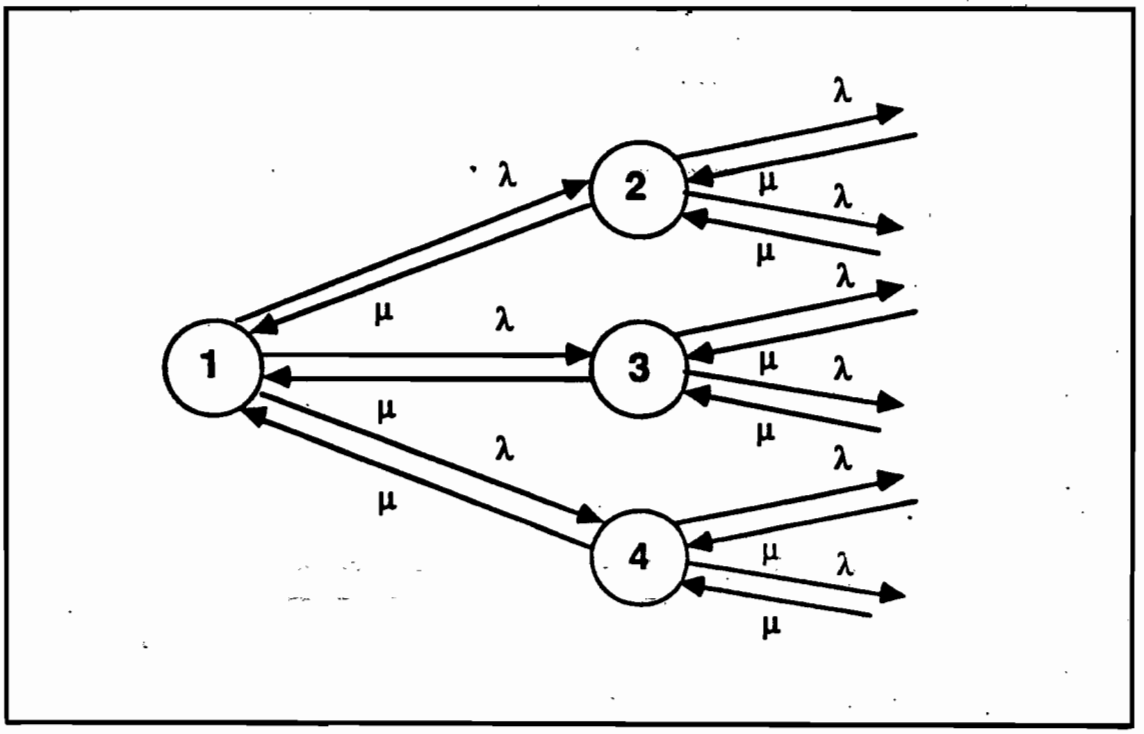

Figure 3.3a Three-Component Model - First Failure Level

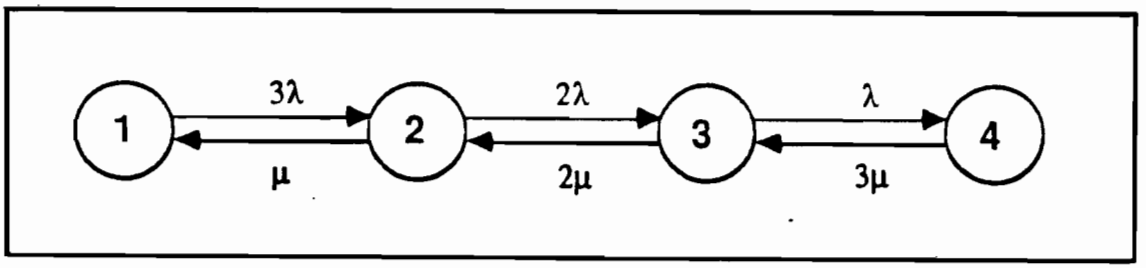

Figure 3.3b Three-Component Chain Model

The chain model has this simple form since all of its components have the same failure rate and the same repair rate. The implications on system operation are only dependent on the number failed, not which specific components are failed. Further, the chain model of Figure 3.3b contains an assumption of at least three repairmen. Note that the aggregation from individual states at each failure level to one state at each failure level accomplishes a very substantial reduction in the state space.

Consider now the chain model for N components of a given type. This results in the model shown in Figure 3.4. The failure rate for each component is λ and the repair rate is μ. The states are numbered *from 0 to N* so the state number corresponds to the number of failed components in that state. A typical value for N in ATCS is 100. The chain model would therefore have 101 states, which is not an intractable number of states.

In this special case, it can be shown that the state probabilities are given by

$$P(i) = \frac{1}{\left[1+\left(\lambda/\mu\right)\right]^N} \binom{N}{i} \left(\lambda/\mu\right)^i \qquad i = 0,1,2,\ldots,N \tag{12}$$

Notice that the probability for state i depends only on i, N, and the ratio (λ/μ); the absolute magnitudes of λ and μ do not affect the results. This is a direct consequence of the steady - state treatment adopted for this model. Figures 3.5 and 3.6 show the probability of i failures for various ratios of (λ/μ). Figure 3.5 is the case where there are 500 components (N = 500) and Figure 3.6 is for a chain of 1000 components.

Examining these plots shows the probability of more components failed dropping off rather steeply, particularly for the smaller (λ/μ) ratios. However, this is not always the case. If the value of N is greater than μ/λ, then a state where one or more components are failed will be the most probable. This can be derived from Figure 3.4. In steady state the flows into a state must equal those leaving the state. The transition from state 0 to state 1 has a rate of $N\lambda$ in one direction and a rate of μ in the other. Setting the flows between states 0 and 1 equal for the steady state gives:

$$P(0)\, N\, \lambda = P(1)\, \mu \tag{13}$$

Therefore, if $N\lambda > \mu$ (or $N > \mu/\lambda$), P(1) must be greater than P(0). A similar calculation can be done to find the condition for P(2) > P(1), etc. Note in Figure 3.6 that for the ratio $(\lambda/\mu) = 10^{-3}$ the probabilities for states 0 and 1 (0 and 1 component failed, respectively) are identical. This results immediately from Equation (13), for $(\lambda/\mu) = 10^{-3}$ and N = 1000.

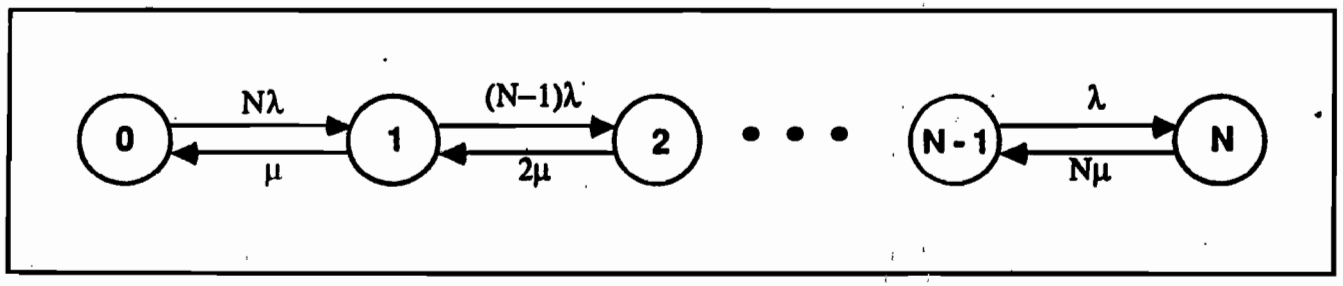

Figure 3.4 N-Component Chain Model

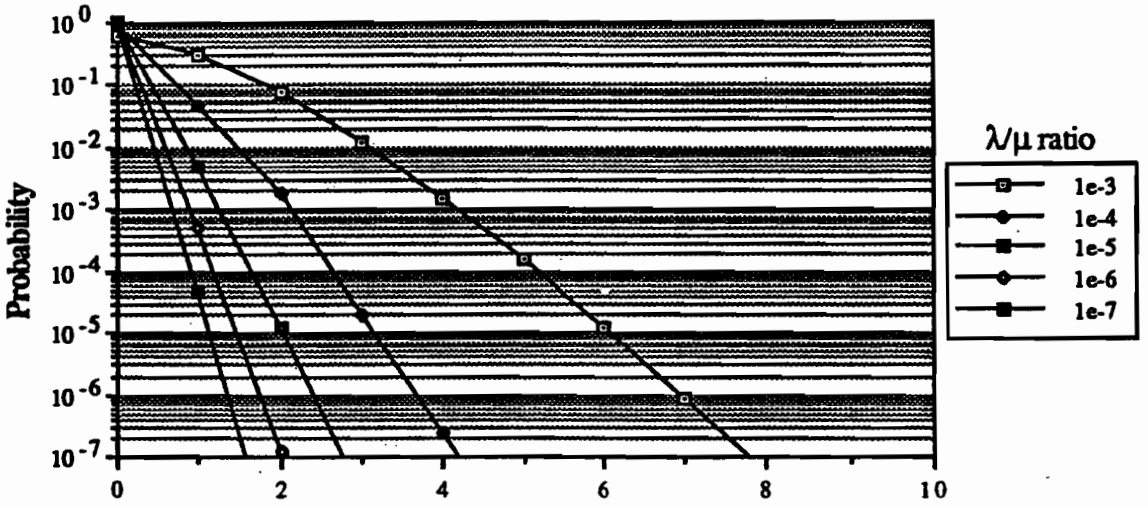

Figure 3.5 Number of Components Failed out of 500

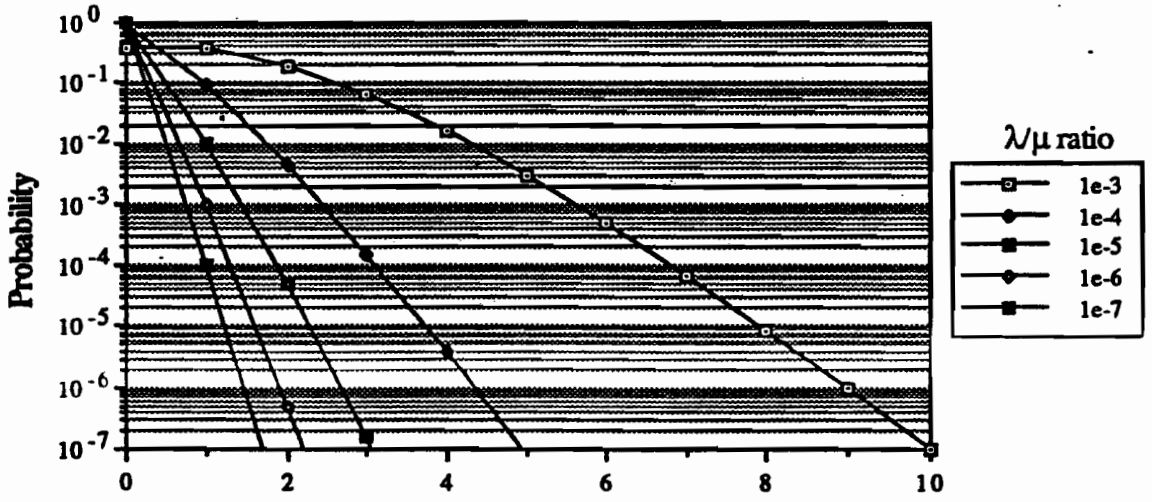

Figure 3.6 Number of Components Failed out of 1000

A point that has so far been ignored in this analysis is that these chains assume there are N repairmen. It is unlikely that there are 100 repairmen assigned to a component type for which there are 100 components. The impracticality of this is indicated by the probability that all 100 would be failed at once, and thus require a force of 100 repairmen. The lack of 100 repairmen does not invalidate the chain model. It can be easily verified that the probability of having more than a few components failed becomes exceedingly small. Thus, the lack of sufficient repairmen for the cases where most components are failed does not impact the results.

To summarize, the ATCS model is divided into submodels to reduce the intractable size of the state space. The most common submodels deal with collections of components of one type. A complete model of a group of 100 components would take 10^{30} states. However, since no distinction is required of which component is failed, i.e., only the number of failures is needed, the states at each failure level are aggregated into one state. This simplification drastically reduces the number of states to only 101 without any approximations. The resulting model is called a chain model and has some interesting properties in the steady state. The majority of the states in the chain do not contribute significantly to the solution and the N-repairmen assumption (important for our formalism) is perfectly adequate.

3.6.3 Submodel Independence

Decomposing a complex model into submodels such as chains is clearly productive only if the submodels can be solved individually and then efficiently recombined. These issues revolve around the nature of the independence of the submodels. In general, an "a priori" judgement must be made based on a careful examination of the system's architecture and operation. Direct verification of the hypothesis is obviously not practical, because it would entail constructing the complete model, which is exactly what we are trying to avoid. To illustrate the concept, however, we will provide a simple example for which we can easily find the solution of the complete model as well as of the corresponding submodels.

