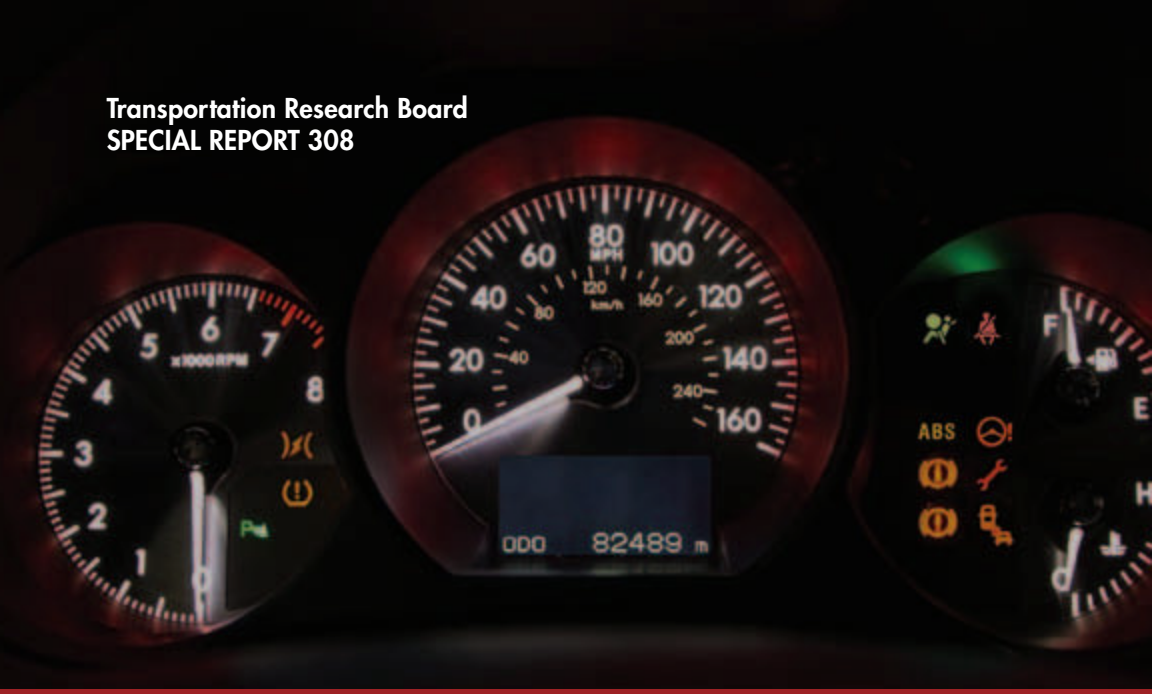
Transportation Research Board
SPECIAL REPORT 308



The Safety Promise and Challenge of Automotive Electronics

INSIGHTS FROM UNINTENDED ACCELERATION

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

Transportation Research Board
SPECIAL REPORT 308

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 Special Report 308

Subscriber Categories
Policy; safety and human factors; vehicles and equipment

Transportation Research Board publications are available by ordering individual publications directly from the TRB Business Office, through the Internet at www.TRB.org or national-academies.org/trb, or by annual subscription through organizational or individual affiliation with TRB. Affiliates and library subscribers are eligible for substantial discounts. For further information, contact the Transportation Research Board Business Office, 500 Fifth Street, NW, Washington, DC 20001 (telephone 202-334-3213; fax 202-334-2519; or e-mail TRBsales@nas.edu).

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competencies and with regard for appropriate balance.

This report has been reviewed by a group other than the authors according to the procedures approved by a Report Review Committee consisting of members of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine.

This report was sponsored by the National Highway Traffic Safety Administration of the U.S. Department of Transportation.

Cover and inside design by Debra Naylor, Naylor Design.
Cover photo by George Dolgikh, shutterstock.com.
Typesetting by Circle Graphics, Inc.

Library of Congress Cataloging-in-Publication Data

National Research Council (U.S.). Committee on Electronic Vehicle Controls and Unintended Acceleration.
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.
p. cm.—(Transportation Research Board special report ; 308)
ISBN 978-0-309-22304-1
1. Automobiles—Electronic equipment—United States—Reliability.
2. Automobiles—Handling characteristics—United States. I. Title.
TL272.5.N38 2012
363.12'51—dc23
2012001092

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. On the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Ralph J. Cicerone is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Charles M. Vest is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, on its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Ralph J. Cicerone and Dr. Charles M. Vest are chair and vice chair, respectively, of the National Research Council.

The **Transportation Research Board** is one of six major divisions of the National Research Council. The mission of the Transportation Research Board is to provide leadership in transportation innovation and progress through research and information exchange, conducted within a setting that is objective, interdisciplinary, and multimodal. The Board's varied activities annually engage about 7,000 engineers, scientists, and other transportation researchers and practitioners from the public and private sectors and academia, all of whom contribute their expertise in the public interest. The program is supported by state transportation departments, federal agencies including the component administrations of the U.S. Department of Transportation, and other organizations and individuals interested in the development of transportation. **www.TRB.org**

www.national-academies.org

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

Alfred Z. Spector, NAE, Google, Inc., 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 Research Board

Preface

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.[1] 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,[2] 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."

[2] One ABC News report in particular, broadcast on February 22, 2010, received considerable public attention. The report claimed that Toyota's electronic throttle control system could malfunction to cause unintended acceleration. http://abcnews.go.com/Blotter/toyota-recall-electronic-design-flaw-linked-toyota-runaway-acceleration-problems/story?id=9909319.

complaints of unintended acceleration episodes with NHTSA.[3] Congress held hearings,[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

[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).

[4] Hearings before the U.S. House of Representatives Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, February 23, 2010, and May 20, 2010. http://democrats.energycommerce.house.gov/index.php?q=hearing/hearing-on-update-on-toyota-and-nhtsa-s-response-to-the-problem-of-sudden-unintended-acceler.

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 Hubing, 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

NHTSA. 2011. *Technical Assessment of Toyota Electronic Throttle Control (ETC) Systems.* http://www.nhtsa.gov/staticfiles/nvs/pdf/NHTSA-UA_report.pdf.

Reuters. 2011. U.S. Judge Denies Toyota Lawsuit Dismissal Attempt. April 29. http://www.reuters.com/article/2011/04/29/toyota-ruling-idUSN2917985520110429.

Contents

Summary

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

BOX S-1

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.

Box S-1 (*continued*) Summary of Findings

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

(continued on next page)

Box S-1 (*continued*) Summary of Findings

of traffic crash data indicating where focused research can further the introduction of new regulations and vehicle capabilities aimed at mitigating known safety problems.

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.

Box S-1 (*continued*) Summary of Findings

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)

Box S-1 (*continued*) Summary of Findings

pedal misapplication, and to aid investigators in identifying pedal entrapment by floor mats as the likely cause.

Finding 5.7: ODI's investigation of unintended acceleration in Toyota vehicles indicated how data saved in EDRs can be retrieved from vehicles involved in crashes to supplement and assess other information, including circumstantial evidence, in determining causal and contributing factors.

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.

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.

Box S-3 (*continued*) Recommendations to NHTSA

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.

1

Background and Charge

The National Highway Traffic Safety Administration (NHTSA) requested this study of its efforts to determine the possible causes of unintended acceleration in vehicles in order to advise on ways to strengthen the agency's regulatory, research, and defect investigation capabilities as automobiles become more electronics-intensive. While NHTSA has investigated complaints of unintended acceleration for many decades, an unusually large number of such complaints have been made in recent years, particularly by owners of Toyota vehicles.[1] Many complaints have involved high-power acceleration, which NHTSA's investigators concluded was attributable to drivers applying the accelerator pedal by mistake and to certain other mechanical causes, including sticking pedal assemblies and pedals becoming obstructed or entrapped.[2] Pedal misapplication, entrapment, and sticking have often been identified by NHTSA as causes of unintended acceleration, along with various other mechanical causes such as throttle icing and damage to the physical linkages between the pedal and throttle assemblies.[3] However, the proliferation of electronics systems, and particularly the introduction of

[1] According to data presented to the committee by NHTSA, about 35 percent of the complaints it received between 2004 and 2010 alleging unintended acceleration were by drivers of Toyota vehicles. Presentation by Daniel C. Smith, NHTSA Associate Administrator, Enforcement, June 30, 2010, Slide 17. http://onlinepubs.trb.org/onlinepubs/UA/100630DOTSlidesSmith.

[2] NHTSA investigations into the causes of unintended acceleration in Toyota vehicles are discussed in Chapter 5.

[3] The National Transportation Safety Board has also investigated pedal misapplication by drivers of school buses and other heavy vehicles (NTSB 2009).

electronic throttle control systems (ETCs) during the past decade, has prompted questions about whether faults in these systems were responsible for some of the complaints of unintended acceleration.[4] The Toyota vehicles that NHTSA concluded were susceptible to pedal sticking and entrapment were equipped with ETCs.

NHTSA's initial findings of pedal entrapment caused by floor mats prompted Toyota to issue a series of recalls involving millions of vehicles. The first recalls involved redesigned floor mats and notifications to owners and dealers about the dangers of unsecured and incompatible floor mats and how to respond safely to pedal entrapment should it happen. In subsequent recalls, Toyota reshaped the accelerator pedal to make it less prone to floor mat interference and to install software that causes brake application to override the throttle on vehicles equipped with push-button ignition systems. The latter step was taken as evidence emerged that some drivers were unfamiliar with how to turn off the engine by holding down the start–stop button during an emergency while the vehicle is in motion.[5] Even as these multiple recalls proceeded, questions persisted about the adequacy of Toyota's remedies and whether its ETC technology was to blame, particularly after media reports of more cases of Toyota vehicles exhibiting unintended acceleration, some involving fatalities.[6,7]

ETCs were mass introduced beginning about 10 years ago. They replaced the physical connection between the accelerator pedal and the

---

[4] As recounted in Chapter 5, NHTSA received consumer petitions starting in 2003 requesting that the agency investigate the Toyota ETC as the possible cause of unintended acceleration.

[5] In addition, in late 2009 Toyota observed through its field reports, and NHTSA confirmed through its review of consumer complaints, that a sticking pedal assembly component was causing episodes in which vehicles were not slowing down in response to the driver reducing pressure on the accelerator pedal. In early 2010, Toyota initiated a recall to fix a mechanical defect in the pedal assembly, which involved many of the same Toyota vehicles subject to the floor mat recalls.

