Proceedings of the 2001 Winter Simulation Conference
B. A. Peters, J. S. Smith, D. J. Medeiros, and M. W. Rohrer, eds.

SIMULATION OF RARE EVENTS IN TRANSPORTATION SYSTEMS

Lori M. Kaufman
Ted C. Giras

Center for Safety-Critical Systems
School of Engineering and Applied Science
University of Virginia
351 McCormick Road
P.O. Box 400743
Charlottesville, VA 22904-4743, U.S.A.

ABSTRACT

Prior to the deployment of any new or replacement component within a transportation system, it should be demonstrated that the modified system meets or exceeds the safety requirements of the original system. Since the occurrence of a mishap in such a system is a rare event, it is neither cost nor time effective to build and to test a prototype in an actual system prior to deployment. The Axiomatic Safety-Critical Assessment Process (ASCAP) is a simulation methodology that models the complete system and analyzes the effects of equipment changes. By carefully constraining the amount of the overall system state space required for analyses, it probabilistically determines the sequence of events that lead to mishaps. ASCAP is applicable to any transportation system that is governed by a well-defined operational environment.

1 INTRODUCTION

The need to effectively model transportation systems and to predict their associated risk is a matter of extreme importance. These systems are quite pervasive in everyday life and their existence is an integral part of modern society. Since the application of such systems is safety-critical in nature, it is expected that the occurrence of any mishap is a rare event. Hence, little if any failure data exists for these systems.

In many applications, past history can be used to predict future events, however for most transportation systems, such data is of limited use. In order for data to be statistically appropriate for such predictions, the operational environment from which the data is collected must be identical or very similar to the operational environment for which the prediction is to be made. However as technology evolves, the environment in which these systems operate is under constant flux, which limits the applicability of past history data.

In order to obtain mishap data for new or replacement components to be used in these systems, there is a definite need to test these components prior to their actual deployment to demonstrate that the modified system meets or exceeds the minimum safety requirements for its intended application. It is neither cost effective nor practical to attempt to build and test a new or replacement component within a complete system prior to actual deployment due to the time needed to generate the rare event mishap data. If a simulation methodology could be developed that can generate this rare event mishap data in lieu of testing prototypes in actual operational environments, then the statistical basis for predicting the system risk would exist. The Axiomatic Safety-Critical Assessment Process (ASCAP) (Kaufman and Giras 2000; Monfalcone, Kaufman and Giras 2001) is such a simulation methodology.

ASCAP is concerned with probabilistically determining the sequence of events that lead to various mishap scenarios as constrained by the operational environment to which a given vehicle is exposed. By identifying these mishap sequences, their risk potential and their likelihood of occurrence can be quantified. In ASCAP, the simulated behavior of a given transportation system is modeled using a hybrid of time and event driven simulations. During this simulation, the entire system is sufficiently tested to produce the rare event mishap data that is used to quantify system risk. In this paper, the both the methodology required to implement ASCAP and results from its application to a freight train system are presented. The organizational structure of the remainder of this paper is as follows: Section 2: ASCAP Simulation Methodology provides an overview of ASCAP and its management of the system state space; Section 3: Example Application demonstrates the application of ASCAP to an existing freight train system as a proof of concept; and Section 4: Conclusions and

Future Work presents the lessons learned from this work and areas of future research that are being undertaken to further refine the ASCAP methodology.

2 ASCAP SIMULATION METHODOLOGY

The ASCAP methodology analyzes a given transportation system from a vehicular-centric perspective. That is, the simulation reflects the simultaneous movement of *n*-vehicles concurrently from the perspective of each individual vehicle. The movement of each vehicle is predicated upon the behavioral state of the humans influencing the vehicle and the various physical devices encountered by the vehicle during travel. Depending upon the vehicle's interaction with these various entities, the resulting movement may generate a sequence of events that lead to a mishap.

