Risk Analysis of Autonomous Vehicles in Mixed Traffic Streams

Parth Bhavsar, Plaban Das, Matthew Paugh, Kakan Dey, and Mashrur Chowdhury

The introduction of autonomous vehicles in the surface transportation system could improve traffic safety and reduce traffic congestion and negative environmental effects. Although the continuous evolution in computing, sensing, and communication technologies can improve the performance of autonomous vehicles, the new combination of autonomous automotive and electronic communication technologies will present new challenges, such as interaction with other nonautonomous vehicles, which must be addressed before implementation. The objective of this study was to identify the risks associated with the failure of an autonomous vehicle in mixed traffic streams. To identify the risks, the autonomous vehicle system was first disassembled into vehicular components and transportation infrastructure components, and then a fault tree model was developed for each system. The failure probabilities of each component were estimated by reviewing the published literature and publicly available data sources. This analysis resulted in a failure probability of about 14% resulting from a sequential failure of the autonomous vehicular components alone in the vehicle's lifetime, particularly the components responsible for automation. After the failure probability of autonomous vehicle components was combined with the failure probability of transportation infrastructure components, an overall failure probability related to vehicular or infrastructure components was found: 158 per 1 million mi of travel. The most critical combination of events that could lead to failure of autonomous vehicles, known as minimal cut-sets, was also identified. Finally, the results of fault tree analysis were compared with real-world data available from the California Department of Motor Vehicles autonomous vehicle testing records.

According to the recent ASCE report card, traffic congestion in 2014 in the United States resulted in a loss of $160 billion, which is higher than the total annual gross domestic product of 130 countries (*1, 2*). In addition to the loss of revenue and resources, the congested conditions on any roadway have a tendency to increase risky driving behaviors (*3*). According to a 2013 report from NHTSA, traffic crashes were responsible for 90 deaths per day on U.S. highways, and of those deaths, nine were caused by distracted driving (*4*). Identifying causes behind those crashes and finding solutions are challenging as human behavioral factors are responsible for 94% of all road crashes in the United States (*5, 6*). A study by Fagnant and Kockelman estimated that with a 90% market penetration, autonomous vehicles could reduce more than 4 million crashes and save more than 21,000 lives per year (*7*). Automotive companies and academic researchers have been developing and testing these technologies to improve the safety and efficiency of surface transportation systems. The autonomous vehicles could drastically change current land use practices by reducing the parking spots, and even billboards could be replaced by ads on vehicle windshields (*8*).

Autonomous vehicles have the potential to become a safe, sustainable, yet personal, mode of transportation. Despite the significant benefits of autonomous vehicles, they must be evaluated before mass deployment. According to annual disengagement reports submitted to the California Department of Motor Vehicles (DMV) by various companies that are testing autonomous vehicles, nonautonomous vehicles driven by human drivers were the primary cause for a significant number of incidents (*9–13*). In addition to the vulnerability of nonautonomous (i.e., conventional) vehicles, autonomous vehicles are vulnerable to software and hardware glitches and hacking. While testing self-driving cars, operators activated 2,700 disengagements in which control was taken over from the automation system and went to the manual driving mode because of nonideal autonomous driving situations, such as potholes, poor lane markings, construction zones, and bad weather (*14–16*). Researchers recently developed a system consisting of low-power lasers and a pulse generator that can fool autonomous vehicle sensors, such as lidar, into seeing objects where none really exists (*17*). Ensuring the cybersecurity of autonomous vehicles will be critical for mass acceptance. It has been found that hackers could remotely take over the control of brakes, acceleration, and other components (*18*). Hence, it is essential to assess risks associated with autonomous vehicles before implementation.

The objective of this study was to perform a comprehensive risk analysis of autonomous vehicles with a fault tree analysis method. For this study, an autonomous vehicle is defined as a fully autonomous passenger car or a similar vehicle that closely represents Level 4 automation as defined by NHTSA and does not include transit or other type of on- or off-the-road vehicles (*19*).

RELATED WORK

The risk analysis process focuses on overcoming potential threats of failure to ensure a safer system. The fault tree analysis is one of the risk analysis methods that focuses on identifying the hierarchical failure of a system. This method is used in various fields, including aircraft design processes (*20*), nuclear power plant design (*21*),

P. Bhavsar, P. Das, and M. Paugh, Department of Civil and Environmental Engineering, Henry M. Rowan College of Engineering, Rowan University, 201 Mullica Hill Road, Glassboro, NJ 08028. K. Dey, Department of Civil and Environmental Engineering, Benjamin M. Statler College of Engineering and Mineral Resources, West Virginia University, Office 647 ESB, Morgantown, WV 26506. M. Chowdhury, Glenn Department of Civil Engineering, College of Engineering, Computing, and Applied Sciences, Clemson University, 216 Lowry Hall, Clemson, SC 29634. Corresponding author: P. Bhavsar, bhavsar@rowan.edu.

Transportation Research Record: Journal of the Transportation Research Board, No. 2625, 2017, pp. 51–61.
http://dx.doi.org/10.3141/2625-06

industrial plant designs (*22, 23*), bridge failure analysis (*24*), construction project management (*25*), toxic goods transport (*26*), hazardous site management performance (*27*), and medicine (*28*). For risk analysis, a failure can be quantified as the difference between the actual outputs and the expected outputs (*29*). The fault tree analysis method was used for this study because of its capability of providing the shortest path (i.e., cut-sets) to failure from a single component failure to autonomous vehicle failure.

Comprehensive risk analysis of an autonomous vehicle system could lead to a safe and reliable transportation system. Several researchers have focused on developing or integrating risk assessment methods for various subsystems of the autonomous vehicle. Lefevre et al. surveyed motion prediction methods and relevant risk assessment methods that focused on collision prediction (*30*). Collision-related risk scenarios were identified by deriving the intersection point(s) or overlapping region(s) between the shapes of two vehicles in future trajectories; different shapes were considered, that is, set of points (*31*), circles (*32*), and polygons (*33*), and then the risk probability was calculated as the percentage of overlap. Instead of using a straight line, differentiable continuous curves were adopted to generate a better representation of vehicle trajectories on curved road sections (*34*). These risk analysis methods, however, are computationally expensive as they must be coupled with motion prediction models to improve efficiency. Wardzinski also developed a risk assessment method for motion planning based on physical parameters of a vehicle; however, the study did not include weather conditions and road surface characteristics (*35*). Laugier et al. updated the collision risk estimation method and used hidden Markov models and Gaussian process models to estimate risks as stochastic variables for simple traffic scenarios (*36*). Researchers also considered predefined nominal behaviors of a vehicle (i.e., speeds approaching an intersection) (*37*), real trajectories (*38*), weather conditions, and fatigue level of the driver (*39*) to develop various risk analysis models. Data from vehicle sensors were also used to develop knowledge-based risk assessment frameworks (*40, 41*). The risk related to subsystems of the autonomous vehicles, such as lane departure warning (*42, 43*) and driving assistance subsystem (*44–46*), was also evaluated. Mohammad et al. developed a framework using the ontology tool to successfully identify and assess risks resulting from pedestrian behavior in different traffic scenarios; however, they did not consider road types, environment conditions, and incoming traffic (*47*). Recently, Duran et al. used fault trees for risk analysis of autonomous vehicles based on the Bayesian belief network approach method (*48*), in which they considered only vehicle optical systems (lidar and camera).

