TRB Special Report 308: The Safety Challenge and Promise of Automotive Electronics: Insights from Unintended Acceleration

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Pages</td>
<td>157</td>
</tr>
<tr>
<td>Size</td>
<td>6x9</td>
</tr>
<tr>
<td>Year</td>
<td>2012</td>
</tr>
</tbody>
</table>

Visit the National Academies Press online and register for...

- Instant access to free PDF downloads of titles from the
  - NATIONAL ACADEMY OF SCIENCES
  - NATIONAL ACADEMY OF ENGINEERING
  - INSTITUTE OF MEDICINE
  - NATIONAL RESEARCH COUNCIL
- 10% off print titles
- Custom notification of new releases in your field of interest
- Special offers and discounts

Distribution, posting, or copying of this PDF is strictly prohibited without written permission of the National Academies Press. Unless otherwise indicated, all materials in this PDF are copyrighted by the National Academy of Sciences. Request reprint permission for this book

Copyright © National Academy of Sciences. All rights reserved.
The National Highway Traffic Safety Administration (NHTSA) requested this National Research Council (NRC) study of how the agency’s regulatory, research, and defect investigation programs can be strengthened to meet the safety assurance and oversight challenges arising from the expanding functionality and use of automotive electronics. To conduct the study, NRC appointed a 16-member committee of experts tasked with considering NHTSA’s recent experience in responding to concerns over the potential for faulty electronics to cause the unintentional vehicle acceleration as reported by some drivers.

The subject matter of the committee’s findings is summarized in Box S-1 and provided in full at the end of each chapter. These findings indicate how the electronics systems being added to automobiles present many opportunities for making driving safer but at the same time present new demands for ensuring the safe performance of increasingly capable and complex vehicle technologies. These safety assurance demands pertain both to the automotive industry’s development and deployment of electronics systems and to NHTSA’s fulfillment of its safety oversight role. With regard to the latter, the committee recommends that NHTSA give explicit consideration to the oversight challenges arising from automotive electronics and that the agency develop and articulate a long-term strategy for meeting the challenges. A successful strategy will reduce the chances of a recurrence of the kind of controversy that drove NHTSA’s response to questions about electronics causing unintended acceleration. As electronics systems proliferate to provide
Summary of Findings

The Electronics-Intensive Automobile

Finding 2.1: Electronics systems have become critical to the functioning of the modern automobile.

Finding 2.2: Electronics systems are being interconnected with one another and with devices and networks external to the vehicle to provide their desired functions.

Finding 2.3: Proliferating and increasingly interconnected electronics systems are creating opportunities to improve vehicle safety and reliability as well as demands for addressing new system safety and cybersecurity risks.

Finding 2.4: By enabling the introduction of many new vehicle capabilities and changes in familiar driver interfaces, electronics systems are presenting new human factors challenges for system design and vehicle-level integration.

Finding 2.5: Electronics technology is enabling nearly all vehicles to be equipped with event data recorders (EDRs) that store information on collision-related parameters as well as enabling other embedded systems that monitor the status of safety-critical electronics, identify and diagnose abnormalities and defects, and activate predefined corrective responses when a hazardous condition is detected.

Safety Assurance Processes for Automotive Electronics

Finding 3.1: Automotive manufacturers visited during this study—and probably all the others—implement many processes during product design, engineering, and manufacturing intended (a) to ensure that electronics systems perform as expected up to defined failure probabilities and (b) to detect failures when they occur and respond to them with appropriate containment actions.
Finding 3.2: Testing, analysis, modeling, and simulation are used by automotive manufacturers to verify that their electronics systems, the large majority of which are provided by suppliers, have met all internal specifications and regulatory requirements, including those relevant to safety performance.

Finding 3.3: Manufacturers face challenges in identifying and modeling how a new electronics-based system will be used by the driver and how it will interface and interact with the driver.

Finding 3.4: Automotive manufacturers have been cooperating through the International Organization for Standardization to develop a standard methodology for evaluating and establishing the functional safety requirements for their electronics systems.

**NHTSA Vehicle Safety Programs**

Finding 4.1: A challenge before NHTSA is to further the use and effectiveness of vehicle technologies that can aid safe driving and mitigate hazardous driving behaviors and to develop the capabilities to ensure that these technologies perform their functions as intended and do not prompt other unsafe driver actions and behaviors.

Finding 4.2: NHTSA’s Federal Motor Vehicle Safety Standards are results-oriented and thus written in terms of minimum system performance requirements rather than prescribing the means by which automotive manufacturers design, test, engineer, and manufacture their safety-related electronics systems.

Finding 4.3: Through the Office of Defects Investigation (ODI), NHTSA enforces the statutory requirement that vehicles in consumer use not exhibit defects that adversely affect safe vehicle performance.

Finding 4.4: NHTSA refers to its vehicle safety research program as being “data driven” and decision-oriented, guided by analyses
Finding 4.5: NHTSA regularly updates a multiyear plan that explains the rationale for its near-term research and regulatory priorities; however, the plan does not communicate strategic considerations, such as how the safety challenges arising from the electronics-intensive vehicle may require new regulatory and research responses.

Finding 4.6: The Federal Aviation Administration’s (FAA’s) regulations for aircraft safety are comparable with the performance-oriented Federal Motor Vehicle Safety Standards in that the details of product design and development are left largely to the manufacturers; however, FAA exercises far greater oversight of the verification and validation of designs and their implementation.

Finding 4.7: The U.S. Food and Drug Administration’s (FDA’s) and NHTSA’s safety oversight processes are comparable in that they combine safety performance requirements as a condition for approval with postmarketing monitoring to detect and remedy product safety deficiencies occurring in the field. FDA has established a voluntary network of clinicians and hospitals known as MedSun to provide a two-way channel of communication to support surveillance and more in-depth investigations of the safety performance of medical devices.

NHTSA Initiatives on Unintended Acceleration

Finding 5.1: NHTSA has investigated driver complaints of vehicles exhibiting various forms of unintended acceleration for decades, the most serious involving high engine power indicative of a large throttle opening.
Summary

Finding 5.2: NHTSA has most often attributed the occurrence of unintended acceleration indicative of a large throttle opening to pedal-related issues, including the driver accidentally pressing the accelerator pedal instead of the brake pedal, floor mats and other obstructions that entrap the accelerator pedal in a depressed position, and sticking accelerator pedals.

Finding 5.3: NHTSA’s rationale for attributing certain unintended acceleration events to pedal misapplication is valid, but such determinations should not preclude further consideration of possible vehicle-related factors contributing to the pedal misapplication.

Finding 5.4: Not all complaints of unintended acceleration have the signature characteristics of pedal misapplication; in particular, when severe brake damage is confirmed or the loss of braking effectiveness occurs more gradually after a prolonged effort by the driver to control the vehicle’s speed, pedal misapplication is improbable, and NHTSA reported that it treats these cases differently.

Finding 5.5: NHTSA’s decision to close its investigation of Toyota’s electronic throttle control system (ETC) as a possible cause of high-power unintended acceleration is justified on the basis of the agency’s initial defect investigations, which were confirmed by its follow-up analyses of thousands of consumer complaints, in-depth examinations of EDRs in vehicles suspected to have crashed as a result of unintended acceleration, and the examination of the Toyota ETC by the National Aeronautics and Space Administration.

