Magplane Design for Safety and Risk Assessment Framework

Ted C. Giras, Ph.D.
Magplane Technology, Inc., Charlottesville, VA 22911, USA

D. Bruce Montgomery, Ph.D.
Magplane Technology, Inc., Bedford, MA 01730, USA

Zongli Lin, Ph.D.
University of Virginia, Charlottesville, VA 22904-4743, USA, and CheungKong Professor, Shanghai Jiao Tong University, Shanghai, China

Keywords: ASCAP, Monte Carlo, safety exposure, human factors, risk assessment, EPAD's

ABSTRACT: A Magplane [1] design for safety and risk assessment framework is presented. The framework is built on the Axiomatic Safety Critical Assessment Process (ASCAP) [2]. It is a hybrid Monte Carlo simulation toolset that is compliant with the Federal Railroad Administration (FRA) of the United States. A feature of ASCAP is the calculation of Events Passed at Danger (EPADS) by the vehicles that results in the automatic generation of Dynamic Fault Trees (DFTA). Comprehensive Monte Carlo models of the guideway, vehicles, wayside propulsion converters, dispatch center human-factors, wayside-centric IEEE communication-based train control (CBTC) and the on-board vehicle distributed control architecture are supported by the framework. Finally, a rapid prototyping proof-of-concept example is given with an alignment in Beijing, China.

1 OVERVIEW

1.1 Historical

An FRA compliant object-oriented Monte Carlo Magplane Design for Safety and Risk Assessment toolset was developed at the University of Virginia over the past decade [2]. Magplane enhancements have been implemented based on the ASCAP Transrapid Pennsylvania Project Safety Framework and the New York City Transit (NYCT) Canarsie Line Communication-based Tran Control (CBTC) safety risk assessment. The enhancements have been structured to meet the Magplane high performance safety qualification regulatory requirements for both rapid prototyping and regulatory revenue service compliant risk assessment requirements.

1.2 Basic Monte Carlo Simulation Principles

Basic implementation principles guide the formulation of the methodology such as: (1) the Unified Modeling Language (UML), (2) object-oriented implementation, (3) traffic density dynamic exposure that establishes the level of safety and (4) the coincidence of vehicles in time and position with Monte Carlo generated unsafe events that can create an Incident/Accident-pair or a near-miss called an Event Passed at Danger (EPAD). In addition, the ASCAP implementation builds Dynamic Safety Exposure Event Trees that result in the automatic generation of a dynamic fault tree analysis (DFTA).

The ASCAP Monte Carlo methodology provides a unique tool set to perform a Magplane Reliability, Availability, Maintainability and Safety (RAMS) simulation and analysis.

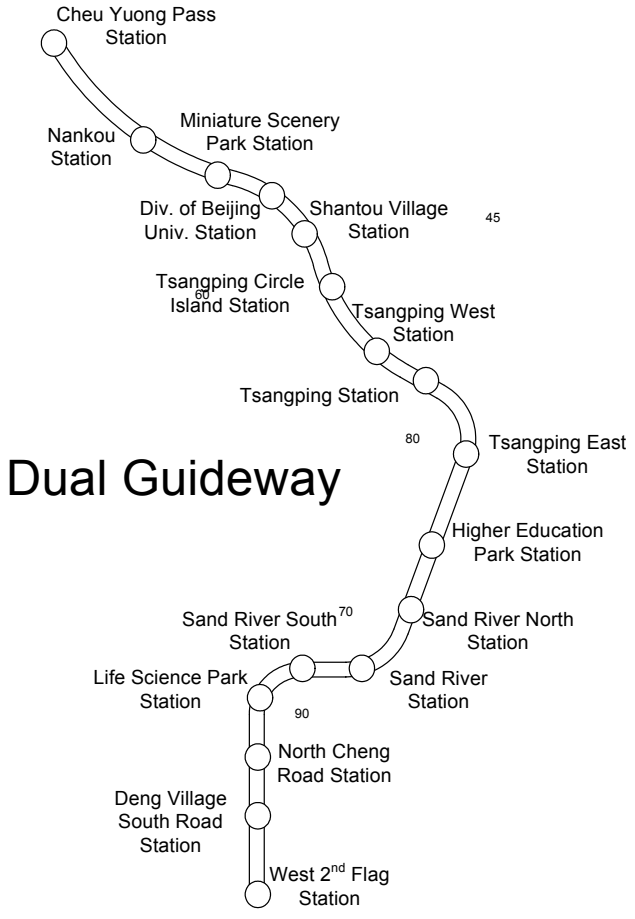

Figure 1: Beijing Alignment Example.

