STOCHASTIC TRAIN DOMAIN THEORY FRAMEWORK

Theo C. Giras, Zongli Lin
Center of Rail Safety-Critical Excellence, Department of Electrical and Computer Engineering
University of Virginia, P.O. Box 400743, Charlottesville, VA 22904-4743, U.S.A.
tgiras@virginia.edu, zl5y@ee.virginia.edu

Abstract The Axiomatic Safety-Critical Assessment Process (ASCAP) is illustrated as a Stochastic Train Domain Theory Framework "Plug & Play" large-scale Monte Carlo simulation vision. The framework supports the US traditional railway system component models as generalized operational train line taxonomy. The railway domain can be Direct Traffic Control (DTC), Centralized Traffic Control (CTC), Cab Signaling, Positive Train Control (PTC) or a Maglev system. The train line taxonomy is characterized as a stochastic train domain that provides either a design for safety or a risk assessment framework. The design for safety domain is the dual of the risk assessment domain. A significant property of the stochastic vision is that it handles the stochastic quantification of safety for processor-based train systems integrated with structural and electromechanical devices.

The stochastic Train Domain Theory Framework vision is illustrated with a Maglev guideway reliability, availability, maintainability and safety (RAMS) Monte Carlo risk assessment component model. A Monte Carlo discrete event simulation method is used to illustrate and extend traditional guideway RAMS analysis beyond the traditional methods of a static Fault Tree Analysis (FTA) to a dynamic RAMS analysis that is based on the movement of all the vehicles and their intersection with unsafe guideway substructures, guideway switch conditions and/or electrical and propulsion segment "out of service" events.

The need for a formalized validation, verification and certification vision is presented that includes individual component models, the overall Monte Carlo properties of the simulation and the statistical behavior of the Design for Safety and Risk Assessment methodologies.

1. Stochastic Train Domain Taxonomy

The ASCAP train domain framework is decomposed as a set of component models that describe the detailed stochastic and deterministic operation of a railway track plan infrastructure, rolling mixed mode passenger and freight stock, processor-based signaling and train control system, train movement schedul-

ing and train dynamic behavior to aid in the assessment of an Incident/Accident risk cost severity metric. The risk cost metric is the societal cost versus train miles traveled for all accumulated Incident/Accidents. In addition, the operational rule book of the railway is characterized as an Artificial Intelligence (AI) Blackboard that evaluates the dispatcher, train crew and road way worker human-factors compliance and non-compliance to the operational rules. Finally, extensive logging is provided for all Events of Interest (EOI's) that describe the details of the safety-critical behavior.

The stochastic framework is illustrated in Fig. 1.

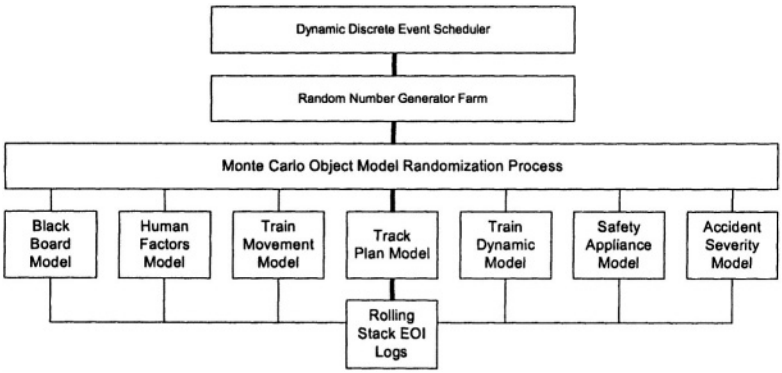

Figure 1. The Stochastic Framework of ASCAP

All the ASCAP component models are implemented with a common generalized probabilistic state mode domain: (1) operational, (2) fail-safe, (3) fail-unsafe, (4) rule book compliant and (5) rule book non-compliant. In addition, a deterministic train dynamic model is included. A fundamental axiom of ASCAP is that Incident/Accidents can only occur when a train intersects with a component unsafe state. When all the components are interconnected, they form a large-scale Monte Carlo probabilistic train dynamic behavior domain. ASCAP executes either as a hazard-free train domain that provides a proof-of-correctness of the train line operation or non hazard-free domain that provides a proof-of-the-safety level.

The basic principle of the stochastic Train Domain Framework is illustrated with a Maglev example (Fig. 2). The vehicles travel along the guideway and interest with all the component models as defined by the Maglev system guideway. At each intersection the probabilistic behavior of the intersected component model is calculated and its impact evaluated as operational, fail-safe or fail-unsafe as determined by the Maglev operational rule book. The result is that the vehicle operational modalities such as speed and acceleration are modified.