Comprehensive risk analysis for any system includes considering all possible failures of associated subsystems, components, and technologies. To the best of the authors' knowledge, a fault tree–based risk analysis focusing on autonomous vehicles that considers vehicular components and other road users navigating in a mixed traffic stream has not yet been performed. However, several original equipment manufacturers and software companies, such as Google, are developing and evaluating prototypes of autonomous vehicles. The outcomes of these experiments are used to validate results.

METHODOLOGY

In this study, risk analyses were conducted by following three distinct and interconnected phases as identified by White: (*a*) risk identification, (*b*) risk estimation, and (*c*) evaluation of the fault tree model (*49*). Figure 1 illustrates the research approach adopted in this research. Risk identification of autonomous vehicle failure is the first crucial step in performing a risk analysis, which consists of compiling different types of autonomous vehicle failure information that includes (*a*) the nature and extent of the failure sources, (*b*) chain of events, (*c*) pathways and processes that connect the cause to the effect, and (*d*) relationship between risk sources and effects (*50*). Risk estimation can be performed with various analysis methods. In this study, the fault tree analysis method is used. Finally, the risk estimations were validated with their comparison with the real-world data. In the following subsections, details about three autonomous vehicle risk analysis phases adopted in this research are discussed.

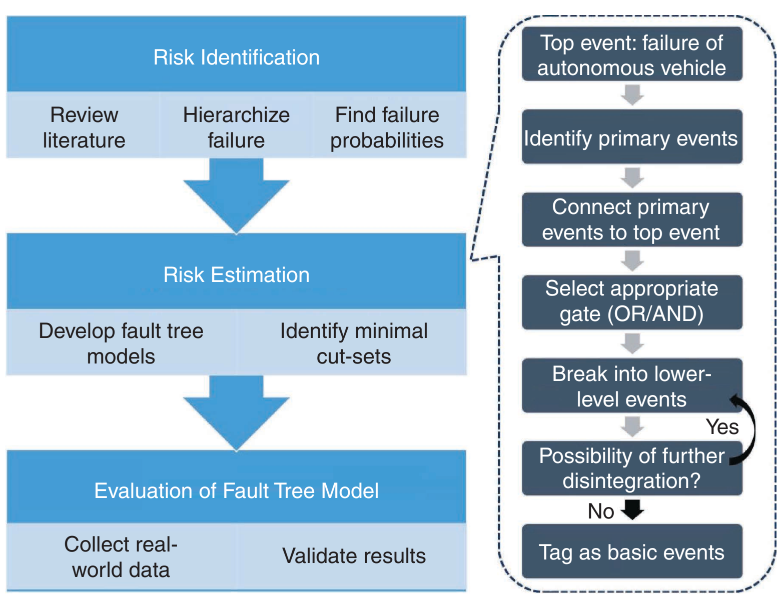

FIGURE 1 Research approach.

Risk Identification

To begin the risk identification step, the autonomous vehicle system is disintegrated into each of its individual components, the behavior of these components are then examined, and the failure rate is determined for each component. A literature review has been conducted of published reports, peer-reviewed conference and journal papers, and other published materials to develop hierarchical and logical relationships between the top-level event (i.e., failure of an autonomous vehicle) and different autonomous vehicle components.

It is fair to assume that for a surface transportation system of any region, the transition from a conventional vehicle fleet (i.e., nonautonomous) to an autonomous vehicle fleet will not take place in a short period (i.e., a few years). A gradual penetration of autonomous vehicles during a period of many years is a viable assumption. That assumption suggests that autonomous vehicles will be sharing the roadway with conventional vehicles, such as cars, transit buses, trucks, as well as bicycle riders, motorcyclists, and pedestrians. To estimate failure risks of autonomous vehicles related to all transportation system components, the risk identification process was divided into two subcategories. The first category focused on identifying threats from vehicular components, and the second category focused on identifying threats from infrastructure components, including the threats from other nonautonomous vehicles. As presented in the section on risk estimation, two fault tree models were developed: (*a*) a fault tree model for autonomous vehicle failure resulting from vehicular component failures and (*b*) a fault tree model for autonomous vehicle failure resulting from transportation infrastructure component failures. These models were combined afterward to estimate the overall risk of failure, that is, the failure of an autonomous vehicle in mixed traffic stream.

Autonomous Vehicle Components

All vehicular components were classified into four major subsystems: hardware, software, communication, and a human–machine interface. All sensors—such as lidar, GPS, wheel encoders, and the integration platform—were included in the hardware subsystem; the software subsystem consisted of the data collection and processing software required for sensors and autonomous navigation. The communication subsystem included a vehicle-to-vehicle or vehicle-to-infrastructure communication platform, and a human–machine interface included a personal assistant system that filters human voice for commands to control various autonomous driving functions. In this study, only additional new technologies that convert a conventional human-operated vehicle into an autonomous vehicle were considered. For example, lidar, the primary technology being used for autonomous navigation, can fail owing to several reasons, including laser malfunction and electrical failures (*48*). Similarly, other autonomous vehicle components were identified, and the failure probability for each component is summarized in Table 1 according to findings from the literature review. The failure of the vehicle's mechanical system was not considered in this study as it is not part of the system that converts a conventional vehicle into an autonomous vehicle.

Transportation Infrastructure Components

Failure of the autonomous vehicle as a result of the surrounding infrastructure, including other nonautonomous vehicles and the transportation infrastructure, can contribute to the failure of an autonomous vehicle system. According to reports submitted by companies conducting the testing of autonomous vehicles, most autonomous vehicle–involved crashes are the result of human drivers sharing the road with autonomous vehicles (*9–13*). At a low market penetration level of autonomous vehicles, nonautonomous vehicle driver errors could be an important issue involving driving in mixed traffic streams. Crash records related to reckless driving, distraction, hardware breakdown, and tiredness, as well as the incident rate owing to poor weather and road conditions were collected from the Virginia Department of Transportation (DOT) and the New York State DOT traffic crash reports (*61, 62*). To calculate the failure probability of an autonomous vehicle traveling in a mixed traffic stream, a penetration rate of 10% autonomous vehicles was considered. To consider the worst-case scenario, it was assumed that 10% of total crashes (reported by the Virginia DOT and the New York State DOT) will involve an autonomous vehicle and a nonautonomous vehicle.

The data collected from the departments of transportation are then converted into crash rate per miles of autonomous vehicle travel and used in the fault tree as the failure probability of basic events. The following example presents failure probability calculations for an autonomous vehicle when it is involved in a crash resulting from reckless driving, tiredness, and distraction by a driver of a nonautonomous vehicle, as well as the breakdown of the nonautonomous vehicle (see Equation Box 1).

Crashes related to bicyclists and pedestrians were also considered. A study in Hawaii found that 83.5% of collisions between motor vehicles and cyclists were caused by motorists and the other 16.5% of collisions were caused by cyclists (*63*). Also considered were construction work zones, particularly rear-end crashes in the work zone (*64*). The failure probabilities of these infrastructure components are given in Table 2.

Risk Estimation

The fault tree analysis method was used to estimate risk. Two fault tree models based on the outcomes of the risk identification phase were developed, as explained in the following subsections.

Fault Tree for Autonomous Vehicular Component Failures

The first fault tree model focused on the failure of an autonomous vehicle owing to vehicular components. Isograph FaultTree+ software, which allows various statistical models to model the basic event failure probability distribution, was used for fault tree analysis (*71*). For this study, a "fixed probability" statistical model was used to perform the risk analysis. The development of the fault tree began with a top-level event—"an autonomous vehicle failure related to vehicular components." The top-level failure probability was estimated in regard to the number of times autonomous vehicle operations could be stopped during the vehicle's lifetime as a result of the occurrence of one or more basic events.