[6] In particular, a fatal crash involving a Lexus 350 ES that occurred in the city of Santee in San Diego County, California, on August 28, 2009, received considerable media, public, and congressional attention. NHTSA and the San Diego County Sheriff's Department later concluded that the cause of the crash was pedal entrapment as a result of an incompatible all-weather floor mat. See San Diego County Sheriff's Department Incident Report concerning August 2009 crash in Santee, California (Case No. 09056454).

[7] The origins of the initial driver concerns over Toyota's ETC as a possible cause of unintended acceleration remain unclear. However, these concerns appear to have increased after a report prepared by David W. Gilbert for the advocacy group Safety Research and Strategies, Inc., which purported to demonstrate how Toyota's ETC could operate with undetected faults in its pedal position sensors. A videotape of Gilbert's demonstration was broadcast on February 22, 2010, on ABC News: http://abcnews.go.com/Blotter/toyota-recall-electronic-design-flaw-linked-toyota-runaway-acceleration-problems/story?id=9909319. The Gilbert paper can be found at http://www.safetyresearch.net/Library/Preliminary_Report022110.pdf.

throttle with an electronic connection consisting of sensors, wires, microprocessors, other circuitry, and a motorized throttle actuator. ETCs are now commonplace in new vehicles across the fleet. Concerns about public confidence in this common technology prompted NHTSA to take several actions.

First, the agency's Office of Defects Investigation (ODI) rescreened and reanalyzed all vehicle owner complaints for all vehicle makes during the past decade to identify and examine any that might be indicative of unintended acceleration. In its analysis, ODI observed a range of reported vehicle behaviors that could be described as unintended acceleration, from vehicles hesitating or lurching during gear changes to abrupt increases in engine power and vehicle speed that suggested a large throttle opening. In many of the latter cases in particular, ODI observed that reported brake application was described by the driver as being ineffective in controlling acceleration. Reports of lost braking capacity also raised the possibility of brake defects, although brake damage or degradation was confirmed only in a relatively small number of cases in which the vehicle traveled at a high rate of speed for several miles and the brake pedal was depressed by the driver for a long time or repeatedly pumped. In NHTSA's view, cases in which alleged immediate and profound brake loss could not be explained were consistent with pedal misapplication. The latter cases of unintended acceleration involving degraded braking capacity were believed to be caused by pedal entrapment, pedal sticking, and other identifiable mechanical problems.

NHTSA did not find any unusual patterns in the warranty repair data submitted by Toyota or any other manufacturer related to ETCs, and the agency believed that its rescreening of consumer complaints did not suggest any new explanations for unintended acceleration involving vehicle electronics. Nevertheless, NHTSA undertook further analyses and investigations of Toyota's ETC in response to the growing public concern. First, ODI investigators conducted more detailed examinations of a small subset of complaints involving crashes of Toyota vehicles in which information from the vehicles' electronic event data recorders was retrieved and analyzed (NHTSA 2011). These investigations, discussed in more detail later in this report, did not provide any reason for the agency to question its earlier findings and conclusions about pedal misapplication, entrapment, and sticking being the causes of high-power unintended acceleration in Toyota vehicles. Second, NHTSA commissioned a team of engineers with expertise in electronics and software testing from the

National Aeronautics and Space Administration (NASA) to investigate whether vulnerabilities exist in the design and implementation of Toyota's ETC that could have plausibly produced any of the unintended acceleration behaviors reported by consumers.[8]

While these latter investigations were under way, NHTSA requested the National Research Council to convene an independent committee to conduct this study. The committee's task was to inform a broader examination of the safety assurance challenges arising from the proliferation and growing complexity of automotive electronics and their implications for NHTSA's vehicle safety programs. In performing its task, the committee was to consider the pending results of the ODI and NASA investigations as well as the results of past NHTSA investigations. The committee was not tasked with conducting its own investigations of the incidence and potential causes of unintended acceleration. For study background, NHTSA asked the committee to review the means by which automotive manufacturers seek to ensure the safe and secure performance of their electronics systems and to consider how safety assurance is handled in other industries such as aviation. This report describes these safety assurance processes but does not critique them or make recommendations to the automotive industry.

These requested reviews proved valuable to the study. The committee learned, for example, that ETCs are simple and mature systems in comparison with the many other automotive electronics systems being developed and deployed that can affect vehicle control. The public apprehension over whether ETCs were the cause of unsafe vehicle behaviors thus raises the prospect, in the committee's view, that similar or even more serious concerns could arise as more complex electronics systems are introduced into the fleet. That prospect is troubling because, as the committee describes in this report, electronics-intensive systems are now central to vehicle functionality and provide many significant benefits to motorists, including safety benefits. Indeed, NHTSA is promoting the development and introduction of many new crash-avoidance systems that have become possible only as a result of advancements in electronics technology.

[8] The investigation was conducted by NASA's Engineering and Safety Center and the results reported to NHTSA in January 2011 in *National Highway Traffic Safety Administration Toyota Unintended Acceleration Investigation: Technical Support to the National Highway Traffic Safety Administration (NHTSA) on the Reported Toyota Motor Corporation (TMC) Unintended Acceleration (UA) Investigation*. Released to the public on NHTSA's website in February 2011. http://www.nhtsa.gov/staticfiles/nvs/pdf/NASA-UA_report.pdf.

Innovations in the automobile will be driven extensively by developments in electronics technology. Therefore, the emphasis of this report is not on second-guessing the past actions of NHTSA but instead on steps that can be taken to ensure that the agency's programs are aligned with meeting the safety assurance challenges likely to accompany these developments.

More background on many of the issues raised above and a description of how the report is organized to address the study charge are given next. The background begins with an overview of NHTSA's vehicle safety oversight role and its past responses to concerns over unintended acceleration. The chapter concludes by explaining the study goals and the report's organization.

NHTSA's AUTOMOTIVE SAFETY ROLE

Legislation enacted 45 years ago that introduced a federal role in ensuring traffic safety, and that soon led to NHTSA's creation within the U.S. Department of Transportation (DOT), called for the establishment of regulations specifying minimum safety features and capabilities in motor vehicles.[9] At the time, automobiles were almost entirely mechanical in their function, having no computing capabilities, software, or internal networks. Nevertheless, the automobile of about 1970 was the product of a steady stream of innovations in designs, materials, and engineering by original equipment manufacturers (OEMs) and their suppliers. To avoid impeding this innovation, NHTSA was charged with writing the Federal Motor Vehicle Safety Standards (FMVSSs) in terms of minimum performance requirements and thus avoiding prescriptions about how manufacturers should meet the requirements through their product design, development, and production processes.[10]

The FMVSSs promulgated by NHTSA consist of three main categories of regulations covering crash avoidance, crashworthiness, and postcrash integrity. The first category covers vehicle capabilities essential to preventing a crash, such as minimum capabilities for braking, visibility, and

[9] More details on the laws establishing NHTSA and its vehicle safety mission are given in Chapter 4.

[10] The FMVSSs, along with other NHTSA regulations, are incorporated into Chapter 5 of Title 49, *Code of Federal Regulations*. The authorizing law defines an FMVSS as a "minimum standard for motor vehicle performance, or motor vehicle equipment performance, which is practicable, which meets the need for motor vehicle safety, and which provides objective criteria."

accelerator control. The second contains regulations intended to make vehicles more capable of withstanding crash forces and protecting occupants in the event of a crash, such as by having certain restraint systems and crush resistance. The third specifies requirements for maintaining vehicle integrity after a crash has occurred, such as fire resistance. NHTSA sets and enforces several other standards that are not contained within these three categories of FMVSSs, such as requirements for vehicles equipped with event data recorders and mandated reporting to NHTSA of certain safety-related data.

Automobile manufacturers are not required to notify NHTSA when they introduce a new component or system design, even if it pertains to an FMVSS. Each manufacturer is responsible for determining whether the product design and its implementation meet all relevant FMVSSs, and in so doing the manufacturer may consult NHTSA for interpretations of the requirements. NHTSA does not set its own design and implementation standards, nor does it demand that manufacturers follow third-party standards to guide design, development, and evaluation processes such as testing of software code, materials properties, and electromagnetic compatibility. Automotive manufacturers must determine for themselves which processes are best suited to their product designs and are required to certify that their vehicles meet all relevant FMVSSs.[11]

Because the FMVSSs are intended to be technology neutral, the changeover from mechanical to electronics systems in recent years has not necessitated substantial regulatory revisions. For example, NHTSA officials informed the committee that the introduction of keyless ignition systems occurred within the context of the existing FMVSS 114.[12] The agency has interpreted the standard's requirements governing the use of a "key" as encompassing both a traditional physical key and codes that are electronically transmitted by a fob or entered by the driver using a keypad inside the vehicle. Likewise, the introduction of ETCs in the late 1990s occurred in accordance with the original FMVSS 124 on accelerator control systems, which was promulgated in the early 1970s. FMVSS 124 requires that a vehicle's throttle plate return to the idle position when the driver removes the actuating force from the accelera-

[11] Certification of a vehicle's compliance with relevant FMVSSs must be shown by a label or tag permanently affixed to the vehicle.

[12] The committee was provided this explanation by Nathaniel Beuse, Director, Office of Crash Avoidance Standards, in a briefing titled "Government and Voluntary Standards as They Related to Unintended Acceleration," June 30, 2010.

tor control, even if there is a disconnection. NHTSA officials explained to the committee that in this case the agency interprets a "disconnection" to cover separations of physical linkages as well as separations of electrical connections.[13]

For technical support of its regulatory activities, NHTSA relies on its vehicle safety research program. NHTSA officials explained to the committee that its neutrality with respect to the technologies used by manufacturers to meet the FMVSSs does not mean that the agency can afford to neglect technological developments taking place in the automotive sector. Accordingly, NHTSA's Office of Vehicle Safety Research is charged with keeping abreast of existing and emerging technologies that may create safety assurance challenges or that may provide opportunities to make driving safer. The content and priorities of the research program are thus driven by ongoing regulatory needs (such as the development of a performance test for a new standard) and by evidence from crash records indicating safety problems that may be candidates for mitigation through advancements in vehicle technologies.[14]

NHTSA's main method for ensuring that manufacturers comply with the FMVSSs is through its Office of Vehicle Safety Compliance, which inspects and tests samples of vehicles to assess their conformance to the regulations.[15] However, a vehicle may be in full compliance with all FMVSSs and still exhibit a safety defect in use. The committee was informed by NHTSA that for the agency to order a safety recall, it must be able to demonstrate that (*a*) a defect exists as shown by a significant number of real-world failures and (*b*) the defect poses an unreasonable risk to safety.[16] Furthermore, NHTSA (2011, 1) states: "To demonstrate the existence of a safety defect . . . NHTSA would need to prove that a substantial number of failures attributable to the defect have occurred or are likely to occur in consumers' use of the vehicle or equipment and that the failures pose an unreasonable risk to motor vehicle safety."