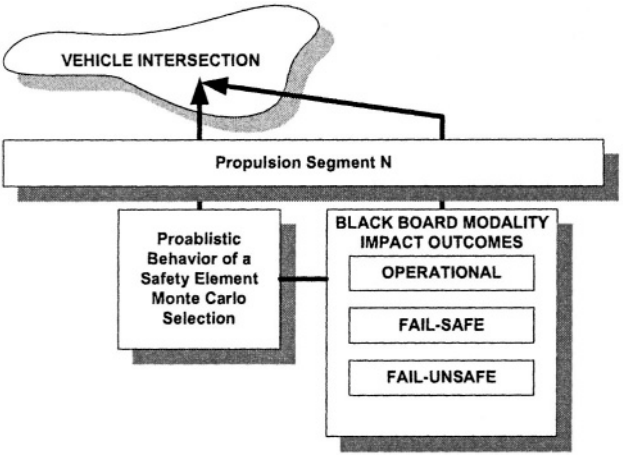

Figure 2. Train Domain Framework for a Maglev System

2. A Maglev Guideway Illustrative Example

The Maglev guideway "plug & play" component model is a dynamic risk impact model that decomposes the guideway propulsion segments into safety-critical elements. The safety-critical elements are further decomposed into individual beams and pillars. The decomposition methodology allows the guideway model to characterize four levels of structural and electrical probabilistic behavior: (1) propulsion segment behavior, (2) switch segment behavior, (3) safety element behavior and (4) the behavior of each beam and its three supporting pillars.

The electrical safety behavior of the propulsion and switch segments are considered, along with the structural behavior of the guideway construction for the guideway RAMS analysis. The beam/pillar decomposition is generalized to accommodate unique alignments as may be required for a Maglev system in the United Sates. This model is applicable to steel, concrete as well as hybrid guideway beam configurations.

The guideway RAMS structural and switch analysis simulate an eighty-year life cycle. The ASCAP RAMS risk assessment simulation estimates the risk versus millions of vehicle miles traveled as a bounded risk containment region subject to a high degree of confidence.

The ASCAP RAMS risk assessment Monte Carlo methodology extends the more traditional safety assessment conducted with a static Fault Tree Analysis (FTA) safety analysis. The ASCAP simulation extends the static FTA method with a dynamic risk assessment analysis that is based on the travel exposure of the vehicles to guideway unsafe events. The unsafe events shall be the time and position events that are coincident with the travel of the vehicle that are

potential accidents. In this way, the traditional requirements of the RAMS methodology are extended to include "safety-related exposure" as determined by vehicle miles traveled over the life cycle of the guideway. In addition, the concept of guideway near term repairs to correct detected failures and a phased-interval long term maintenance policy to mitigate undetected failures is simulated to ensure real world safety risk estimates of the guideway structure.

The RAMS assessment partitions the guideway into safety-critical elements similar to a structural finite element analysis. A three state Markov probabilistic model is used to describe the safety element probabilistic behavior. A similar model is implemented for the switch segments that include the electrical motor behaviors and the redundant motor mechanism that shall provide the switch safety coverage. Each safety element consists of a set of beams and their supporting pillars. The alignment shape and the types of beams that are required determine the number of safety elements used to describe a propulsion segment. The ASCAP Monte Carlo risk assessment methodology for the Maglev system requires that the probabilistic behavior of the guideway be considered as a sequence of potential hazards to be mitigated. The ASCAP methodology quantifies the likelihood of occurrence of such potential guideway hazards along with their respective risk consequences. These consequences result in either performance degradation of the vehicle speeds, overall headway performance reduction and/or accidents.

The guideway structural plan is decomposed into *N*-propulsion segments (see Fig. 3), where a propulsion segment is a contiguous collection of *M*-safety-critical elements. Each ASCAP safety-critical element is a contiguous set of *K* beams, where three pillars support each beam. The number of beams per safety element is determined by the guideway alignment characteristics, which are specific to a given Maglev system. For the ASCAP simulation of the system under analysis, the number of safety elements, *M,* are selected to characterize the alignment curvature in the three-dimensional space.

In order to develop the risk assessment for the guideway, a series of ASCAP simulations with various propulsion segments out of service are used to identify vehicle "out of service" routing versus normal operation and the impact on system headway performance. A guideway propulsion segment is designated "out of service" due to either electrical and/or structural failures. In the event that a safety element failure takes place, the propulsion segment is placed in a degraded mode of service depending on the state of the failure: fail-safe or fail-unsafe. That is, the velocity of the vehicles traversing that particular segment may be required to travel at a lower speed or that propulsion segment may be taken out of service and no travel over the segment is allowed. Each beam that used to assemble a propulsion segment and its related three supporting pillars is described with a minimum probabilistic three state model. The safety element model is based on an exponential failure law.