Finding 5.6: The Vehicle Owner’s Questionnaire consumer complaint data appear to have been sufficient for ODI analysts and investigators to detect an increase in high-power unintended acceleration behaviors in Toyota vehicles, to distinguish these behaviors from those commonly attributed to

(continued on next page)
more vehicle functions, neither industry nor NHTSA can afford such recurrences—nor can motorists.

**UNINTENDED ACCELERATION AND ELECTRONIC THROTTLE CONTROL**

NHTSA has investigated complaints of vehicles exhibiting unintended acceleration for decades. These complaints have encompassed a wide range of reported vehicle behaviors, the most serious involving high engine power indicative of a large throttle opening (see Finding 5.1). NHTSA has often—and most recently in investigating Toyota vehicles—concluded that these occurrences were the result of the driver accidentally pressing the accelerator pedal instead of the brake; floor mats and other obstructions that entrap the accelerator pedal; and damaged or malfunctioning mechanical components such as broken throttles, frayed and trapped connector cables, and sticking accelerator pedal assemblies (see Finding 5.2).

During the past decade, many of the mechanical links between the pedal and the throttle have been eliminated by electronic throttle control systems (ETCs), which were introduced for a number of reasons, including the desire for more flexible and precise control of air to the engine for improved emissions, fuel economy, and drivability. Typically, these systems use duplicate sensors to determine the position of the pedal and additional sensors to monitor the throttle opening. Electrical signals
are transmitted by wire from the sensors to the computer in the engine control module, which in turn commands the throttle actuator and engine torque. These electronics systems have therefore reduced the number of mechanical components that can break or malfunction, while introducing the possibility of faulty electronics hardware and software. Of course, ETCs have not done away with the foot pedal as the driver interface, meaning that pedal-related conditions such as entrapment, sticking, and driver misapplication can continue to be a source of unintended acceleration.

Because pedal-related problems have been a recognized source of unintended acceleration for decades, they are the immediate suspect in any reported event. Key in assessing the pedal’s role is determination of the sequence of brake application and its effectiveness. In all vehicles that it has examined—with and without ETCs—NHTSA has found no means by which the throttle control system can disable a vehicle’s brakes. The agency, therefore, cannot explain how the application of previously working brakes, as asserted by some drivers, would fail to overcome engine torque and halt acceleration commencing in a vehicle that had been stationary or moving slowly. Absent physical evidence of damaged or malfunctioning brakes, NHTSA has long concluded that complaints of unintended acceleration involving reports of unexplainable loss of braking result from pedal misapplication and do not warrant examination for other causes. The committee finds this rationale to remain valid and relevant for NHTSA’s allocation of its investigative resources, but with the caveat that it should not preclude further consideration of vehicle-related factors that can prompt or contribute to pedal misapplication (see Finding 5.3).

Not all complaints of unintended acceleration have the signature characteristics of pedal misapplication. When severe brake damage is confirmed or the loss of braking effectiveness occurs more gradually through overheating and vacuum loss following a prolonged effort by the driver to control the vehicle’s speed, pedal misapplication is improbable, and as a result NHTSA reports that it treats these cases differently (see Finding 5.4). In its investigations of such cases, NHTSA has usually concluded that the acceleration was caused by faulty mechanical components in the throttle control system or by the accelerator pedal becoming struck or entrapped, often by a floor mat. Having produced evidence of these latter causal mechanisms—and finding no physical evidence of other problems, including errant electronics—NHTSA initially decided against
undertaking more in-depth investigations of possible faults in the ETCs of Toyota vehicles that had been recalled during 2009 and 2010.

Faced with persistent questions about the basis for this decision, in early 2010 NHTSA commissioned this study and another by a team of engineering and safety specialists from the National Aeronautics and Space Administration (NASA). The charge of the NASA team was to investigate the potential for vulnerabilities in Toyota’s ETC to cause reported cases of unintended acceleration. NASA’s investigation was multiphased. After establishing the critical functions of the ETC, the NASA team examined how the electronics system is designed and implemented to guard against failures and to respond safely when failures do occur. Potential vulnerabilities in the system’s design and its implementation were sought by identifying circumstances in which a failure could occur and go undetected so as to bypass system fail-safe responses. To assess whether an identified vulnerability had led to failures causing unintended acceleration, the team reviewed consumer complaints in a search for hallmarks of the failures and tested vehicles previously involved in instances of unintended acceleration.

On the basis of its vulnerability analysis, the NASA team identified two scenarios that it described as having at least a theoretical potential to produce unintended acceleration characteristic of a large throttle opening: 

(a) a systematic failure of software in the ETC’s central processing unit that goes undetected by the supervisory processor and 

(b) two faults in the pedal position sensing system that mimic a valid acceleration command.

NASA investigators used multiple tools to analyze software logic paths and to examine the programming code for paths that might lead to the first postulated scenario. While the team acknowledged that no practical amount of testing and analysis can guarantee that software will be free of faults, it reported that extensive analytic efforts uncovered no evidence of problems. To examine the second postulated scenario, the team tested numerous potential software and hardware fault modes by using bench-top simulators and by testing vehicles involved in reported cases of unintended acceleration, including tests for electromagnetic interference. The testing did not produce acceleration indicative of a large throttle opening. The team also examined records from consumer complaints involving unusual accelerator pedal responses. In so doing it recovered a pedal assembly that contained a low-resistance path, which was determined to have been caused by an electrically conductive crystalline
structure\(^1\) that had formed between signal outputs from the pedal position sensors.

Consideration was given to whether low-resistance paths in the pedal position sensing system could have produced unintended acceleration indicative of a large throttle opening. The NASA team concluded that if a single low-resistance path were to exist between the pedal sensor outputs, the system could be vulnerable to unintended acceleration if accompanied by a second specific fault condition. The team noted, however, that to create such a vulnerability the two sensor faults would need to escape detection by meeting restrictive criteria consisting of a specific resistance range as needed to create an exact circuit configuration in a correct time phase. In this case, the fault condition would not log a diagnostic trouble code; otherwise, the faults would be detected and trigger a fail-safe response such as reduced engine power.

To gain a better understanding of the probability of the dual-fault conditions occurring, the NASA team examined warranty repair data and consumer complaints of high-power unintended acceleration. The team posited that for every instance in which two undetected faults had produced unintended acceleration, numerous pedal repairs associated with detected sensor faults could be expected because single faults that leave error codes are likely to occur much more often than two faults escaping detection. In reviewing warranty repair data, the NASA team found no evidence to this effect and thus concluded that this postulated failure pathway represented an implausible explanation for the high-power unintended acceleration reported in consumer complaints.

Not having produced evidence of a safety-related defect in Toyota’s ETC, NHTSA elected to close its investigation into this system as a suspect cause of reported cases of high-power unintended acceleration and stood by its earlier conclusions attributing these events to pedal misapplication, entrapment, and sticking. The committee finds NHTSA’s decision to close its investigation justified on the basis of the agency’s initial defect investigations, which were corroborated by its follow-up analyses of thousands of consumer complaints, examinations of event data recorders (EDRs) in vehicles suspected to have crashed because of unintended acceleration, and the results of NASA’s study (see Finding 5.5).