Consider the two-component system with repairs previously discussed and focus on obtaining the steady-state solution. As already mentioned, the equations satisfied by the steady-state solution are obtained from their time-dependent counterparts by setting all the time derivatives equal to zero. This leads to:

$$\mathbf{A}\,\mathbf{P} = \mathbf{0} \tag{14}$$

where $\mathbf{0}$ is a vector whose elements are all equal to 0. We should note at this point that matrix A is singular. In fact, if it were not, the only solution possible would be the "trivial" solution, i.e.,

$$P = [0, 0, 0, 0]^T$$

The singularity of A is a direct consequence of the probability flow conservation discussed earlier. Indeed if we add all the rows in the matrix we obtain a row containing only zero entries, thus proving that the matrix is singular. The implication is that the equations are not linearly independent, in other words we have fewer "bona fide" equations than unknowns. This indeterminacy is removed by replacing any of the four equations (14) by the probability conservation condition, i.e.,

$$P_1 + P_2 + P_3 + P_4 = 1 \tag{15}$$

The resulting system of equations can be solved (in this relatively simple example) by symbolic Gaussian elimination. Let us substitute Equation (15) for the first equation in (14) and add the right-hand-side as the fifth column to form the "augmented" matrix:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ -\lambda_1 & (\lambda_2+\mu_1) & 0 & -\mu_2 & 0 \\ -\lambda_2 & 0 & (\lambda_1+\mu_2) & -\mu_1 & 0 \\ 0 & -\lambda_2 & -\lambda_1 & (\mu_1+\mu_2) & 0 \end{bmatrix}$$

A sequence of forward elimination steps leads to the following upper triangular augmented matrix:

$$\begin{bmatrix} 1\ 1\ 1\ 1 & 1 \\ 0\ 1\ 0\ 1 & \lambda_1/(\lambda_1+\mu_1) \\ 0\ 0\ 1\ 1 & \lambda_2/(\lambda_2+\mu_2) \\ 0\ 0\ 0\ 1 & \lambda_1\lambda_2/[(\lambda_1+\mu_1)(\lambda_2+\mu_2)] \end{bmatrix}$$

Backsubstitution immediately yields the solution of this system of equations:

$$P_1 = \mu_1\mu_2 / [(\lambda_1 + \mu_1)(\lambda_2 + \mu_2)] \tag{16}$$
$$P_2 = \lambda_1\mu_2 / [(\lambda_1 + \mu_1)(\lambda_2 + \mu_2)] \tag{17}$$
$$P_3 = \lambda_2\mu_1 / [(\lambda_1 + \mu_1)(\lambda_2 + \mu_2)] \tag{18}$$
$$P_4 = \lambda_1\lambda_2 / [(\lambda_1 + \mu_1)(\lambda_2 + \mu_2)] \tag{19}$$

This is the steady-state solution of the complete model of the two-component system.

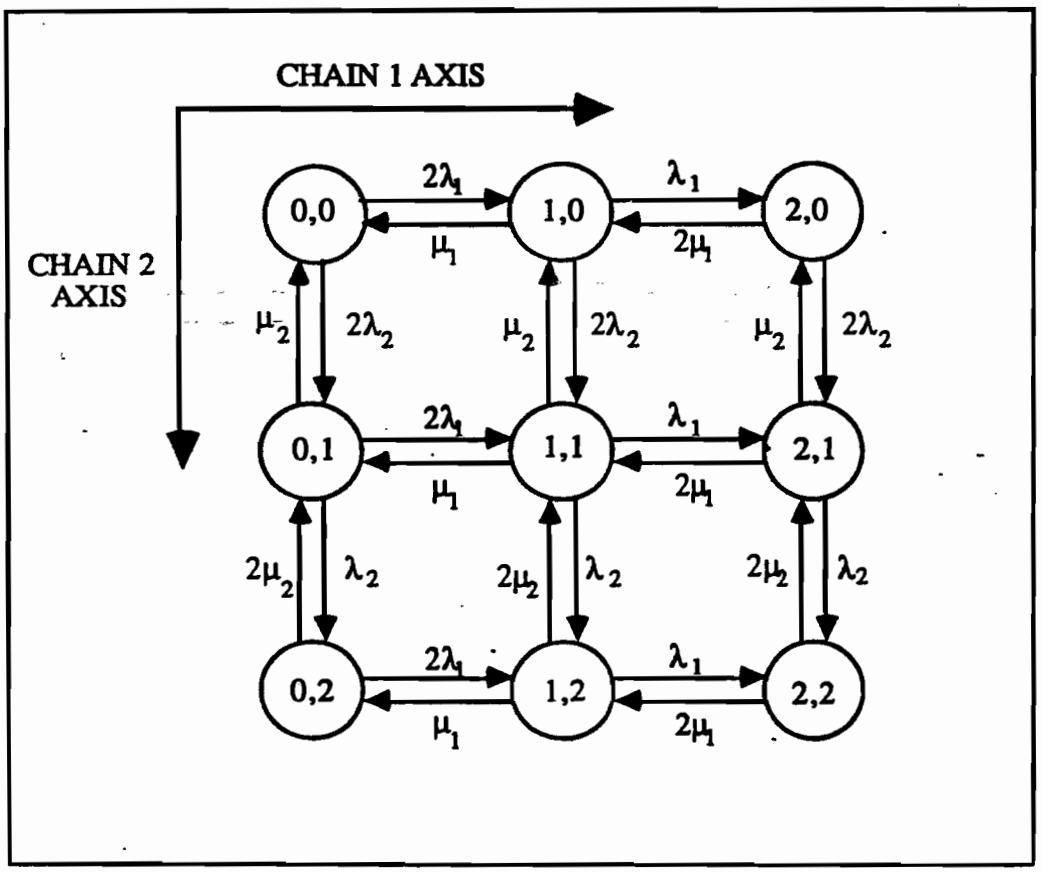

Figure 3.7 Full Two-Chain Model

An examination of this system indicates that events (failure or repair) related to one component have no effect at all on the other component. Thus, if we model the behavior of each component separately, the resulting submodels are independent. In this case, each submodel is a "chain" representing one component. Chain 1 has one component with a failure rate λ_1 and a repair rate μ_1, while chain 2 has one component with a failure rate λ_2 and a repair rate μ_2.

Figure 3.7 shows the model comprising these two chains. The state numbers are ordered pairs, "i,j", indicates a state where there are "i" failed components in chain 1 and "j" failed components in chain 2. Starting from the no failure state, "0,0", the possible transitions are that one component in chain 1 may fail or one component in chain 2 may fail. The diagram is structured such that failure and repair events concerning chain 1 are on the horizontal axis and those of chain 2 are on the vertical axis. Notice that the same transition appears repeatedly along any horizontal or vertical line. For example, the transition between states "0,0" and "1,0" is the same as that between "0,1" and "1,1". Such chains are called orthogonal because of the overall symmetry and limitation of chain 1 events to one axis and chain 2 events to the other axis. Notice that the chain 1 events are potential events from every state of chain 2 and vice versa. Thus, it seems reasonable that chain 1 could be modeled independently of chain 2. Chain 1's probability of having its component operational would be distributed over states "0,0" and "0,1" based on the ratios of states 0 and 1 in chain 2. A similar situation exists for chain 1's probability of having its component failed. Thus, all states in the model of Figure 3.7 could be found. The orthogonality of the chains provides a simple means of merging their results.

Each chain is solved *alone* using Equation (11). The state probabilities for chains 1 and 2 are:

$$P^1(0) = \mu_1 / (\lambda_1+\mu_1)$$
$$P^1(1) = \lambda_1 / (\lambda_1+\mu_1)$$
$$P^2(0) = \mu_2 / (\lambda_2+\mu_2)$$
$$P^2(1) = \lambda_2 / (\lambda_2+\mu_2)$$

where the notation $P^k(i)$ indicates the probability of having "i" failures in chain "k". Taking the product of any of the probabilities of chain 1 with one of the probabilities of chain 2 gives the probability of the joint event :

$$P^1(0)\,P^2(0) = P(0,0) = [\mu_1 / (\lambda_1+\mu_1)][\mu_2 / (\lambda_2+\mu_2)] \quad (20)$$
$$P^1(1)\,P^2(0) = P(1,0) = [\lambda_1 / (\lambda_1+\mu_1)][\mu_2 / (\lambda_2+\mu_2)] \quad (21)$$
$$P^1(0)\,P^2(1) = P(0,1) = [\mu_1 / (\lambda_1+\mu_1)][\lambda_2 / (\lambda_2+\mu_2)] \quad (22)$$
$$P^1(1)\,P^2(1) = P(1,1) = [\lambda_1 / (\lambda_1+\mu_1)][\lambda_2 / (\lambda_2+\mu_2)] \quad (23)$$

Clearly, Equations (20-23) are identical to the expressions found with the full model, Equations (16-19). Therefore, it is possible to obtain the probability of any state in the two-chain model without ever solving the two-chain model. Instead, each chain is solved independently and the appropriate products are taken to determine the two-chain state probabilities.

The decomposition method provides an impressive reduction in the size of the state space. Considering two chains with 100 states, a full model would have 10,000 states, while the decomposition allows the solution of each 100-state chain separately. It should be noted that this concept is easily generalized to any number of orthogonal chains. The probability of being in one specific state in the full multi-chain model is simply the product of the appropriate states from the independent solution of each chain.

4 ATCS Safety Model

After introducing and developing the basic concepts and techniques in the previous section, we proceed now to construct the ATCS safety model, the objective of which being the prediction of accident rates under the proposed system.

Clearly, this is a very large and complex system, which may exhibit an enormous number of failure modes. However, careful consideration of the system's operation, characteristics and composition reveals the fact that there is only a limited set of effects to be analyzed. While the system contains a very large number of components, there are only a few different component types. For a given component type, assessing the vulnerability of the system to failure requires tracking only the number of failed components and not the state of the individual components. This is the basic premise that allows the use of the previously described "chain" model. Moreover, it is obvious that failures of components of a given type do not cause failures of components of another type. In other words, a failure of a component of type A is totally independent of a failure of a component of type B. This key observation enables us to decompose the system into chains of components of a particular type, investigate the accident potential due to each individual chain and finally recombine the individual chains to generate the global accident model.

The accidents we are considering in developing the safety model are initiated by hardware failures. Such failures may have a two-fold impact on the system. If the component failed is vital and its failure is not detected, the system will act based on incorrect information, leading very likely to an accident condition. In fact, the analysis conservatively assumes that undetected failures always result in an accident. On the other hand, if a component failed, with the system knowing it, the system reverts to a mode of operation which exposes it to those potential human errors that the failed hardware was supposed to protect against.

There are other, system-specific considerations which are accounted for in assembling the final safety model. Such considerations are discussed later in this section.

4.1 Accident Rate Formulation

The objective of this section is to generate a model allowing a prediction of potential accident rates, due to both undetected hardware failure and human error. As already mentioned, we start with the analysis of a generic individual chain, indicate then the manner in which a number of chains are merged and finally address the "overlap" problem to properly account for the number of humans involved in various states of the system.

4.1.1 Individual Chain

Each state possesses a potential for accident, due to either human error or undetected hardware failure. In principle, an accident occurrence changes the system in that it may

reduce the number of components in use and obviously it may cause additional damage. To simplify the analysis, we make the assumption that an accident does not change the system. In view of the size of the system, this is a very mild assumption. It may also be argued that, following an accident, a "spare" train is immediately placed in service, thus restoring the system to its nominal size. An equivalent way to state this assumption is that, on the average, there is a constant number of components in the system. With this assumption, the state probabilities representing the system in various failure conditions remain unaffected by transitions to accidents. These transitions therefore are treated as "virtual" transitions, not being directly involved in the Markov model.

Once the state probabilities have been obtained, the accident rate A for a chain is determined as an expectation value:

$$A_j = P(0)V_0 + P(1)V_1 + \bullet\bullet\bullet + P(N)V_N \qquad (4.1)$$

where V_i's are the virtual transition rates. Each term in this sum represents the rate of accident occurrence from a certain system state times the probability of the system being in that state. Thus A is the expected accident rate, expressed in accidents per unit time (most often, per year).

As already mentioned, accident may be caused by either an undetected hardware failure or by a human error. Consider first a component that has vital, dualized internal elements such as the wayside interface unit (WIU). The component can create an accident potential by having an uncovered failure. The uncovered failure occurs with a rate $\lambda(1\text{-}c)$, where c is the coverage factor derived in the coverage model.

In state 0, where no components have failed, the system is vulnerable to any of the N components having an uncovered failure. Therefore, the virtual transition from state 0 is:

$$V_0 = N\lambda(1 - c)$$

State 1 has N-1 components operating. Thus, the system is vulnerable to N-1 uncovered failures from this state, i.e.

$$V_1 = (N - 1)\lambda(1 - c)$$

In general, for a state corresponding to i failures, the virtual transition rate is:

$$V_i = (N - i)\lambda(1 - c)$$

Thus, the total accident rate contributed to by this chain is:

$$A_U = P(0)\,N\lambda(1\text{-}c) + \bullet\bullet\bullet + P(i)\,(N\text{-}i)\lambda(1\text{-}c) + \bullet\bullet\bullet + P(N\text{-}1)\lambda(1\text{-}c)$$

Using the expression for P(i) given in Equation (3.12) with λ replaced by λc and noting that

$$\binom{N}{i}(N-i) = \binom{N-1}{i}N$$

the total accident rate due to uncovered failures in this chain can be written as:

$$A_U = N\lambda(1-c)/[1+(\lambda c/\mu)] \qquad (4.2)$$

Consider now a chain where the components do not have uncovered failures due to hardware operation, but the failure of a component leads to operation in a backup mode which exposes the system to human errors. For example, a failure of a component used for communication between the central dispatch computer (CDC) and the train leads to temporary operation under voice radio blocking rules. Clearly this type of operation removes the authority enforcement capability, thus exposing the system to train operator error. Furthermore, the CDC and the dispatcher (for now it is assumed that there is only one dispatcher for the region) may no longer have updates on the train status and position, exposing the system to dispatcher errors as well.