[13] The committee was provided the information by Nathaniel Beuse, Director, Office of Crash Avoidance Standards, in a briefing titled "Government and Voluntary Standards as They Related to Unintended Acceleration," June 30, 2010.

[14] Presentation to the committee by John Maddox, Associate Administrator, Vehicle Safety Research, Research Capabilities, Program Prioritization, and Resources: "National Highway Traffic Safety Administration—Research Overview," January 27, 2011.

[15] The Office of Vehicle Safety Compliance (as well as the Office of Rulemaking) also receives reports from manufacturers when they determine that some of their vehicles do not comply with one or more FMVSSs.

[16] Presentation to the committee by Richard Boyd, Acting Director, ODI, October 22, 2010.

The responsibility for identifying and investigating safety defects rests with ODI. ODI fulfills this responsibility with significant assistance from consumers, who file complaints of unsafe vehicle behaviors and conditions. ODI analysts regularly screen and analyze consumer complaints to detect vehicle behaviors and conditions indicative of defects or other vehicle-related problems that present a safety concern.[17] Such concerns may prompt ODI to investigate further by examining more complaints, reviewing warranty repair records submitted by manufacturers, inspecting and testing vehicles and their parts, interviewing drivers and repair technicians, and consulting with and seeking more detailed information from manufacturers.[18] When a deeper investigation of a suspect problem establishes that a vehicle safety deficiency exists and is sufficient in magnitude and scope to pose an unreasonable safety risk, ODI has authority to compel the manufacturer to issue a product recall. In practice, most recalls are initiated by the manufacturer before ODI even opens an investigation, and nearly all are initiated without ODI having to take an enforcement action.[19]

EARLIER NHTSA INITIATIVES ON UNINTENDED ACCELERATION

The committee learned that ODI has fielded and investigated driver reports of unintended acceleration for more than 40 years.[20] More than three dozen investigations of such concerns were conducted by ODI during the 1980s alone, resulting in a number of manufacturer recalls (Pollard and Sussman 1989). Nearly all of the recalls from that era addressed mechanical problems, including pedal entrapment by floor mats, broken parts in the throttle, malfunctions in the vacuum actuators

[17] According to NHTSA (2011, 1), the agency receives 30,000 to 40,000 consumer complaints each year. According to the USDOT Office of Inspector General, from 2002 to 2009 NHTSA screened roughly 40,000 consumer complaints annually, leading to 77 investigations for safety defects (see Report MH-2012-001, issued October 6, 2011, p. 1).

[18] Presentation to the committee by Gregory E. Magno, Defects Assessment Division Chief, ODI, titled "Use of VOQ Data in ODI Screening of Unintended Acceleration and Vehicle Electronics," and by Jeffrey L. Quandt, Vehicle Control Division Chief, ODI, titled "Use of Data in ODI Investigations of Unintended Acceleration and Vehicle Electronics," October 22, 2010.

[19] According to statements in the agency's report (NHTSA 2011, 2), the majority of recalls are initiated by manufacturers without NHTSA opening a formal investigation.

[20] This report recounts investigations since the mid-1980s, when electronics started to become suspected causes of defects. During the 1970s, NHTSA conducted an 8-year-long investigation of possible mechanical causes of unintended acceleration involving more than 1,700 crashes (ODI Report EA78-110).

that mechanically moved the throttle, and faulty physical linkages that caused the throttle to remain open even when the driver released the accelerator pedal.

Even though ODI typically received complaints of unintended acceleration by owners of a wide range of vehicle makes and models, complaint analysts noticed that starting in the early 1980s an inordinate number had involved the Audi 5000.[21,22] The Audi importer, Volkswagen, believed that the high complaint rate stemmed from the layout of the brake and accelerator pedals. In 1982 and 1983, Volkswagen initiated recalls to modify the Audi's accelerator pedal to prevent interference by the floor mat and elevate the brake pedal relative to the accelerator pedal to reduce the chance of pedal misapplication. A continued high rate of complaints prompted ODI to enlist U.S. DOT's Volpe Transportation Systems Center (TSC) to conduct a more thorough investigation of the problem, first by examining the reports involving Audi (Walter et al. 1988) and then by examining the complaints lodged during the previous decade involving all other vehicle makes and models (Pollard and Sussman 1989).[23]

The TSC investigators examined means by which electronics systems in the Audi could lead to unintended acceleration. While vehicles manufactured during the mid- to late 1980s typically had computer-based engine control units, the throttle remained connected to the accelerator pedal through a cable and other physical connectors. However, in testing the Audi 5000, TSC investigators found that some versions of the vehicle had an electronically controlled idle stabilizer prone to defects that could intermittently cause high engine idling and unexpected increases in engine power, which the investigators characterized as "surging."[24] The idle stabilizer was composed of an electronic control unit and an

[21] From 1978 to 1987, Audi's complaint rate for unintended acceleration was 586 per 100,000 vehicles in the fleet.

[22] The November 1986 broadcast of "Out of Control" by the CBS news program *60 Minutes* interviewed individuals who had allegedly experienced sudden acceleration by Audi vehicles and were suing the importer (Volkswagen). The broadcast also presented a video purporting to show an Audi 5000 surging forward while the brake pedal was depressed. The segment heightened public concern over unintended acceleration. The demonstration in the video was executed by individuals associated with the plaintiffs; indeed, NHTSA maintains that the Audi 5000 in the demonstration was extensively modified by a plaintiff's consultant (*Federal Register,* Vol. 65, No. 83, pp. 25026–25037).

[23] During roughly the same period of time, Transport Canada (Marriner and Granery 1988) and the Japanese Ministry of Transport (1989) conducted their own studies of the phenomenon.

[24] The idle speed control systems of the era would more appropriately be called idle stabilization systems, since they only provided a "trimming function" around the normal operating point to help achieve smoother idle quality.

electromechanical air valve.[25] The TSC investigators suspected that the intermittent malfunctions observed in the control unit might have gone undetected during normal Audi-specified testing or in postcrash inspections. They concluded that the resulting surging differed from high-power acceleration reported by drivers and that such reported episodes of acceleration were most likely the result of drivers mistakenly applying the accelerator pedal instead of the brake.[26] They surmised that the intermittent surging could have startled or even panicked some drivers, prompting them to misapply the accelerator pedal. The TSC investigators also observed that the pedal and seating layouts of the Audi 5000 differed significantly from those of peer domestic vehicles. These differences, the investigators reported, may have further contributed to a higher incidence of pedal misapplication in the Audi, particularly among drivers lacking familiarity with the vehicle.

Apart from the defective idle stabilizer, TSC investigators could not identify an electronic or mechanical anomaly that could cause the Audi's high rate of complaints. The investigators did observe that a large portion of the consumer complaints involved acceleration occurring at the same moment as the reported occurrence of brake failure. The investigators were unable to identify any combination of malfunctions in the vehicle that could create such a simultaneous failure of two independent systems without leaving physical evidence, especially in the brakes. The TSC researchers also found that many of the motorists reported experiencing sudden acceleration during maneuvers in parking lots and driveways and in other low-speed situations. Typically in these cases, the brakes were alleged to have been completely ineffective in stopping the acceleration, and the episode ended within seconds with a crash. In a follow-up to the Audi report, therefore, NHTSA commissioned TSC to examine more closely the large portion of complaints, as reported across many makes and models, involving sudden acceleration from a low-speed or stationary position and allegations of major brake failure. This

[25] The electronic control unit monitored the engine revolutions per minute (RPM), engine coolant temperature, throttle plate state, air conditioner on–off switch, and air conditioner clutch operation. On the basis of the measurements taken, the control unit selected the appropriate engine idle RPM.

[26] The TSC investigators were not the first to associate pedal misapplication with unintended acceleration, although the TSC work provided a clearer model for how to identify such cases. For example, ODI had concluded that pedal misapplication was the cause of many episodes of unintended acceleration during the previous 20 years of case investigations. Pedal misapplication had also received attention in the human factors literature (see, for example, Schmidt 1989; Rogers and Wierwille 1988; Vernoy and Tomerlin 1989).

second study led to the TSC report that is now commonly referred to as the Silver Book (Pollard and Sussman 1989).

The Silver Book researchers tested 10 vehicles of different makes and model years to identify all possible factors that could cause or contribute to sudden acceleration. They examined the vehicles' engines, transmissions, and cruise control systems to determine whether and how they might produce unwanted power; the effect of electromagnetic interference on the functioning of these systems; the effectiveness of fail-safe mechanisms built into vehicles to prevent or control unwanted acceleration; the pedal effort required and effectiveness of brakes in stopping a vehicle with wide-open throttle; the means by which braking systems can fail spontaneously and recover; and the role of vehicle design factors that might contribute to pedal misapplication. Because these tests were conducted on 1980s-era vehicles, many of the results have limited relevance to contemporary vehicles that utilize much different technologies and designs for many of their control systems. However, one conclusion of the TSC investigators remains relevant: sudden acceleration commencing in a vehicle that had been stationary or moving slowly should be controllable by brake application.

Referring to testing that showed the stopping effectiveness of brakes and their independence from the throttle,[27] the TSC investigators could not offer a credible explanation, apart from pedal misapplication, for how drivers claiming to have applied the brakes promptly would not have been able to stop a vehicle during the onset of acceleration or how the alleged complete brake failure would not be accompanied by physical evidence of a malfunction. In particular, the investigators observed that a large portion of incidents occurred at the start of the driving cycle when drivers were shifting out of park. This circumstance suggests that the drivers had inadvertently pressed the accelerator pedal instead of the brake. During the 1980s, most vehicles in the fleet did not have brake transmission shift interlock systems requiring the driver to depress the brake pedal in order to shift out of park.[28] Thus,

[27] The Silver Book's Appendix E refers to brake force and performance tests conducted at NHTSA's test center by R. G. Mortimer, L. Segal, and R. W. Murphy: "Brake Force Requirements: Driver–Vehicle Braking Performance as a Function of Brake System Design Variables."