---

\(^1\) A “tin whisker.”
Nevertheless, it is troubling that the concerns associated with unintended acceleration evolved into questions about electronics safety that NHTSA could not answer convincingly, necessitating a request for extensive technical assistance from NASA. Relative to the newer electronics systems being developed, ETCs are simple and mature technologies. As more complex and interacting electronics systems are deployed, the prospect that vehicle electronics will be suspected and possibly implicated in unsafe vehicle behaviors increases. The recommendations offered in this report presume that NHTSA will need the capacity to detect defects in these complex systems, assess their potential causes and proposed remedies with confidence, and make prudent decisions about when to seek the technical assistance of outside experts such as NASA.

**CHALLENGE OF ELECTRONICS SAFETY ASSURANCE**

Electronics are central to the basic functionality of modern automobiles (see Finding 2.1). They provide many new and enhanced vehicle capabilities that confer significant benefits on motorists, including safety benefits. Electronics systems in vehicles are increasingly connected to one another and to devices and networks external to the vehicle. The growing interconnectivity and resulting complexity create opportunities to improve safety, fuel economy, emissions, and other vehicle performance characteristics and lead to new demands for ensuring the safe performance of these systems (see Findings 2.2. and 2.3). Many existing and planned electronics applications, for both vehicle control and active safety capabilities, depend on real-time coordination among various systems and subsystems. Coordination demands more software functionality and more interactions among features in one or more electronic control units. Growing design complexity could increase the chances of design flaws escaping manufacturer safety assurance. In the more distant future, features such as vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications will likely require further increases in software complexity, new sensor technologies and other hardware that will require dependability assessments, and the deployment of additional technologies such as wireless connections that could increase vehicle susceptibility to cyberattack.

Exploiting these many technological advancements to bring about more reliable and capable vehicles, provide more effective crash protec-
tion systems, and enable a wide range of crash-avoidance systems is in the shared interest of motorists, the automotive industry, and NHTSA. Nevertheless, the manufacturer has the initial and primary responsibility for ensuring that these and other electronics systems in the vehicle work as intended, do not interfere with the safe performance of other systems, and can be used in a safe manner by the driver.

While the specifics of automotive development differ among manufacturers, those visited by the committee described a series of processes carried out during product design, engineering, and fabrication to ensure that products perform as intended up to defined failure probabilities (see Finding 3.1). As a backup for the occurrence of failures, manufacturers reported having established failure monitoring and diagnostics systems. These systems are designed to implement predefined strategies to minimize harm when a failure is detected. For example, the driver may be notified through a dashboard light, the failed system may be shut off if it is nonessential, or engine power may be reduced to avoid stranding the motorist and to enable the vehicle to “limp home” for repair. The integrity of hardware and fail-safe applications is validated through testing and analysis (see Finding 3.2). While software programs are also tested for coding errors, manufacturers reported emphasizing sound software development processes. They recognize that even the most exhaustive testing and the strictest adherence to software development prescriptions cannot guarantee that interacting and complex software will behave safely under all plausible circumstances. In addition, all manufacturers reported having experts in human factors engaged early in the design of their new electronics systems and throughout the later stages of product development and evaluation (see Finding 3.3).

The committee cannot know whether all automotive manufacturers follow the safety assurance practices described as robust by the original equipment manufacturers (OEMs) visited and whether all execute them with comparable diligence and consistency. However, the committee found that despite proprietary and competitive constraints, many automotive manufacturers are working with standards organizations to further their safety assurance practices out of recognition that electronics systems are creating new challenges for safe and secure product design, development, and performance (see Finding 3.4). Most prominent among these efforts is the consensus standard expected to be released in early 2012 by the International Organization for Standardization (ISO), ISO 26262, for the functional safety of automotive electronics systems.
This standard will provide OEMs and their suppliers with guidance on establishing safety requirements for their electronics systems, performing hazard and risk assessments on them, tailoring appropriate safety assurance processes during system development and production, and carrying out functional safety audits and confirmation reviews.

**Implications for NHTSA’s Oversight and Engagement with Industry**

In light of the increasing use and complexity of electronics systems for vehicle control functions, the question arises as to whether NHTSA should oversee and otherwise exert more influence over the safety assurance processes followed by industry during product design, development, and manufacturing. For NHTSA to engage in comprehensive regulatory oversight of manufacturer assurance plans and processes, as occurs in the aviation sector, would represent a fundamental change in the agency’s regulatory approach that would require substantial justification and resources (see Finding 4.6). The introduction of increasingly autonomous vehicles, as envisioned in some concepts of the electronics-intensive automobile, might one day cause the agency to consider taking a more hands-on regulatory approach with elements similar to those found in the aviation sector. At the moment, such a profound change in the way NHTSA regulates automotive safety does not appear to be a near-term prospect.

A more foreseeable change is the automotive industry’s use of the aforementioned ISO 26262. Although release of the final standard is pending, many manufacturers appear to be committed to following its guidance in whole or in large part. Without necessarily endorsing or requiring adherence to the standard, NHTSA nevertheless has a keen interest in supporting the standard’s ability to produce the desired safety results for those manufacturers who do subscribe to it. As these manufacturers reassess and adjust their safety assurance processes in response to the standard’s guidance, some may need more information and analyses—including knowledge in areas such as cybersecurity, human factors, the electromagnetic environment, and multifault detection and diagnosis. In collaboration with industry, NHTSA may be able to help meet these research and analysis needs and in so doing enable agency technical personnel to become even more familiar with industry safety assurance methods, issues, and challenges.

Accordingly, the committee recommends that NHTSA become more familiar with and engaged in standard-setting and other efforts involv-
ing industry that are aimed at strengthening the means by which manufacturers ensure the safe performance of their automotive electronics systems (Recommendation 1). In the committee’s view, such cooperative efforts represent an opportunity for NHTSA to gain a stronger understanding of how manufacturers seek to prevent safety problems through measures taken during product design, development, and fabrication. By engaging in these efforts, the agency will be better able to influence industry safety assurance and recognize where it can contribute most effectively to strengthening such preventive measures. Several candidate topics for collaborative research and analysis are identified in this report and summarized in Box S-2.

Exploration of other means by which NHTSA can interact with industry in furthering electronics safety assurance will also be important. Exploiting a range of opportunities will be critical in the committee’s view, since it is unrealistic to expect NHTSA to hire and maintain personnel having all of the specialized technical expertise and design knowledge relevant to the growing field of automotive electronics. As a starting point for obtaining access to this expertise, the committee recommends that NHTSA convene a standing technical advisory panel comprising individuals with backgrounds in the disciplines central to the design, development, and safety assurance of automotive electronics systems, including software and systems engineering, human factors, and electronics hardware. The panel should be consulted on relevant technical matters that arise with respect to all of the agency’s vehicle safety programs, including regulatory reviews, defect investigation processes, and research needs assessments (Recommendation 2).

**Implications for Defect Surveillance and Investigation**

NHTSA does not prescribe how manufacturers design, develop, or manufacture vehicle systems. Hence, responsibility for minimizing the occurrence of safety defects resides primarily with automotive manufacturers and their safety assurance processes (see Finding 4.2). NHTSA’s main role in this regard is to spot and investigate safety deficiencies that escape these processes and to prompt manufacturers to correct them quickly and effectively. This postmarket surveillance and investigative capability has always been an important function for NHTSA and has resulted in many safety recalls.

Electronics systems are replacing many mechanical and hydraulic systems and are being used to manage and control many new vehicle
BOX S-2

Candidate Research and Analysis

To Inform Industry Safety Assurance Processes

- Review state-of-the-art methods used within and outside the automotive industry for detecting, diagnosing, isolating, and responding to failures that may arise from multiple, intermittent, and timing faults in safety-critical vehicle electronics systems.