In state 0 there are no components failed so there is no exposure to human errors, therefore $V_0 = 0$. In state 1 there is one component failed so the system is exposed to two humans, the dispatcher and the operator of the affected train, that generate errors at the rates H_D and H_O, respectively. The virtual transition rate leaving state 1 is:

$$V_1 = H_D + H_O$$

In state 2, two components have failed removing communication from two segments of track. The system is exposed to three humans: the dispatcher and two train operators. The virtual transition rate leaving state 2 is:

$$V_2 = H_D + 2H_O$$

In general, the virtual transition exiting state i reflects exposure to the dispatcher and i train operators:

$$V_i = H_D + iH_O$$

Then the total dispatcher-caused accident rate as a result of this chain is:

$$A_D = H_D[P(1) + \bullet\bullet\bullet + P(i) + \bullet\bullet\bullet + P(N)] \qquad (4.3)$$

Noting that the expression between the brackets is just [1 - P(0)] and using Equation

(3.12) with λ replaced by λc, the dispatcher-induced accident rate becomes:

$$A_D = H_D \{1 - 1/[1+(\lambda c/\mu)]^N\} \quad (4.4)$$

The total operator-caused accident rate is:

$$A_O = H_O [P(1)1 + \bullet\bullet\bullet + P(i)\, i + \bullet\bullet\bullet + P(N)\, N] \quad (4.5)$$

Again using Equation (3.12) and noting that

$$\binom{N}{i} i = \binom{N-1}{i-1} N$$

the operator-induced accident rate can be written as:

$$A_O = H_O N (\lambda c/\mu)/[1+(\lambda c/\mu)] \quad (4.6)$$

It is interesting to note that both the total accident rate due to uncovered hardware failure and that due to operator error are proportional to the number of components in the system. This proportionality is also approximately displayed by the dispatcher-induced accident rate. Indeed, for $\lambda c/\mu << 1$, Equation (4.4) may be rewritten as:

$$A_D = H_D N (\lambda c/\mu)/[1+N(\lambda c/\mu)]$$

Thus, the accident rate has an essentially linear relationship to the size of the system.

To summarize, closed-form expressions have been obtained for the accident rate caused by failures in a single chain. While the hardware failure is responsible for accidents, both direct effects, due to undetected component failures and indirect effects, due to human error during a fall-back operation mode, have been considered.

4.1.2 Train Operator Overlap

Once we have a formulation for an individual chain accident rate, the next logical step is merging the relevant chains to create a composite accident rate. However, a preliminary step is needed to ascertain correctly the number of humans involved, i.e., avoid multiple counting and the inherent overly conservative results that would follow.

In the previous section, we obtained the accident rate due to train operator errors, occurring during a backup mode of operation. The formulation implied that with each component failure an additional operator is brought into play. However, the actual situation is a considerably more complex. Consider the full component complement on a ATCS-equipped locomotive: Data Radio, Message Processor, On-Board Computer,

Tachometer(s) and Interrogator. When there are only a few failures in the system, there is a high likelihood that they will occur on different locomotives and that indeed, each failure will introduce an operator, with his potential for accident-causing errors. On the other hand, states with many failures may likely involve the same locomotive(s). Consequently, fewer operators will be introduced in the system, compared to what an actual failure count would predict. For example, if the radio and the computer fail on the same locomotive, the subsequent backup operation using voice radio will introduce only one instead of two operators. The fact that multiple failures may occur on the same locomotive is what we refer to as overlap.

In this section, we will derive the formula for the actual number of operators involved when an arbitrary number of failures occurs in a multichain model.

Consider two chains of N components of the types installed on a ATCS-equipped locomotive, for instance the chain of Data Radios and the chain of On Board Computers. There are, say, i failures in chain 1 and j failures in chain 2. If these i+j failures all occurred on different locomotives, then there would be i+j trains operating under radio blocking rules, thus involving i+j operators. However, this is not the case.Some failures always occur, on the average, on the same locomotives, thus exposing the system to fewer operators. The degree of overlap is rather small when only few failures are considered, but it becomes considerable when dealing with many failures. The extreme situation, when no component is still operational, clearly implies that there are two failures on each locomotive. Obviously, however, there are only N operators involved. The actual number of operators when i components of type 1 and j components of type 2 have failed is given by:

$$O_{ij} = i + j - ij / N \tag{4.7}$$

where the term ij/N represents the overlap, ranging indeed from 0 to N.

If a third chain of N components is added to the model, "contributing" k failures, the actual number of operators, accounting for all possible overlaps, is:

$$\begin{aligned} O_{ijk} &= k + O_{ij} - kO_{ij} / N \\ &= i + j + k - ij/N - jk/N - ik/N + ijk/N^2 \end{aligned} \tag{4.8}$$

The pattern is now obvious: the reader may recognize a similar formula used to calculate the probability of occurrence for the union of a number of non mutually exclusive events.

In this form, the equation is somewhat unwieldy to generalize and use when many chains are involved. A more convenient form will now be obtained. Starting with Equation (4.7), we have:

$$O_{ij} = N\,(O_{ij}/N) = N\,(i/N + j/N - ij/N^2)$$
$$= N\,[1 - (1 - i/N - j/N + ij/N^2)]$$
$$= N\,[1 - (1 - i/N)(1 - j/N)]$$

Similarly, for three chains, Equation (4.8) may be recast as:

$$O_{ijk} = N\,[1 - (1 - i/N)(1 - j/N)(1 - k/N)]$$

Based on the clearly emerging pattern, a general formula applicable to an arbitrary number of chains can now be obtained. Let $i_1, i_2, \ldots, i_M$ be the number of failures in M chains of equal length N. Accounting for the overlaps, the number of operators involved at the $i_1 i_2 \ldots i_M$ failure level is given by:

$$O_{i_1 \ldots i_M} = N\,[1 - \prod_{m=1}^{M} (1 - i_m/N)] \tag{4.9}$$

This equation will be used to formulate the accident transition rate for the multichain model.

4.1.3 Composite Accident Rate

We are now in a position to combine the individual chains to construct a composite accident rate. Invoking the orthogonality of the chains, the combined probability of having i_1 failures in chain 1, i_2 failures in chain 2, etc., is simply the product of corresponding probabilities considering each chain alone:

$$P_{i_1 \ldots i_M} = \prod_{m=1}^{M} P_{i_m} \tag{4.10}$$

The transition rate from state $i_1 i_2 \ldots i_M$ per unit human error rate is defined as:

$$T_{i_1 \ldots i_M} = P_{i_1 \ldots i_M} O_{i_1 \ldots i_M}$$

or, using Equations (4.10) and (4.9),

$$T_{i_1 \ldots i_M} = N\,(\prod_{m=1}^{M} P_{i_m})\,[1 - \prod_{m=1}^{M} (1 - i_m/N)] \tag{4.11}$$

Then, the total transition rate, over all chains, per unit human error rate, is:

$$T = \sum_{i_1=0}^{N} \cdots \sum_{i_M=0}^{N} T_{i_1 \ldots i_M} \tag{4.12}$$

Substituting Equation (4.11) into Equation (4.12) gives rise to two terms. The first term is:

$$N \sum_{i_1=0}^{N} \cdots \sum_{i_M=0}^{N} \left(\prod_{m=1}^{M} P_{i_m} \right)$$

$$= N \prod_{m=1}^{M} \left(\sum_{i_m=0}^{N} P_{i_m} \right) = N \tag{4.13}$$

In this expression we used the commutivity of the summation and product operators and the obvious fact that the sum of all probabilities in a chain is equal to one. Turning now to the second term, we have:

$$N \sum_{i_1=0}^{N} \cdots \sum_{i_M=0}^{N} \left[\prod_{m=1}^{M} P_{i_m} (1 - i_m/N) \right]$$

$$= N \prod_{m=1}^{M} \left[\sum_{i_m=0}^{N} P_{i_m} - \frac{1}{N} \sum_{i_m=0}^{N} P_{i_m i_m} \right]$$

$$= N \prod_{m=1}^{M} [1 - T_m/N] \tag{4.14}$$

where T_m is just the accident rate for chain m alone, considering unit operator error rate (see Equation (4.5)). Combining these intermediate results leads to the following form of Equation (4.12):

$$T = N \left[1 - \prod_{m=1}^{M} [1 - T_m/N] \right] \tag{4.15}$$

Using Equation (4.6) and considering a rate of operator errors H_O, we finally obtain the operator-induced accident rate for the entire multichain model:

$$A_O^{total} = H_O N \left[1 - \prod_{m=1}^{M} \frac{1}{1+(\lambda c/\mu)_m}\right] \qquad (4.16)$$

A few remarks are in order regarding this expression. First of all, it is interesting to note the proportionality to the "size" of the system, N. This has an importance consequence with regard to applying a human error rate predicated on the current system. We will elaborate further on this aspect in Section 5 when addressing the input to our model. It is also worth noting that the expression reduces properly in the extreme case of "everything failed":

$$A_O^{total} \left[\text{ for } (\lambda c/\mu)_m >> 1 \right] \rightarrow H_O N$$

In other words, as expected, when all the components constituting the communication and enforcement capabilities are failed, the system becomes vulnerable to human errors caused by all the train operators in the region. At the other extreme, assuming the repairs are performed extremely fast when compared to the failure rates, the accident rate due to operator errors reduces to zero, i.e.

$$A_O^{total} \left[\text{ for } (\lambda c/\mu)_m << 1 \right] \rightarrow 0$$

Finally, the reader should note that T in Equation (4.15) may also be interpreted as the *expected* number of "failed" trains. We will use this interpretation in the next subsection.

To summarize, we have obtained a closed-form solution for the rate of accidents caused by train operator errors when operating under fallback conditions, i.e., when digital communication and enforcement capabilities are lost.

4.1.4 Dispatcher Overlap

We have already noted the overlap problem regarding the train operators. A similar situation exists with respect to the dispatchers. When the communication link between the Central Dispatch Computer and some train is not operational, the dispatcher will communicate directly with the operator of that train. Additional equipment failures will bring into play more train operators. A dispatcher however normally handles a number of trains within a region. An additional "failed" train may or may not involve an additional dispatcher. To avoid the very complex combinatorial problem of exactly apportioning failed trains to dispatchers, we take a simplified, but conservative and quite justifiable approach. We will assume that each failed train adds a dispatcher to the human count. While obviously conservative, the assumption is not at all unreasonable, given the small expected number of trains failed and the size of the territory associated with a region. On the other

hand, the number of dispatchers involved clearly may not exceed the total number of dispatchers available.

Based on these considerations and recalling the interpretation of Equation (4.15), the accident rate due to dispatcher errors is given by:

$$A_D^{total} = H_D \min\left\{ D, N\left[1 - \prod_{m=1}^{M} \frac{1}{1+(\lambda c/\mu)_m}\right]\right\} \qquad (4.17)$$

where D is the number of dispatchers available for the region.

Equations (4.16) and (4.17) constitute the mathematical basis of the ATCS accident rate model.

4.2 Coverage Model For Dualized Vital Elements

ATCS system integrity is maintained by the use of dualized vital elements. It is necessary for the system to know when its vital elements are not operating correctly. If this is known in a timely fashion then the system can drop down to a fail-safe mode of operation. For example, it is required that the system know the position of a switch. This information is relayed to the Central Dispatch Computer (CDC) through a wayside interface unit (WIU). If the WIU fails *and* the system is not aware of the failure, it will "think" it knows the switch position when, in fact, it does not. This is a very dangerous situation. However, if the CDC *always* knows when the WIU has failed, a fail-safe procedure can be implemented. This may involve directing inspection of the switch position by the locomotive engineer before proceeding across it. While this reduces the system performance, it permits safe operation even though a component has failed.

There are other vital elements in the system as well. Given the need for detecting virtually all vital element failures, what procedures are used to obtain this detection ability? A common approach is to use two identical elements performing the same tasks at the same time. These dualized elements continually compare their outputs and shutdown if they do not agree. Thus the vital elements of a component are duplicated so that there is a means of detecting the failure of this vital component. It should be noted however that this detection procedure does not provide an indication of *which* of the two elements has failed and therefore this approach does not generally offer fault-tolerance. In ATCS this is an acceptable outcome, because the system may continue to operate in a backup, fail-safe mode until the condition is rectified. This approach of dualizing vital elements of key system components is used in ATCS to insure that single hardware failures cannot lead directly to an accident.

In the above discussion it is assumed that the dualized elements will find most failures within an acceptable time. A Markov model can be used to quantify the process of the

coverage. The failure of an element has two possible outcomes: the failure is covered and the system continues to operate (in a backup mode), or the failure is not covered and an accident may result. Deciding which outcome occurs involves modeling the failure and detection processes for the element. The modeling requires many intermediate states to keep track of the competing actions of failures and detection. If this detailed modeling was included in the complete system model each state (i.e., each failure) would require many states to decide its outcome. The Markov model, which is already too large to analyze, would grow further if this detailed coverage modeling was included.

The alternative to detailed modeling of the coverage process *within* the complete model is to model the process in a separate model, whose output is a coverage factor representing the fraction of failures that are covered. This approach is actually used quite often because the time scale of the detection/reconfiguration process is much shorter than that on which failure or repair events occur. Practically, the detection and reconfiguration take place nearly instantaneously and therefore a steady-state coverage factor is entirely justified even if a time-dependent reliability analysis were carried out. For the steady-state analysis of the ATCS, there is, in fact, no approximation involved in such an approach. The coverage factor is simply used to assign two exit transitions to every failure in the complete model, one reflecting the covered fraction of the failures and the other the uncovered fraction.

In summary, the dualized vital elements are needed to provide coverage of single hardware failures. The effectiveness of this coverage and its impact on system safety must be quantified. Explicitly including the details of the coverage process in the complete model would contribute to the state proliferation. Instead, independent coverage models are made and their results incorporated in the complete model as a fraction of the failures that are covered.