[28] NHTSA now requires (in FMVSS 114 as of September 2010) the installation of brake transmission shift interlocks on all new cars equipped with automatic transmissions, but these devices have been common in vehicles since the 1990s. The use of these devices was shown to be effective almost immediately in reducing the occurrence of pedal misapplication in vehicles with automatic transmissions (Reinhart 1994).

the Silver Book recommended that NHTSA conduct more studies to consider this design solution and to examine other factors associated with vehicle designs that may contribute to pedal misapplication and that warrant mitigation.

NHTSA officials explained to the committee that the conditions and circumstances characteristic of pedal misapplication, as enumerated in the Silver Book, remain relevant today as ODI screens complaints alleging unintended acceleration. In receiving hundreds of complaints of this behavior each year (among the tens of thousands of other complaints lodged), ODI decides how best to deploy its investigatory resources to assess the safety relevance and causes of these and other complaints. According to the Silver Book, if a complainant alleges high-power acceleration occurring at the same time as the loss of braking, pedal misapplication should be presumed to be the cause. ODI therefore notes the presence of such signature characteristics of pedal misapplication when it screens complaints.[29]

According to ODI, consumer complaints alleging unintended acceleration that do not exhibit these signature characteristics are subject to further analysis. For example, ODI reported to the committee that a number of complaints by drivers of Toyota vehicles alleging unintended acceleration involved a loss of braking capacity after a prolonged effort by the driver to slow the vehicle through brake application.[30] According to ODI, these complaints stood out from the more common complaints alleging the simultaneous occurrence of high-power acceleration and complete brake loss.[31] Further investigation of these complaints led ODI to conclude that their cause was not pedal misapplication, but rather entrapment of the accelerator pedal by the floor mat.[32]

NHTSA requested that this committee assess the continued relevance of the Silver Book in identifying and investigating incidents involving unintended acceleration. Such an assessment is offered in this report, but not for every aspect of the Silver Book's investigations. The committee presumes, for example, that NHTSA is not interested in an assess-

[29] TSC researchers could identify no mechanism that could cause the throttle to open because of brake application. They found that any engine power increases that may occur during a brake application should be controllable by the driver.

[30] As explained subsequently, NHTSA later attributed the loss in braking capacity to depletion of the vacuum assist and to brake overheating.

[31] Presentation by Jeffrey L. Quandt, Vehicle Control Division Chief, ODI, "Use of Data in ODI Investigations of Unintended Acceleration and Vehicle Electronics," October 22, 2010.

[32] Presentation by Jeffrey L. Quandt, Vehicle Control Division Chief, ODI, "Use of Data in ODI Investigations of Unintended Acceleration and Vehicle Electronics," October 22, 2010.

ment of the Silver Book's testing of the electronics systems in 1980s-era vehicles, which differ fundamentally from those in the fleet today.[33] It is self-evident that the results of these tests would have limited applicability for current technologies. Indeed, ODI did not indicate to the committee that its investigators consult the results of the Silver Book's electronics testing when they investigate behaviors in later model vehicles, nor did the committee find any recent cases in which ODI had cited the Silver Book for this purpose.[34] The content of the Silver Book that remains influential is its characterization of the circumstances indicative of pedal misapplication. Thus, this is the aspect of the Silver Book that was examined by the committee for continued relevance.

THE REVOLUTION IN AUTOMOTIVE ELECTRONICS

The 1980s-era vehicles discussed in the Silver Book were not devoid of electronics, but the state of technology marked the beginning of the electronics revolution that is now well under way. Until the mid-1970s, radios, cassette players, and ignition systems were the most sophisticated electronics in vehicles. During the late 1970s, solid-state circuits were introduced in systems such as electro-vacuum cruise controllers, and elementary microprocessors were introduced for ignition timing and control of the fuel–air mixture, the latter to meet demands for improved emissions performance (Cook et al. 2007).[35] As microprocessors and integrated circuits evolved to become smaller and more powerful, manufacturers started using computers to control other systems, from fuel injectors to antilock brakes and interior climate controls. By the 1980s, most new vehicles had computer-based engine control units, and some had a separate electronic control module for the cruise control (Bereisa 1983). Mechanical and hydraulic systems remained predominant, however.

[33] For example, cruise control systems no longer use a vacuum servo; fully electronic cruise control systems were phased into the fleet during the 1990s.

[34] The last significant reference the committee could find of NHTSA referencing the Silver Book's testing of vehicle electronics and mechanical components was in a denial of a petition for a defect investigation on April 28, 2000 (*Federal Register*, Vol. 65, No. 83, pp. 25026–25037). The petition in that case stemmed from a 1995 traffic incident involving a 1988 Lincoln Town Car having a cruise control system similar to those tested in the Silver Book.

[35] The first production engine control unit was a single-function controller used for electronic spark timing in the 1977 General Motors Oldsmobile Toronado (Bereisa 1983).

Initial growth in computerized vehicle electronics centered on replacing existing mechanical and hydraulic systems; adding new vehicle capabilities and features received less emphasis. Processors, sensors, and actuators were thus distributed throughout the vehicle, with each processor often dedicated to controlling a specific vehicle task that was once handled through mechanical or hydraulic means. Although constraints on computing capacity presented practical limits on the ability of the new controllers to interconnect, their isolation and dedication to specific tasks had the advantage of reducing the weight, cost, and complexity of wiring one module to another.

The modular approach to system architecture corresponded to the traditional model of vehicle production. According to this model, OEMs retained responsibility for overall vehicle design and assembly but depended on specialized suppliers for the development and engineering of the many individual vehicle components and subsystems. Suppliers were thus able to specialize in production and achieve scale economies by selling their electronics systems to multiple manufacturers, and the need for OEMs to invest in increasingly specialized and fast-changing areas such as electronics design and manufacturing was reduced.

As computing capacity expanded and became less expensive, OEMs outfitted their vehicles with dozens of computers capable of controlling more varied and complicated vehicle tasks. As these systems grew in number, their isolation from one another became impractical and costly because of the demand for dedicated wiring and lost opportunities to share sensors and information. The introduction of networks, which are discussed in more detail in the next chapter, solved this problem.[36] The networking of electronics systems not only has improved the capabilities and performance of many existing features—such as allowing for the integration of interior lights, locks, and power windows—but also has made more feasible the introduction of many new capabilities, including those promising to aid motorists in driving safely.[37]

The capabilities that electronics systems now provide in vehicles are extensive. They include comfort and convenience features, lower emissions, improved fuel economy, enhanced driving performance, and new

[36] In 1985, Bosch introduced the controller area network (CAN), a widely used peer-to-peer network that precludes the need for a master controller. As a node in the network, each connected device receives messages from and transmits messages to other devices on the CAN bus. Each device has a CAN controller chip that enables it to prioritize and use relevant messages.

[37] A more detailed review of the history of automotive software is given by Broy et al. (2007).

safety features; many more examples of these capabilities are given in the next chapter. Advancements in electronics are, in essence, transforming the automobile every few years and thus changing the driving experience itself. Electronics are enabling the introduction of many new vehicle capabilities, creating new driver interfaces, and affecting the division of responsibilities between the driver and vehicle for maintaining vehicle control.

Some of the interface changes are evident in features such as push-button ignition and dashboard display and control media free of the physical constraints that dictated their designs for decades. Other interface changes are less evident, such as a perceptible but small change in the feel of a pedal connected by wire rather than by a mechanical linkage.[38] Electronics are enabling new vehicle capabilities, such as blind spot surveillance and active collision avoidance, and some of the new capabilities will undoubtedly affect driving behavior in both positive and negative ways. Designing these new systems to minimize their potential to introduce safety hazards, while maximizing the joint performance of the driver and the technology, is becoming a major challenge for OEMs.

In addition to overcoming design challenges associated with human factors, OEMs strive to ensure that the new electronics systems perform their functions reliably. For example, when mechanical and hydraulic systems are replaced with electronics, OEMs want to make sure that the new technologies are at least as dependable as the earlier systems. In most cases, manufacturers expect each new generation of technologies to yield improved performance in all respects. This assurance can present a particular challenge for entirely new systems, especially as systems interconnect and interact with one another in new and potentially unanticipated ways. How automotive manufacturers are meeting these safety assurance challenges is discussed in this report.

STUDY GOALS AND REPORT ORGANIZATION

The full charge to the committee is contained in the statement of task in Box 1-1. The overarching study goals, given at the outset of the statement, are to (*a*) review past and ongoing NHTSA and industry analyses

[38] Such differences in pedal feel, at least for one type of vehicle (the Toyota Camry with and without ETCs), are documented by NHTSA (2011, 53).

BOX 1-1

Statement of Task

The objective of this study is to provide NHTSA with an independent review of past and ongoing industry and NHTSA analyses to identify possible causes of unintended acceleration (UA) and make recommendations on:

- NHTSA research, rulemaking, and defects investigation activities; and,
- Human, infrastructure, and financial resources required for NHTSA to assure the safety of electronic throttle controls and other electronic vehicle control functions.

In accordance, the study committee shall:

A. Conduct a broad review and assessment of electronic vehicle controls, systems, and UA across the industry and safeguards used by manufacturers and suppliers to ensure safety. The committee's review, assessment, and recommendations shall, at a minimum, encompass the following subject areas:
   (1). Vehicle control electronics design and reliability:
      - Software life-cycle process including specification, design, implementation, change control, and testing;
      - Computer hardware design and testing methods and integration with the software;
      - Vehicle systems engineering, including how combinations of electronics and mechanical design are used to jointly achieve safety objectives;

   (2). Electromagnetic compatibility and electromagnetic interference;
   (3). Environmental factors;
   (4). Existing relevant design and testing standards (SAE, ISO, IEEE, etc.);
   (5). Vehicle design and testing methods for safety;
   (6). Human system integration/human factors;
   (7). Potential forensic/problem-solving methods not already in use by industry and regulatory agencies;
   (8). Cybersecurity of automotive electronic control systems.