After basic event failure probabilities were allocated and the fault tree was solved with Isograph FaultTree+ software, a failure rate of 14.22% was found for the failure of an autonomous vehicle resulting from its components' failure, which means that autonomous vehicle operations could be stopped 14.22 times during the vehicle's lifetime. Figure 2 illustrates the fault tree with failure probabilities, including only autonomous vehicle components.

TABLE 1 Failure Probabilities of Autonomous Vehicular Components

Basic Event	Description	Methods	Experiment Type	Failure Probability (%)
Lidar failure	Laser malfunction, mirror motor malfunction, position encoder failure, overvoltage, short-circuit, optical receiver damages	Bayesian belief network	Simulation	10.0000 (*48*)
Radar failure	Detection curves drawn with respect to signal and noise ratios	Chi-square distribution	Mathematical modeling	2.0000 (*51*)
Camera failure	Foreign particles, shock wave, overvoltage, short-circuit, vibration from rough terrain, etc.	Bayesian belief network	Simulation	4.9500 (*48*)
Software failure	System had to generate outputs from array definition language statements	Extended Markov Bayesian network	Experiment (3,000 runs)	1.0000 (*52*)
Wheel encoder failure	Encoder feedback unable to be transferred, which can cause loss of synchronization of motor stator and rotor positions	Kalman filter	Experiment	4.0000 (*53*)
GPS failure	Real-life tests performed with high-sensitivity GPS in different signal environments (static and dynamic) for more than 14 h	Least squares	Experiment (at 4 locations)	0.9250 (*54*)
Database service failure	Using new empirical approach, connectivity and operability data of a server system were collected.	Generic quorum-system evaluator	Experiment (for 191 days)	3.8600 (*55*)
Communication failure	Wi-Fi: Periodic transmission of 1,000-byte frames (average conditional probability of success after previous success considered)	In IEEE 802.11b network	Experiment (with 10 vehicles)	5.1250 (*56*)
	LTE: Network unavailability during location update in mobility was considered here	Application of CAP theorem	Experiment	5.8800 (*57*)
Integrated platform failure	A two-state model with failure rates was developed to estimate the computer system availability.	Markov chain model	Mathematical modeling	2.0000 (*58*)
Human command error	Three data sets of over 115 months from NASA were analyzed and then validated by three methods (THERP, CREAM, and NARA) to facilitate NASA risk assessment.	Human reliability analysis	Experiment (from December 1998 to June 2008)	0.0530 (*59*)
System failed to detect human command	System unable to detect the accurate acoustic command; driver inputs the wrong command, and system unable to detect wrong commands	Artificial neural networks on clean speech	Experiments (37 subjects: 185 recording)	1.4000 (*60*)

EQUATION BOX 1 Sample Calculation

Number of crashes resulting from reckless driving = 69,284 per 100 million mi (*61*)

Number of crashes resulting from tiredness = 3,121 per 100 million mi (*61*)

Number of crashes resulting from distraction = 51,496 per 100 million mi (*61*)

Number of crashes resulting from vehicle breakdown = 10,000 per 100 million mi (*62*)

Total nonautonomous vehicle–involved crashes = 133,901 per 100 million mi.

Failure probability resulting from tiredness, reckless driving, distractions, and vehicle breakdown

$$= \frac{133{,}901}{100 \times 1{,}000{,}000} \times 100\% = 0.1339\% \text{ per mi}$$

Failure probability of an autonomous vehicle involved in a crash with a nonautonomous vehicle = $0.1339 \times 10\% = 0.01339\%$ per mi

TABLE 2 Failure Probabilities of Basic Transportation System Infrastructure Components

Basic Event	Description	Number of Crashes	Failure Probability (% per mi)	References
Nonautonomous vehicles crashes	Crashes resulting from reckless driving, tiredness, hardware and distractions considered	133,901 (per 100 million mi)	0.0134	(*61, 62*)
Cyclists	Daily 9 million bike trips made; crashes that cyclists were responsible for are included here	3,090	4.0897×10^{-6}	(*65, 66, 67*)
Pedestrians	Crashes with pedestrians at fault for the annual 42 billion walking trips	8,625	2.9337×10^{-6}	(*65, 66, 68, 69*)
Construction zones	Among all work zones, 41.33% of crashes were rear-end crashes.	36,208	7.6264×10^{-6}	(*64, 70*)
Weather-related incidents	Adverse weather conditions such as fog, mist, rain, severe crosswind, sleet, snow, dust, and smoke	22,375 (per 100 million mi)	0.0022	(*61*)
Road conditions	Crashes related to improper lane marking and pavement conditions	656 (per 100 million mi)	6.5600×10^{-5}	(*62*)

Fault Tree for Infrastructure Component Failures

The top-level event for the second fault tree model was "failure of autonomous vehicle owing to infrastructure components." This model included failure of the autonomous vehicle because of other road users, weather, construction zones, or road conditions. Following the steps followed in the first fault tree, the second was constructed with other road users and the infrastructure failure probabilities. The infrastructure components–based fault tree is illustrated in Figure 3. It was found that the failure probability of an autonomous vehicle related to other road users and infrastructure was 0.01571%.

Combined Fault Tree

NASA estimates the failure probabilities of basic events through methods such as experimental estimation and simulation modeling (*72*). Opinions of subject matter experts are also considered in probability estimations (*73*). The risk analysis of NASA's missions often involves the integration of models that include failure probabilities computed by various methods (*72, 73*). Similarly, to estimate the failure probability of an autonomous vehicle traveling in a mixed traffic stream, the failure probabilities of vehicular and infrastructure components were combined (illustrated in Figure 4).

Table 1 presents failure probabilities of individual vehicular components estimated by researchers considering various conditions. However, when these components become parts or subsystems of an autonomous vehicle, the car manufacturer will ensure that they remain operational throughout the life of the vehicle with periodic health monitoring and maintenance. The typical lifetime of a conventional vehicle is about 150,000 mi (*74*). This information can be integrated to calculate the autonomous vehicle failure probability per mile. Given that the overall probability of autonomous vehicle failure related to vehicular components is 14.22%, the failure probability per mile can be estimated as 0.0000948% (14.22%/150,000). For the combined fault tree, it is assumed that the failure related to vehicular components and the failure related to the infrastructure system are independent of each other and can be combined with an "OR" gate to estimate the failure probability of the overall autonomous vehicle system. The following equation was used to calculate the failure probability for the top-level event (i.e., failure of autonomous vehicle) of the combined fault tree. The plus sign represents an OR gate. Autonomous navigation could be stopped 158 times in 1 million mi of travel because of the failure of either vehicular components or infrastructure components in a mixed traffic stream. The combined fault tree is shown in Figure 4.

$$\begin{aligned} P(A) &= P(\mathrm{VC}) + P(\mathrm{IC}) = 0.000000948 + 0.0001571 \\ &= 0.000158048 \text{ per mi of travel} \end{aligned}$$

where

$P(A)$ = overall failure probability of autonomous vehicle system per mi of travel,
$P(\mathrm{VC})$ = autonomous vehicle failure from vehicular components per mi of travel, and
$P(\mathrm{IC})$ = autonomous vehicle failure from infrastructure components per mi of travel.

Risk Hierarchy

One of the primary benefits of a fault tree analysis is its ability to develop the cut-sets, which are essentially the hierarchical sequence of events that can result in the failure of the main event. Cut-sets also help engineers and decision makers to prioritize which components need to be addressed first to improve the safety performance of an autonomous vehicle. Once all cut-sets are identified, they can be ranked with associated failure probabilities.