The potential for a mishap exists when a vehicle is coincident in both time and space with an unsafe condition (event). These unsafe conditions (events) result from violations of the prescribed safety-critical protocol that defines safe system operation. Such protocol violations result from inappropriate human action(s) and/or from the stimulation of hazards within the various physical devices that a given vehicle encounters. In order to develop a simulation scheme that can effectively capture such system behavior in an efficient manner, careful attention must be given to the management of these various interactions affecting vehicle movement. ASCAP achieves such efficiency by carefully partitioning the simulation model and by constraining the system state used during analysis.

2.1 State Space Management

Within ASCAP, the underlying simulation model is partitioned into both time and event driven portions. The time driven portion of the simulation determines the relative position, velocity and direction of the vehicle under analysis; the event driven portion reflects the interactions of the vehicle with its operational environment. One of the major concerns in simulating any system is determining how much of this overall system state information is needed to completely analyze the various interactions. The complete state model for any transportation system can be very complex and extremely large. As a result, the time required to traverse such a state space would have extensive computational and time costs. If however only a portion of this system state space is required for analysis at any time during simulation, then both the computational and time costs could be greatly reduced and allow for sufficient testing to produce the rare event mishap data. The ASCAP methodology implements a very succinct sampling approach that provides a greatly truncated search space to achieve this goal.

Each vehicle has its own route and schedule information that specifies what portion of the overall system state space it will traverse. An example routing plan for a vehicle is shown in Figure 1. In this example, the entire system state space consists of *N*-physical devices, however, the particular vehicle routing demonstrates that only a subset of these devices is actually encountered. The actual state space from the vehicular-centric perspective consists of the following devices:

$$\{\text{Device}_3, \text{Device}_5, \text{Device}_6, \text{Device}_8, ..., \text{Device}_N\} \quad (1)$$

Hence, the portion of the overall system state space that is needed by any given vehicle is defined by its route. The exploration of this state space is further reduced due to the vehicular-centric aspect of the simulation.

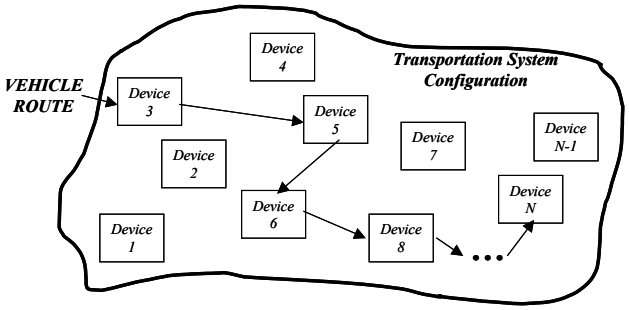

Figure 1: Example Routing

Since a mishap can occur if and only if a vehicle is coincident in both space and time with an unsafe event, a given vehicle is only concerned with device's state and/or the human's behavior at the time of intersection. The result from this vehicular-centric approach is that only the state space for the encountered device and/or the human needs to be analyzed to determine its impact on vehicle movement. A summary of this vehicular-centric approach is presented in Figure 2. Obviously, there is a need to coordinate this information among the various vehicles to guarantee that the simulation is accurately reflecting system behavior.

Within ASCAP, the oversight of the simulation process, which replicates the transportation system's actual management, is maintained by an arbiter. The arbiter manages all information defining the operational environment and oversees the movement of the various vehicles for the transportation system under test. This information, which is summarized in Figure 3, defines the complete system state and is sampled on an as needed basis by each vehicle within the system to determine its movement. Hence, the arbiter supports the interaction between the time and event driven portions of the simulation.