- Survey and identify the sources, characteristics, and probability of occurrence of electromagnetic environments produced by other vehicles, on-board consumer devices, and other electromagnetic sources in the vicinity of the roadway.

- Explore the feasibility and utility of a remote or in-vehicle system that continually logs the subsystem states, network traffic, and interactions of the vehicle and its electronics systems and is capable of saving relevant data for querying in response to unexpected vehicle behaviors.

- Examine security vulnerabilities arising from the increase in remote access to and interconnectivity of electronics systems that can compromise safety-critical vehicle capabilities such as braking, exterior lighting, speed control, and steering.

- Examine the implications of electronics systems for the means by which automotive manufacturers are complying with the intent of the Federal Motor Vehicle Safety Standards, how changes in technology could both aid and complicate compliance with the regulations, and how the regulations themselves are likely to affect technological innovation.

- Assess driver response to nontraditional controls enabled by electronic interfaces, such as push-button ignition design systems, and the degree to which differences among vehicles may confuse and delay responses in time-pressured and emergency situations.
### Box S-2 (continued) Candidate Research and Analysis

- Examine driver interaction with the vehicle as a mixed initiative system using simulator and naturalistic driving studies to assess when designers’ assumptions of drivers’ responses diverge from drivers’ expectations of system operation.

- Collaborate with the automotive industry in developing effective methods for communicating the operational status of vehicle electronics to the driver.

### To Support ODI Functions and Capabilities

- Examine modifications to the Vehicle Owner’s Questionnaire that can make it more useful to ODI analysts and investigators by facilitating the ability of consumers to convey the vehicle conditions and behaviors they experience more precisely and by making the information more amenable to quantitative evaluation.

- Examine a cross section of safety-related recalls whose cause was attributed to deficiencies in electronics or software and identify how the defects escaped verification and safety assurance processes.

- Investigate ways to obtain more timely and detailed Early Warning Reporting–type data for defect surveillance and investigation—for example, by examining opportunities for voluntary data collection relationships and networks with automotive dealers.

- Examine how the data from consumer complaints of unsafe experiences in the field can be mined electronically and how the complaints might offer insight into safety issues that arise from human–systems interactions.

See Chapter 6 for details on the research topics.
functions. NHTSA’s Office of Defects Investigation (ODI) can therefore anticipate that an increasing share of its time and resources will be devoted to recognizing and investigating potential defects involving electronics systems and to assessing the corrective actions proposed by manufacturers for recalls involving software reprogramming and other fixes to the hardware of electronics systems. Whether the proliferation of electronics systems will add substantially to the complexity and technical requirements of ODI’s surveillance and investigative activities remains to be seen. The committee believes that it will.

One reason for this belief is that failures associated with electronics systems—including those related to software programming, dual and intermittent electronics hardware faults, and electromagnetic disturbances—may not leave physical evidence to aid investigations into observed or reported unsafe vehicle behaviors. Similarly, many errors by drivers using or responding to new electronics systems may not leave a physical trace. The absence of physical evidence, as illuminated by the controversy surrounding unintended acceleration, has complicated past investigations of incident causes and thus may become even more problematic for ODI as the number, functionality, and complexity of electronics systems grow. Another important reason for the committee’s concern is that electronics systems are networked and interconnected with one another and with electronic devices external to the vehicle, and a growing number of the interconnected electronics systems have nonsafety purposes and may not be held to the same expectations for safety and security assurance. These complex systems will introduce new architectures and may couple and interact in unexpected ways. Anticipating and recognizing the potentially unsafe behaviors of these systems likely will present a challenge not only for automotive manufacturers during product design and development but also for ODI in spotting such behaviors in the fleet and working with OEMs to assess their causes and possible corrections (see Finding 2.4).

To ensure that NHTSA’s defect surveillance and investigation capabilities are prepared for the changing safety challenges presented by the electronics-intensive automobile, the committee recommends that NHTSA undertake a comprehensive review of the capabilities that ODI will need in monitoring for and investigating safety deficiencies in electronics-intensive vehicles. A regular channel of communication should be established between NHTSA’s research program and ODI to ensure that (a) recurrent vehicle- and driver-related safety problems
observed in the field are the subjects of research and (b) research is committed to furthering ODI’s surveillance and investigation capabilities, particularly the detail, timeliness, and analyzability of the consumer complaint and early warning data central to these capabilities (Recommendation 3). Candidate research topics to inform and support ODI’s functions and capabilities are identified in Box S-2.

REACTION TO NHTSA’s PROPOSED NEXT STEPS

In its Research and Rulemaking Priority Plan for 2011–2013, NHTSA has identified a number of rulemaking and research initiatives that appear to have been influenced by the recent experience with unintended acceleration. They include plans to (a) initiate a rulemaking that would mandate the installation of EDRs on all light-duty vehicles and a proposal to consider future enhancements of EDR capabilities, (b) change the standard governing keyless ignitions to ensure that drivers are able to turn off the engine in the event of an on-road emergency, and (c) undertake pedal-related research that would examine pedal placement and spacing practices to reduce the occurrence of pedal entrapment and misapplication.

The committee cannot know where these initiatives should rank among all of NHTSA’s research and rulemaking priorities. Nevertheless, the committee concurs with NHTSA’s intent to ensure that EDRs be commonplace in all new vehicles and recommends that the agency pursue this outcome, recognizing that the utility of more extensive and capable EDRs will depend in large part on the extent to which the stored data can be retrieved for safety investigations (Recommendation 4). NHTSA’s stated plan is to consider “future enhancements” to EDRs, which is particularly intriguing for the following two reasons. First, failures in electronics systems, including those related to software programming, intermittent electrical faults, and electromagnetic disturbances, may not leave physical traces to aid investigations into the causes. Second, mistakes by drivers also may not leave a physical trace, even if these errors result in part from vehicle-related factors such as startling vehicle noises or unexpected or unfamiliar vehicle behaviors. The absence of such physical evidence has hindered investigations of the ETC’s role in unintended acceleration and may become even more problematic as the number and complexity of automotive electronics systems
grow. Advanced data recording systems may help counter some of these problems if the data can be accessed by investigators (see Finding 5.7). In the committee’s view, the technical feasibility and practicality of equipping vehicles with more advanced recording systems that can log a wider range of data warrant further study.

The committee also endorses NHTSA’s stated plan to conduct research on pedal design and placement and keyless ignition design requirements but recommends that this research be a precursor to a broader human factors research initiative in collaboration with industry and that the research be aimed at informing manufacturers’ system design decisions (Recommendation 5). Examples of research that could be pursued are given in Box S-2.

**STRATEGIC OUTLOOK WITH REGARD TO PRIORITIES**

As vehicles become even more dependent on electronics systems for their critical functions, NHTSA’s regulatory, research, and investigation programs will need to keep pace with changing safety demands placed on them. This report describes how NHTSA researchers are working with the automotive industry, universities, and other government agencies to examine future crash avoidance concepts such as V2V and V2I communications systems. Such systems will enable even greater vehicle autonomy and necessitate advancements in vehicle electronics and their capabilities that will go well beyond any systems now being deployed. In the same vein, changes in the division of responsibility between the driver and the vehicle will present new demands for and interpretations of NHTSA’s Federal Motor Vehicle Safety Standards, heighten the need for safety assurance processes that instill high levels of public confidence in these systems, and place many new demands on ODI’s surveillance and investigative activities. While the technical, societal, and economic feasibility of V2V, V2I, and other intelligent transportation systems are not considered in this study, it is difficult to imagine NHTSA overseeing their safe introduction and use without adapting its regulatory, research, and investigative framework.