The Markov model used in determining the coverage of dualized vital elements is shown in Figure 4.1. The component is assumed to be made up of some simplex elements which have a total failure rate of λ_2 and some dualized elements that have a failure rate of λ_1 for each half of the dual. The detection process is represented by the rate λ_3.

In state 1 there are no failed elements. The failure of the simplex portion leads to state 2 and the failure of either half of the dual elements ($2\lambda_1$) leads to state 4. In state 4 there are two competing processes: the detection rate λ_3 vs. the failure of one of the remaining elements. The detection transition leads to the detected state (state 3) where the system goes into the fail-safe mode. The transition to state 6 accounts for a failure of the remaining half of the dualized elements occurring before the first failure is detected. This near-coincident failure state will be detected unless the failures are so similar that both halves of the duplex appear, to the failure detection mechanism, to be in agreement with each other. Although the probability of such a false agreement occurring is small, quantifying that probability is difficult, so the worst case assumption is made, i.e., the probability of similar failures is

assumed to be 1, thus all near coincident failures are uncovered.[1] The remaining transition from state 4 is the failure of the simplex elements leading to state 5.

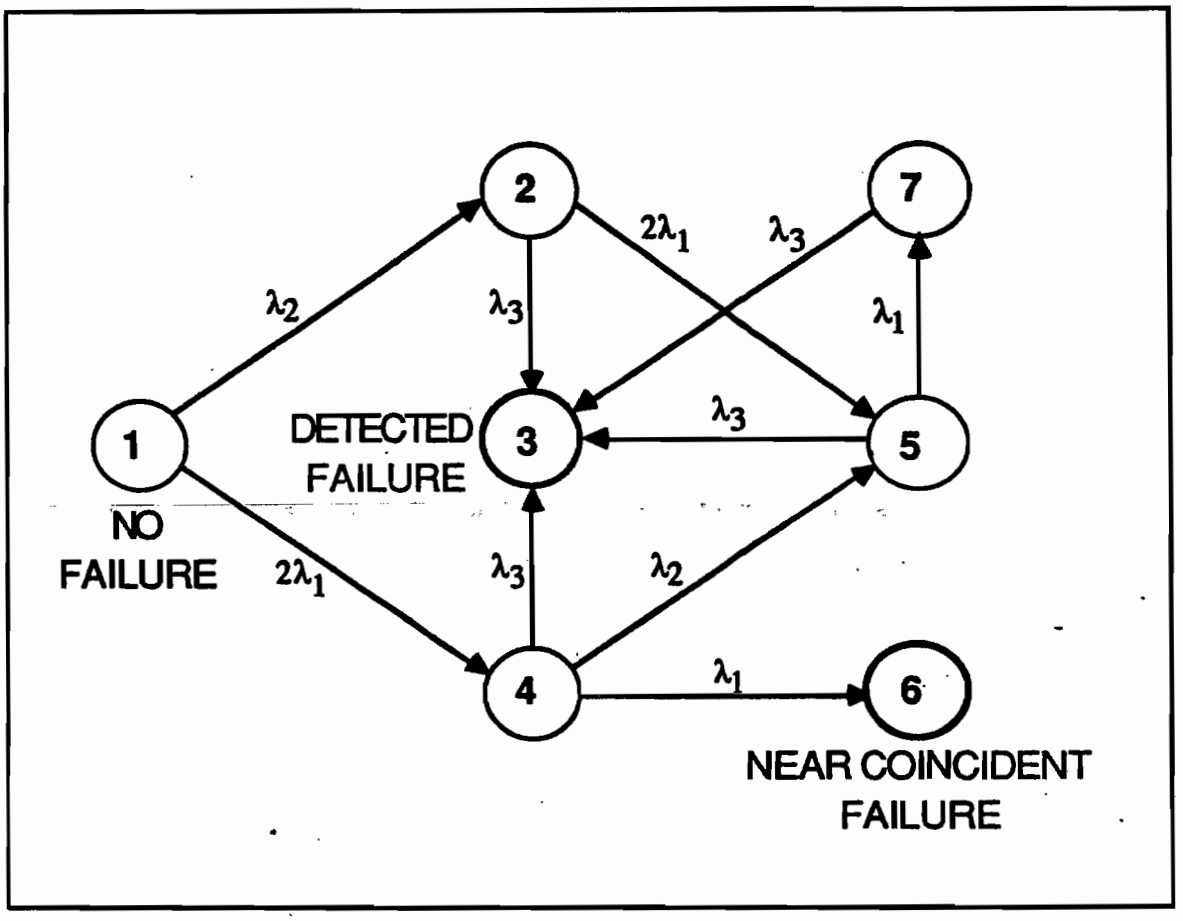

Figure 4.1 Coverage Model for a Dualized Vital Element

State 2 also shows a competition between the detection rate λ_3 vs. the failure of one of the remaining elements. In state 2 the failed component is the simplex element and it is assumed that this component's failure can always be detected within an acceptable time. Since a comparison is not needed to detect failures of the simplex element there is no transition to the near-coincident failure state. Instead, the only subsequent failures are one half of the dualized element. This leads to state 5.

In state 5 both the simplex and one-half of the dualized elements are failed. It is assumed that the component will not be labeled as operational if the simplex part is failed. Therefore, independent of the outcome of the dualized comparison, the component would

[1] The spreadsheet formula does, however, allow for the specification of the probability of similar failures in the near coincident failures case.

be labeled as failed since its simplex element has failed. Thus, this state does not include an exit transition to the near-coincident failure state. The exits from state 5 are a detection transition to state 3 and a failure of the remaining half of the dualized elements which leads to state 7. In state 7 all elements of the component are failed and the detection, presumed to be accomplished by not replying to queries by other parts of the system, is the only subsequent event.

The model in Figure 4.1 permits an evaluation of the dualized vital component's coverage. The coverage value is the fraction of the faults that are detected such that the system can go to a fail-safe mode. The total probability that a fault has occurred is the sum of the probabilities of states 2 through 7. Therefore, the coverage value c is:

$$c = [P_2 + P_3 + P_4 + P_5 + P_7] / [P_2 + P_3 + P_4 + P_5 + P_6 + P_7]$$

The complement of the coverage, the fraction of faults that are near coincident and, therefore, not detectable, is:

$$(1 - c) = P_6 / [P_2 + P_3 + P_4 + P_5 + P_6 + P_7]$$

The model in Figure 4.1 has two trapping states: 3 and 6. All of the other states are transient. At steady-state, all probability must end up in one of the two trapping states. Therefore the expression for the coverage value reduces to:

$$c = P_3 / (P_3 + P_6) = P_3 = 1 - P_6 \qquad (4.17)$$

In a model with no repairs, the steady-state probabilities can be easily determined. Such model may be viewed as a network with nodes representing the states and edges (or connections) representing the transitions. The source is the node associated with the no failure state and the sinks are the nodes corresponding to the trapping states. Each edge is associated with a probability, P_{ij}, where i and j are the starting and the destination nodes, respectively. With the transition rates known, this probability is given by:

$$P_{ij} = \lambda_{ij} / \sum \lambda_{ij} \qquad (4.18)$$

where the sum is taken over all the transitions originating in node i. The probability for a path between nodes k and l (not necessarily neighbors) is given by the product of the probabilities of the edges making up that path, i.e., the events associated with each edge are assumed independent. Then, to obtain the total probability of reaching node l from node k, the probabilities of all paths, considered mutually exclusive, are summed up.

The approach outlined above allows us to obtain an expression of the coverage factor as a function of failure and detection rates. For the proposed model, we are interested in the paths between node 1 and node 3:

$$P_3 = P_{12}P_{23} + P_{14}P_{43} + (P_{12}P_{25} + P_{14}P_{45})(P_{53} + P_{57}P_{73}) \qquad (4.19)$$

where:

$$P_{12} = \lambda_2/(2\lambda_1+\lambda_2) \qquad P_{23} = \lambda_3/(2\lambda_1+\lambda_3) \qquad P_{43} = \lambda_3/(\lambda_1+\lambda_2+\lambda_3)$$
$$P_{14} = 2\lambda_1/(2\lambda_1+\lambda_2) \qquad P_{25} = 2\lambda_1/(2\lambda_1+\lambda_3) \qquad P_{45} = \lambda_2/(\lambda_1+\lambda_2+\lambda_3)$$
$$P_{53} = \lambda_3/(\lambda_1+\lambda_3) \qquad P_{57} = \lambda_1/(\lambda_1+\lambda_3) \qquad P_{73} = 1$$

The result, after substitutions and simple algebraic manipulations, is:

$$P_3 = 1 - [2\lambda_1/(2\lambda_1+\lambda_2)][\lambda_1/(\lambda_1+\lambda_2+\lambda_3)] \qquad (4.20)$$

As expected, the second term in the equation above is just P_6, i.e.

$$P_6 = P_{14}P_{46}$$

As an example, consider $\lambda_1 = \lambda_2 = \lambda$ and let $\delta = \lambda_3/\lambda$ be the detection-to-failure rate ratio. The coverage factor becomes

$$P_3 = 1 - (2/3)[1/(2+\delta)] \qquad (4.21)$$

Table 4.1 shows the strong dependence of c on δ. Since typical MTBFs are on the order of 10^2 to 10^4 hours, whereas detection times range from fractions of a second to possibly (very conservatively) minutes, it is obvious that extremely high coverage can be achieved using dualized components of only moderate quality or reliability.

Detection-to-Failure Rate Ratio	Fraction of Undetected Failures
10^0	$.222222*10^0$
10^1	$.555555*10^{-1}$
10^2	$.653595*10^{-2}$
10^3	$.665336*10^{-3}$
10^4	$.666533*10^{-4}$
10^5	$.666653*10^{-5}$
10^6	$.666665*10^{-6}$
10^7	$.666666*10^{-7}$

Fraction of Undetected Failures as a Function of the Detection-to-Failure Rate Ratio
Table 4.1

This coverage model, which assumes that all second failures result in an uncovered state, is a conservative approximation of the real situation. This turns out not to be a problem however, because despite conservative modeling, the resulting coverage values are sufficiently high that uncovered failures contribute only insignificantly to the total accident rate.

4.3 Incorporation of Human Error Rate into the Model

Under both the current control systems and the ATCS, the human operator is a key element of the system, and the human error rate is a key parameter in predicting system accident rate. Attempting to predict human error rate based on psychological models is complicated at best, and unlikely to produce data which is useful in determining *which* of the human errors will actually result in an accident. By the same token, attempting to gather data on operator mistakes, such as paperwork violations, and to extract meaningful information is also a questionable exercise.

Since the desired parameter is really *the rate of human error that results in accidents*, then the best available source is the system accident statistics themselves. This data can be extracted from any compilation of railroad accidents desired, as long as

1. The accidents extracted are related to control system operations
2. The definition of "accident" is consistent across various applications of the model

Thus, the human error rate (e.g., errors per operator-hour that result in accidents) is simply the number of human caused accidents over some time interval divided by the total number of operator-hours put into the system over that same time interval. "Operators" means engineers and dispatchers.

The value of human error rate derived in this way will probably vary widely from derivation to derivation. Considered in a vacuum, the value provides no useful information. But when applied in a comparative analysis, to the region from which the original accident statistics were extracted, it provides an accurate linkage between the accidents that actually occurred in the past and those that can be expected to occur under ATCS.

The ATCS accident rate prediction can be done in two ways. The first way sums human accidents in all accident categories to generate a composite human error rate, and then applies that rate to the ATCS hardware chains. The second way deals with each accident category one-by-one, effectively generating a different human error rate for each accident category, using those human error rates to calculate the predicted accident rate for each category and then summing the results across all accident categories.

The latter approach provides more visibility into the way that the ATCS deals with each specific type of accident hazard. However, it requires sorting of the accidents into the

proper categories, which introduces the philosophical question of which categories ought really to be considered as part of the control system.

In both cases, the number of operator-hours is derived from the average number of trains on the region and cancels with the number of trains in most of the formulas. Thus the model is relatively insensitive to manipulations of train density in the region.

Finally, there is the question of whether the human operator is going to exhibit the same rate of critical errors under ATCS as under the current systems. On one hand, he may well will be under less stress with ATCS (no need to resolve overlaps himself, no need to commit the total situation to memory and, in general, a more relaxed atmosphere). On the other hand, he may be given a greater workload to handle, and he will acquire less manual train control experience and thus be less sharp when operating in the voice backup mode, the situation where errors really hurt. Of course he will rarely have to control more than one train at a time manually. We have eschewed speculation and assumed that the human operator is going to exhibit the same rate of critical errors under ATCS as under the current systems.

4.4 Other Modeling Considerations

4.4.1 Backup Operating Modes

Nominally, when a hardware item is not operative, control is effected by a voice dialog between the train engineer and the dispatcher working that train. Unavailability of hardware on-board the train produces exposure to errors of the engineer and the related dispatcher. Unavailability of a base station produces exposure to a number of engineers equal to the number of trains within the range of that base station plus the dispatcher working that area. The affected trains no longer have the enforcement protection of Level 30 operation.

An alternative backup mode has been defined that retains Level 30 enforcement protection for failures of certain elements in the digital data communications network, namely the Cluster Controller (CC), the Base station (BCP), and the Mobile Communications Package (MCP) on-board the train. By using the dispatcher and engineer to relay strings of data via the voice radio, the function of these hardware elements can be performed (although inefficiently — a dispatcher would not want to handle more than one train at time using this method). If the vital elements that generate and consume the data encode it in manner similar to that done for the digital data transmissions then errors inserted by the dispatcher and engineer will be detected. This approach is called Voice Level 30. The ability to select this alternative is incorporated into the spreadsheet implementation of the safety model.