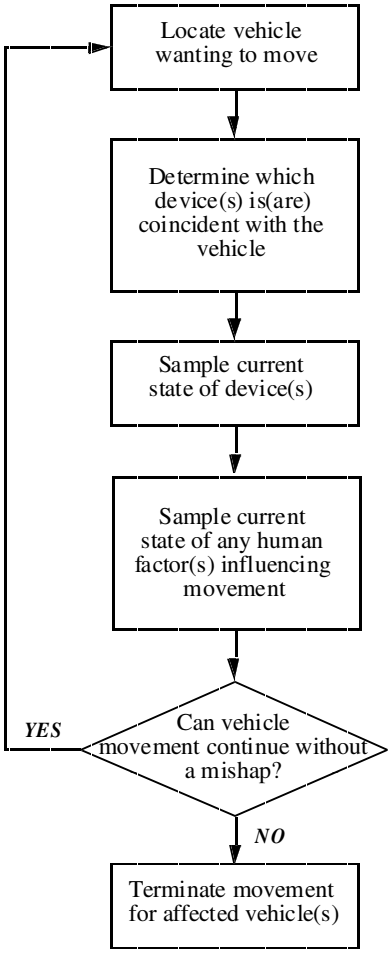

Figure 2: Arbiter Tasks

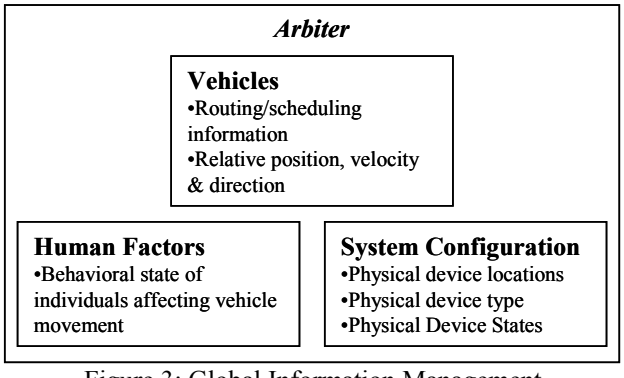

Figure 3: Global Information Management

2.2 ASCAP Movement Modality Selection

Within ASCAP, vehicle movement modalities are derived from the vehicle's interaction with either a human and/or a physical device at a particular time. This simulated behavior is taken directly from the actual safety-critical protocol that defines the operating procedures for the system under analysis. In general, the movement modalities for a given system can be classified as follows:

- All human behavior correct and all devices operational: vehicle moves as prescribed by system safety-critical protocol.
- A detected human violation and/or detected device failure occurs: vehicle movement is restricted to the most conservation action as prescribed by the safety-critical protocol.
- An undetected human violation and/or undetected device failure occurs: vehicle movement is allowed to maintain is current behavior, which may or may not violate the prescribed safety-critical protocol. If this modality violates the safety-critical protocol for the system under analysis, then a mishap may occur. This determination is application specific and is derived by assessing how abhorrent movement impacts safety.

From these movement modalities, the sequence of events to which a given vehicle is exposed during its travel is generated. Hence, ASCAP derives potential "mishap scenarios" for the various vehicles contained within the system as part of its simulation process for generating this rare event data.

2.2.1 Device Modeling

The devices encountered by a vehicle represent physical entities whose failure and restoration rates are known constants. The time that the device has spent in a particular state is not needed; that is, the device model is memoryless. Hence, the device model can be represented as a Markov chain (Cassandros 1993). Furthermore, the ASCAP simulation is based on the concept that the safety-critical behavior of each device is characterized as the probability being in one of three states:

1. Operational: device fully functional
2. Fail-safe: a detected hazard has occurred and the device is operating in a safe manner or it has been successfully shutdown for repair; that is, the hazard can be mitigated by the safety-critical protocol.
3. Fail-unsafe: an undetected hazard has occurred and the device is operating in an unsafe manner that may lead to an accident; that is, the hazard cannot be mitigated by the safety-critical protocol.

In the presence of a given hazard, a given object's state depends on its ability to recognize the hazard occurrence, which implies that coverage (Kaufman and Johnson 1998) is included in the device model. The Markov model used by all of the devices is shown in Figure 4. The probability of being in a given state at a particular time can be found by

solving the homogeneous differential equations that describe the Markov model. Once the state probabilities are determined, then the simulator selects the actual device state using a Monte Carlo (Cassandros 1993) process.