Ten cut-sets were distinguished in the analyzed fault trees considering the failure probabilities of vehicular components and infrastructure components with the use of Isograph FaultTree+ software. These cut-sets were ranked in order of their failure probabilities. Table 3 presents ranked cut-sets with their failure probabilities. It was found that the failure of the communication system could be the most vulnerable event of all of the basic events; the failure probability is 9.513%. Hardware system failure, which is caused by sensitive sensor and actuator failures, was found in the second position with a failure probability of 4.249%.

Evaluation of Fault Tree Model

A fault tree analysis model could be validated qualitatively and quantitatively. The qualitative validation method considers the

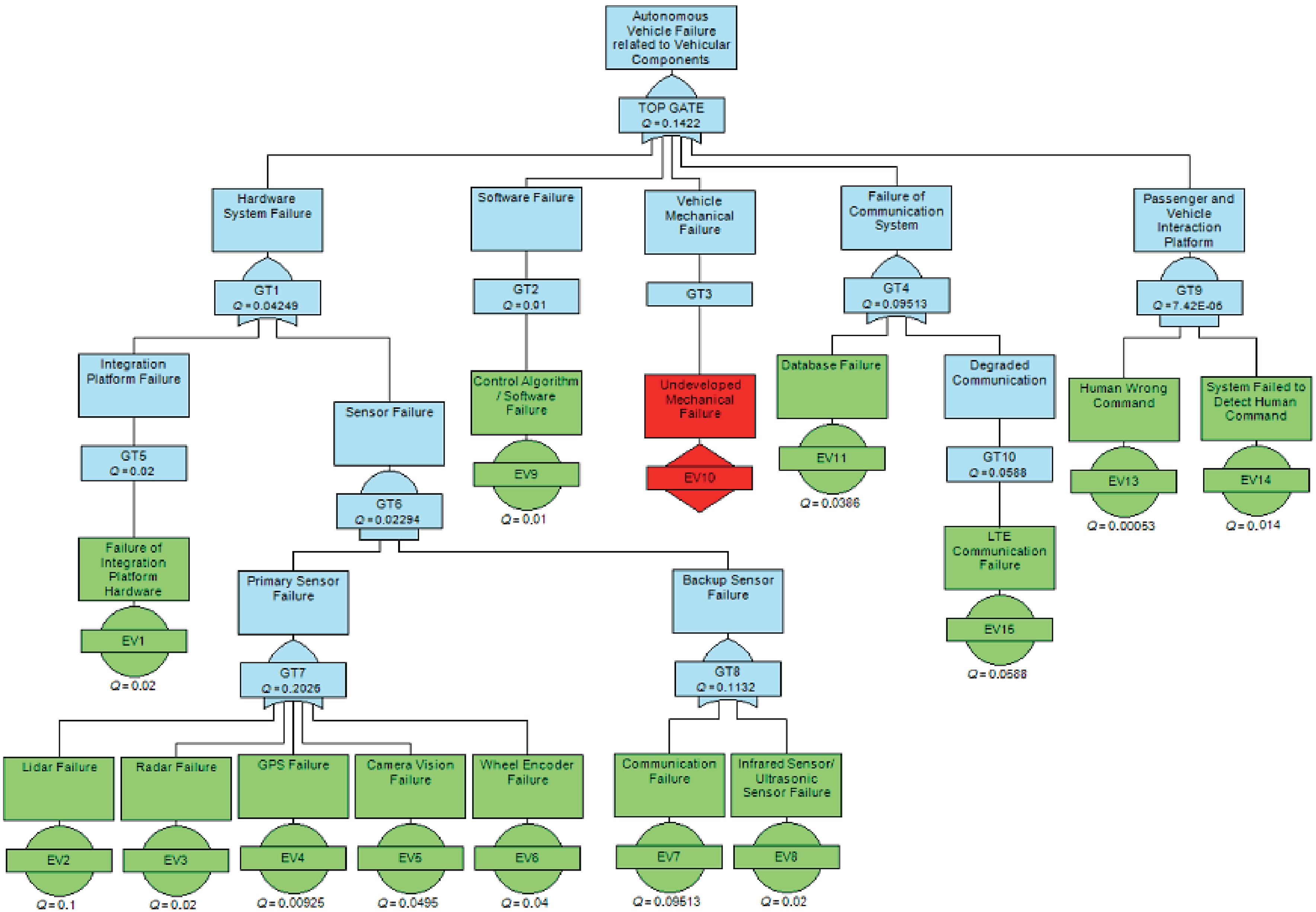

FIGURE 2 Fault tree analysis considering failure related to vehicular components (*Q* = probability value either inputted into the fault tree or calculated by fault tree analysis).

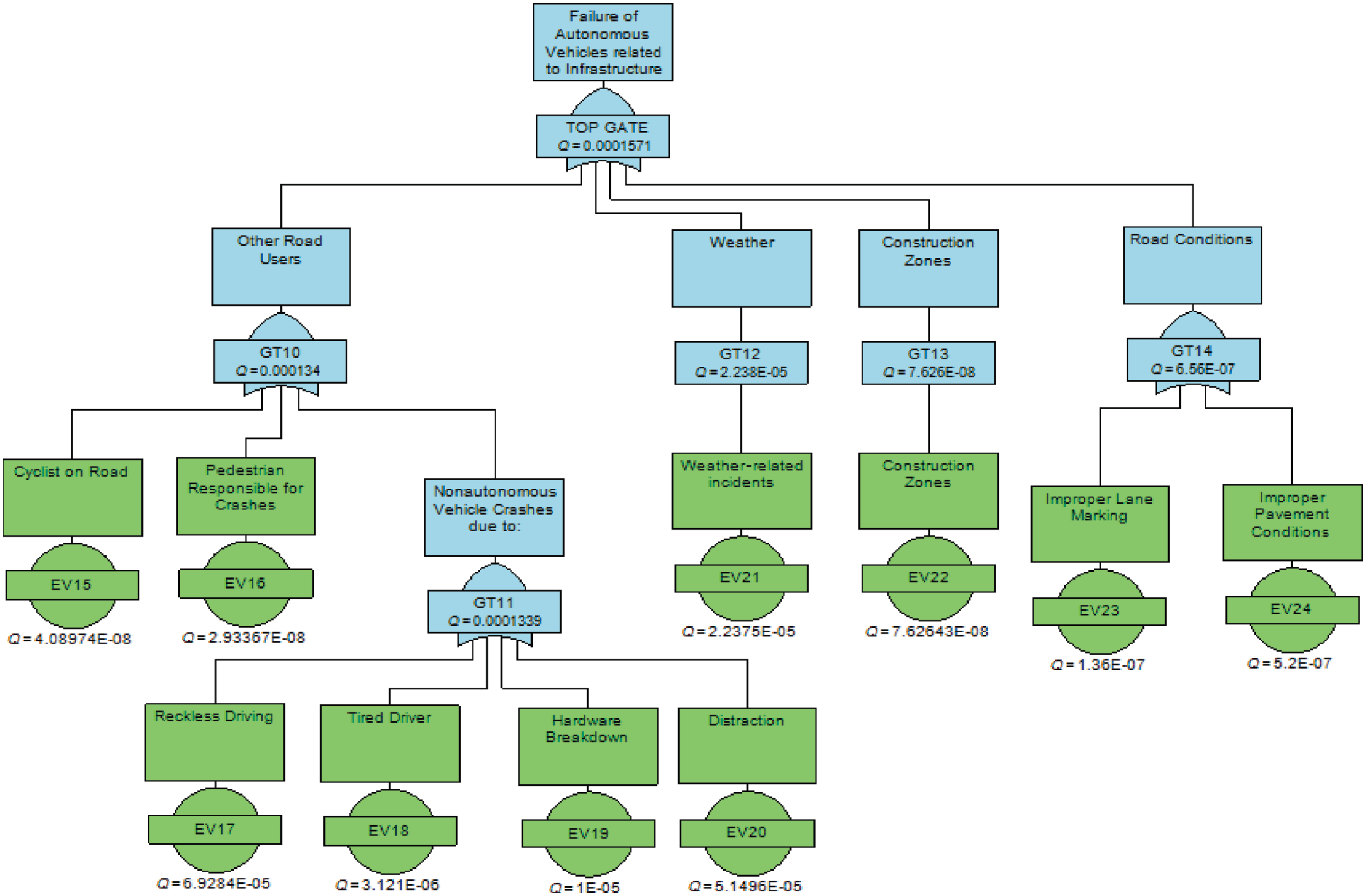

FIGURE 3 Fault tree analysis considering failure related to transportation infrastructure components.