4.4.2 Communications Network

A reliability model of the elements of the communications network between the CDC/FEP and the Base Station is complex and highly specific to each regional configuration. These elements are not addressed explicitly by this model because a previous study[1] has shown that network hardware failures and atmospheric outages on the microwave system have a minimal effect on the system accident rate. This is due to the fact that there are sufficient alternative data paths (provided by some combination of "backfeed" over a captive microwave network, leased lines and dial-up lines) such that a failure in the network is not likely to impact more than a single Base Station. The effect of failures in these intermediate communications elements can be incorporated, if desired, as a lower MTBF of the Base Station.

4.4.3 Radio Coverage and Resource Status Monitoring

The ATCS operating concept does not mandate that all track be monitored for integrity, that all switches have their positions monitored centrally or that all track be within radio coverage of the data communications system.

The percentage of monitored track and switches of both the current system and the ATCS has to be reflected in the model in order to map current system accidents into ATCS accidents in the proper way. For example, the number of accidents resulting from the inability to detect loss of track integrity will probably remain unchanged if the percentage of unmonitored territory under ATCS remains the same as it was under a previous system. If however, more territory is monitored under ATCS, then there should be a proportional decrease in accidents, and vice versa.

The percentage on monitored track and switches that are *within* ATCS radio coverage is also a required parameter, as the set of hardware failures that expose the system to human error is different when under radio coverage than when outside radio coverage.

4.4.4 Maintenance and Repair Characteristics

In the context of the ATCS safety model, mean time to repair (MTTR) means the average time to return a required ATCS element (such as a base station) to operational status, *or* the average time to remove a non-required element (such as a train) from active participation in the ATCS control process.

If the system contains a known inoperative element, then some trains, by definition, are being controlled in a backup mode over a voice radio link. If the inoperative element is a fixed resource, e.g., a base station, then until it is *repaired*, all trains traversing its jurisdiction will be required to use the backup mode. If the inoperative element is a moving resource, e.g., a train, then it suffices merely to *remove* it from active participation in the

[1] Safety Analysis of ARES.

system, since no other resource depends on it for control support. Removal can be accomplished either by stopping on a siding to wait for repair or by travelling to some yard for repair, at which point the need for control of that train ceases to exist. Actual repair of the train hardware is not the issue. The actual density of trains on the system is assumed to be unaffected by such occasional removals.

The scheduled maintenance cycle for various equipments can play a role in detecting latent failures in vital equipment that could lead to an uncovered failure situation. The effect of such preventative maintenance is to provide a relatively slow return transition from failure state M of a chain to failure state M-1. These transitions have not been included in the model because they reflect only an insignificant improvement of the uncovered failure cases, which are themselves already insignificant compared to the dominant effect of the residual human errors.

4.5 Chain Elements

This subsection provides a brief description of the makeup of the elements that appear in the various chain formulas in the model. The components of these elements are either basic ATCS hardware items or groups of such items collectively accomplishing a certain function in a manner that does not justify individual treatment. The specification of the basic MTBF inputs to the model is discussed in Section 5.1.1. The formulas used for combining the individual MTBFs of hardware items into a composite MTBF for the chain element can be found in the Appendix.

A covered failure of a vital element or (the implicitly covered) failure of a non-vital element exposes the system to the possible effects of an error on the part of one or more human operators. These situations are combined in to a number of composite chains that are applied to the different hazard categories. In addition, an uncovered failure of a vital element (CDC/FEP, OBC, Tachometer and WIU) can result in an accident without any operator involvement. These situations are each represented by a single chain.

Central Dispatch Computer / Front End Processor

The Safety System portion of the Central Dispatch Computer and its gateway to the digital network, the Front End Processor, have been combined into a single entity which has a vital section, assumed duplex in our model, and a non-vital simplex section, connected in series. The CDC participates in all train–dispatcher transactions and in all train–WIU transactions, except when the train is out of data radio coverage.

Cluster Controller

This is a basic ATCS hardware element which manages a portion of the groundline / microwave network that connects the CDC/FEP to the Base Stations (and to some of the WIUs). It is not vital in that it does not generate or process messages, so it is assumed to be simplex. The Cluster Controller is not required in the Voice Level 30 backup mode.

Base Communication Package

This component incorporates the Base Radio and the Base Station Controller, in a series configuration. This is a non-vital component and is not required in the Voice Level 30 backup mode.

Mobile Communication Package

This non-vital component on-board the train comprises two basic hardware elements: the Mobile Radio and the Communications Management Unit. This equipment is not required in the Voice Level 30 backup mode.

Wayside Interface Unit

This entity incorporates a non-vital element, the Mobile Radio (or the Base Radio in "dark" territory) and a vital part, assumed to be implemented as duplex, comprising the actual Wayside Interface Unit, the Wayside Device Controller and the Communications Management Unit.

On-Board Computer

This is the vital on-train component responsible for the enforcement of movement authorities. It is assumed to be implemented as duplex.

Transponder Interrogator

This basic element is non-vital, serving to calibrate the dualized tachometer's location indication.

Tachometer

The tachometer is used to provide train location information between transponder fixes and thus it is a vital piece of equipment. Two healthy tachometers are required to maintain Level 30 operation.

5 Applying of the Model

The analytical ATCS safety model described in section 4 was implemented as an Excel spreadsheet to provide ease in assessing the impact of implementing ATCS on a given operating region. Using the model involves the specification of the model input parameters which are described in Section 5.1 and proper interpretation of the results, discussed in Section 5.2.

5.1 Inputs

Information is input to the model in Blocks 1 through 6 of the spreadsheet. Each of these blocks contains an input status message that indicates whether specified input values are improper (e.g., negative or zero), or whether required values have not be specified.

5.1.1 Hardware Failure Rates

The failure rates for the basic ATCS hardware elements, specified as Mean Time Between Failure in hours, are input in Block 4 of the spreadsheet (see Appendix). Those elements are:

1. Base Radio — This is the *base station radio* listed in Section 3.1.1 of ATCS Specification 230.

2. Base Station Controller — This is the hardware item that supports the remaining functions listed in Section 3.1.1 of ATCS Specification 230.

3. Mobile Radio — This is the radio listed in Section 3.1.1 of ATCS Specification 210.

4. Communications Management Unit (CMU) — This is the hardware item that supports the remaining functions listed in Section 3.1.1 of ATCS Specification 210.

5. WIU — This is a hardware item that comprises the Wayside Interface Unit and Device Controllers described in ATCS Specification 530, and the Communications Management Unit functions of item 4 above. This is a vital entity and is therefore assumed to implemented as duplex. The model expects the input value of MTBF to be for the total of all the redundant parts.

6. CDC/FEP — The Safety System portion of the Central Dispatch Computer (ATCS Specification 400) and the Front End Processor (ATCS Specification 220) have been combined into a single entity for modeling purposes. This item has a vital section that is assumed to be duplex, and a non-vital section that is simplex. The model expects the input value of MTBF for the vital section to be for the total of all the redundant parts in the vital section.

7. Cluster Controller — This item represents the functions defined in ATCS Specification 225.

8. On–Board Computer — This item represents the functions described in Section 3.2.3 of ATCS Specification 300. This is a vital entity and is assumed to be implemented as duplex. The model expects the input value of MTBF to be for the total of all the redundant parts.

9. Tachometer — The locomotive will have two tachometers on–board. The MTBF specified for this item is for a single tachometer (or odometer) unit.

10. Interrogator — This item represents the functions described in ATCS Specification 335.

Block 3 of the spreadsheet combines sets of these basic units to generate a calculated MTBF for each of the main model chains. These calculated values can be overridden in Block 3. This allows a direct input of a chain MTBF value without having to manipulate the MTBFs of the basic elements in Block 4.

5.1.2 Repair Rates

Mean Time To Repair (MTTR) for the set of hardware items in a chain is specified, in hours, in Block 3 of the spreadsheet. The interpretation of MTTR, in the context of the ATCS safety model is given in Section 4.4.4.

5.1.3 Coverage

Coverage values are generated in Block 1 of the spreadsheet. Coverage for vital elements is calculated by using the formulation developed in Section 4.2. The MTBFs used in the formula are extracted from Block 4 of the spreadsheet. Two values must be specified in Block 1: (1) The minimum interval at which comparisons between the two halves of the device are executed (detection times), and (2) the probability that near-coincident failures (i.e., failures occurring closer together in time than the minimum detection interval) in each half of the vital item will be so similar as to fool the comparison mechanisms used for error detection.

Coverage for non-vital items is defined as being equal to 1, since hardware failures of these items cannot by themselves cause undetected erroneous information to enter the system. The Cluster Controller, Base Station and Mobile Radio do not generate or consume control information, they only transfer it. Errors in data transfers are covered by the cyclic redundancy checks. The probability of undetected errors occurring via this route has been estimated, by Arinc, to be less than 10^{-16}. Thus the coverage ($> 1–10^{-16}$) is effectively 1 for these devices. In addition, this coverage is not affected by equipment MTBFs or detection time parameters as is the coverage value calculated for vital items.

Finally, interrogator location fixes are compared with dead reckoning information from *two* tachometers. Any disagreement among the three measurements will cause the train to revert to the voice radio backup mode. Since all three items must fail at once in order to inject erroneous train location information into the system, the coverage of the interrogator is effectively equal to one. (Between interrogator fixes coverage the tachometers is calculated like that of the other duplex vital elements.)

It is also possible in Block 1 to override the calculated coverage values. This allows the user to examine sensitivity to coverage values directly, without having to manipulate the MTBFs of the basic elements in Block 4.

5.1.4 Regional Configuration

Information about the control region configuration is input in Blocks 2, 3 and 5 of the spreadsheet.

A control region is defined as having a single CDC/FEP combination. The numbers of Cluster Controllers, Base Stations and Wayside Units in the region are specified in Block 3. The numbers of train based units appear in Block 3, based upon operator information from Block 5A.

Block 5 allows the specification of the number of operators in the region both under the current operation (Block 5B) and under the assumed ATCS operation (Block 5A). A train is assumed to have one responsible operator, namely the engineer. The average number of trains (hence the average number engineers) and the average number of dispatchers under current operation must be specified in Block 5B. These numbers are assumed to be the same for ATCS operation unless specified differently in Block 5A.

Two other values in Block 5 are used in one of the alternate calculation of system accident rate. The first is the average number of trains operating under joint ATCS authorities. This is assumed to be zero unless specified. The second is a composite human error rate (errors that result in accidents per person per hour) based upon the average number of operators currently in the region and the current accident statistics for the region. This number can be overridden directly to see the effect of human error rate changes.

Block 2 requires input of the percentages of track and switched that are monitored under both the current regional configuration and the assumed ATCS configuration, and the percentage of monitored track and switches that are under radio coverage under the assumed ATCS configuration.

5.1.5 Current System Accident Statistics

Current system accident statistics by Federal Railroad Administration accident cause codes are inserted in Block 6 of the spreadsheet. The data entered into the sheets in this report are hypothetical and do not represent any specific railroad. These data are chosen to

demonstrate the wide range of potential benefits that accrue from the analysis of the current accident data. To apply the analysis to a specific railroad, data would need to be obtained from that railroad.

If total accident rate data is specified in the upper portion of Block 6, then the spreadsheet will use the composite human error rate generated in Block 5B to predict the ATCS accident rate. This allows the model to be used when a detailed breakdown of accidents by hazard is not available. If these inputs are left blank, then the spreadsheet will use the accident data itemized by hazard in the lower portion of Block 6. Depending upon the actual distribution of accidents by hazard, the results of these two approaches may differ significantly.

5.1.6 Operating Policies

The Voice Level 30 switch allows the user to specify whether such a backup operating mode is to be considered. Voice Level 30 simply substitutes voice radio communication between a dispatcher and train engineer for the digital data link, if that link becomes inoperative due to a hardware failure. The messages are presumed to still be encoded with the appropriate redundancy checks, so that human transmission errors will be caught.

There are two "policy" switches which allow the user to specify whether fouling detection at a switch is considered to be part of the switch itself or part of the normal track block circuit.

Finally there is a policy switch that specifies how to treat the question of a vandal stealing a train. If the switch is off, then the model assumes that if the vandal succeeds in starting the train that the normal enforcement mechanisms (given the lack of a movement authority) will prevent him from going anywhere (unless some of the ATCS hardware is not working properly). If the switch is on, then the the model assumed that the vandal succeeds in moving the train. The probability that this action results in an accident is taken from the adjacent policy value.

5.2 Interpreting the Results

The results are presented in two blocks at the bottom of the spreadsheet. The block entitled Accident Rate Calculations gives a breakdown of the components of the predicted ATCS accident rate per year by (1) human error when in voice radio backup mode, (2) undetected failure of vital elements, and (3) human error when operating under joint

authorities[1]. The total predicted accident rate is also given, as well as the ratio of the predicted ATCS accident rate to the actual current accident statistics (i.e., the Improvement Factor).

The model will produce a reasonable result, even for unrealistic input values, i.e., MTBFs of hours and MTTRs of days. If selected MTBFs are reduced to minutes, then the coverage for vital elements could be reduced to the point where the ATCS will look worse than the current systems. This is to be expected, because such a scenario would introduce a great deal of equipment that is able to cause a significant number of accidents due to its own undetected failures, a situation that does not now exist.