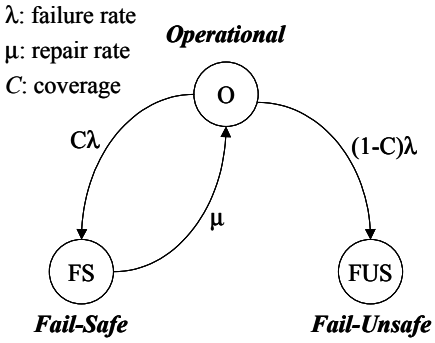

Figure 4: Device Markov Model

2.2.2 Human Behavior Modeling

For most transportation systems, the influence of human behavior serves as safety-critical components. Stimuli that need to be recognized on a cognitive level include communications among individuals and their interpretation of the visual, the physical and the operational environment to which they are exposed. The effect of these stimuli on human behavior is reflected in the Petri net shown in Figure 5.

The transitional probabilities reflect the types of errors that human behavior can create. In response to a given stimulus or set of stimuli, humans must recognize the need to perform a given action. If such recognition is not made, then an error of omission occurs. Such an error is denoted within Figure 5 by the transitional probability of non-response, $P_{non\text{-}resp}(t)$. Once the need for an action has been recognized, then the human must determine if the perceived stimuli is correct. The ability to detect the presence of an inappropriate stimuli and to subsequently correct for its error is denoted within this model as "coverage." The transitional probability for coverage is P_C. Once an individual identifies the need to perform the intended action and processes the received stimuli, then an individual can take action. If this action is performed incorrectly, then an error of commission occurs. The likelihood of such an error is denoted within Figure 5 by the transitional probability of non-compliance, $P_{non\text{-}comp}(t)$. The human behavioral state is selected using a Monte Carlo process.

2.2.3 Vehicle Movement Algorithm

In addition to providing global information management, the arbiter must also govern the vehicle movement. Movement is predicated upon predetermined routes and schedules governing the individual vehicles contained within the system. In order to completely replicate actual

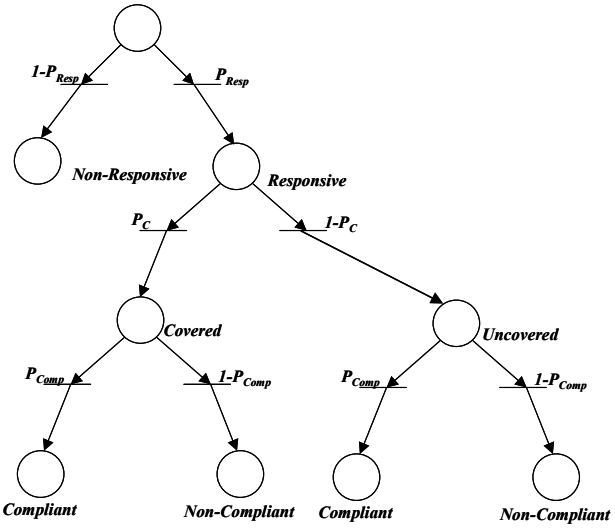

Figure 5: Human Behavioral State Model

system behavior, the governance of movement must also support possible random behavior from certain vehicles. Within ASCAP, the rules constraining these movement modalities are derived from the safety-critical protocol governing the system under test. This environment must be sufficiently defined to allow for the derivation of the logical representations of various movement modalities for the vehicles contained within the system. Once defined, it is these modalities that provide the arbiter the capability of coordinating and controlling the movement of the *n*-vehicles contained within the ASCAP simulation.

3 EXAMPLE APPLICATION

The ASCAP simulation methodology has been applied to a freight train system as a proof of concept. In this system, a collection of 24 loaded and unloaded freight trains traverse a 127-mile span of single track containing 1084 physical devices that consist of switches, bridges, signs and rail. In order to allow trains traveling in opposing directions simultaneous track access, nine (9) sidings are included in the track layout to divert traffic. Each train contains a crew and the movement of the 24 trains is determined by a dispatcher's interaction with the various crews. All movement modalities emulate the function of actual direct traffic control (DTC) train systems (CSX 1997). The DTC operating rules define how information is conveyed among the train crews and the dispatcher and their respective procedures to ensure safe travel. Hence, the DTC rules define the safety-critical protocol for this system.