The vehicle time and position safety constraints provide n-vehicle dynamic travel motion, headway and safety-critical exposure to subsystem and component safety device failure events intersected along the guideway travel. The intersected safety events exist in one of three possible states as: (1) operational, (2) fail-safe and (3) fail-unsafe. An Incident/Accident-pair and/or an EPAD can only occur at the intersection of a vehicle mobile object with a failed unsafe stationary or mobile object and/or a human-factor error.

The ASCAP Magplane methodology framework is illustrated with a Chinese transit railway feasibility study report alignment example. The example illustrates the rapid feasibility prototyping capability of the methodology available in the early design stages of a Magplane system. As the Magplane design matures, the ASCAP methodology will provide a detailed risk assessment required for regulatory revenue service.

Finally, the ASCAP design for Safety and Risk Assessment is compliant with the US Federal Railroad Administration (FRA) Rule 49 CFR Part 209/234/235 Standards, Processor-based Regulatory Rule.

2 ASSUMPTIONS

2.1 Rapid Prototyping Proof-of-Concept

The Magplane system is in its early design phase and the final detailed design data required for a compliant risk assessment remains to be completed, validated and verified. However, the preliminary design data available does support a rapid prototype feasibility simulation. As additional design data becomes available, it will be included in the simulation following the Spiral Method of validation and verification, along with progressive testing.

The key assumptions are listed as follows:

1. The vehicle attitude control subsystem is simulated with the aid of an on-board Kalman Filter inertial subsystem;
2. The apparent propulsion power is calculated. Detailed propulsion configuration data is not available to make phase angle calculations required to perform real and reactive power calculations;
3. The IEEE Standard Communication-based Train Control (CBTC) signaling and control subsystem is implemented with virtual signaling devices at the Dispatch Center;
4. An on-board safety duplex inertial positioning, velocity and acceleration Kalman filter subsystem is integrated with the CBTC subsystem;
5. Guideway beam failures are simulated;
6. The stopping distance of each vehicle is controlled by a dynamic Speed versus Distance-to-Go Braking Curve with quality of passenger ride constraints;
7. The human-factors error behavior at the Dispatch Center is simulated.

3 MULTI-STAGE TAXONOMY

3.1 Rapid Design for Safety Prototyping

The multi-stage taxonomy decomposes the simulation into subsystems and components that include the alignment guideway beam sheet infrastructure, n-vehicles, vehicle on-board controls, suspension and motion sensors, wayside propulsion converters, wayside-centric CBTC, communication and human-factors.

ASCAP is implemented as a multi-stage hybrid continuous/discrete event simulation. Stage 1 calculates the dynamic motion, acceleration, velocity and position of the n-vehicles as a set of non-linear continuous differential equations. The vehicle equations consider the aerodynamic, magnetic, guideway geometry, grade and wind drag forces. The vehicle driving function is the guideway propulsion thrust force. The continuous simulation calculates the vehicle dynamic motion behavior, travel schedules, headways, guideway route travel, stations stops and the power consumption as each vehicle travels along the guideway.

3.2 Expert System Taxonomy Builds

The topographical system alignment, subsystems and components are characterized as a collection of stationary and mobile objects. The major subsystems such as the guideway beams, CBTC virtual dispatch center signaling and the wayside-centric propulsion converters are implemented with the aid of an embedded Expert System.

3.3 Safety-Critical Intersection Constraints

As the n-vehicles move along the guideway, the intersection with both the stationary and mobile objects, along with the various agents determine the n-vehicle operational modalities.

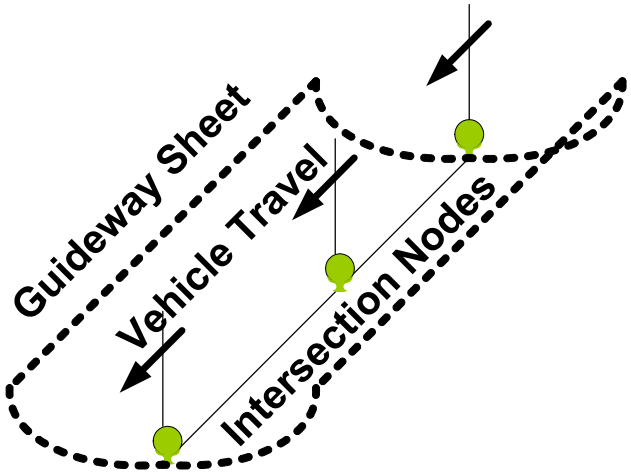

Figure 2: Guideway Sheet Intersection Nodes.