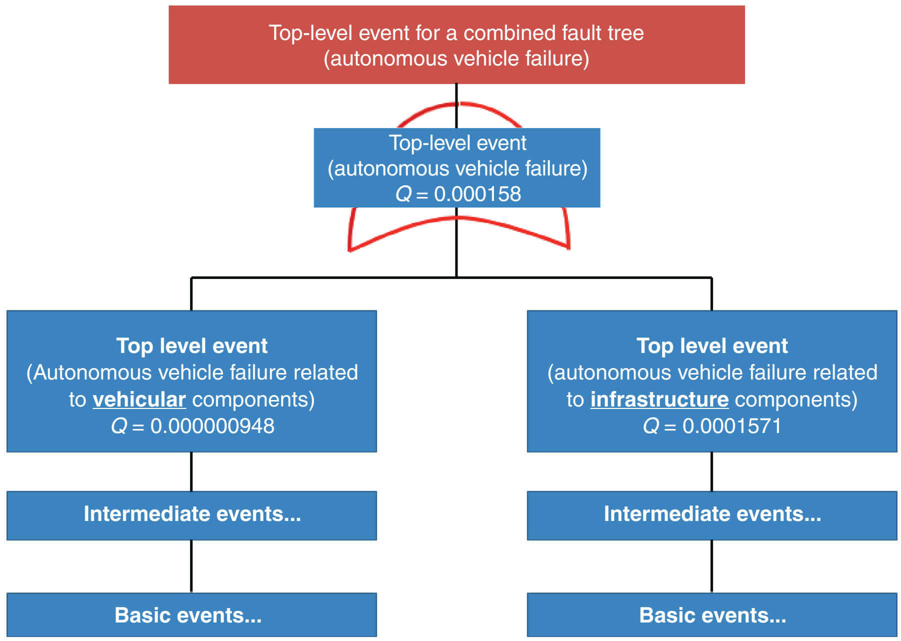

FIGURE 4 Fault tree analysis considering failure of autonomous vehicles in mixed traffic streams.

basic events identification and their relationship with the top-level event(s). Quantitative method reviews measure the failure probabilities (*75*). Results were validated with the real-world data available from the California DMV autonomous vehicle testing records (*9–13*). According to California DMV autonomous vehicle testing regulations, all autonomous vehicle manufacturers and developers holding a permit to test have to forward crash and disengagement reports (*76*). The collected data are summarized in Table 4.

The failure probabilities of cut-sets were compared to validate the fault tree analysis findings with the percentages of each crash type from California DMV autonomous vehicle reports as these crashes represent the same basic event failures that lead to cut-sets. Figure 5 presents a comparison of the rank given to each reason for system failure by the final combined fault tree model versus the real-world data. In Figure 5, for each reason of system failure, the failure probability decreases with the increase in number. For example, a rank of 2 for hardware system failure suggests that there is a high probability of failure compared with a rank of 8 for failure related to construction zones.

As illustrated in Figure 5, the communication system failure with a rank of 1 from fault tree estimation and real-world data has significant effects on autonomous vehicle operations. The significant difference in ranking of the failure related to "wrong command" suggests that in the real world, the software system and algorithms are going through an evaluation process. The higher ranking (i.e., lower failure probability) provided by the fault tree model for this particular event also suggests that an artificial neural network can significantly improve the speech recognition process and reduce incidents for the autonomous vehicle (*60*). The lower real-world ranking (i.e., higher failure probability) of weather events and nonautonomous vehicle events suggests that autonomous vehicles are not tested in various weather conditions and at different penetration levels. Similarly, the higher fault tree ranking for road condition events may be an indicator of the lower performance of the lane-marking detection system.

TABLE 3 Minimal Cut-Sets

Rank	Cut-Sets	Boolean Expression	Failure Probability (%)
1	Failure of communication system (GT4)	EV11 + EV12	9.5130
2	Hardware system failure (GT1)	EV1 + [(EV2 + EV3 + EV4 + EV5 + EV6) * (EV7 + EV8)]	4.2490
3	Software system failure (GT2)	EV9	1.0000
4	Nonautonomous vehicles crashes (GT11)	EV17 + EV18 + EV19 + EV20	0.0134
5	Weather (GT12)	EV21	0.0022
6	Passenger and vehicle interaction platform (wrong command) (GT9)	(EV13 * EV14)	7.4200×10^{-4}
7	Road condition (GT14)	EV23 + EV24	6.5600×10^{-5}
8	Construction zones (GT13)	EV22	7.6264×10^{-6}
9	Cyclists	EV15	4.0897×10^{-6}
10	Pedestrians	EV16	2.9337×10^{-6}

TABLE 4 California DMV Autonomous Vehicles Testing Data

System Failure	Description	No. of Incidents	Percentage of Incidents	Rank	References
Hardware system	Hardware discrepancy, issue with tuning and calibration, and unwanted maneuver	288	17.8439	3	(*9–11*)
Software system	Software discrepancy and unable to detect vehicle or obstacles	80	4.9566	5	(*9*)
Communication system	Planner data not received, drop off on received data, communication evaluation management failure	642	39.777	1	(*12, 13*)
Nonautonomous vehicle crashes	Nonautonomous vehicle behaviors at low penetration level of autonomous vehicles	68	4.2131	6	(*9–11*)
Wrong command	Human uncomfortable to continue automation	487	30.1735	2	(*12*)
Construction zones	Signs, hand signals, lane closures, and sudden reduction of speed represent the construction zone scenarios.	31	1.9207	7	(*9, 10*)
Road conditions	Lane marking and adverse road surface conditions	111	6.4125	4	(*9, 10*)
Weather	Rainy, sun glare, twilight, cloudy: poor sunlight conditions and nighttime are considered here.	18	1.1152	8	(*9, 10*)

CONCLUSIONS

Autonomous vehicles have the potential to transform existing transportation systems into a truly safe and sustainable next-generation transportation system. Thus, performing a comprehensive risk analysis of an autonomous vehicle is the first crucial step toward developing safe autonomous vehicles and supporting transportation infrastructure. Tackling the risks related to these early autonomous vehicle technologies will help fix considerable issues before the mass deployment of the vehicles on public roads. Successful identification of the risks related to the vehicle and the surrounding infrastructure helps researchers and developers to improve the technology.