The committee was tempted to offer a series of specific recommendations on the capabilities and resources that NHTSA may need in each of these program areas. To offer such advice without knowing more about how the agency intends to proceed on a more strategic level would be
presumptuous in the committee’s view. For example, urging the agency to hire more electronics or system safety engineers or to invest in new specialized research and testing facilities would make little sense without knowing more about the specific functions they would perform. Nor can the committee know what other safety issues are demanding NHTSA’s time, resources, and attention. These are broader, strategic issues that are outside the committee’s charge.

The committee notes that NHTSA states its intention to develop such a strategic document for the period 2014–2020 in the introduction to its Priority Plan. Presumably, this strategic plan could provide a road map for NHTSA’s decisions with regard to the safety assurance challenges arising from the electronics-intensive vehicle. From its discussions with NHTSA officials, however, the committee understands that this planning process has only just begun and its purpose has not been articulated. The committee believes that strategic planning is fundamental to sound decision making and thus recommends that NHTSA initiate a strategic planning effort that gives explicit consideration to the safety challenges resulting from vehicle electronics and that gives rise to an agenda for meeting them. The agenda should spell out the near- and longer-term changes that will be needed in the scope, direction, and capabilities of the agency’s regulatory, research, and defect investigation programs (Recommendation 6). Some of the key elements of successful strategic planning are outlined in this report. In the committee’s view, it is vital that the planning be (a) prospective in considering the safety challenges arising from the electronics-intensive vehicle, (b) introspective in considering the implications of these challenges for NHTSA’s vehicle safety role and programs, and (c) strategic in guiding critical decisions concerning matters such as the most appropriate agency regulatory approaches and associated research and resource requirements.

The committee further recommends that NHTSA make development and completion of the strategic plan a top goal in its coming 3-year priority plan. NHTSA should communicate the purpose of the planning effort, define how it will be developed and implemented commensurate with advice in this report, and give a definite time frame for its completion. The plan should be made public so as to guide key policy decisions—from budgetary to legislative—that will determine the scope and direction of the agency’s vehicle safety programs (Recommendation 7). All seven of the committee’s recommendations are contained in Box S-3.
Recommendations to NHTSA

Recommendation 1: The committee recommends that NHTSA become more familiar with and engaged in standard-setting and other efforts involving industry that are aimed at strengthening the means by which manufacturers ensure the safe performance of their automotive electronics systems.

Recommendation 2: The committee recommends that NHTSA convene a standing technical advisory panel comprising individuals with backgrounds in the disciplines central to the design, development, and safety assurance of automotive electronics systems, including software and systems engineering, human factors, and electronics hardware. The panel should be consulted on relevant technical matters that arise with respect to all of the agency’s vehicle safety programs, including regulatory reviews, defect investigation processes, and research needs assessments.

Recommendation 3: The committee recommends that NHTSA undertake a comprehensive review of the capabilities that ODI will need in monitoring for and investigating safety deficiencies in electronics-intensive vehicles. A regular channel of communication should be established between NHTSA’s research program and ODI to ensure that (a) recurrent vehicle- and driver-related safety problems observed in the field are the subjects of research and (b) research is committed to furthering ODI’s surveillance and investigation capabilities, particularly the detail, timeliness, and analyzability of the consumer complaint and early warning data central to these capabilities.

Recommendation 4: The committee concurs with NHTSA’s intent to ensure that EDRs be commonplace in new vehicles and recommends that the agency pursue this outcome, recognizing that the utility of more extensive and capable EDRs will depend in large part on the extent to which the stored data can be retrieved for safety investigations.
Recommendation 5: The committee endorses NHTSA's stated plan to conduct research on pedal design and placement and keyless ignition design requirements but recommends that this research be a precursor to a broader human factors research initiative in collaboration with industry and that the research be aimed at informing manufacturers’ system design decisions.

Recommendation 6: The committee recommends that NHTSA initiate a strategic planning effort that gives explicit consideration to the safety challenges resulting from vehicle electronics and that gives rise to an agenda for meeting them. The agenda should spell out the near- and longer-term changes that will be needed in the scope, direction, and capabilities of the agency’s regulatory, research, and defect investigation programs.

Recommendation 7: The committee recommends that NHTSA make development and completion of the strategic plan a top goal in its coming 3-year priority plan. NHTSA should communicate the purpose of the planning effort, define how it will be developed and implemented commensurate with advice in this report, and give a definite time frame for its completion. The plan should be made public so as to guide key policy decisions—from budgetary to legislative—that will determine the scope and direction of the agency’s vehicle safety programs.
The Safety Promise and Challenge of Automotive Electronics

INSIGHTS FROM UNINTENDED ACCELERATION

Committee on Electronic Vehicle Controls and Unintended Acceleration, Transportation Research Board
Board on Energy and Environmental Systems
Computer Science and Telecommunications Board

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

Transportation Research Board
Washington, D.C.
2012
www.TRB.org
Transportation Research Board
Executive Committee*

Chair: Sandra Rosenbloom, Professor of Planning, University of Arizona, Tucson
Vice Chair: Deborah H. Butler, Executive Vice President, Planning, and CIO, Norfolk Southern Corporation, Norfolk, Virginia
Executive Director: Robert E. Skinner, Jr., Transportation Research Board

J. Barry Barker, Executive Director, Transit Authority of River City, Louisville, Kentucky
William A. V. Clark, Professor of Geography (emeritus) and Professor of Statistics (emeritus), Department of Geography, University of California, Los Angeles
Eugene A. Conti, Jr., Secretary of Transportation, North Carolina Department of Transportation, Raleigh
James M. Crites, Executive Vice President of Operations, Dallas–Fort Worth International Airport, Texas
Paula J. C. Hammond, Secretary, Washington State Department of Transportation, Olympia
Michael W. Hancock, Secretary, Kentucky Transportation Cabinet, Frankfort
Chris T. Hendrickson, Duquesne Light Professor of Engineering, Carnegie Mellon University, Pittsburgh, Pennsylvania
Adib K. Kanafani, Professor of the Graduate School, University of California, Berkeley (Past Chair, 2009)
Gary P. LaGrange, President and CEO, Port of New Orleans, Louisiana
Michael P. Lewis, Director, Rhode Island Department of Transportation, Providence
Susan Martinovich, Director, Nevada Department of Transportation, Carson City
Joan McDonald, Commissioner, New York State Department of Transportation, Albany
Michael R. Morris, Director of Transportation, North Central Texas Council of Governments, Arlington (Past Chair, 2010)
Tracy L. Rosser, Vice President, Regional General Manager, Wal-Mart Stores, Inc., Mandeville, Louisiana
Henry G. (Gerry) Schwartz, Jr., Chairman (retired), Jacobs/Sverdrup Civil, Inc., St. Louis, Missouri
Beverly A. Scott, General Manager and CEO, Metropolitan Atlanta Rapid Transit Authority, Atlanta, Georgia

*Membership as of April 2012.
Cynthia L. Quarterman, Administrator, Pipeline and Hazardous Materials Safety Administration, U.S. Department of Transportation (ex officio)