The concept of an object-oriented intersection with the dynamic movement of each vehicle is illustrated with an example that describes the behavior for a section of the guideway as illustrated in Figure 2.

As a vehicle travels along the guideway sheet, it intersects with discrete Monte Carlo safety nodes positioned along the sheet. Each guideway sheet has a minimum of three Monte Carlo nodes. Additional nodes can be added by the Expert System build as required to ensure statistical significance of the RAMS results.

3.4 Vehicle Operational Modalities $\lambda(t)$

The vehicle operational modalities are defined by mobile and stationary object-oriented behavior, system operating rules and procedures, along with the interactive dispatcher human-factors and guideway maintenance personnel that support the Magplane system as each node is intersected by a vehicle.

Once a node is intersected, the operational modalities define a large-scale dynamic probabilistic event tree. As a vehicle travels along the guideway, it builds a sequence of dynamic event trees that automatically generates a fault tree analysis (FTA). More importantly, these trees include the dynamic safety exposure as a function of the variable traffic density required for regulatory safety compliance.

3.5 FRA Compliant Taxonomy

Each vehicle within the simulation is an independent "mobile" object that creates a simulation environment of n-vehicle-centric mobile objects moving asynchronously along the guideway and the intersection of objects generates a sequential dynamic fault tree analysis that travels along the guideway with each vehicle. This vehicle movement strategy meets the FRA compliance requirement to include the total system exposure as a function of varying traffic density.

The actual vehicle movement modalities are predicted based on the state behavior defined by the object and agent Monte Carlo failure interactions. As the vehicles move along the guideway, the sequence of safety events that constrain the movement are generated with the simulation. Therefore, if an Incident/Accident-pair occurs, then the sequence of events that lead to the Incident/Accident-pair event are known in complete detail. Stage 2 is enabled when the dynamic motion behavior between objects, stationary and mobile, approaches a steady-state condition for a given vehicle. The selection of Stage 2 is based on a prediction algorithm that searches ahead of a vehicle to decide the simulation mode of operation – Stage 1 or Stage 2.

The purpose of the simulation stage 2 is to increase the calculation performance to ensure that the number of km traveled by each vehicle exceeds the Monte Carlo requirements that determine the statistical high degree of confidence required for a credible risk assessment simulation. Failure rates are determined with a non-linear "bathtub" function that considers the safety infant mortality rate, failure rate variance as a function of time, environment and accelerated failure rates to software processor-based enhancements.

A random number generator with a period of 2^{191} is implemented, along with a Weibull distribution function that implements a non-linear failure function for each safety-critical device and the hum-factors errors.

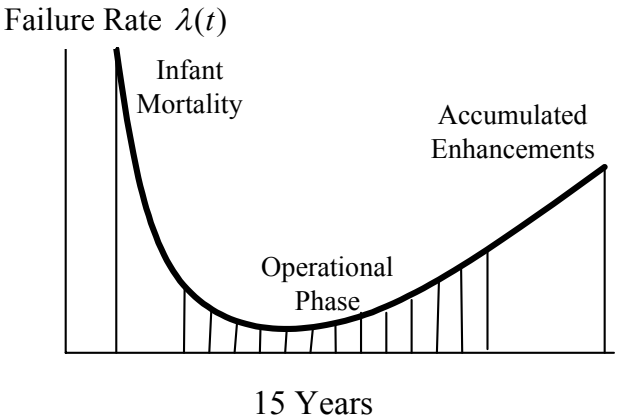

Figure 3: Non-Linear Failure Rate

The dynamic motion of the i-th vehicle is expressed as a longitudinal non-linear differential equation expressed as follows:

$$(Nmg)^i \frac{dv^i(t)}{dt} = -F^i_{Drag} + K^i_{Pwr} * Pwr^i / v^i(t) \qquad (1)$$

Where N is the number of vehicle sections; i is the i-th vehicle, m is the vehicle section mass; g is the gravity constant, $v(t)$ is the vehicle velocity; F is the total vehicle drag, K is the power calibration constant and Pwr is the apparent propulsion power.

The speed and power performance estimates are illustrated in Figure 4. An important outcome of these calculations is the braking profile required by the CBTC signaling and control subsystem.