The ASCAP simulation software implementation is achieved using MODSIM III (CACI Products Company 1997), which is an object-oriented discrete event simulation software. By exploiting the object oriented nature of MODSIM III, the modeling of both the physical devices

and the human behavior can be implemented to reflect the structure of the ASCAP methodology.

The partitioning of the physical devices and the human element within the ASCAP paradigm is translated to code as class structures. Within the human behavior class, separate objects exist for both the dispatchers and the train crews. Similarly within the physical device class, separate objects exist for the various types of devices contained within the track layout. The modeling constructs used to determine the states of the physical devices and the humans at the time of interaction with a given vehicle are implemented via methods. The object instantiation occurs when the track layout, which is the actual location and configuration of the various physical devices, is initialized during simulation. The actual train movement is defined within the simulation using a Traffic Management Algorithm (TMA) (Joshi, Kaufman and Giras 2001).

The TMA reflects the behavior of the dispatcher and the train crews relative to train movement using a well-defined set of behavioral rules. The rule modality is derived from the DTC operating rules. Within ASCAP, it is the realization of this vehicle movement protocol that supports the vehicle-centric nature of the simulation methodology. The TMA is an event-driven algorithm that translates the DTC operating rules to a well-defined set of predicate logic, which provides ASCAP with the capability of moving a given train through the defined track layout in a manner analogous to actual system operation. Hence, the TMA provides the ASCAP prototype software the ability to simultaneously move the 24 trains through the defined corridor.

The completed prototype software was tested for accuracy of results in many ways. The ASCAP software was executed on a 550 MHz PC with configured with 256 MB RAM. Within this simulation, 1,000,000 cumulative train miles, which corresponds to approximately one year of system use, were simulated with a simulation time of approximately fifteen minutes. The areas of greatest concern in verifying the adequacy of the ASCAP representation of the system was the correctness of the TMA and the interaction of the human behavior model with the TMA.

In assessing the correctness of the TMA, the reasonability of the traffic flow was addressed. It was found that the average speed for the loaded and unloaded trains in simulation was approximately 15 MPH and the average speed for the actual trains traversing the same track configuration was approximately 17 MPH, which was nominally the same. Additionally, the train routing within ASCAP was identical to that of the real system. In assessing the correctness of the human behavioral model within ASCAP, a comparative analysis with existing mishap data for the actual system was performed.

The validation of the human behavior modeling structure within ASCAP is limited by the lack of available information quantifying the various aspects of train control system specific human behavior. The only available data for such applications are Federal Railroad Administration (FRA) accident databases, which collects information from various train lines without making any distinctions for variations in train system control or track configuration. This information was mined to determine the appropriate data for comparison. The data used for the comparative analysis consisted of reported accidents for similar train control systems. The accident data reported from 1997 to 2000 showed that an average of 9 accidents occurred per year on a similar train control system, with a minimum of 4 accidents occurring in 1998 and a maximum of 12 accidents occurring in 2000. The variation for this average is 12 accidents. Hence, the expected number of accidents from the FRA data is between 0 and 21. The ASCAP simulation identified 13 potential mishap scenarios, which is within the range of expected FRA accidents.

4 CONCLUSIONS AND FUTURE WORK

The ASCAP methodology is a simulation-based approach that replicates the actual behavior of a transportation system from a vehicular-centric perspective. By constraining the simulation to this perspective, the amount of the overall system state space that needs to be examined is "dynamically pruned." A given vehicle only needs to traverse the state space for the device it is encountering and/or the human affecting it movement to determine its movement modality. Hence, the simulation time spent searching the system state space is greatly reduced.