Peter M. Rogoff, Administrator, Federal Transit Administration, U.S. Department of Transportation (ex officio)

David L. Strickland, Administrator, National Highway Traffic Safety Administration, U.S. Department of Transportation (ex officio)

Joseph C. Szabo, Administrator, Federal Railroad Administration, U.S. Department of Transportation (ex officio)

Polly Trottenberg, Assistant Secretary for Transportation Policy, U.S. Department of Transportation (ex officio)


Barry R. Wallerstein, Executive Officer, South Coast Air Quality Management District, Diamond Bar, California (ex officio)

Gregory D. Winfree, Acting Administrator, Research and Innovative Technology Administration, U.S. Department of Transportation (ex officio)
Board on Energy and Environmental Systems

Andrew Brown, Jr., NAE, Delphi Corporation, Troy, Michigan, Chair
William F. Banholzer, NAE, Dow Chemical Company, Midland, Michigan
Marilyn Brown, Georgia Institute of Technology, Atlanta
William Cavanaugh, NAE, Progress Energy (retired), Raleigh, North Carolina
Paul A. DeCotis, Long Island Power Authority, Albany, New York
Christine Ehlig-Economides, NAE, Texas A&M University, College Station
Sherri Goodman, CNA, Alexandria, Virginia
Narain Hingorani, NAE, Consultant, Los Altos Hills, California
Robert J. Huggett, Consultant, Seaford, Virginia
Debbie Niemeier, University of California, Davis
Daniel Nocera, NAS, Massachusetts Institute of Technology, Cambridge
Michael Oppenheimer, Princeton University, Princeton, New Jersey
Dan Reicher, Climate Change & Energy Initiatives, Google
Bernard Robertson, NAE, DaimlerChrysler Corporation (retired), Bloomfield Hills, Michigan
Gary Rogers, FEV, Inc., Auburn Hills, Michigan
Alison Silverstein, Consultant, Pflugerville, Texas
Mark H. Thiemens, NAS, University of California, San Diego
Richard White, Oppenheimer & Company, New York

Staff

James J. Zucchetto, Senior Program/Board Director
John Holmes, Senior Program Officer and Associate Board Director
Dana Caines, Financial Manager
Alan Crane, Senior Scientist
Jonna Hamilton, Program Officer
LaNita Jones, Administrative Coordinator
Alice Williams, Senior Project Assistant
E. Jonathan Yanger, Senior Project Assistant
Computer Science and Telecommunications Board

Robert F. Sproull, NAE, Oracle Corporation (retired), Chair
Prithviraj Banerjee, Hewlett-Packard Company, Palo Alto, California
Steven M. Bellovin, NAE, Columbia University, New York, New York
Jack L. Goldsmith III, Harvard Law School, Cambridge, Massachusetts
Seymour E. Goodman, Georgia Institute of Technology, Atlanta, Georgia
Jon M. Kleinberg, NAE, Cornell University, Ithaca, New York
Robert Kraut, Carnegie Mellon University, Pittsburgh, Pennsylvania
Susan Landau, Harvard University, Cambridge, Massachusetts
Peter Lee, Microsoft Research, Redmond, Washington
David E. Liddle, U.S. Venture Partners, Menlo Park, California
Prabhakar Raghavan, NAE, Yahoo! Labs, Sunnyvale, California
David E. Shaw, NAE, D. E. Shaw Research, New York, New York
John Stankovic, University of Virginia, Charlottesville
John A. Swainson, Dell, Inc., Round Rock, Texas
Peter Szolovits, IOM, Massachusetts Institute of Technology, Cambridge
Peter J. Weinberger, Google, Inc., New York, New York
Ernest J. Wilson, University of Southern California, Los Angeles
Katherine Yelick, University of California, Berkeley

Staff

Jon Eisenberg, Director
Renee Hawkins, Financial and Administrative Manager
Herbert S. Lin, Chief Scientist
Lynette I. Millett, Senior Program Officer
Emily Ann Meyer, Program Officer
Virginia Bacon Talati, Associate Program Officer
Enita A. Williams, Associate Program Officer
Shenae Bradley, Senior Program Assistant
Eric Whitaker, Senior Program Assistant
Committee on Electronic Vehicle Controls and Unintended Acceleration

Louis J. Lanzerotti, NAE, New Jersey Institute of Technology, Newark, Chair
Dennis C. Bley, Buttonwood Consulting, Inc., Oakton, Virginia
Raymond M. Brach, University of Notre Dame, South Bend, Indiana
Daniel L. Dvorak, Jet Propulsion Laboratory, Pasadena, California
David Gerard, Lawrence University, Appleton, Wisconsin
Deepak K. Goel, TechuServe LLC, Ann Arbor, Michigan
Daniel Jackson, Massachusetts Institute of Technology, Cambridge
Linos J. Jacovides, NAE, Grosse Pointe Farms, Michigan
Pradeep Lall, Auburn University, Auburn, Alabama
John D. Lee, University of Wisconsin, Madison
Adrian K. Lund, Insurance Institute for Highway Safety, Arlington, Virginia
Michael J. Oliver, MAJR Products, Seagertown, Pennsylvania
William A. Radasky, Metatech Corporation, Goleta, California
Nadine B. Sarter, University of Michigan, Ann Arbor
James W. Sturges, Greer, South Carolina
Dennis F. Wilkie, NAE, Birmingham, Michigan

National Research Council Staff
Thomas R. Menzies, Jr., Study Director, Transportation Research Board
Alan Crane, Senior Scientist, Board on Energy and Environmental Systems
Jon Eisenberg, Director, Computer Science and Telecommunications Board
Mark Hutchins, Program Officer, Transportation
From summer 2009 through spring 2010, news media were filled with reports of drivers claiming that their cars accelerated unintentionally. The nature of the claims varied. Some drivers reported that their vehicles sped up without pressure being applied to the accelerator pedal, and others reported that gentle pressure on the accelerator pedal caused rapid or inconsistent acceleration. Other drivers reported that their vehicles continued to be propelled forward by engine torque even after the accelerator pedal had been released. The National Highway Traffic Safety Administration (NHTSA) observed a spike in motorist complaints about these phenomena. Toyota Motor Corporation, whose vehicles were the subject of many of the complaints, issued recalls for millions of vehicles to address accelerator pedals that could be entrapped by floor mats and to fix pedal assemblies that were susceptible to sticking. Scores of lawsuits were filed against Toyota by vehicle owners (Reuters 2011). In the wake of the highly publicized Toyota recalls, hundreds of other drivers filed

1 As described later in the report, the term “unintended acceleration” is often used interchangeably in reference to these and other vehicle behaviors reported in consumer complaints such as hesitation when the accelerator pedal is pressed, lurching during gear changes, and fluctuation in engine idle speeds. This report does not define the behaviors that constitute unintended acceleration but refers to definitions used by NHTSA. In its report Technical Assessment of Toyota Electronic Throttle Control (ETC) Systems, NHTSA (2011, vi, footnote 1) defines unintended acceleration as “the occurrence of any degree of acceleration that the vehicle driver did not purposely cause to occur.”

complaints of unintended acceleration episodes with NHTSA.\textsuperscript{3} Congress held hearings,\textsuperscript{4} and individuals with expertise ranging from human factors to electronics hardware and software offered theories on other possible causes. The electronics in the automobile throttle control system were at the center of many of these theories.