However, over any reasonable set of input values—those MTBFs that can be confidently achieved with available hardware technologies and manufacturing techniques, coverage attainable by properly implemented duplex hardware, and MTTRs on the order of hours—the ATCS will always look better that the current systems. This is because the ATCS conflict checking and enforcement mechanisms greatly reduce the exposure of the system to the effects of human errors. The system is exposed to the possibility of human error only in those cases when the ATCS equipment is not working. Since only a small percentage of the equipment is down, on average, at any one time, the amount of human exposure for those hazard categories that are addressed by ATCS is one to two orders of magnitude less than under the current systems.

Almost all current control system related accidents are due to human error, so reducing the human exposure eliminates most of the accidents that now occur. Those few that currently result from signal system failures will also be eliminated, since this hardware will no longer be critical even it is kept in place. Undetected failures of ATCS hardware will contribute accidents that were not possible in any of the current systems. But for any ATCS hardware implemented so as to obtain achievable levels of coverage, this number is insignificant compared to the number of human caused accidents that are eliminated.

When the model uses current accident data itemized by hazard, the value of the improvement factor is heavily dependent upon the distribution of those accidents. There are two instances, however, that are not included in the analysis: first, when any current accident cause, like false proceed, is eliminated by ATCS and second, when the accident category, like derailed train on adjacent track, is unaffected by ATCS. The first instance, if included, could, under certain circumstances, drive the improvement factor to infinity. The second instance creates an argument of whether or not to include in the analysis accidents which ATCS has no material effect opon. If these accidents were included, then the analysis would no longer be specific to ATCS but would address a broader issue of train control. However, if the user is tempted to ignore this distinction, these types of accidents can be included in the analysis by inserting a number in the appropriate category. Both

[1] In the case where the accidents inputs are not itemized by hazard this is shown explicitly, when accident inputs are itemized, this value shows up in the itemization in Block 6.

these categories are fully defined in the appendices entitled "Table of Hazard Categories and Mappings".

The Block entitled Relative Contribution by Chain provides a chain–by–chain breakdown of the predicted ATCS accident rate using the human error rate calculated in Block 5B. These figures, when normalized, give a relative indication of the contribution of each hardware item to the accident rate (due to the combination of an item's failure causing exposure to human errors and causing undetected errors on its own). This information can be used to determine where the greatest safety benefit will be obtained by enhancing the reliability of hardware. Making the most reliable element even more reliable will generally show very little safety improvement, because it is the least reliable element that drives the system safety.

By adjusting the various accident categories, three substantially different improvement factors were developed, as shown in the spreadsheet layouts A through C in the appendix. These results were obtained simply by adjusting the current accidents. Improvement factors for all railroads will fall somewhere in that range depending upon the type of current accidents.

APPENDIX

SPREADSHEET IMPLEMENTATION

This appendix provides three snapshots of the Excel spreadsheet used to implement the safety model. Following this, the formulas used on the spreadsheet are enumerated, as is the hazard categorization used for the specification of current system accident data.

The three spreadsheet layouts A through C shown in the appendix contain realistic values for all inputs, without being specific to any particular railroad. The examples correspond to three different scenarios, using the same conservative hardware failure rates, coverages and mean times to repair, but considering three distinct current accident groups.

ATCS SAFETY ANALYSIS WORKSHEET — C. S. DRAPER LABORATORY, CAMBRIDGE, MA

1–COVERAGE CALCULATIONS

Input Values are OK

Coverage Inputs	MTBF of Duplex Part	MTBF of Simplex Part	Detection Time (in sec)	Probability of Similar Failures	Calculated Coverage	Specified Coverage
CDC/FEP	10,000	2,000	5	1	0.99999996	
Cluster Controller					1	
Base Station					1	
WIU	16,000	5,000	5	1	0.999999967	
Mobile Radio					1	
OBC	10,000		5	1	0.999999861	
Tachometer	30,000		5	1	0.999999954	
Interrogator					1	

2–SYSTEM CONFIGURATION DATA

Percentage of track monitored	
Current System	0.50
ATCS	0.80
Percentage of switches monitored	
Current System	0.3
ATCS	0.8
Percentage of monitored track and switches that are in radio coverage *under ATCS*	0.50

Configuration values are OK

3–MTBFs AND MTTRs FOR CHAINS

Chain Inputs are OK

Chain	Calculated MTBF	Specified MTBF (in hours)	MTTR (in hours)	Num of elements (under ATCS)
CDC/FEP	1,429		1	1
Cluster Controller	5,000		4	10
Base Station	3,077		6	240
Wayside Unit	3,077		4	600
Mobile Communication	4,167		6	157
On-Board Computer	5,000		6	157
Tachometer	15,000		6	157
Interrogator	5,000		6	157

This table calculates MTBFs (in hours) for the chains from the baseline MTBFs (Table 3).
If a "specified MTBF" value (not = 0) is entered, the MTBF calculation will use this value.
(MTTR*C/MTBF, P(state 0) and Chain calculations are used in the accident rate formulas.)

INTERMEDIATE CALCULATIONS

MTTR*C/MTBF	P(State 0)
0.00070000	0.99930049
0.00080000	0.99203509
0.00195000	0.62653898
0.00130000	0.45863829
0.00144000	0.79778401
0.00120000	0.82837691
0.00040000	0.93914308
0.00120000	0.82837689

Chain Formulas, Functions and Flags

"Chains"	0.00765553
"InCovChains"	0.00894390
"OutOfCovChains"	0.00552130
"EngineerChains"	0.00765553
"DispChains"	0.03434051
"UnmonTrack"	0.40000000
"MonTrack"	0.01157216
"UnmonSwitch"	0.28571429
"MonSwitch"	0.01928694
"VL30Flag"	off

Total human accidents from itemization	8
Total non–human accidents from itemization	0

4–MTBFs FOR INDIVIDUAL ELEMENTS

MTBF Inputs are OK

Base Radio	5,000	
Station Controller	8,000	
Mobile Radio	5,000	
CMU	25,000	
WIU (vital part)	8,000	Total for redundant vital parts
CDC/FEP (vital part)	5,000	Total for redundant vital parts
CDC/FEP (simplex part)	2,000	
Cluster Controller	5,000	
On-Board Computer	5,000	Total for redundant vital parts
Tachometer	30,000	For single unit
Interrogator	5,000	

Baseline MTBFs are in hours. MTBF must be greater than zero.
The base radio serves as the simplex part of the wayside package.

5A–ATCS HUMAN OPERATOR DATA

Inputs are OK

Ave number of trains per region under ATCS	157	"Trains"
Equal to the current system value unless specified here		
Ave number of dispatchers per region under ATCS	35	"Disp"
Equal to the current system value unless specified here		
Ave number of trains under joint authorities in ATCS		"Joint"

5B–CURRENT SYSTEM HUMAN OPERATOR DATA

Inputs are OK

Ave number of trains per region in present system	157	"TrainsNow"
Ave number of dispatchers per region in present system	35	"DispNow"
Calculated composite human error rate / person / hour	2.3782E-06	"HumanErrorRate"
If a specific value is desired, enter it here.		

SAMPLE A

ATCS SAFETY ANALYSIS WORKSHEET C. S. DRAPER LABORATORY, CAMBRIDGE, MA

6-CURRENT ACCIDENT DATA	Over	2	Years	Over	1	Regions	*Accident Inputs are OK* *Policy Inputs are OK*

Total human caused accidents when detailed categorization is not used		Total Current Accidents/Region/Year	4.0000
Total of non-human related accidents when detailed categorization is not used		Current Human Caused Accidents/R/Y	4.0000

<<These values must be set to zero or blank for categorization to be used!>>

Accident Category	Voice Level 30 Switch	Policy Switch	Policy Value	Current Accidents	Under ATCS	ATCS/Current
200 Fixed signal improperly displayed (defective)				0		
201 Radio communication equipment failure				0		
202 Other communication equipment failure				0		
203 Block signal displayed false proceed				0		
204 Interlocking signal displayed false proceed				0		
205 Automatic cab signal displayed false proceed				0		
206 Automatic cab signal inoperative				0		
207 Automatic train-stop device inoperative				0		
208 Automatic train control device inoperative				0		
209 Other signal and communication failures				0		
502 Failure to properly secure engine(s) (railroad employee)				0		
506 Failure to properly secure engine(s) or car(s) (non-railroad employee)				0		
509 Use of brakes, other				0		
510 Impairment of efficiency and judgment because of drugs or alcohol				0		
511 Incapacitation due to injury or illness				0		
512 Employee restricted in work or motion				0		
513 Employee asleep				0		
515 Employee physical condition, other				0		
519 Fixed signal improperly displayed				0		
52A Block signal, failure to comply			0.5	0		
52B Interlocking signal, failure to comply			"	0		
52C Automatic cab signal, failure to comply			"	0		
52D Automatic cab signal cut out			"	0		
52E Automatic train-stop device cut out			"	0		
52F Automatic train control device cut out			"	0		
520 Fixed signal, failure to comply			"	0		
521 Flagging, improper or failure to flag				0		
522 Flagging signal, failure to comply			"	0		
526 Radio communication, failure to comply				0		
527 Radio communication, improper				0		
528 Radio communication, failure to give/receive				0		
529 Flagging, fixed, hand and radio signals, other				0		
530 Car(s) shoved out and left out of clear		track		1	0.20578608	0.20578608
531 Cars left foul		Switch		1	0.20578608	0.20578608
533 Failure to stop train in clear				0		
535 Instruction to train/yard crew improper				0		
536 Motor car or on-track equipment rules, failure to comply				0		
537 Movement of engine(s) or car(s) without authority, (railroad employee)				0		

541	Special operating instruction, failure to comply	0		
542	Train order or timetable authority, failure to comply	0		
543	Train orders, radio, error in preparation, transmission or delivery	0		
544	Train orders, written, error in preparation, transmission or delivery	0		
549	Rules and instruction, other	2	0.69466403	0.34733201
555	Train outside yard limits under clear block, excessive speed	0		
559	Speed, other	0		
560	Spring Switch not cleared before reversing	0		
561	Switch improperly lined	1	0.20578608	0.20578608
562	Switch not latched or locked	1	0.20578608	0.20578608
563	Switch previously run through	0		
569	Use of switches, other	0		
599	Other train operation/human factors	2	1.00765553	0.50382776

ACCIDENT RATE CALCULATIONS		*All Inputs are OK*
Human error chains	Itemized	1.2627E+00
Wayside unit chain		5.6957E-05
Uncovered OBC		3.8158E-05
Uncovered tachometer		4.2431E-06
Uncovered CDC/FEP		2.4316E-07
Accidents under joint operations		(Included via itemization)
Total Accidents / Year		**1.2628**
Improvement factor over current system		**3.17**

RELATIVE CONTRIBUTIONS BY CHAIN
(Using Aggregate Human Error Rate)

	(Normalized)	(Unnormalized)
CDC/FEP	0.0503	0.00230280
Cluster Controller	0.0607	0.00278051
Base Station	0.3088	0.01414615
Wayside Unit	0.0012	0.00005696
Mobile Communication	0.1946	0.00891606
On-Board Computer	0.1645	0.00753393
Tachometer	0.0563	0.00257991
Interrogator	0.1636	0.00749578
Totals	1	0.0458

ADDITIONAL NOTES

Section 1 —
This section calculates the coverages for various ATCS elements from the inputs shown. Duplex and simplex MTBFs are derived from Table 3.
MTBFs are in hours, detection time is in seconds. Non-vital elements, such as radios, are assumed to have a coverage of 1.
If a "specified coverage" (not = 0) is entered, the coverage calculation will use this value. This feature can be used to test the sensitivity to a particular coverage value directly.
Both "Detection Time" and "Probability of Similar Failures" must be specified.

Section 2 —
Monitored switches are those where the position of the switch transmitted to the dispatch center or directly to the cab.
Monitored track is that for which the physical integrity is measured by track circuits, slide fences, etc.

Section 6 —
If the Voice Level 30 Switch is set to 0, blank,"no",or "off" then VL30 is not used as a backup mode, otherwise it is.
The policy value for 52A-F, 520, and 522 moves the corresponding outputs along a range from "n/a" (not occurring at all under ATCS) to EngineerChains. The value should be between 0 and 1; 0 corresponds to n/a, 1 to EngineerChains.
If the policy switches for 530 or 531 are set to "switch" the formula uses the "switch" percentages from Section 2.
Otherwise the formula uses the "track" percentages from Section 2.

SAMPLE B

ATCS SAFETY ANALYSIS WORKSHEET — C. S. DRAPER LABORATORY, CAMBRIDGE, MA

1–COVERAGE CALCULATIONS

Input Values are OK

Coverage Inputs	MTBF of Duplex Part	MTBF of Simplex Part	Detection Time (in sec)	Probability of Similar Failures	Calculated Coverage	Specified Coverage
CDC/FEP	10,000	2,000	5	1	0.99999996	
Cluster Controller					1	
Base Station					1	
WIU	16,000	5,000	5	1	0.999999967	
Mobile Radio					1	
OBC	10,000		5	1	0.999999861	
Tachometer	30,000		5	1	0.999999954	
Interrogator					1	

2–SYSTEM CONFIGURATION DATA

Percentage of track monitored	
Current System	0.50
ATCS	0.80
Percentage of switches monitored	
Current System	0.3
ATCS	0.8
Percentage of monitored track and switches that are in radio coverage *under ATCS*	0.50

Configuration values are OK

3–MTBFs AND MTTRs FOR CHAINS

Chain Inputs are OK

Chain	Calculated MTBF	Specified MTBF (in hours)	MTTR (in hours)	Num of elements (under ATCS)
CDC/FEP	1,429		1	1
Cluster Controller	5,000		4	10
Base Station	3,077		6	240
Wayside Unit	3,077		4	600
Mobile Communication	4,167		6	157
On-Board Computer	5,000		6	157
Tachometer	15,000		6	157
Interrogator	5,000		6	157

This table calculates MTBFs (in hours) for the chains from the baseline MTBFs (Table 3).
If a "specified MTBF" value (not = 0) is entered, the MTBF calculation will use this value.
(MTTR*C/MTBF, P(state 0) and Chain calculations are used in the accident rate formulas.)