Box 1-1 (*continued*) Statement of Task

B. The study committee shall review the 1989 "Silver Book" to analyze its continued relevance with respect to technologies, possible defects, and failure modes associated with UA. The committee shall report on the current understanding of possible causes of UA and how the increasing prevalence of electronic throttle controls, other electronic vehicle control systems (e.g. brakes), event data recorders, and the like, which have emerged since the 1980s, may require supplementing the Silver Book. The committee shall provide guidance on factors NHTSA should consider in light of these developments.
C. The study committee shall review NHTSA policies, procedures, and practices as they are applied in Office of Defects Investigation (ODI) UA investigations of UA and make recommendations for improvement with respect to the possible involvement of electronic control systems in UA. In doing so, the committee shall:
   (1). Review the general history of and process used in NHTSA's defect investigations related to UA;
   (2). Provide recommendations and suggest priorities for the manner in which future possible defects involving electronic control systems should be investigated; and
   (3). Make recommendations and suggest priorities for future research that may support investigations of such systems.
D. Review possible sources of UA other than electronic vehicle controls, such as human error, mechanical failure, and mechanical interference with accelerator mechanisms.
E. Examine best practices for assuring safety in other sectors, such as avionics, and consider any lessons that might apply to vehicle safety design and assurance.
F. Discuss the limitations of testing in establishing the causes of rare events.
G. Describe improvements in design, development process, testing, and manufacturing, including countermeasures and fail-safe strategies that could be used to increase confidence in electronic throttle controls and other electronic vehicle control systems.

of the possible causes of unintended acceleration and (*b*) make recommendations on NHTSA's research, rulemaking, and defect investigation activities, including the capabilities required for the agency to ensure the safe performance of ETCs and other electronic vehicle controls.

With respect to the first goal, the focus of the study's review of unintended acceleration is on NHTSA's initiatives to monitor for, analyze, and investigate this problem. The committee could think of no practical way to examine the means by which each of the large number of OEMs handles consumer reports of unintended acceleration specifically, although OEM safety assurance and field monitoring capabilities in general are discussed in Chapter 3. As discussed above, NHTSA has undertaken and commissioned several major investigations of unintended acceleration over the past 40 years, including the Audi and Silver Book reports by TSC during the 1980s. More recently, NHTSA enlisted the help of NASA (NHTSA 2011). All of these investigations were presumably undertaken to inform NHTSA's decisions on whether to pursue recalls or take other regulatory and research steps. The committee's review of these agency initiatives, therefore, centers on their relevance to informing such agency decisions.

With respect to the second goal in the statement of task, the committee used the insights gained from examining the concerns over unintended acceleration to inform its advice to NHTSA on steps the agency should take to prepare for and meet the safety challenges arising from the electronics-intensive automobile. The statement of task calls for recommendations on NHTSA's research priorities and required human, infrastructure, and financial resources to oversee the safety of automotive electronics. NHTSA needs to rank its policy priorities on the basis of competing safety demands. The committee does not know all of NHTSA's safety priorities and their associated resource requirements. The report therefore offers suggestions on relevant research topics and recommends a means by which NHTSA can make more strategic choices with regard to allocating its resources to meet the safety oversight challenges arising from automotive electronics.

The committee's review and findings are contained in the remainder of this report. Chapter 2 provides more background on the electronics systems in today's vehicles and those of the not-too-distant future. Chapter 3 describes the safety assurances processes used by automotive manufacturers during the design and development of electronics systems and efforts at the industry level to standardize aspects of these pro-

cesses. Chapter 4 describes NHTSA's oversight of vehicle electronics safety through its regulatory, research, and defect investigation programs and compares this oversight with the federal role in overseeing the safety of the design and manufacture of aircraft and medical devices. Chapter 5 reviews NHTSA's initiatives on unintended acceleration, including the Silver Book, more recent ODI investigations, and the NASA study. In Chapter 6, key findings from the chapters are synthesized and assessed to make recommendations to NHTSA.

REFERENCES

Abbreviations

NHTSA National Highway Traffic Safety Administration
NTSB National Transportation Safety Board

Bereisa, J. 1983. Applications of Microcomputers in Automotive Electronics. *Institute of Electrical and Electronics Engineers Transactions on Industrial Electronics,* Vol. IE-30, No. 2, May.

Broy, M., I. H. Kruger, A. Pretschner, and C. Salzmann. 2007. Engineering Automotive Software. *Proceedings of the Institute of Electrical and Electronics Engineers,* Vol. 95, No. 2, Feb., pp. 356–373.

Cook, J. A., I. V. Kolmanovsky, D. McNamara, E. C. Nelson, and K. V. Prasad. 2007. Control, Computing and Communications: Technologies for the Twenty-First Century Model T. *Proceedings of the Institute of Electrical and Electronics Engineers,* Vol. 95, No. 2, Feb., pp. 334–355.

Japanese Ministry of Transport. 1989. *An Investigation on Sudden Starting and/or Acceleration of Vehicles with Automatic Transmissions.*

Marriner, P., and J. Granery. 1988. *Investigation of Sudden Acceleration Incidents.* ASF3282-8-18. Transport Canada.

NHTSA. 2011. *Technical Assessment of Toyota Electronic Throttle Control (ETC) Systems.* http://www.nhtsa.gov/staticfiles/nvs/pdf/NHTSA-UA_report.pdf.

NTSB. 2009. *Highway Special Investigation Report: Pedal Misapplication in Heavy Vehicles.* http://www.ntsb.gov/doclib/safetystudies/SIR0902.pdf.

Pollard, J., and E. D. Sussman. 1989. *An Examination of Sudden Acceleration.* Report DOT-HS-807-367. Transportation Systems Center, U.S. Department of Transportation.

Reinhart, W. 1994. The Effect of Countermeasures to Reduce the Incidence of Unintended Acceleration Accidents. Paper 94 S5 O 07. *Proc., 14th International Technical Conference on Enhanced Safety of Vehicles,* Washington, D.C., Vol. 1, pp. 821–845.

Rogers, S. B., and W. W. Wierwille. 1988. The Occurrence of Accelerator and Brake Pedal Actuation Errors During Simulated Driving. *Human Factors,* Vol. 31, No. 1, pp. 71–81.

Schmidt, R. A. 1989. Unintended Acceleration: A Review of Human Factors Contributions. *Human Factors,* Vol. 31, No. 3, pp. 345–364.

Vernoy, M. W., and J. Tomerlin. 1989. Pedal Error and Misperceived Centerline in Eight Different Automobiles. *Human Factors,* Vol. 31, No. 4, pp. 369–375.

Walter, R., G. Carr, H. Weinstock, E. D. Sussman, and J. Pollard. 1988. *Study of Mechanical and Driver-Related Systems of the Audi 5000 Capable of Producing Uncontrolled Sudden Acceleration Incidents.* Report DOT-TSC-NHTSA-88-4. Transportation Systems Center, U.S. Department of Transportation.

2

The Electronics-Intensive Automobile

A major upgrade in automotive performance over the past two decades that has not had its basis in electronics, particularly in advances in computer and software technologies, would be difficult to identify. It would be surprising if this were not the case, given the proliferation of software-intensive electronics in nearly all high-value consumer products. As discussed in Chapter 1, today's electronics-intensive vehicle is fundamentally different from the mostly mechanical vehicle of the 1970s and 1980s. The electronics in the contemporary automobile contain hundreds of sensors, drive circuits, and actuators that are connected to scores of microprocessors running on increasingly complex software and exchanging information through one or more communications networks (Krüger et al. 2009). It has been estimated that electronics account for about 35 percent of the cost of designing and producing some vehicles (Charette 2009; Simonot-Lion and Trinquet 2009). Even today's entry-level models contain far more sophisticated and capable electronics than premium-class models did less than a decade ago (Charette 2009). And given the history of technology dispersion in the automotive sector, many of the advanced electronics systems found in premium-class vehicles today can be expected to migrate through the fleet quickly.

This chapter describes some of the major vehicle electronics systems that are now in vehicles, that will soon be deployed, and that are being developed and explored but whose mass introduction remains on the more distant horizon. Consideration is then given to the nature of the

safety assurance challenges that automobile manufacturers face as they design, develop, and integrate these systems for use by vehicles and drivers. The chapter concludes with relevant findings from the discussion that inform the committee's recommendations to the National Highway Traffic Safety Administration (NHTSA) offered later in this report.

USE OF ELECTRONICS IN VEHICLES TODAY

Figure 2-1 shows the multitude of electronics systems that are now or soon will be available in vehicles. It shows that there are few, if any, vehicle functions that are not mediated by computers. A majority of the functions shown would not be feasible or cost-effective if not for the

FIGURE 2-1 Types of electronics systems in modern automobiles.
(*Source:* Clemson University Vehicular Electronics Laboratory.)

advancements that have taken place in microprocessors, sensors, other hardware, and software during the past 30 years.

Some of these electronics systems have improved on the capabilities once provided by mechanical, electromechanical, and hydraulic systems. Increasingly, however, electronics are enabling new capabilities, as evident in the many convenience, comfort, entertainment, and performance applications indicated in Figure 2-1. Few systems provide these capabilities in stand-alone fashion; instead, they rely on interconnections and communications with one another. For some time, this interconnectivity has permitted enhancements to certain safety and comfort features such as seat belt pretensioning before a crash and adjustment of the radio volume in relation to travel speed. However, the level of system interconnectivity is growing rapidly to provide a richer array of capabilities. For example, some adaptive cruise control (ACC) systems are sampling data from the Global Positioning System (GPS) to adjust headway limits depending on the vehicle's proximity to a highway exit ramp.

These systems provide one or more capabilities for the following, among others:

- Entertainment, information, and navigation assistance—radios, satellite radio, CD and DVD players able to interpret a wide array of data formats, USB and other multimedia ports, Wi-Fi and Internet connectivity, GPS navigation, travel advisories;
- Convenience—seat and mirror position memory, remote and keyless entry and ignition, automatic lights and wipers, embedded and Bluetooth-connected mobile phones;
- Comfort and ease of use—suspension adjustment, brake and steering assist, heated and cooled seats, cabin temperature control, interior noise and vibration suppression, parking assist, hill hold, mirror and light dimming;
- Emissions, energy, and operating performance
  - Concerted control of fuel flow, air intake, throttle position, and valve timing; cylinder deactivation; transmission control; traction and cornering control; tire pressure monitoring; regenerative braking;
  - Power train and battery charging control for hybrid and electric-drive vehicles;

- Safety and security—crash-imminent seat belt tensioning and air bag deployment, antilock braking, ACC, crash warning and brake control, blind spot detection and warning, lane departure warning, yaw and stability control, backup sensors and cameras, tire pressure monitoring, 9-1-1 crash notification; and
- Reliability and maintainability—onboard diagnostics systems, remote diagnostics, vibration control, battery management.

The foundation for all of this system interconnectivity derives from the communications networks and protocols (messaging rules) that allow for the exchange of information, the sensors that gather the information, and the software programs that make use of it. The critical roles of communications networks, sensors, and software are discussed next before an overview of some of the major electronics systems that use them is provided.