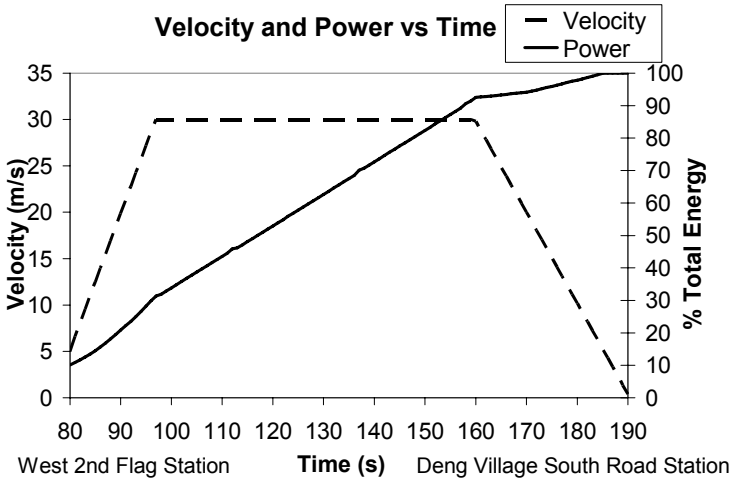

Figure 4: Beijing Example Alignment Speed and Power.

4 OBJECT INTERACTION AND COVERAGE

4.1 Object-Agent Failure Covered Interactions

Object entities, stationary and mobile, interact with each other in a variety of ways, along with human-factor agents. Object-to-object interactions are modeled to allow specified objects to "cover' the failure of other objects and are implemented using the Dynamic Exposure Trees.

Object-to-Agent and Agent-to-Agent interactions allow Agents to "cover" the failures of various objects and to "cover" the failures of other Agents. Agent failure protection is limited to the Dispatch Center and the guideway maintenance personnel. Human-factors are integrated with the vehicles and other safety-critical devices.

These interactions are implemented within ASCAP using traditional Artificial Intelligence concepts called "blackboards" The blackboards describe the set of possible agent actions in response to the set of possible stimuli from the interacting object(s) or agent(s). As a rapid prototyping tool set, ASCAP provides a platform to validate and verify the Magplane Operational Rule Book required for regulatory compliance.

4.2 CCC Dispatcher Agents

The CCC Dispatcher Agents are not error free. Agents can take incorrect actions in response to stimuli from various objects and agents. A detailed Human-factors Choice Model is based on five basic error probabilities as: (1) recognition, (2) interpretation, (3) stimuli predictability, (4) coverage and (5) compliance. All of which when taken together. describe the agent action to a particular stimulus and environment. The probabilities are obtained with a Monte Carlo draw.

5 INCIDENT/ACCIDENT-PAIRS

The ASCAP risk assessment metric is evaluated based on the frequency of occurrence of Incident/Accident-pairs that occur per million km of passenger travel. The Likelihood of Occurrence of an Incident/Accident-pair is a direct function of the total system traffic density and the failure rates of the objects intersected by the n-vehicles. In addition, the failures of guideway beams that result in cross-over routing on a dual guideway can result in Incident/Accident-pairs.

The risk results for the Magplane China rapid prototyping feasibility analysis are presented as Mishaps versus Passenger km traveled. When the Magplane deployment is for revenue service, the risk assessment is presented as Societal Cost versus passenger km traveled. In either case, millions of passenger km traveled are required to achieve a degree of confidence of the Monte Carlo Incident/Accident-pair results. The Mishap risk assessment is illustrated in Figure 5.

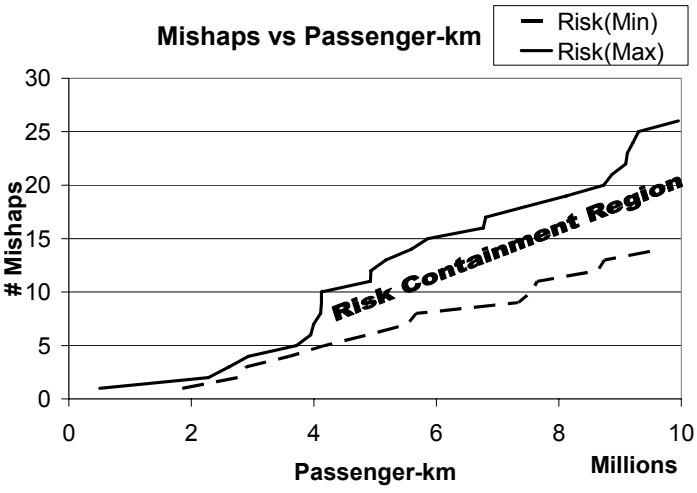

Figure 5: Risk Containment Region

The Risk Containment Region provides the system design and safety assessor decision makers to determine the impacts that failed subsystems, components and human-factors can have on the expected

safety performance of proposed system architecture. The Risk Containment Region when considered together with supporting evidences for the parametric allocation, provide the "Credible and Convincing Safety-Critical Evidences" High Degree of Confidence as required for a revenue service FRA waiver.