This study used the fault tree–based risk analysis method to identify the most critical basic events that could lead to an autonomous vehicle failure. Findings from the fault tree analysis could be used to develop risk minimization strategies to eliminate or reduce component failure risks that will improve overall autonomous vehicle reliability. Through this process, specific components were found to be crucial in determining risk minimization strategies. For example, the lidar, radar, cameras, GPS systems, and wheel encoder sensors together have a failure probability of more than 20%. However, continuous innovations in computing and communication technologies can significantly reduce this failure probability. In addition, installing backup sensors can significantly reduce failure probability.

A gradual introduction of autonomous vehicles into the future traffic stream was assumed; hence, it is important to analyze autonomous vehicle failure related to nonautonomous vehicles or human drivers. Reckless human drivers were found to be a primary concern for autonomous vehicles in the mixed traffic stream. However, with the increased market penetration of autonomous vehicles, this scenario could change and could reduce the failure probability for safe autonomous navigation.

LIMITATIONS OF THIS RESEARCH

This study did not consider failure of mechanical systems as they are not a part of the automation. However, automation technologies will also be integrated with mechanical systems and must be analyzed together for in-depth analysis. The available literature was relied on significantly to identify the failure probabilities of basic

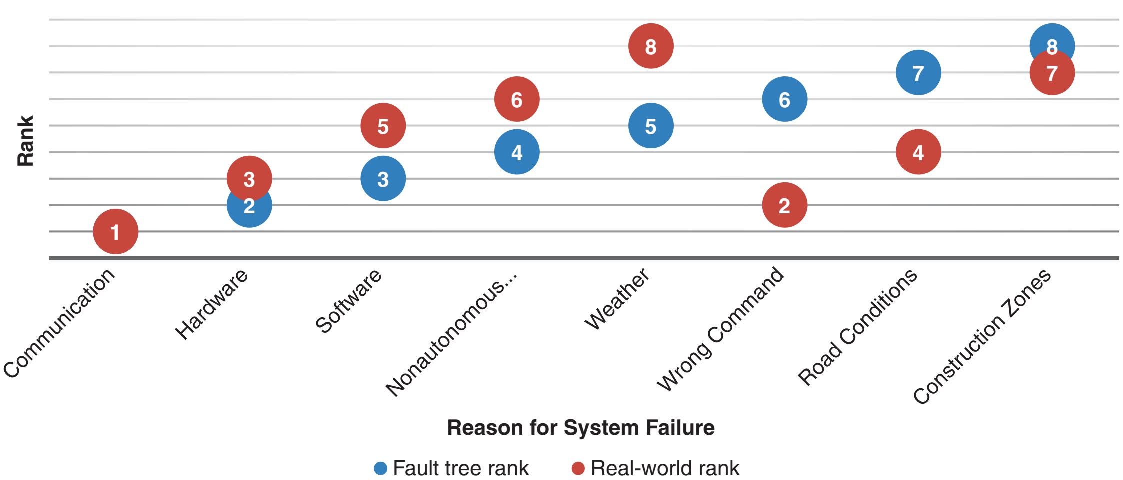

FIGURE 5 Validation: fault tree estimation versus real-world data.

events. Because of the limited availability of the data, it was not possible to statistically validate periential failure probabilities identified in this study. Furthermore, for this study it was assumed that the failure rate of autonomous vehicles will remain constant over time. Basic events for each fault tree were assumed independent. However, correlations may exist between basic events in some cases. For example, a lidar sensor (Figure 2) may rely on the power supply provided by a vehicle battery. In addition, it was assumed that a failure of an autonomous vehicle related to vehicular components and a failure related to transportation infrastructure components are two independent events and were combined with an OR gate for the combined fault tree. The interdependency of these two events, as well as the correlation between basic events, requires further investigation to improve the risk estimation for autonomous vehicles.

ACKNOWLEDGMENTS

This research was supported by the U.S. Department of Transportation Region 2 University Transportation Research Center. Umashanger Thayasivam from the Department of Mathematics at Rowan University is acknowledged for providing theoretical assistance.