Communications Networks and Protocols

All electronics systems that control vehicle functions consist of a control module containing one or more computer processors. The control module receives input for its computations from a network of sensors (e.g., for engine speed, temperature, and pressure) and sends commands to various actuators that execute the commands, such as turning on the cooling fan or changing gear. In addition, these control modules need to connect to other control modules—for example, to shift gears the transmission control module must have received information on the engine speed.

In the early days of automotive electronics, the handful of controller systems in a vehicle could be linked through point-to-point wiring (Navet and Simonot-Lion 2009, 4-2). However, as the number of systems grew, the complexity and cost of wiring systems in this way increased substantially. The approach required not only costly and bulky wire harnesses but also repeated changes in wire designs depending on the specific modules included in a given vehicle. For example, a vehicle equipped with antilock brakes would require wiring different from that of a vehicle not equipped with this feature. The industry's solution was to install a network in the vehicle and "multiplex" (combine data streams into a single transmission) their communications among system elements. The multiplexed networks are referred to as communication buses. A module plugged into the bus would thus be able to sample data from and communicate with all other networked modules. In this way, each module

would serve as a node in the network, controlling the specific components related to its function while using a standard protocol to communicate with other modules.

To work in the automotive environment, these communications networks had to be designed to achieve low production and maintenance costs, immunity from electromagnetic interference, reliability in harsh operating environments, and the flexibility to vary options without alternative wiring architectures. Although automotive manufacturers did not emphasize data throughput capacity when these networks were introduced 25 years ago, the subsequent demand for onboard computing has been driving changes to networks to support higher bandwidth and higher-speed communications among modules.

Today, multiple networks and communications protocols are used in vehicles for data exchange depending on factors such as required transmission speed, reliability, and timing constraints. The protocols are accompanied by a variety of physical media to provide the required connections among system components on the network, including single wires, twisted wire pairs, fiber-optic cables, and communication over the vehicle's power lines. Many automotive manufacturers are seeking a standard protocol, but none has emerged. Not every protocol can be described here, but a number of them appear in the following list of example networking buses and communications protocol standards (Navet and Simonot-Lion 2009, 4-2).

- CAN (controller area network): an inexpensive low-speed serial bus for interconnecting automotive components;
- VAN (vehicle area network): similar to CAN but not widely used;
- FlexRay: a general-purpose, high-speed protocol to support time-triggered architecture;
- LIN (local interconnect network): a low-cost in-vehicle subnetwork;
- SAE-J1939 and ISO 11783: an adaptation of CAN for agricultural and commercial vehicles;
- MOST (Media-Oriented Systems Transport): a high-speed multimedia interface that supports user applications such as GPS, radios, and video players;
- D2B (domestic digital bus): a high-speed multimedia interface;

- Keyword Protocol 2000 (KWP2000): a protocol for automotive diagnostic devices (runs either on a serial line or over CAN);
- DC-BUS [1]: automotive power line communication multiplexed network;
- IDB-1394;
- SMARTwireX;
- SAE-J1850, SAE-J1708, and SAE-J1587; and
- ISO-9141-I/-II.

Because a typical vehicle will have a variety of networking speed and capacity needs, it will have multiple networks and will often host different control units and use different protocols and physical media. The networks are often intended to be isolated from one another for various reasons, including bandwidth and integration concerns (e.g., entertainment network isolated from the network containing the engine controller).[1] In cases where information must be shared among networks, there will typically be a gateway module to control, and in certain cases isolate, the communications. For example, the CAN bus typically used for electronic engine controls may have a connection to other networks on the vehicle to share information, but control signals from these other networks are precluded from access to the CAN by a gateway control module. As noted below, the effectiveness of these access controls is coming into question as electronic systems are connecting more with one another and with external devices that could provide access points for cyberattacks.

Sensors

Sensors are essential to the function of nearly all vehicle electronics systems, many of which depend on multiple sensing technologies. A variety of sensors are deployed to measure positions and properties such as temperature, direction and angle, oil pressure, vacuum, torque, seat position, and engine speed and then to convert the measurements into electrical signals (digital or analog) that can be used by computers in one or more embedded electronics systems. New technologies are providing

[1] As discussed in Box 2-2, it is not evident that this separation has been adequately designed for cybersecurity concerns.

even greater sensing capability for applications such as distance ranging, motion detection, and vehicle position identification.

The amount and types of sensors in vehicles have grown dramatically over the past 20 years as a consequence of advances in technology and in response to new demands for safety, emissions control, fuel economy, and customer convenience. Although there are too many sensor types and technologies to describe here, the following examples illustrate their range of uses. To support operation of the catalytic converter, oxygen sensors with zirconia tips probe exhaust gases. The zirconia reacts with the gases and develops a signal voltage, which is transmitted to a controller. Simple and low-cost sensors used in many vehicle applications are the potentiometer and the Hall effect sensor. The former can be used to determine the angle or direction of a component, such as the position of the accelerator pedal or throttle plate in an electronic throttle control system (ETC). It is designed with three terminals: a power input, ground, and variable voltage output. Acting as a transducer, the potentiometer's voltage output varies with the position of a movable contact (such as the pedal or throttle shaft) across or around a fixed resistor. The output voltage is higher or lower depending on whether the contact is near the power supply or ground. The Hall effect sensor, in comparison, detects its position relative to that of a magnet and thus has no moving parts that can degrade over time, as can those in potentiometers. From a technical standpoint, the decision to use one sensor technology over another can depend on the needed accuracy, durability, task (e.g., linear, rotary, range, temperature measuring), and integration ability (e.g., space constraints). In practice, the cost of the sensor is also important.

Sensor technology is becoming more sophisticated and varied, especially to support the functionality of many new convenience, comfort, and safety-related electronic systems. Advanced sensor technologies that are being used more often include the following:

- Ultrasound (e.g., backup warning, parking assist);
- Inertial sensors, accelerometers, yaw-rate sensors (e.g., stability control, air bag deployment, suspension control, noise and vibration suppression);
- Radar and light detection and ranging (lidar) (ACC);
- Cameras (e.g., lane keeping, ACC); and
- GPS (e.g., advanced ACC).

In discussing the array of electronics systems being deployed in modern vehicles, the current and emerging roles of these new sensing technologies are noted. Continued advances in sensing reliability and capability, of course, will be central in enabling the development and deployment of many next-generation electronics-based systems.

Software

As the discussion above indicates, automobiles today are literally "computers on wheels." A modern luxury car contains tens of millions of lines of software code executed in and across the scores of networked electronic control units. By some estimates, more than 80 percent of automotive innovations derive from software (Charette 2009; Krüger et al. 2009). Automotive manufacturers now depend so much on software rather than on hardware for functionality because the former is easier to evolve and extend, and it is often the only feasible way to achieve a desired function. For years automakers have been leveraging the power of networked controllers and advances in software development to introduce active safety features, many of which are described below. Between 2,000 and 3,000 individual vehicle functions are estimated to be performed with the aid of software in a premium-class car (Charette 2009). This trend is almost certain to continue as the capabilities and performance of microprocessors, networks, and software grow.

Software is contained in all controller modules and is used to direct and integrate their actions. The software that monitors and controls vehicle systems and their use is part of what is commonly known as an embedded real-time system (ERTS). Since its earliest use for electronic ignition timing in the 1977 Oldsmobile Toronado, ERTS software (and the processors that run it) has grown in size, state space, and complexity, in large part because of added functions and the demands of coordinating actions among systems. For example, for the Lexus emergency steering assist system to function, it must have close interaction with the vehicle's variable gear ratio steering and adaptive variable suspension systems, among others.[2] The software needed to support this real-time coordination among the safety-related subsystems is substantially more challenging to design, develop, and validate than are relatively self-contained features such as a door-lock controller. Software development and safety assurance processes are discussed further in Chapter 3.

[2] http://www.worldcarfans.com/10608296343/lexus-ls460-achieves-world-first-in-preventative-safety.

Control of Engine, Transmission, and Throttle

Before there was a need for in-vehicle communications networks, computerized engine control units were introduced in vehicles in the late 1970s to meet federal emissions regulations. These early units governed the air–fuel mixture to enable more efficient fuel combustion to minimize emissions. An exhaust gas oxygen sensor provided a signal to the engine control unit so that it could regulate fuel levels to achieve an even more precise air–fuel mixture. As emissions standards were tightened and electronic fuel injectors were introduced, additional functions were added to the engine controller for such purposes as more precise and consistent spark timing and regulation of the flow of fuel during a cold start.

Coincidental with these changes, automobile manufacturers began to introduce other computer controllers for transmission and throttle functions. These controllers were also designed to exchange information with and be regulated jointly by the engine controller. Automatic transmissions had previously relied on hydraulics to operate valves that engaged and disengaged clutches in planetary gear sets. With electronic controls, the shift point could be better controlled by using inputs from a network of sensors in the engine, transmission, and wheels.

ETCs were introduced in the late 1990s, eliminating the physical linkage between the accelerator pedal and throttle by a cable and other connectors. A typical ETC consists of a control unit, a pair of throttle valve position sensors, a pair of pedal position sensors, and an electric motor that actuates the throttle. Depressing the accelerator pedal causes the pedal sensors to send a signal to the controller, which in turn sends a command to the throttle motor to open or close the throttle. Sensors on the throttle confirm its position and correspondence to the signals being sent by the sensors in the accelerator pedal. ETCs allow for more precise regulation of fuel consumption and emissions by the engine control unit and provide other benefits, such as a reduction in the cost of electronic cruise and stability control systems and an increase in their feasibility.

Figure 2-2 shows some of the sensors and actuators in the vehicle that provide input to and receive commands from the engine control unit. In having such a wide array of inputs (e.g., coolant temperature, exhaust gas composition, mass air flow) and the ability to orchestrate so many outputs (e.g., spark timing, air and fuel flow, throttle opening), the engine control unit has been a major source of fuel economy and emissions performance improvements in vehicles over the past two decades.