The ASCAP methodology, in particular the model constructs defining physical devices and human behavior, lends itself to the development of software within the object-oriented paradigm. As a proof of concept, an ASCAP simulation was applied to an existing DTC freight train system. While executing this software on a 550 MHz PC with configured with 256 MB RAM, 1,000,000 cumulative train miles, which corresponds to approximately one year of system use, were simulated with a simulation time of approximately fifteen minutes. In order to determine the adequacy of the ASCAP representation of the system, the simulation results were compared to available information for the train line under analysis. It was determined that the TMA reasonably represented the traffic flow of the actual system and that the number of potential mishaps identified was with range the actual number of accidents reported to the FRA between 1997 and 2000 for similar train control systems. Hence, this proof of concept demonstrates the viability of using the ASCAP methodology to model and to determine potential mishaps in safety-critical applications and to determine the effects of component replacement/modification.

Currently, the ASCAP methodology is being extended to other freight train systems, transit systems and high speed rail systems. As these systems are analyzed, the modeling paradigms for both the physical devices and the

human behavior are being tested and refined to better represent actual system behavior. The brevity of the simulation runtimes is allowing for extensive validation and verification of the various models. As a result, ASCAP can be used as a predictive tool in quantifying the occurrence of rare mishap events in these safety-critical applications.

ACKNOWLEDGMENTS

This document was prepared based on the ongoing research in the University of Virginia's Center for Safety-Critical Systems. The work regarding the example application was sponsored by the Federal Railroad Authority (FRA). We thank Mr. Bill Goodman and Mr. Manuel Galdo from the FRA for their assistance throughout this entire effort.

REFERENCES

CACI Products Company. September 1997. *Reference Manual MODSIM III Object-Oriented Simulation*. La Jolla, California: CACI Products Company.

Cassandros, C. G. 1993. *Discrete Event Systems: Modeling and Performance Analysis.* Boston, Massachusetts: Richard D. Irwin, Inc.

CSX Transportation. October 1, 1997. *CSX Operating Rules Manual*.

Joshi, V. V., L. M. Kaufman and T. C. Giras. 2001. Human Behavioral Modeling in Train Control Systems. In *Proceedings of the Reliability and Maintainability Symposium*, 183-188. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers.

Kaufman, L. M. and T. C. Giras. 2000. The Axiomatic Safety-Critical Assessment Process (ASCAP) Simulation Methodology. In *Proceedings of the 9th IFAC Symposium on Control in Transportation Systems*, *Volume 2*, ed. E. Schneider and U. Becker, Braunschweig, Germany, June 2000, 534-539.

Kaufman, L. M. and B. W. Johnson. 1998. The Importance of Fault Detection Coverage in Safety Critical Systems. In *Proceedings of the Twenty-Sixth Water Reactor Safety Information Meeting, Volume 2*, 5-28. Washington D.C.: U.S. Nuclear Regulatory Commission.

Monfalcone, M. E., L. M. Kaufman and T. C. Giras. 2001. Safety Assessment of a Direct Traffic Control (DTC) Train Control System using the Axiomatic Safety-Critical Assessment Process (ASCAP). In *Proceedings of the Reliability and Maintainability Symposium*, 352-357. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers.

AUTHOR BIOGRAPHIES

LORI M. KAUFMAN is currently a Principal Scientist in the Center for Safety-Critical Systems at the University of Virginia. She received the B.S., the M.S. and the Ph.D. degrees in Electrical Engineering from the University of Virginia. Her current research interests include railway safety-critical signaling and train control systems, safety-critical ground transportation systems, human behavior modeling and analysis and software/hardware reliability engineering. Dr. Kaufman is member of Eta Kappa Nu, Tau Beta Pi and a senior member of the IEEE. Her email address is <lmk2q@virginia.edu>.

TED C. GIRAS received a B.S. in Electronic Engineering at the University of Massachusetts at Lowell, followed by the M.S. and Ph.D. degrees in Electrical Engineering at Carnegie Mellon University. He now holds the position of Research Professor and Co-Director of the Center for Safety-Critical Systems at the University of Virginia. His areas of research include railroad and transit railway safety-critical signaling and train control systems, safety-critical ground transportation systems, and power system security. Dr. Giras is an IEEE Fellow. His email address is <tgiras@virginia.edu>.