INTERMEDIATE CALCULATIONS

MTTR*C/MTBF	P(State 0)
0.00070000	0.99930049
0.00080000	0.99203509
0.00195000	0.62653898
0.00130000	0.45863829
0.00144000	0.79778401
0.00120000	0.82837691
0.00040000	0.93914308
0.00120000	0.82837689

Chain Formulas, Functions and Flags

"Chains"	0.00765553
"InCovChains"	0.00894390
"OutOfCovChains"	0.00552130
"EngineerChains"	0.00765553
"DispChains"	0.03434051
"UnmonTrack"	0.40000000
"MonTrack"	0.01157216
"UnmonSwitch"	0.28571429
"MonSwitch"	0.01928694
"VL30Flag"	off

Total human accidents from itemization	21
Total non–human accidents from itemization	0

4–MTBFs FOR INDIVIDUAL ELEMENTS

MTBF Inputs are OK

Base Radio	5,000	
Station Controller	8,000	
Mobile Radio	5,000	
CMU	25,000	
WIU (vital part)	8,000	Total for redundant vital parts
CDC/FEP (vital part)	5,000	Total for redundant vital parts
CDC/FEP (simplex part)	2,000	
Cluster Controller	5,000	
On-Board Computer	5,000	Total for redundant vital parts
Tachometer	30,000	For single unit
Interrogator	5,000	

Baseline MTBFs are in hours. MTBF must be greater than zero.
The base radio serves as the simplex part of the wayside package.

5A–ATCS HUMAN OPERATOR DATA

Inputs are OK

Ave number of trains per region under ATCS	157	"Trains"
Equal to the current system value unless specified here		
Ave number of dispatchers per region under ATCS	35	"Disp"
Equal to the current system value unless specified here		
Ave number of trains under joint authorities in ATCS		"Joint"

5B–CURRENT SYSTEM HUMAN OPERATOR DATA

Inputs are OK

Ave number of trains per region in present system	157	"TrainsNow"
Ave number of dispatchers per region in present system	35	"DispNow"
Calculated composite human error rate / person / hour	6.2429E-06	"HumanErrorRate"
If a specific value is desired, enter it here:		

SAMPLE B

ATCS SAFETY ANALYSIS WORKSHEET C. S. DRAPER LABORATORY, CAMBRIDGE, MA

6-CURRENT ACCIDENT DATA	Over	2	Years	Over	1	Regions	*Accident Inputs are OK* *Policy Inputs are OK*

Total human caused accidents when detailed categorization is not used	
Total of non-human related accidents when detailed categorization is not used	
<<These values must be set to zero or blank for categorization to be used!>>	

Total Current Accidents/Region/Year	10.5000
Current Human Caused Accidents/R/Y	10.5000

Accident Category	Voice Level 30 Switch	Policy Switch	Policy Value	Current Accidents	Under ATCS	ATCS/Current
200 Fixed signal improperly displayed (defective)				0		
201 Radio communication equipment failure				0		
202 Other communication equipment failure				0		
203 Block signal displayed false proceed				0		
204 Interlocking signal displayed false proceed				0		
205 Automatic cab signal displayed false proceed				0		
206 Automatic cab signal inoperative				0		
207 Automatic train-stop device inoperative				0		
208 Automatic train control device inoperative				0		
209 Other signal and communication failures				0		
502 Failure to properly secure engine(s) (railroad employee)				1	0.00765553	0.00765553
506 Failure to properly secure engine(s) or car(s) (non-railroad employee)				0		
509 Use of brakes, other				0		
510 Impairment of efficiency and judgment because of drugs or alcohol				0		
511 Incapacitation due to injury or illness				0		
512 Employee restricted in work or motion				0		
513 Employee asleep				0		
515 Employee physical condition, other				0		
519 Fixed signal improperly displayed				0		
52A Block signal, failure to comply			0.5	0		
52B Interlocking signal, failure to comply			"	0		
52C Automatic cab signal, failure to comply			"	0		
52D Automatic cab signal cut out			"	0		
52E Automatic train-stop device cut out			"	0		
52F Automatic train control device cut out			"	0		
520 Fixed signal, failure to comply			"	2	0.00765553	0.00382776
521 Flagging, improper or failure to flag				0		
522 Flagging signal, failure to comply			"	0		
526 Radio communication, failure to comply				0		
527 Radio communication, improper				0		
528 Radio communication, failure to give/receive				0		
529 Flagging, fixed, hand and radio signals, other				0		
530 Car(s) shoved out and left out of clear		track		1	0.20578608	0.20578608
531 Cars left foul		Switch		0		
533 Failure to stop train in clear				2	0.01531106	0.00765553
535 Instruction to train/yard crew improper				3	0.10302153	0.03434051
536 Motor car or on-track equipment rules, failure to comply				0		
537 Movement of engine(s) or car(s) without authority, (railroad employee)				1	0.00765553	0.00765553

541 Special operating instruction, failure to comply	0		
542 Train order or timetable authority, failure to comply	2	0.01531106	0.00765553
543 Train orders, radio, error in preparation, transmission or delivery	3	0.10302153	0.03434051
544 Train orders, written, error in preparation, transmission or delivery	0		
549 Rules and instruction, other	0		
555 Train outside yard limits under clear block, excessive speed	3	0.02296658	0.00765553
559 Speed, other	0		
560 Spring Switch not cleared before reversing	0		
561 Switch improperly lined	1	0.20578608	0.20578608
562 Switch not latched or locked	0		
563 Switch previously run through	2	0.40000000	0.20000000
569 Use of switches, other	0		
599 Other train operation/human factors	0		

ACCIDENT RATE CALCULATIONS		*All Inputs are OK*
Human error chains	Itemized	5.4709E-01
Wayside unit chain		5.6957E-05
Uncovered OBC		3.8158E-05
Uncovered tachometer		4.2431E-06
Uncovered CDC/FEP		2.4316E-07
Accidents under joint operations		(Included via itemization)
Total Accidents / Year		**0.5472**
Improvement factor over current system		**19.19**

RELATIVE CONTRIBUTIONS BY CHAIN (Using Aggregate Human Error Rate)	(Normalized)	(Unnormalized)
CDC/FEP	0.0503	0.00604445
Cluster Controller	0.0608	0.00729884
Base Station	0.3092	0.03713364
Wayside Unit	0.0005	0.00005696
Mobile Communication	0.1949	0.02340466
On-Board Computer	0.1642	0.01971457
Tachometer	0.0563	0.00676536
Interrogator	0.1638	0.01967642
Totals	1	0.1201

ADDITIONAL NOTES

Section 1 —
This section calculates the coverages for various ATCS elements from the inputs shown. Duplex and simplex MTBFs are derived from Table 3.
MTBFs are in hours, detection time is in seconds. Non-vital elements, such as radios, are assumed to have a coverage of 1.
If a "specified coverage" (not = 0) is entered, the coverage calculation will use this value. This feature can be used to test the sensitivity to a particular coverage value directly.
Both "Detection Time" and "Probability of Similar Failures" must be specified.

Section 2 —
Monitored switches are those where the position of the switch transmitted to the dispatch center or directly to the cab.
Monitored track is that for which the physical integrity is measured by track circuits, slide fences, etc.

Section 6 —
If the Voice Level 30 Switch is set to 0, blank,"no",or "off" then VL30 is not used as a backup mode, otherwise it is.
The policy value for 52A-F, 520, and 522 moves the corresponding outputs along a range from "n/a" (not occurring at all under ATCS) to EngineerChains. The value should be between 0 and 1; 0 corresponds to n/a, 1 to EngineerChains.
If the policy switches for 530 or 531 are set to "switch" the formula uses the "switch" percentages from Section 2.
Otherwise the formula uses the "track" percentages from Section 2.

SAMPLE C

ATCS SAFETY ANALYSIS WORKSHEET — C. S. DRAPER LABORATORY, CAMBRIDGE, MA

1–COVERAGE CALCULATIONS

Input Values are OK

Coverage Inputs	MTBF of Duplex Part	MTBF of Simplex Part	Detection Time (in sec)	Probability of Similar Failures	Calculated Coverage	Specified Coverage
CDC/FEP	10,000	2,000	5	1	0.99999996	
Cluster Controller					1	
Base Station					1	
WIU	16,000	5,000	5	1	0.999999967	
Mobile Radio					1	
OBC	10,000		5	1	0.999999861	
Tachometer	30,000		5	1	0.999999954	
Interrogator					1	

2–SYSTEM CONFIGURATION DATA

Percentage of track monitored	
Current System	0.50
ATCS	0.80
Percentage of switches monitored	
Current System	0.3
ATCS	0.8
Percentage of monitored track and switches that are in radio coverage *under ATCS*	0.50

Configuration values are OK

3–MTBFs AND MTTRs FOR CHAINS

Chain Inputs are OK

Chain	Calculated MTBF	Specified MTBF (in hours)	MTTR (in hours)	Num of elements (under ATCS)
CDC/FEP	1,429		1	1
Cluster Controller	5,000		4	10
Base Station	3,077		6	240
Wayside Unit	3,077		4	600
Mobile Communication	4,167		6	157
On-Board Computer	5,000		6	157
Tachometer	15,000		6	157
Interrogator	5,000		6	157

This table calculates MTBFs (in hours) for the chains from the baseline MTBFs (Table 3).
If a "specified MTBF" value (not = 0) is entered, the MTBF calculation will use this value.
(MTTR*C/MTBF, P(state 0) and Chain calculations are used in the accident rate formulas.)

INTERMEDIATE CALCULATIONS

MTTR*C/MTBF	P(State 0)
0.00070000	0.99930049
0.00080000	0.99203509
0.00195000	0.62653898
0.00130000	0.45863829
0.00144000	0.79778401
0.00120000	0.82837691
0.00040000	0.93914308
0.00120000	0.82837689

Chain Formulas, Functions and Flags

"Chains"	0.00765553
"InCovChains"	0.00894390
"OutOfCovChains"	0.00552130
"EngineerChains"	0.00765553
"DispChains"	0.03434051
"UnmonTrack"	0.40000000
"MonTrack"	0.01157216
"UnmonSwitch"	0.28571429
"MonSwitch"	0.01928694
"VL30Flag"	off

Total human accidents from itemization	6
Total non–human accidents from itemization	0

4–MTBFs FOR INDIVIDUAL ELEMENTS

MTBF Inputs are OK

Base Radio	5,000	
Station Controller	8,000	
Mobile Radio	5,000	
CMU	25,000	
WIU (vital part)	8,000	Total for redundant vital parts
CDC/FEP (vital part)	5,000	Total for redundant vital parts
CDC/FEP (simplex part)	2,000	
Cluster Controller	5,000	
On-Board Computer	5,000	Total for redundant vital parts
Tachometer	30,000	For single unit
Interrogator	5,000	

Baseline MTBFs are in hours. MTBF must be greater than zero.
The base radio serves as the simplex part of the wayside package.

5A–ATCS HUMAN OPERATOR DATA

Inputs are OK

Ave number of trains per region under ATCS	157	"Trains"
Equal to the current system value unless specified here		
Ave number of dispatchers per region under ATCS	35	"Disp"
Equal to the current system value unless specified here		
Ave number of trains under joint authorities in ATCS		"Joint"

5B–CURRENT SYSTEM HUMAN OPERATOR DATA

Inputs are OK

Ave number of trains per region in present system	157	"TrainsNow"
Ave number of dispatchers per region in present system	35	"DispNow"
Calculated composite human error rate / person / hour	1.7837E-06	"HumanErrorRate"
If a specific value is desired, enter it here.		