REFERENCES

1. Schrank, D., B. Eisele, T. Lomax, and J. Bak. *2015 Urban Mobility Scorecard.* Texas A&M Transportation Institute and Inrix, Inc., 2015.
2. National Accounts Main Aggregates Database*.* United Nations Statistics Division, United Nations Department of Economic and Social Affairs, 2015.
3. Salomon, I., and P.L. Mokhtarian. Coping with Congestion: Understanding the Gap Between Policy Assumptions and Behavior. *Transportation Research Part D, Transport and Environment,* Vol. 2, No. 2, 1997, pp. 107–123. https://doi.org/10.1016/S1361-9209(97)00003-5.
4. NHTSA, U.S. Department of Transportation. *Traffic Safety Facts 2013: A Compilation of Motor Vehicle Crash Data from the Fatality Analysis Reporting System and the General Estimates System.* Publication DOT HS 812 139. 2015.
5. Petridou, E., and M. Moustaki. Human Factors in the Causation of Road Traffic Crashes. *European Journal of Epidemiology,* Vol. 16, No. 9, 2000, pp. 819–826. https://doi.org/10.1023/A:1007649804201.
6. Williams, A.F., and B. O'Neill. On the Road Driving Records of Licensed Race Drivers. *Accident Analysis and Prevention,* Vol. 72, No. 3/4, 1974, pp. 260–272.
7. Fagnant, D.J., and K. Kockelman. Preparing a Nation for Autonomous Vehicles: Opportunities, Barriers and Policy Recommendations. *Transportation Research Part A, Policy and Practice,* Vol. 77, 2015, pp. 167–181. https://doi.org/10.1016/j.tra.2015.04.003.
8. Skinner, R., and N. Bidwell. Making Better Places: Autonomous Vehicles and Future Opportunities. WSP, Parsons Brinckerhoff Engineering Services, and Farrells, 2016.
9. Google. *Autonomous Vehicles Annual Disengagement Report.* California Department of Autonomous Vehicles, 2016.
10. Delphi. *Autonomous Vehicles Annual Disengagement Report.* California Department of Autonomous Vehicles, 2016.
11. Nissan. *Autonomous Vehicles Annual Disengagement Report.* California Department of Autonomous Vehicles, 2016.
12. Mercedes-Benz. *Autonomous Vehicles Annual Disengagement Report.* California Department of Autonomous Vehicles, 2016.
13. Volkswagen. *Autonomous Vehicles Annual Disengagement Report.* California Department of Autonomous Vehicles, 2016.
14. Vincent, J. Google's Self-Driving Cars Would've Hit Something 13 Times If Not for Humans. *The Verge.* http://www.theverge.com/2016/1/13/10759424/google-self-driving-car-accidents-driver-disengagements. Accessed Feb. 15, 2016.
15. Fingas, J. *Self-Driving Cars Can Be Fooled by Fake Signals.* Engadget. http://gizmodo.com/6-simple-things-googles-self-driving-car-still-cant-han-1628040470. Accessed Feb. 15, 2016.
16. Sorokanich, R. *6 Simple Things Google's Self-Driving Car Still Can't Handle.* Gizmodo. http://www.engadget.com/2015/09/05/self-driving-car-lidar-exploit. Accessed Feb. 15, 2016.
17. Harris, M. Researcher Hacks Self-driving Car Sensors. *IEEE Spectrum.* http://spectrum.ieee.org/cars-that-think/transportation/self-driving/researcher-hacks-selfdriving-car-sensors. Accessed Feb. 15, 2016.
18. Simonite, T. Your Future Self-Driving Car Will Be Way More Hackable. *MIT Technology Review,* Massachusetts Institute of Technology, Cambridge, 2016.
19. Aldana, K. U.S. Department of Transportation Releases Policy on Automated Vehicle Development. *National Highway Traffic Safety Administration (NHTSA) New Release,* 2013.
20. Ericson, C.A. Fault Tree Analysis—A History. In *Proceedings of 17th International System Safety Conference.* Orlando, Fla., 1999, pp. 1–9.
21. Volkanovski, A., M. Cepin, and B. Mavko. Application of the Fault Tree Analysis for Assessment of Power System Reliability. *Reliability Engineering & System Safety,* Vol. 94, No. 6, 2009, pp. 1116–1127. https://doi.org/10.1016/j.ress.2009.01.004.
22. Alonso, C., and J. Gavalda. A Method to Determine Environmental Risk in Chemical Process Industries. *Ninth International Symposium Loss Prevention and Safety Promotion in the Process Industries,* 1998, pp. 1219–1227.
23. Schlechter, W.P.G. Facility Risk Review as a Means to Addressing Existing Risks During the Life Cycle of a Process Unit, Operation or Facility. *International Journal of Pressure Vessels and Piping,* Vol. 66, No. 1/3, 1996, pp. 387–402. https://doi.org/10.1016/0308-0161(95)00113-1.
24. Davis-McDaniel, C., M. Chowdhury, W.C. Pang, and K. Dey. Fault-Tree Model for Risk Assessment of Bridge Failure: Case Study for Segmental Box Girder Bridges. *Journal of Infrastructure Systems,* Vol. 19, No. 3, 2013, pp. 326–334. https://doi.org/10.1061/(ASCE)IS.1943-555X.0000129.
25. Chapman, C. Project Risk Analysis and Management—PRAM the Generic Process. *International Journal of Project Management,* Vol. 15, No. 5, 1997, pp. 273–281. https://doi.org/10.1016/S0263-7863(96)00079-8.
26. Tiemessen, G., and J.P. van Zweeden. Risk Assessment of the Transport of Hazardous Materials. In *Proceedings of 9th International Symposium Loss Prevention and Safety Promotion in the Process Industries,* 1998, pp. 299–307.
27. Hurst, N.W., S. Young, I. Donald, H. Gibson, and A. Muyselaar. Measures of Safety Management Performance and Attitudes to Safety at Major Hazard Sites. *Journal of Loss Prevention in the Process Industries,* Vol. 9, No. 2, 1996, pp. 161–172. https://doi.org/10.1016/0950-4230(96)00005-8.
28. Bogen, K.T. *Uncertainty in Environmental Health Risk Assessment.* Garland Publishing, New York, 1990.
29. Ammar, H.H., B. Cukic, A. Mili, and C. Fuhrman. A Comparative Analysis of Hardware and Software Fault Tolerance: Impact on Software Reliability Engineering. *Annals of Software Engineering,* Vol. 10, No. 1/4, 2000, pp. 103–150. https://doi.org/10.1023/A:1018987616443.
30. Lefevre, S., D. Vasquez, and C. Laugier. A Survey on Motion Prediction and Risk Assessment for Intelligent Vehicles. *ROBOMECH Journal,* Vol. 1, No. 1, 2014, pp. 1–14. https://doi.org/10.1186/s40648-014-0001-z.
31. Batz, T., K. Watson, and J. Beyerer. Recognition of Dangerous Situations within a Cooperative Group of Vehicles. In *Proceedings of 2009 IEEE Intelligent Vehicles Symposium,* 2009. pp. 907–912. https://doi.org/10.1109/IVS.2009.5164400.
32. Ammoun, S., and F. Nashashibi. Real-Time Trajectory Prediction for Collision Risk Estimation Between Vehicles. In *Proceedings of IEEE 5th International Conference on Intelligent Computer Communication and Processing,* 2009. pp. 417–422. https://doi.org/10.1109/ICCP.2009.5284727.
33. Broadhurst, A., S. Baker, and T. Kanade. Monte Carlo Road Safety Reasoning. In *2005 IEEE Proceedings, Intelligent Vehicles Symposium,* 2005, pp. 319–324.
34. Katrakazas, C., M. Quddus, W.-H. Chen, and L. Deka. Real-Time Motion Planning Methods for Autonomous On-Road Driving: State-of-the-Art and Future Research Directions. *Transportation Research Part C, Emerging Technologies,* Vol. 60, 2015, pp. 416–442. https://doi.org/10.1016/j.trc.2015.09.011.
35. Wardzinski, A. Dynamic Risk Assessment in Autonomous Vehicles Motion Planning. In *Proceedings of 1st IEEE International Conference on Information Technology,* 2008. pp. 1–4. https://doi.org/10.1109/INFTECH.2008.4621607.