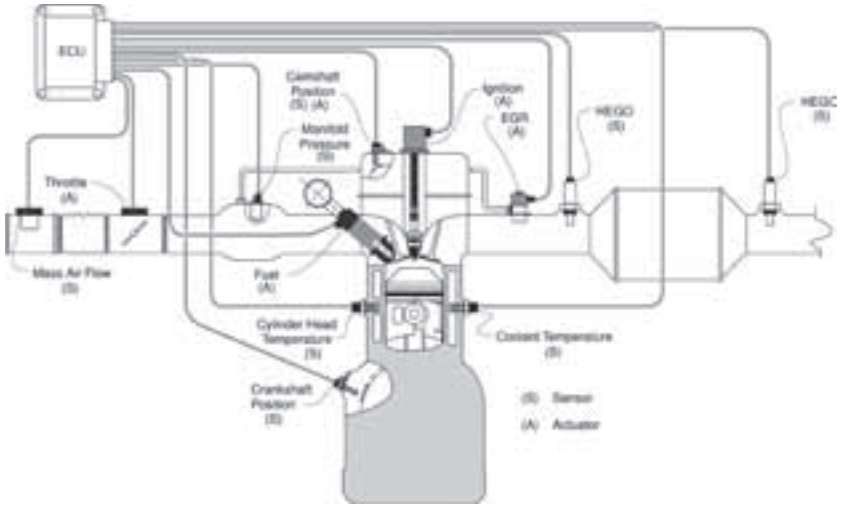


FIGURE 2-2 Engine control sensor and actuator network (ECU = engine control unit; EGR = exhaust gas recirculation; HEGO = heated exhaust gas oxygen sensor).
(*Source:* Cook et al. 2007.)

Concerns over transportation's dependence on imported oil and emissions of greenhouse gases have generated increased interest in electric-drive vehicles. These vehicles all have batteries and electric motors that provide some or all of the vehicle's propulsion. The main types of electric-drive vehicles are conventional hybrid vehicles (HEVs), plug-in hybrid electric vehicles (PHEVs), and pure electric vehicles (EVs). While these vehicles have many of the same electronic capabilities as conventional vehicles, they have different control needs with implications for their electronics, as discussed in Box 2-1.

Brake Power Assistance and Lockup Control

Brakes continue to rely fundamentally on hydraulic lines that transmit the pressure at the brake pedal to actuators at the wheels to force the brake pads into contact with a drum or disc on the wheel. The generated friction slows and eventually stops the vehicle. For greater safety assurance, the hydraulics are split (as required by regulation) so the left front and right rear wheels use half the system and the right front and left rear

BOX 2-1

Electronic Controls in Electric-Drive Vehicles

The most common electric-drive vehicles in production are HEVs, which have been available for more than a decade. These vehicles have either one or two electric machines and a gasoline engine in parallel to drive the wheels. When the vehicle decelerates, the motor acts as a generator to recharge the battery with energy that would otherwise be lost in braking (regenerative braking). HEVs, therefore, require complicated electronic controls to optimize performance of the two power trains and ensure proper charging of the battery. Manufacturers are now introducing PHEVs with batteries charged from the electric grid. PHEVs come in two forms. One is similar to a conventional hybrid but has a bigger battery that can be charged from a power line to allow electricity-only driving for about a dozen miles. The forthcoming plug-in Toyota Prius is an example of this type of PHEV. The General Motors (GM) Volt is a series PHEV in which the wheels are powered by electricity only. The battery is bigger than that in the parallel PHEV and may be capable of traveling 40 miles on a charge. Pure EVs such as the Nissan Leaf or the Tesla roadster have a larger battery that can power driving for 80 miles or more. The battery is charged only from regenerative braking or a power outlet. Pure EVs are mechanically and electronically simpler than the hybrids, since they have an electric motor but no engine and no need to balance two power trains.

Power Train Control in Electric Vehicles

All electric-drive vehicles require sophisticated power train control to manage power flow from the battery to the motor and from the motor/generator to the battery during regenerative braking and, in the case of parallel hybrids (either HEV or PHEV), to coordinate the sharing of loads between the engine and the electric motor. Parallel hybrid controls must optimize operations to minimize fuel consumption while meeting emissions requirements. Parallel hybrid vehicles may start repeatedly without fully

(continued on next page)

Box 2-1 (*continued*) Electronic Controls in Electric-Drive Vehicles

warming up. Because engines produce higher emissions when they are started cold, meeting emissions requirements is a concern. In addition, the battery charge status needs to be monitored so that it stays within limits to maximize its life. In series hybrids, control is less complex because loads are not shared between motor and engine. The battery state of charge must be monitored so that when it reaches a lower limit the engine is started and is turned off when the battery is sufficiently charged. In comparison, EV power train control is simple since there is no concern over emissions and the only processes that need to be controlled are those involving the transmission from the battery to the motor and from regenerative braking back to the battery. Because switching large current either in the charger or in the power electronics for propulsion is done quickly to minimize losses, the potential for transients to be created in wiring harnesses that could cause electromagnetic interference and malfunctioning microprocessors is an area of design concern.

Controlling Battery Charging

EV and PHEV battery charging is handled through a sophisticated controlled rectifier that takes power from the plug, at 120 or 220 volts alternating current, which is converted to direct current for the battery. The charging voltage needs to be carefully monitored since overcharging can reduce battery life and lead to fire risks. EVs and PHEVs may use in-vehicle systems such as GM's OnStar and Ford's Sync to communicate with the charger, allowing the monitoring of the battery state of charge through an Internet-enabled phone. Similarly, the charger may communicate with a smart meter through the Internet, allowing charging to occur when electricity rates are lowest.

Braking and Stability Control in Electric Vehicles

Regenerative braking is an important contributor to the high fuel economy of hybrids. However, this type of braking only works

Box 2-1 (*continued*) Electronic Controls in Electric-Drive Vehicles

with the driving wheels, whereas conventional hydraulic brakes work on all four wheels and are more powerful. For safety, hybrids and EVs also need hydraulic brakes that act in concert with regenerative braking so that the driver does not feel a difference from conventional cars. In an electric-drive vehicle with wheel motors, stability control can involve decreasing power to the drive wheels on one side of the car and possibly selective braking of individual wheels. With parallel hybrid vehicles, the addition of electric motor power means that the systems can be controlled precisely.

wheels use the other half.[3] If one system fails, the other will provide degraded but balanced braking.

The majority of today's vehicles have power-assisted brakes. Most of these systems use an actuator (vacuum booster) that maintains vacuum derived from the engine during part load operation. When the driver depresses the brake pedal, the booster provides additional hydraulic pressure to the brakes, so the pedal force required by the driver is reduced. The vacuum booster has sufficient capacity for successive brake applications depending on how forcefully the pedal is applied. In general, the assist capacity will be reduced if the driver applies and releases the brake repeatedly so as to deplete the vacuum in the booster. Under these circumstances, the pedal force required for an emergency stop will increase substantially.

Most new vehicles today also have an antilock brake system (ABS) that provides greatly improved braking on slippery surfaces. When the coefficient of friction between the tire and the road is low, firm application of the brake tends to lock the wheels, causing a loss of steering control. The ABS was introduced widely in the 1980s. A typical system uses an electronic control unit and speed sensors in the wheels. The control unit constantly monitors the speed of each wheel. If it detects a wheel rotating more slowly than the others, which indicates an impending wheel lock, the unit will reduce the brake pressure at the affected wheel.

[3] Front and rear wheel splits are legal in addition to the more common diagonal splits.

In the event of an ABS failure, the system reverts to conventional braking, in which the pressure applied to the brake pedal by the driver is not modulated by the computer and skidding can occur on slippery surfaces.

Traction and Stability Control

In conditions in which there is a low coefficient of friction, if one of the drive wheels spins, the opposite wheel will produce no force because of the action of the differential, which can cause the vehicle to become stuck. Electronic traction control systems, which were first introduced in the early 1990s, use the same wheel speed sensors as the ABS to detect wheel spin. These systems reduce the throttle opening and perhaps apply the brake to the spinning wheel to help restore traction. Electronic stability control systems (ESCs) evolved from traction control systems. The main difference is that they are designed to improve vehicle handling. For example, if the driver attempts to make a sharp turn at high speed, the tires may not sustain enough lateral force for the vehicle to follow the driver's intended path accurately, depending on other vehicle dynamics factors such as braking, which may cause the vehicle to overrotate (spin) or underrotate (plow). To predict this potential, the ESC uses the steering wheel angular position, the wheel speed sensors in the ABS, and the yaw-rate sensor. The system will reduce engine power by decreasing the throttle opening. If this response is insufficient, the system will apply the brakes to the appropriate wheels. These two actions will help change the yaw rate of the vehicle to match the driver's intent more closely. When roll stability control is provided, it is integrated into the ESC. This feature helps to reduce tilting propensity by activating the brakes or special bars for stability. As in the case of the ABS, loss of these ESC capabilities puts responsibility back on the driver to avoid and react appropriately to events that risk destabilizing the vehicle.

Suspension Control

Electronically controlled suspension systems adapt the suspension of the car to the driver's preferences for a stiffer or softer ride by taking into account vehicle speed, road surface, and cornering and acceleration requirements. Accelerometers sense and measure the motion and pitch of the car. In cars equipped with an air suspension system, the volume of the air in the cushions in all four corners of the car is regulated by a compressor, which is controlled by a processor interpreting signals from the

accelerometers. In cars with traditional shock absorbers, several other technologies exist to change damping rates that affect the ride quality.[4]

Power Steering Assist

As vehicles became heavier, hydraulic power steering was introduced in the 1950s. These systems used a pump driven by the engine to provide assistance to the driver through a hydraulic motor. The driver input is applied to a torsion bar that opens a valve in proportion to the difference between the steering wheel position and the angular position of the wheels. Electric power steering was introduced in the 1990s, primarily to reduce the amount of energy that had been used by the hydraulic pump and thus to improve vehicle fuel economy.[5] The torsion bar modifies compliance to facilitate stability, but an electrical sensor determines the angular displacement. The power assist is provided by an electric motor controlled by a microprocessor. Failures in electric power steering could lead to unintended steering or resistance to the driver's attempt to steer; however, by design the system detects such conditions and deactivates the assist feature. At highway speeds, deactivation is manageable because only small displacements are needed. Deactivation at slow speeds and during parking makes steering more difficult.

Adaptive Cruise Control

Conventional cruise control systems, which were introduced in the late 1950s, control the vehicle's speed to a point set by the driver. Early systems used a vacuum actuator to pull and release the throttle cable. The system was turned on and off through toggling a switch and was disengaged by tapping the brake pedal. As an additional safety feature, the system disengaged at some minimum low speed and, in cars with manual transmission, when the driver changed gears. After ETCs were introduced, cruise control systems could use the throttle control motor rather than pull a cable to control the throttle position.

ACC systems have a forward-looking sensor, usually radar-based, to determine the vehicle's distance from other vehicles and obstacles ahead. Depending on the operating speed, the system calculates a safe following

[4] These technologies include continuously variable real-time damping shocks and a magnetically controlled suspension system that has no valves or other moving parts.