SAMPLE C

ATCS SAFETY ANALYSIS WORKSHEET C. S. DRAPER LABORATORY, CAMBRIDGE, MA

6-CURRENT ACCIDENT DATA Over 2 Years Over 1 Regions

Accident Inputs are OK
Policy Inputs are OK

Total human caused accidents when detailed categorization is not used	
Total of non-human related accidents when detailed categorization is not used	

<<These values must be set to zero or blank for categorization to be used!>>

Total Current Accidents/Region/Year 3.0000
Current Human Caused Accidents/R/Y 3.0000

Voice Level 30 Switch

Accident Category	Policy Switch	Policy Value	Current Accidents	Under ATCS	ATCS/Current
200 Fixed signal improperly displayed (defective)			0		
201 Radio communication equipment failure			0		
202 Other communication equipment failure			0		
203 Block signal displayed false proceed			0		
204 Interlocking signal displayed false proceed			0		
205 Automatic cab signal displayed false proceed			0		
206 Automatic cab signal inoperative			0		
207 Automatic train-stop device inoperative			0		
208 Automatic train control device inoperative			0		
209 Other signal and communication failures			0		
502 Failure to properly secure engine(s) (railroad employee)			0		
506 Failure to properly secure engine(s) or car(s) (non-railroad employee)			0		
509 Use of brakes, other			0		
510 Impairment of efficiency and judgment because of drugs or alcohol			0		
511 Incapacitation due to injury or illness			0		
512 Employee restricted in work or motion			0		
513 Employee asleep			0		
515 Employee physical condition, other			0		
519 Fixed signal improperly displayed			0		
52A Block signal, failure to comply		0.5	1	0.00382776	0.00382776
52B Interlocking signal, failure to comply		"	3	0.01148329	0.00382776
52C Automatic cab signal, failure to comply		"	0		
52D Automatic cab signal cut out		"	0		
52E Automatic train-stop device cut out		"	0		
52F Automatic train control device cut out		"	0		
520 Fixed signal, failure to comply		"	1	0.00382776	0.00382776
521 Flagging, improper or failure to flag			0		
522 Flagging signal, failure to comply		"	1	0.00382776	0.00382776
526 Radio communication, failure to comply			0		
527 Radio communication, improper			0		
528 Radio communication, failure to give/receive			0		
529 Flagging, fixed, hand and radio signals, other			0		
530 Car(s) shoved out and left out of clear	track		0		
531 Cars left foul	Switch		0		
533 Failure to stop train in clear			0		
535 Instruction to train/yard crew improper			0		
536 Motor car or on-track equipment rules, failure to comply			0		
537 Movement of engine(s) or car(s) without authority, (railroad employee)			0		

ATCS SAFETY ANALYSIS WORKSHEET C. S. DRAPER LABORATORY, CAMBRIDGE, MA

541 Special operating instruction, failure to comply	0	
542 Train order or timetable authority, failure to comply	0	
543 Train orders, radio, error in preparation, transmission or delivery	0	
544 Train orders, written, error in preparation, transmission or delivery	0	
549 Rules and instruction, other	0	
555 Train outside yard limits under clear block, excessive speed	0	
559 Speed, other	0	
560 Spring Switch not cleared before reversing	0	
561 Switch improperly lined	0	
562 Switch not latched or locked	0	
563 Switch previously run through	0	
569 Use of switches, other	0	
599 Other train operation/human factors	0	

ACCIDENT RATE CALCULATIONS	*All Inputs are OK*	
Human error chains	Itemized	1.1483E-02
Wayside unit chain		5.6957E-05
Uncovered OBC		3.8158E-05
Uncovered tachometer		4.2431E-06
Uncovered CDC/FEP		2.4316E-07
Accidents under joint operations		(Included via itemization)
Total Accidents / Year		**0.0116**
Improvement factor over current system		**259.00**

RELATIVE CONTRIBUTIONS BY CHAIN (Using Aggregate Human Error Rate)	(Normalized)	(Unnormalized)
CDC/FEP	0.0502	0.00172716
Cluster Controller	0.0606	0.00208538
Base Station	0.3086	0.01060961
Wayside Unit	0.0017	0.00005696
Mobile Communication	0.1945	0.00668705
On-Board Computer	0.1646	0.00565999
Tachometer	0.0563	0.00193599
Interrogator	0.1635	0.00562183
Totals	1	0.0344

ADDITIONAL NOTES

Section 1 —
This section calculates the coverages for various ATCS elements from the inputs shown. Duplex and simplex MTBFs are derived from Table 3.
MTBFs are in hours, detection time is in seconds. Non-vital elements, such as radios, are assumed to have a coverage of 1.
If a "specified coverage" (not = 0) is entered, the coverage calculation will use this value. This feature can be used to test the sensitivity to a particular coverage value directly.
Both "Detection Time" and "Probability of Similar Failures" must be specified.

Section 2 —
Monitored switches are those where the position of the switch transmitted to the dispatch center or directly to the cab.
Monitored track is that for which the physical integrity is measured by track circuits, slide fences, etc.

Section 6 —
If the Voice Level 30 Switch is set to 0, blank,"no",or "off" then VL30 is not used as a backup mode, otherwise it is.
The policy value for 52A-F, 520, and 522 moves the corresponding outputs along a range from "n/a" (not occurring at all under ATCS) to EngineerChains. The value should be between 0 and 1; 0 corresponds to n/a, 1 to EngineerChains.
If the policy switches for 530 or 531 are set to "switch" the formula uses the "switch" percentages from Section 2.
Otherwise the formula uses the "track" percentages from Section 2.

SPREADSHEET FORMULAS

$$\text{Chains} = 1 - \frac{1}{(1+\text{CDCFEP})(1+\text{CC})(1+\text{BCP})(1+\text{MCP})(1+\text{OBC})(1+\text{Tach})(1+\text{Intgr})}$$

$$\text{InCovChains} = 1 - \frac{1}{(1+\text{CDCFEP})(1+\text{CC})(1+\text{BCP})(1+\text{MCP})(1+\text{OBC})(1+\text{Tach})(1+\text{Intgr})(1+\text{WIU})}$$

{where voice level 30 is *not used* as a backup mode —
if voice level 30 is used then CC, BCP and MCP are set to zero
in Chains and InCovChains}

$$\text{OutOfCovChains} = 1 - \frac{1}{(1+\text{MCP})(1+\text{OBC})(1+\text{Tach})(1+\text{Intgr})(1+\text{WIU})}$$

$$\text{Engineer chains} = \frac{1}{\text{TrainsNow}} \text{Trains} \bullet \text{Chains}$$

$$\text{Dispatcher chains} = \frac{1}{\text{DispatchersNow}} \text{Trains} \bullet \text{Chains}$$

{where Max [Trains • Chains] = Dispatchers}

$$\text{UnmonTrackRatio} = \frac{\%\text{ track unmonitored in ATCS}}{\%\text{ track unmonitored in current system}}$$

$$\text{UnmonSwitchRatio} = \frac{\%\text{ switches unmonitored in ATCS}}{\%\text{ switches unmonitored in current system}}$$

$$\text{MonTrackRatio} = \frac{\%\text{ track monitored in ATCS}}{\%\text{ track monitored in current system}}$$

$$\text{MonSwitchRatio} = \frac{\%\text{ switches monitored in ATCS}}{\%\text{ switches monitored in current system}}$$

%Cov = % of monitored track and switches that are in radio coverage under ATCS

$$\text{MonTrack chains} = \text{MonTrackRatio}\frac{\text{Trains}}{\text{TrainsNow}}[\ \%\text{Cov}\bullet\text{InCovChains}+(1-\%\text{Cov})\bullet\text{OutOfCovChains})]$$

$$\text{MonSwitch chains} = \text{MonSwitchRatio}\frac{\text{Trains}}{\text{TrainsNow}}[\%\text{Cov}\bullet\text{InCovChains}+(1-\%\text{Cov})\bullet\text{OutOfCovChains})]$$

Trains = Number of trains per region under ATCS

TrainsNow = Number of trains per region under current systems

Dispatchers = Number of dispatchers per region under ATCS

DispatchersNow = Number of dispatchers per region under current systems

Values Used in "Chain", "InCovChains" and "OutOfCovChains"

$$\left.\begin{array}{l}\text{CDCFEP}\\ \text{CC}\\ \text{BCP}\\ \text{MCP}\\ \text{OBC}\\ \text{Tach}\\ \text{Intgr}\\ \text{WIU}\end{array}\right\} = \frac{\text{MTTR} \bullet \text{Failure Coverage}}{\text{MTBF}}, \text{ for the respective chains}$$

where the above MTBFs are equal to:

$$\text{MTBF(CDCFEP)} = \frac{1}{\frac{1}{\text{MTBF(CDCFEP, Vital Part)}} + \frac{1}{\text{MTBF(CDCFEP, Simplex Part)}}}$$

$$\text{MTBF(BCP)} = \frac{1}{\frac{1}{\text{MTBF(Base Radio)}} + \frac{1}{\text{MTBF(Station Controller)}}}$$

$$\text{MTBF(MCP)} = \frac{1}{\frac{1}{\text{MTBF(Mobile Radio)}} + \frac{1}{\text{MTBF(CMU)}}}$$

$$\text{MTBF(WIU)} = \frac{1}{\frac{1}{\text{MTBF(Mobile Radio)}} + \frac{1}{\text{MTBF(Wayside Unit, Vital part)}}}$$

$$\text{MTBF(Intgr)} = \text{MTBF(Transponder Interrogator)}$$

$$\text{MTBF(OBC)} = \text{MTBF(On–Board Computer)}$$

$$\text{MTBF(CC)} = \text{MTBF(Cluster Controller)}$$

$$\text{MTBF(Tach)} = \frac{\text{MTBF(Tachometer)}}{2}$$

Coverage Formulas

For the CDCFEP, OBC, WIU and Tachometer —

$$\text{Coverage} = 1 - \frac{2\lambda_{duplex}^2}{(2\lambda_{duplex} + \lambda_{simplex})(\lambda_{duplex} + \lambda_{simplex} + \lambda_{detection})} \cdot \frac{1}{\text{SimFailProb}}$$

where:

$$\lambda_{duplex} = \frac{1}{\text{MTBF(One copy of the duplex item)}}$$

$$\lambda_{simplex} = \begin{cases} \frac{1}{\text{MTBF(Simplex item)}}, & \text{if the item exists} \\ 0, & \text{if the item does not exist} \end{cases}$$

$$\lambda_{detection} = \frac{3600}{\text{Detection interval in seconds}}$$

SimFailProb = The probability that near coincident failures in each half of the duplex part will be similar in nature so as give the appearance of agreement, thus fooling the detection mechanism in believing that the duplex part has not failed.

For the CC, BCP, MCP and Interrogator coverage equals 1.

CONTROL SYSTEM HAZARDS CATEGORIZATION

This section enumerates the possible situations caused by control system hardware failures, human errors and external events that can lead to an accident if not detected and addressed by corrective action in a timely manner. This list includes those hazards that are clearly within the scope of the control system (e.g., generation of an incorrect train movement authority, exceeding speed limits, etc.), *and* those hazards which could be construed as being related to control system operation (e.g., a break in unmonitored track). Although it might be argued that track is not part of the control system, the knowledge of track integrity is, because, in principle, it is possible to monitor the status of all track. The fact that a segment of track is not monitored is an implementation decision. Hazards clearly outside the scope of the control system, such as mechanical failures of locomotives or rolling stock are not included in the list.

The ATCS addresses some of these hazards completely, some partially and some not at all. The hazards are categorized in a manner specifically intended to support the safety model. This categorization has two important characteristics:

(1) In order to provide a hazard-by-hazard breakdown of projected ATCS accidents relative to accidents that have occurred under a current control system, it is necessary to provide current accident statistics broken down by hazard. This breakdown allows for an unambiguous assignment of past accidents to a hazard category.

(2) The ATCS mechanisms that address a hazard category address all situations in that category in the same way, and therefore to the same extent. Thus, there should be no cases in which the ATCS would protect against some situations in a hazard category but not others.

These characteristics of the hazard categorization simplify the formulas that map current accident occurrences to projected ATCS accident occurrences.

Hazards are organized into categories reflecting the generation of incorrect commands and movement authorities, the generation of incorrect knowledge about the system state and incorrect behavior by human operators.

The following table lists the accident categories included in the analysis by cause code and indicates the manner in which the number of current system accidents in each category is mapped onto the number of predicted ATCS accidents. The categories are numbered here in the same way that they are numbered in the spreadsheet.

TABLE OF HAZARD CATEGORIES AND MAPPINGS

	CATEGORY	COMMENT (Scaling Factor)
200	Fixed signal improperly displayed	n/a - manual block signal
201	Radio communication equipment failure	n/a - probability of two simultaneous and spatially coincident failures is negligible
202	Other communication equipment failure	n/a
203	Block signal displayed false proceed	n/a
204	Interlocking signal displayed false proceed	n/a
205	Automatic cab signal displayed false proceed	n/a
207	Automatic cab signal inoperative	n/a
208	Automatic train control device inoperative	n/a
209	Other signal and communication failures	n/a
502, 506	Failure to properly secure engines	engineer chains
509	Use of brakes, other	engineer chains
510	Impairment of efficiency and judgement because of drugs or alcohol	engineer chains
511	Incapacitation due to injury or ilness	engineer chains
512	Employee restricted in work or motion	engineer chains
513	Employee asleep	engineer chains
515	Employee physical condition, other	engineer chains

519 Fixed signal improperly displayed	n/a
52A-52C Block, interlocking or automatic cab signal, failure to comply	engineer chains
52D-52F Automatic cab signal, train stop or train control device cut out	engineer chains
520 Fixed signal, failure to comply	engineer chains
521 Flagging, improper or failure to flag	n/a
522 Flagging signal, failure to comply	engineer chains
526 Radio communication, failure to comply	engineer chains
527, 528 Radio communication improper or failure to give/receive	1/3 dispatcher chains, 2/3 engineer chains
529 Flagging, fixed, hand and radio signals, other	engineer chains
530, 531 Cars shoved out and left out of clear or cars left foul	determined by multiplier developed from the percent of track monitored
533 Failure to stop train in clear	engineer chains
535 Instruction to train/yard crew improper	dispatcher chains
536 Motor car or on-track equipment rules, failure to comply	one to one
537 Movement of engine(s) or car(s) without authority (railroad employee)	engineer chains
541 Special operating instruction, failure to comply	engineer chains
542 Train order or timetable authority, failure to comply	engineer chains
543, 544 Train orders, radio or written, error in preparation, transmission or delivery	dispatcher chains

549	Rules and instructions, other	1/3 dispatcher, 1/3 engineer and 1/3 one to one
555	Train outside yard limits under clear block, excessive speed	engineer chains
559	Speed, other	engineer chains
560	Spring switch not cleared before reversing	n/a
561	Switch improperly lined	ratio of unmonitored switches
562	Switch not latched or locked	ratio of unmonitored switches
563	Switch previously run through	ratio of unmonitored switches; less than second order occurrence on monitored switches
569	Use of switches, other	one to one
599	Other train operation/human factors	1/2 engineer, 1/2 one to one

n/a = not applicable