36. Laugier, C., I.E. Paromtchik, M. Perrollaz, M. Yong, J.D. Yoder, C. Tay, K. Mekhnacha, and A. Negre. Probabilistic Analysis of Dynamic Scenes and Collision Risks Assessment to Improve Driving Safety. *IEEE Intelligent Transportation Systems Magazine,* Vol. 3, No. 4, 2011, pp. 4–19. https://doi.org/10.1109/MITS.2011.942779.
37. Ibanez-Guzman, J., S. Lefevre, A. Mokkadem, and S. Rodhaim. Vehicle to Vehicle Communications Applied to Road Intersection Safety, Field Results. In *Proceedings of 13th International IEEE Conference on Intelligent Transportation Systems* (ITSC), 2010, pp. 192–197. https://doi.org/10.1109/ITSC.2010.5625246.
38. Aoude, G.S., V.R. Desaraju, L.H. Stephens, and J.P. How. Driver Behavior Classification at Intersections and Validation on Large Naturalistic Data Set. *IEEE Transactions on Intelligent Transportation Systems,* Vol. 13, No. 2, 2012, pp. 724–736. https://doi.org/10.1109/TITS.2011.2179537.
39. Worrall, S., D. Orchansky, F. Masson, and E. Nebot. Improving Vehicle Safety Using Context Based Detection of Risk. In *Proceedings of 13th International IEEE Conference on Intelligent Transportation Systems* (ITSC), 2010, pp. 379–385. https://doi.org/10.1109/ITSC.2010.5625185.
40. Schamm, T., and J.M. Zollner. A Model-Based Approach to Probabilistic Situation Assessment for Driver Assistance Systems. In *Proceedings of 14th International IEEE Conference on Intelligent Transportation Systems* (ITSC), 2011, pp. 1404–1409. https://doi.org/10.1109/ITSC.2011.6082930.
41. Lattner, A.D., I.J. Timm, M. Lorenz, and O. Herzog. Knowledge-Based Risk Assessment for Intelligent Vehicles. *International Conference on Integration of Knowledge Intensive Multi-Agent Systems,* 2005, pp. 191–196. https://doi.org/10.1109/KIMAS.2005.1427078.
42. Yizhen, Z., E.K. Antonsson, and K. Grote. A New Threat Assessment Measure for Collision Avoidance Systems. *IEEE Intelligent Transportation Systems Conference,* 2006, pp. 968–975.
43. Gray, A., M. Ali, Y. Gao, J.K. Hedrick, and F. Borrelli. Integrated Threat Assessment and Control Design for Roadway Departure Avoidance. In *Proceedings of 15th International IEEE Conference on Intelligent Transportation Systems,* 2012, pp. 1714–1719. https://doi.org/10.1109/ITSC.2012.6338781.
44. Pollard, E., P. Morignot, and F. Nashashibi. An Ontology-Based Model to Determine the Automation Level of an Automated Vehicle for Co-Driving. Presented at 16th International Conference on Information Fusion (FUSION), 2013, pp. 596–603.
45. Armand, A., D. Filliat, and J. Ibanez-Guzman. Ontology-Based Context Awareness for Driving Assistance Systems. In *2014 IEEE Intelligent Vehicles Symposium Proceedings,* 2014, pp. 227–233. https://doi.org/10.1109/IVS.2014.6856509.
46. Hulsen, M., J.M. Zollner, and C. Weiss. Traffic Intersection Situation Description Ontology for Advanced Driver Assistance. *IEEE Intelligent Vehicles Symposium (IV), 2011,* 2011, pp. 993–999. https://doi.org/10.1109/IVS.2011.5940415.
47. Mohammad, M.A., I. Kaloskampis, Y. Hicks, and R. Setchi. Ontology-Based Framework for Risk Assessment in Road Scenes Using Videos. Presented at 19th International Conference on Knowledge Based and Intelligent Information and Engineering Systems, Singapore, 2015. https://doi.org/10.1016/j.procs.2015.08.300.
48. Duran, D.R., E. Robinson, A.J. Kornecki, and J. Zalewski. Safety Analysis of Autonomous Ground Vehicle Optical Systems: Bayesian Belief Networks Approach. In *Federated Conference on Computer Science and Information Systems* (*FedCSIS*), 2013, pp. 1419–1425.
49. White, D. Application of Systems Thinking to Risk Management: A Review of the Literature. *Journal of Management History (Archive)* merged into *Management Decision,* Vol. 33, No. 10, 1995, pp. 35–45.
50. White, A.V., and I. Burton. *Environmental Risk Assessment.* John Wiley & Sons, 1980.
51. Swerling, P. Radar Probability of Detection for Some Additional Fluctuating Target Cases. *IEEE Transactions on Aerospace and Electronic Systems,* Vol. 33, No. 2, 1997, pp. 698–709. https://doi.org/10.1109/7.588492.
52. Bai, C.G. Bayesian Network Based Software Reliability Prediction with an Operational Profile. *Journal of Systems and Software,* Vol. 77, No. 2, 2005, pp. 103–112. https://doi.org/10.1016/j.jss.2004.11.034.
53. Goel, P., G. Dedeoglu, S.I. Roumeliotis, and G. Sukhatme. Fault Detection and Identification in a Mobile Robot Using Multiple Model Estimation and Neural Network. In *Proceedings of IEEE International Conference on Robotics and Automation, 2000.* (ICRA '00), Vol. 2303, No. 3, 2000, pp. 2302–2309.
54. Kuusniemi, H. *User-Level Reliability and Quality Monitoring in Satellite-Based Personal Navigation.* Institute of Digital and Computer Systems, Tampere University of Technology, Finland. https://doi.org/10.1109/ROBOT.2000.846370.
55. Amir, Y., and A. Wool. Evaluating Quorum Systems over the Internet. *26th International Symposium on Fault-Tolerant Computing* (FTCS-26), IEEE Computer Society Press, Los Alamitos, Calif., 1996. pp. 26–35. https://doi.org/10.1109/FTCS.1996.534591.
56. Eriksson, J., H. Balakrishnan, and S. Madden. Cabernet: Vehicular Content Delivery Using WiFi. In *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking,* 2008, pp. 199–210.
57. Li, Y., Z. Yuan, C. Peng, and S. Lu. CAP on Mobility Control for 4G LTE Networks. Presented at 3rd Workshop on Hot Topics in Wireless, New York, 2016. https://doi.org/10.1145/2980115.2980120.
58. Goyal, A., S.S. Lavenberg, and K.S. Trivedi. Probabilistic Modeling of Computer System Availability. *Annals of Operations Research Part III: Simulation and Computers,* Vol. 8, No. 1, 1987, pp. 285–306. https://doi.org/10.1007/BF02187098.
59. Chandler, F., A. Heard, M. Presley, A. Burg, E. Midden, and P. Mongan. *NASA Human Error Analysis.* NASA, 2010.
60. Dupont, S., and J. Luettin. Audio-Visual Speech Modeling for Continuous Speech Recognition. *IEEE Transactions on Multimedia,* Vol. 2, No. 3, 2000, pp. 141–151. https://doi.org/10.1109/6046.865479.
61. *Virginia Traffic Crash Facts 2014.* Virginia Highway Safety Office, Virginia Department of Motor Vehicles, 2015.
62. *Summary of Motor Vehicle Crashes: 2014 Statewide Statistical Summary.* New York State Department of Motor Vehicles, 2015.
63. Kim, K., and L. Li. Modeling Fault Among Bicyclists and Drivers Involved in Collisions in Hawaii, 1986–1991. *Transportation Research Record,* No. 1538, 1996, pp. 75–80. https://doi.org/10.3141/1538-10.
64. Ullman, G.L., M.D. Finley, J.E. Bryden, R. Srinivasan, and F.M. Council. *NCHRP Report 627: Traffic Safety Evaluation of Nighttime and Daytime Work Zones.* Transportation Research Board, Washington, D.C., 2008.
65. Santos, A., N. McGuckin, H.Y. Nakamoto, D. Gray, and S. Liss. *Summary of Travel Trends: 2009 National Household Travel Survey.* Publication FHWA-PL-ll-022. FHWA, U.S. Department of Transportation, 2011.
66. Schroeder, P., and M. Wilbur. *2012 National Survey of Bicyclist and Pedestrian Attitudes and Behavior, Vol. 1: Summary Report.* Publication DOT HS 811 841. NHTSA, U.S. Department of Transportation, 2013.
67. Bicyclists and Other Cyclists: 2014. *Data Traffic Safety Facts.* Publication DOT HS 812 282. NHTSA, U.S. Department of Transportation, 2016.
68. Pedestrians: 2014 Data. *Traffic Safety Facts.* Publication DOT HS 812 270. 2016.
69. Kuzmyak, J.R., and J. Dill. Walking and Bicycling in the United States: The Who, What, Where, and Why. *TR News,* No. 280, 2012, pp. 4–15.
70. *Facts and Statistics—Work Zone Injuries and Fatalities.* FHWA, U.S. Department of Transportation. http://www.ops.fhwa.dot.gov/wz/resources/facts_stats/injuries_fatalities.htm. Accessed Jan. 20, 2016.
71. *Commercial Software for Fault Tree Analysis.* Isograph Software, United Kingdom.
72. Dezfuli, H., A. Benjamin, C. Everett, G. Maggio, M. Stamatelatos, and R. Youngblood. *NASA Risk Management Handbook.* Publication NASA/SP-2011-3422. NASA, 2011.
73. Safie, F.M., R.G. Stutts, and Z. Huang. Reliability and Probabilistic Risk Assessment—How They Play Together. *2015 Annual Reliability and Maintainability Symposium* (RAMS), 2015, pp. 1–5. https://doi.org/10.1109/RAMS.2015.7105058.
74. Lu, S. *Vehicle Survivability and Travel Mileage Schedules.* Publication DOT HS 809 952. 2006.
75. Tupper, L.L., M. Chowdhury, and J. Sharp. Tort Liability Risk Prioritization through the Use of Fault Tree Analysis. Presented at 93rd Annual Meeting of the Transportation Research Board, Washington, D.C., 2014.
76. Pinto, C. How Autonomous Vehicle Policy in California and Nevada Addresses Technological and Non-Technological Liabilities. *Intersect: The Stanford Journal of Science, Technology and Society,* Vol. 5, 2012.

All opinions, findings, and conclusions or recommendations presented in this paper are those of the authors and do not necessarily reflect the views of the U.S. Department of Transportation Region 2 University Transportation Research Center.

The Standing Committee on Vehicle–Highway Automation peer-reviewed this paper.