Some observers with a long exposure to highway safety were reminded of events 25 years earlier, when owners of Audi cars reported a much higher-than-usual occurrence of unintended acceleration. A major difference is that the Audi and other vehicles manufactured during the 1980s contained relatively few electronics systems, and the control of the vehicle’s throttle was mechanical. NHTSA had attributed the cause of Audi’s problems to drivers mistakenly applying the accelerator pedal when they intended to apply the brake, perhaps confused by the vehicle’s pedal layout or startled by intermittent high engine idle speeds. The design and functionality of these traditional mechanical throttle systems, which use a cable and other mechanical connections running from the accelerator pedal to the throttle to open and close it, are simple and straightforward. In contrast, the electronic throttle control systems (ETCs) in use in nearly all modern automobiles, including the recalled Toyotas, rely on electronic signals transmitted by wire from the pedal assembly to a computer that controls the throttle position. Mass introduced about 10 years ago, the ETC is one of many electronics systems that have been added to automobiles during the past 25 years.

Some failures of software and other faults in electronics systems do not leave physical evidence of their occurrence, which can complicate assessment of the causes of unusual behaviors in the modern, electronics-intensive automobile. Reminded of the adage “the absence of evidence is not evidence of absence,” the committee regularly discussed the potential for such untraceable faults to underlie reports of unsafe vehicle behaviors such as episodes of unintended acceleration. As media attention over unintended acceleration heightened, the distinction that NHTSA had used for decades to identify unintended acceleration cases caused by pedal misapplication was given little regard. Instead, the pedal

\textsuperscript{3} NHTSA shows how driver complaints of unintended acceleration fluctuated during 2009 and 2010 following recall announcements, congressional hearings, and publicized crashes (NHTSA 2011, Figure 2).

misapplication cases were often intermixed in media accounts with other instances of unintended acceleration that NHTSA concluded were caused by pedal entrapment and sticking.

The committee was well into its information-gathering phase before it fully appreciated NHTSA’s reasoning for distinguishing instances of pedal misapplication from other sources of unintended acceleration. While untraceable electronics faults may be suspected causes of unintended acceleration, this explanation is unsatisfactory when the driver also reports experiencing immediate and full loss of braking. However, such reports are common among complaints of unintended acceleration, and NHTSA attributes them to pedal misapplication when investigations offer no other credible explanation for the catastrophic and coincidental loss of braking. This observation has no bearing on the fact that faults in electronics systems can be untraceable, but it indicates the importance of considering the totality of the evidence in investigations of reports of unsafe vehicle behaviors.

During the peak of the unintended acceleration controversy in March 2010, NHTSA enlisted the National Aeronautics and Space Administration (NASA) in an in-depth examination of the potential for vulnerabilities in the electronics of the Toyota ETC. NHTSA also requested this National Research Council (NRC) study to review investigations of unintended acceleration and to recommend ways to strengthen the agency’s safety oversight of automotive electronics systems. In response to NHTSA’s request, NRC appointed the Committee on Electronic Vehicle Controls and Unintended Acceleration to provide a balance of expertise and perspectives relevant to the task statement (contained in Chapter 1).

NHTSA expected the NASA investigation to be completed in time for its results to inform the work of this committee, which held its first meeting on June 30, 2010. The NASA report was completed approximately 7 months after the committee’s first meeting, during February 2011. NASA reported finding no evidence of Toyota’s ETC being a plausible cause of unintended acceleration characteristic of a large throttle opening. The NASA investigators further confirmed NHTSA’s conclusion that the ETC could not disable the brakes so as to cause loss of braking capacity, as often reported by drivers experiencing unintended acceleration commencing in a vehicle that had been stopped or moving slowly.

Not knowing the outcome of the NASA investigation until partway through its deliberations, the committee spent a great deal of time during the early stages of its work considering the broader safety issues
associated with the growth in automotive electronics and the implications for NHTSA's regulatory, research, and defect investigations programs. The consideration of these issues proved beneficial and shaped many of the findings and recommendations in this report. The committee learned how electronics systems are transforming the automobile and how they are likely to continue to do so for years to come. In this respect, controversies similar to that involving the Toyota ETC may recur and involve other automobile manufacturers and other types of electronics systems in vehicles.

Because of NASA's work, the causes of unintended acceleration by Toyota vehicles are clearer today than they were when the committee convened for the first time some 18 months ago. Nevertheless, whether the technical justification for suspecting electronics systems in this particular instance warranted the attention given to them and the commissioning of the detailed NASA study is a question that deserves consideration in view of the potential for electronics to be implicated in many other safety issues as their uses proliferate. Knowing what to look for and when to pursue electronics as a candidate cause of unsafe vehicle behaviors will be increasingly important to NHTSA. It is with this in mind that the committee provides its recommendations to the agency.

The content, findings, and recommendations in this report represent the consensus effort of a dedicated committee of 16 members, all of whom were uncompensated and served in the public interest. Drawn from multiple disciplines, the members brought expertise from automotive electronics design and manufacturing, software development and evaluation, human–systems integration, safety and risk analysis, crash investigation and forensics, electromagnetic testing and compatibility, electrical and electronics engineering, and economics and regulation.

The committee met a total of 15 times—11 times in person and four times through teleconference. During most of these meetings the committee convened in sessions open to the public to gather data to inform its deliberations. The data gathering was extensive, involving more than 60 speakers from NHTSA, NASA, and other government agencies; universities and research institutions; consultants; standards organizations; automotive, aerospace, and medical device companies; consumer research organizations; and advocacy and interest groups. In addition, the committee visited with the automotive manufacturers Ford Motor Company, General Motors Company, and Mercedes-Benz and received briefings from Toyota and Continental Automotive Systems. These visits
were not designed to evaluate each company’s product development processes but instead to obtain background information on how manufacturers strive to ensure that electronics systems perform safely.

The committee also provided a forum for comments by individuals who had reported experiencing unintended acceleration. Although it was not charged with investigating the causes of unintended acceleration, the committee found these firsthand motorist accounts to be revealing of the challenge that NHTSA and other investigators face in trying to ascertain the causes of unexpected vehicle behaviors. The names of the motorists who spoke during this forum as well as the many other individuals who briefed the committee are provided in the acknowledgments section below.

When they were appointed to the committee, the majority of members—all recognized experts in their respective fields—did not have detailed knowledge of the concerns surrounding unintended acceleration or NHTSA’s vehicle safety programs. As a multidisciplinary group, the committee faced a steep learning curve, which these numerous data-gathering sessions, expert briefings, literature and document reviews, and extensive meeting discussions helped to overcome. In being assigned to a highly charged topic, the committee’s objectivity and inquisitiveness were its strengths at the outset of the project. These qualities remained with the committee throughout its deliberations and are reflected in the report.

ACKNOWLEDGMENTS

The committee thanks the many individuals who contributed to its work.