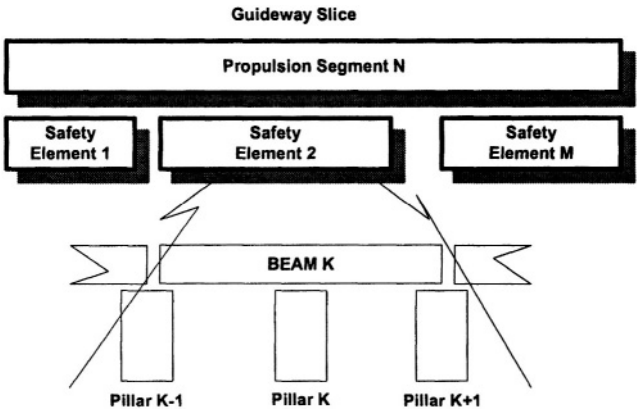

Figure 3. A Propulsion Segment of the Guideway Structure

The RAMS guideway assessment model includes the probabilistic behavior of the pillar and beam configuration identified to form a safety element. These safety elements, as shown in Fig. 3, define the guideway structure object. It is these objects with which a given vehicle intersects at a particular moment in time. The behavioral characteristics of these objects shall be obtained using a multi-state model whose state is selected using a Monte Carlo process.

Guideway Safety Element Decomposition

The guideway shall be decomposed as physical objects for the guideway RAMS ASCAP simulation as follows:

- *N* propulsion segments;
- *M* safety elements per each propulsion segment;
- *K* beams/pillars for each M safety element, where the alignment requirements and the types of beams for each safety element shall determine *K*.

The guideway is a distributed set of safety elements that describe all the attributes of the guideway, as it exists in the physical world. That is, the detailed geometry of the guideway and all the attributes of the geometry such as curves, grades and elevations shall be included to provide an accurate characterization of the guideway alignment. The ASCAP guideway risk assessment model is a set of interconnected objects, where each object describes a given safety element, with which continuously traveling vehicles intersect. At each intersection, the probabilistic behavior of each safety element is calculated. The three primary state behaviors - operational, fail-safe, and fail-unsafe - are reduced to an active state with a Monte Carlo selection method. The active state selected

by the Monte Carlo method is posted as a blackboard entry, which defines the movement modality of the intersecting vehicle. This process is highlighted in the intersection of the vehicle traveling over the safety element sections of the guideway and allows the risk exposure to be calculated as required by the FRA Processor-based Regulatory Rule.

Guideway Safety Element Model

A generic three-state model, as shown in Fig. 3, is developed to represent the behavioral characteristics of the guideway safety element model. The concept of coverage is included in the model to provide the ability of hazard detection. Each safety element contains a potential hazard(s) and the probabilistic model calculates its likelihood of occurrence. Hence, the ASCAP simulation of the real-world physical guideway builds the hazards list and determines their potential consequences.

The transition probabilities that take the model from the Operational State to either the fail-safe state or the fail-unsafe state have the capability to be generalized in the ASCAP Monte Carlo simulation such that structural variations in the guideway RAMS analysis are feasible. The model has the capability to handle different failure laws, along with coverage parameters that describe the behavior of configurations such as hybrid (steel and concrete) beam, pillar and overall bridge structures. In this way, the guideway RAMS behavior has the capability to handle different deployments of the Maglev technology in the United States.

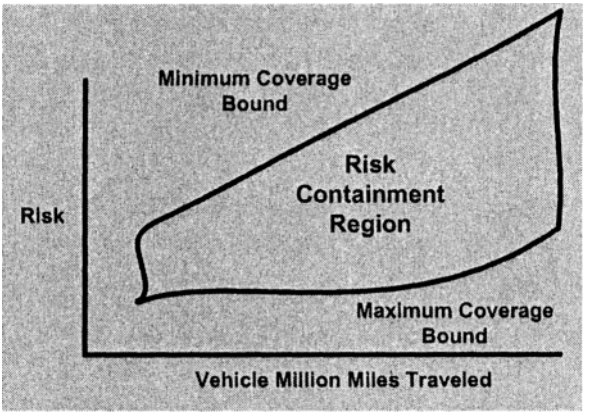

Figure 4. Risk vs Vehicle per Million Miles Traveled

3. Conclusions

ASCAP provides a large-scale Monte Carlo stochastic train domain framework that has the capability to provide a real-world design for safety or risk assessment analysis of a train system. The current limitation is the ability to validate and verify the simulation to insure that the result confirm to the real world. Current validation and verification has focused on the "Peer Review Process".

The next step in the validation and verification process is to proceed with a rigorous development of Formal Methods applied to each of the component models and the overall ASCAP simulation. In addition, the statistical performance of the simulation must be evaluated for vehicle miles traveled sufficiency to insure that all the possible incident/accidents have been revealed by the simulation.