Typical Incident/Accident-pairs are: (1) vehicle head-to-head collision, (2) vehicle head-to-tail collision, (3) vehicle-to-side raking collision and vehicle-to-guideway collision.

6 EVENTS PASSED AT DANGER EPAD'S

6.1 System Level Hazards

System failure Events Passed at Danger (EPADS) may become Incident/Accident-pairs, if a vehicle becomes time and position coincident with a specific hazard condition. When this situation occurs, the intersection of the vehicle with the failed object is termed an EPAD. An EPAD may in turn lead to an Incident/Accident-pair if collision conditions are met.

For example a vehicle running past a Red Virtual Signal would be declared as an EPAD, but this situation may not result in an Incident/Accident-pair if there is no vehicle or other hazardous guideway condition ahead. A key feature of the ASCAP simulation methodology is that ASCAP automatically captures the sequence of events that lead to Incident/Accident-pair in a detail that is time dependent.

Finally, ASCAP maintains a comprehensive log that provides a record of all the dynamic performance, RAMS data collection and EPAD sequential event time information. The EPAD concept is illustrated in Figure 6.

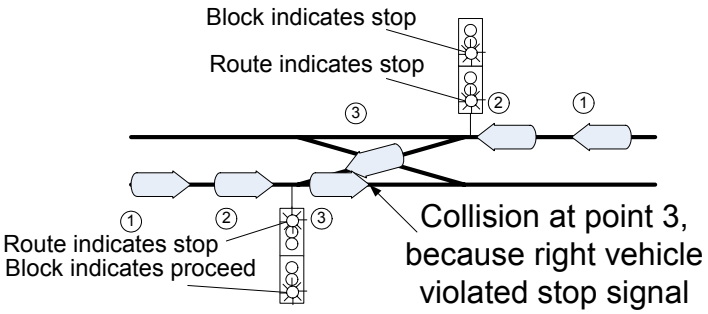

Figure 6: Switch Cross-Over EPDA Diagram.

7 CONCLUSIONS

The Magplane ASCAP framework simulation provides a rapid prototyping and feasibility tool set during the early stages of a Magplane system application.

The rapid prototyping focus is the specification of an alignment and the dynamic movement of *n*-vehicles that travel over the proposed alignment. The dynamic movement considers guideway layout, traffic density flow, string chart vehicle schedules and the power consumption.

As the Magplane system design approaches revenue service deployment, a detailed risk assessment that is USA FRA compliant will be provided.

Expert Systems build the guideway beam layout, CBTC signaling subsystem and the propulsion guideway configuration. In addition, the capability to generate dynamic safety exposure event trees and EPADS provide a new, novel and innovative approach to the development of a tool set that extends the traditional safety toolsets of today.

8 ACKNOWLEDGMENTS

The contributions made by Dr. Jiarong Fang and Mr. Marc Monfalcone are greatly appreciated. The work presented could not have been accomplished without their dedicated effort.

9 REFERENCES

[1] D. B. Montgomery, "Overview of the 2004 Magplane Design", Magplane Technology, Inc., Bedford, MA 01730

[2] E. Cutright, Y. Ou, Y.-Y. Cao, H. Zhang, M. Monfalcone, N. Ghaly and T. Giras., "Axiomatic Safety-Critical Assessment Process (ASCAP) Risk Assessment of a Transit Signaling System," , pp. 2262-2268, Berlin,, *Proceedings of PSAM 7 – ESREL'04*, Germany, 2004.

[3] FRA Rule 49 CFR Part 209/234/235, *Standards for the Use of Processor-based Signal and Train Control Systems*, Federal Register, March 2005.

[4] Fang, Jiarong, Alexey Radovinsky, D. B. Montgomery, "Dynamic Modeling and Control of the Magplane Vehicle", MIT Plasma Science and Fusion Center, 185 Albany Street, Cambridge, MA 02139.