During its information-gathering sessions open to the public, the committee was briefed by the following officials from NHTSA: David Strickland, Administrator; Daniel C. Smith, Senior Associate Administrator, Vehicle Safety; John Maddox, Associate Administrator, Vehicle Safety Research; Richard Boyd, Director, Office of Defects Investigation (ODI); Richard Compton, Director, Office of Behavioral Safety Research; Chip Chidester, Director, Office of Data Acquisitions; Roger Saul, Director, Vehicle Research and Test Center (VRTC); Jeffrey L. Quandt, Vehicle Control Division Chief, ODI; Christina Morgan, Early Warning Division Chief, ODI; Gregory Magno, Defects Assessment Division Chief, ODI; Nathaniel Beuse, Director, Office of Crash Avoidance Standards, Rulemaking; and
Frank Barickman, VRTC. In addition, John Hinch, retired NHTSA Director of the Office of Human–Vehicle Performance Research, briefed the committee on the agency’s rules concerning event data recorders.

The following university researchers briefed the committee: Paul Fischbeck, Professor, Engineering and Public Policy and Social and Decision Sciences, Carnegie Mellon University; Michael Pecht, Chair Professor, Mechanical Engineering, and Director of the Center for Advanced Life Cycle Engineering, University of Maryland; Todd Huling, Michelin Professor, Vehicle Electronic Systems Integration, and Director, Clemson University International Center for Automotive Research; Stefan Savage, Professor, Department of Computer Science and Engineering, University of California, San Diego; and Tadayoshi Kohno, Associate Professor, Department of Computer Science and Engineering, University of Washington.

Information on standards activities was provided by Joseph D. Miller, TRW Automotive Member ISO TC22 SC3, Working Group 16; Margaret Jenny, President, RTCA, Inc.; and Thomas M. Kowalick, Chair, Institute of Electrical and Electronics Engineers Global Standards for Motor Vehicle Event Data Recorders.

Information on safety assurance processes and regulatory oversight and safety analysis in other industries was provided by David Walen, Chief Scientific and Technical Adviser on Electromagnetic Interference and Lightning, Federal Aviation Administration (FAA); Thomas Fancy, Technical Fellow, Gulfstream Aerospace Corporation; Michael D. James, FAA DER Engine Control Systems, Honeywell Aerospace; Thomas Gross, Deputy Director, Post-Market Science, Office of Surveillance and Biometrics, Center for Devices and Radiological Health, U.S. Food and Drug Administration (FDA); Jeffrey Silberberg, Senior Electronics Engineer, Center for Devices and Radiological Health, FDA; Daniel J. Dummer, Engineering Director, Reliability Test, Medtronic CRDM; William DuMouchel, Oracle Health Services; and Brian Murray, United Technologies Research Center.

Additional briefings on varied topics were provided by David Champion, Director, Auto Test Center, Consumers Union; Ronald A. Belt, retired, Honeywell Corporation; Sean Kane, Safety Research and Strategies, Inc.; Ellen Liberman, Felix Click, MLS; Randy Whitfield, Quality Control Systems, Inc.; William Rosenbluth, Automotive Systems Analysis; Keith Armstrong, Cherry Clough Consultants; Joan Claybrook, Public Citizen; and Clarence Ditlow, Center for Auto Safety.
NASA held a special briefing on its investigation led by Michael Kirsch, with participation from Michael Bay, Victoria Regenie, Poul Andersen, Michael Crane, Robert Scully, Mitchell Davis, Oscar Gonzalez, Michael Aguilar, Robert Kichak, and Cynthia Null.

Robert Strassburger of the Alliance of Automobile Manufacturers briefed the committee at its first meeting and was instrumental in arranging visits with and briefings by automotive companies. The committee’s visit with Ford was arranged and led by Ray Nevi and Mark Tuneff. The committee’s visit with General Motors was arranged by Stephen Gehring. Briefings from Continental were led by Philip Headley. Briefings by Mercedes-Benz were arranged by Barbara Wendling and William Craven. Kevin Ro and Kristen Tabar arranged briefings by Toyota, which were led by Seigo Kuzumaki.

The following individuals spoke to the committee about their experiences with unintended acceleration: Eugenie Mielczarek, Kevin Haggerty, Rhonda Smith, Robert Tevis, Richard Zappa, and Francis Visconi.

Thomas Menzies, Alan Crane, Jon Eisenberg, and James Zucchetto were the principal project staff. Menzies managed the study and drafted the report under the guidance of the committee and the supervision of Stephen R. Godwin, Director, Studies and Special Programs, Transportation Research Board (TRB). Norman Solomon edited the report; Janet M. McNaughton handled the editorial production; Juanita Green managed the book design, production, and printing; and Jennifer J. Weeks prepared the final manuscript files for prepublication release and web posting, under the supervision of Javy Awan, Director of Publications, TRB. Mark Hutchins provided extensive support to the committee in arranging its many meetings and in managing documents.

This report has been reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise in accordance with procedures approved by NRC’s Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the institution in making the report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process.

NRC thanks the following individuals for their review of this report: A. Harvey Bell IV, University of Michigan, Ann Arbor; Jeffrey Caird, University of Calgary, Alberta, Canada; William H. DuMouchel, Oracle Health.
Sciences, Tucson, Arizona; Robert A. Frosch, Harvard University, Cambridge, Massachusetts; Brian T. Murray, United Technologies Research Center, East Hartford, Connecticut; Clinton V. Oster, Bloomington, Indiana; R. David Pittle, Alexandria, Virginia; William F. Powers, Boca Raton, Florida; Bernard I. Robertson, Bloomfield Hills, Michigan; L. Robert Shelton III, New Smyrna Beach, Florida; and Peter J. Weinberger, Google, Inc., New York. The review of this report was overseen by Lawrence T. Papay, PQR, LLC, La Jolla, California; and C. Michael Walton, University of Texas, Austin. Appointed by NRC, they were responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of the report rests solely with the authoring committee and the institution. Suzanne Schneider, Associate Executive Director, TRB, managed the report review process.

—Louis J. Lanzerotti, Chair
Committee on Electronic Vehicle Controls and Unintended Acceleration

REFERENCES

Abbreviation
NHTSA National Highway Traffic Safety Administration


Contents

Summary 1

1 Background and Charge 23
   NHTSA’s Automotive Safety Role 27
   Earlier NHTSA Initiatives on Unintended Acceleration 30
   The Revolution in Automotive Electronics 35
   Study Goals and Report Organization 37

2 The Electronics-Intensive Automobile 43
   Use of Electronics in Vehicles Today 44
   Next-Generation Systems 61
   Safety Challenges 63
   Chapter Findings 68

3 Safety Assurance Processes for Automotive Electronics 71
   Safety Assurance Practices in the Automotive Industry 73
   Industry Standards Activities for Electronics Safety Assurance 90
   Chapter Findings 95

4 National Highway Traffic Safety Administration 99
   Vehicle Safety Programs 102
   Rulemaking 104
   Enforcement and Defect Investigation 111
   Vehicle Safety Research 118
Strategic and Priority Planning for Research and Rulemaking  122
Safety Assurance and Oversight in Other Industries  123
Chapter Findings  127

5  Review of National Highway Traffic
Safety Administration Initiatives on Unintended Acceleration  133
Past NHTSA Initiatives on Unintended Acceleration  136
Investigations of Toyota Complaints  141
Recent NHTSA Initiatives on Unintended Acceleration  151
Chapter Findings  163

NHTSA's Current Role with Respect to Vehicle Electronics  170
Keeping Pace with the Safety Assurance Challenges Arising from Vehicle Electronics  176
Strengthening Capabilities for Defect Surveillance and Investigation  182
Reaction to NHTSA's Proposed Next Steps  185
Strategic Planning to Guide Future Decisions and Priorities  188

Study Committee Biographical Information  197