[5] Electric power steering is even more efficient than conventional power steering because the steering motor only needs to provide assistance when the steering wheel is turned, whereas the hydraulic pump must run constantly.

distance and maintains it by adjusting the vehicle's speed. The adjustment is made not only by using the throttle but also by applying the brakes if necessary. Some ACC systems receive input from the vehicle's GPS navigation system and a forward-pointing camera. By combining these features, the ACC can determine whether the lead car is slowing down with its turn signal on to move over to an exit ramp. Whereas a conventional ACC would sense the narrowing headway and slow the vehicle down, this advanced system will make a smaller adjustment to the following speed.

Lane Departure Warning and Keeping

Lane departure warning systems have been available for about a decade. In these systems, a forward-looking camera monitors pavement lane markings. A warning sound is issued when the vehicle drifts out of the lane. More recent systems for active lane-keeping use the ESC and electric power steering to assist the driver in maintaining lane position by applying light brake pressure or countersteering forces.

Parallel Parking Assistance

Some automobile manufacturers have recently introduced systems that automatically control the power train and steering so that the vehicle can parallel park itself. Cameras and sensors judge the size of the parking spot and the distance between the vehicle and adjacent obstacles (other cars, the curb, etc.) to execute the parking maneuver. The system is designed so that if the driver touches the steering wheel or applies the brake firmly, the system will disengage. In addition, if the vehicle exceeds a set speed, the system will turn off.

Navigation and Communications

The navigation and communications systems in vehicles today have multiple capabilities. They are interconnected with one another, with many of the systems described above (e.g., ACC linked to GPS), and with entertainment systems. User peripherals such as short-range wireless devices, mobile phones, and USB devices are routinely attached to the same internal networks. The telecommunications interfaces can also be used for remote vehicle surveillance, reprogramming of software, system diagnostics, and control of certain vehicle systems through connections with external devices. Some of the capabilities made possible through telematics can enhance safety, such as automatic crash response

through notification of air bag deployment and the vehicle's coordinates (via cell tower and GPS).

Occupant Protection Systems

Much of the discussion of safety-related electronics systems in this chapter and elsewhere in the report concerns technologies used for crash avoidance and vehicle controls such as the ETC. Electronics, however, also play a central role in occupant protection systems such as air bags and seat belts. Accelerometers and other sensors positioned in impact zones can detect deceleration or multidirectional acceleration and determine which vehicle seating positions are occupied. On the basis of the sensor information, the control unit can calculate the angle of impact and the force of the crash to determine which air bags to deploy and to what degree and activate additional measures such as seat belt pretensioning. Every time a vehicle is started, the air bag control module self-checks the sensors and the state of the system.

Self-Diagnostics

All vehicles today contain computers that monitor the performance of certain major vehicle components, especially in the engine, and give diagnostic information to the vehicle owner or repair technician. Early self-diagnostic systems, introduced in the 1980s, would simply trigger a dashboard malfunction indicator light if a fault was found but would not indicate the nature of the problem. The self-checking takes place during engine start-up and continually as the vehicle operates, depending on the system. Diagnostics systems in vehicles today provide much more varied functions, including the triggering of corrective actions if necessary.

It has been estimated that about one-third of the embedded software in a modern vehicle is used to run diagnostics (Charette 2009).[6] This is because modern onboard diagnostics systems (OBDs) monitor a wide array of vehicle systems and apply myriad rules to decide whether a fault has occurred. The faults are logged as diagnostic trouble codes (DTCs). The DTCs allow technicians to identify and fix malfunctions rapidly. The setting of a DTC may also trigger actions, such as shutting down a system or alerting the driver through a dashboard light. The use of OBDs for system monitoring and safety assurance functions is discussed in more detail in Chapter 3.

[6] For some electronics systems such as electric power steering, diagnostics can account for the majority of code.

While the U.S. Environmental Protection Agency specifies the type of diagnostic connectors and protocols required in vehicles for emissions control systems, OBDs in vehicles today differ by manufacturer, including the functions they monitor. These differences will undoubtedly grow. Opportunities for innovative diagnostics systems to become a selling point to consumers are already starting to be exploited. For example, onboard communications systems can already transmit vehicle "health" and operating parameters to original equipment manufacturers for remote analysis and diagnostics. These exchanges may be used to identify vehicle systems that require firmware updating and to perform the upgrades remotely or notify the driver of the need to have the vehicle serviced (Charette 2009).

Event Data Recorders

Electronics sensors and connections have enabled automotive manufacturers to install event data recorders (EDRs) on their vehicles. The recorders are usually part of the air bag control module, and they are triggered to save data by a crash event in which an air bag is deployed or the sensors in the air bag system detect rapid deceleration or multidirectional acceleration. The recorders typically capture a few seconds of vehicle data before a crash, including vehicle speed, accelerator pedal position, throttle position, and brake switch position. The recorded information can be retrieved by investigators through the OBD port to help determine the causes of the crash.

Because EDRs are not currently mandated, their usage varies by manufacturer. According to NHTSA, a large majority of vehicles sold in the United States have EDRs, but there is inconsistency among the manufacturers in the array of data items recorded and the means available for accessing the stored data. NHTSA regulations mandate that most light-duty vehicles made on or after September 1, 2011 (Model Years 2012 or later) that are equipped with EDRs record a common set of variables, including precrash speed, brake light status, velocity change, engine revolutions per minute, seat belt use, and the timing of air bag deployment. NHTSA has indicated its intention to initiate a rulemaking to require EDRs on all cars and to expand the number of data items recorded. In addition, a variety of efforts are being pursued through standard-setting organizations to bring greater uniformity to the data collected by EDRs and the technical means for accessing the data. EDRs are discussed further later in this report.

NEXT-GENERATION SYSTEMS

Consumer and manufacturer experience with some of the newer systems described above will affect the rate of introduction and penetration of even more complex electronics systems. While the following systems are in research and developmental stages, many are candidates for deployment during the next 25 years.

Steer-by-Wire and Brake-by-Wire

In steer-by-wire systems, the mechanical link between the steering wheel and the vehicle wheels is removed, and the driver's intent is translated into signals to a motor or motors that turn the wheels. Among possible advantages, steer-by-wire would reduce vehicle weight, eliminate the safety hazard presented by the protruding steering column, offer greater flexibility in designing the car interior, and enable customizable driver interfaces since the steering mechanism could be designed and installed as a modular unit. Brake-by-wire would substitute sensors, computers, and actuators for pumps, hoses, fluids, and master cylinders. These systems would eliminate the direct mechanical connection between the pedal and the brakes by activating motors on each wheel.

Both of these advanced concepts have been demonstrated, but making a convincing case with regard to their operating reliability will be fundamental to their deployment because the only safe state for steering and braking is "operational." Addressing these concerns through the use of redundant systems (as found in aircraft fly-by-wire) may be possible but could negate the purpose of adding the drive-by-wire systems. The challenge will be in finding ways to ensure safety without greatly increasing each system's total cost.

Vehicle-to-Vehicle and Vehicle-to-Infrastructure Communications

Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications are being studied by manufacturers, suppliers, universities, transportation agencies, and NHTSA. As conceived, an equipped vehicle would function as a node in a network able to communicate with other vehicles and roadside units to provide one another with information on such topics as safety warnings and the state of traffic. Electronic messages could notify the driver or perhaps the ACC that the vehicle ahead is

slowing down and thus give more reaction time to the trailing vehicle. Communications through a string of vehicles could warn of traffic slowdowns, and communications between vehicles could reduce crashes at blind intersections. Because V2V would require a substantial number of vehicles equipped with transponders and V2I would require intelligent highway infrastructure, the emergence of these systems will depend not only on further technological advances but also on many safety assurance, institutional, and economic factors.

Partly and Fully Automated Vehicles

In contrast to systems that provide the driver with a warning or assume temporary control over the vehicle in an emergency situation, partial or fully automated systems would provide assistance for routine driving tasks. In the case of partially automated systems, the driver would relinquish control of some driving tasks but retain control of the vehicle generally. Fully automated vehicles are often conceived as providing "hands-off, feet-off" driving, whereby the driver is disengaged from virtually all driving tasks.

The notion of fully automated driving dates back to at least the 1939 World's Fair, which included a GM exhibit on "driverless" cars (Shladover 1990). Even today, there is no agreement on how such an outcome could be achieved from both the technical and the practical standpoints. One possibility is that instrumented vehicles operate autonomously by using artificial intelligence and V2V-type sensors and communications capabilities that enable safe navigation within a highway environment consisting of a mix of automated and nonautomated vehicles. Other possibilities include varying degrees of cooperation among vehicles and infrastructure, perhaps on dedicated lanes. One of the earliest demonstrations of these concepts was organized by the National Automated Highway System Consortium, which demonstrated various forms of automated driving on an Interstate highway outside of San Diego, California, in 1997.[7] The Defense Advanced Research Projects Agency has sponsored several competitions to demonstrate hands-free driving.[8] Recently, Google announced that it has tested several vehicles over 140,000 miles hands free.[9] These

[7] For a review of the National Automated Highway System Consortium research program, see TRB (1998).

[8] http://www.darpa.mil/grandchallenge/index.asp.

[9] http://www.nytimes.com/2010/10/10/science/10googleside.html?_r=2&ref=science.

vehicles use radar, lidar, vision cameras, and GPS, among other contemporary technologies.

All concepts of vehicle automation, both partial and full, face major technological challenges, as well as substantial safety assurance hurdles. Partially automated systems can be more difficult to design and implement because of the potential for confusion over the division of functions between the driver and the machine and the need to maintain driver situation awareness. This study cannot begin to address these and other safety issues associated with the many forms of automation. Although such systems may not emerge on a large scale for decades, opportunities may arise sooner under certain controlled conditions, such as the use of automated snowplow and freight truck convoys (with drivers in the lead trucks) on rural Interstate highways and buses on dedicated transitways (TRB 1998, 60–62).

SAFETY CHALLENGES

As the description in this chapter makes clear, electronics provide a wide array of benefits to motorists. Electronics not only make vehicles more energy- and emissions-efficient and reliable[10] but also improve many capabilities that have clear safety implications, such as reducing the vulnerability of braking to skidding. In addition, electronics allow many new vehicle capabilities intended to improve the safety of driving. Among them are stability control and blind spot, lane-keeping, and headway surveillance. Even after a crash occurs, electronics allow more effective air bag deployment and faster emergency response through automatic emergency responder notification of crash location.

Although electronics provide reliability and safety benefits, they also present safety challenges. One relates to ensuring that software performs as expected under a range of vehicle operating conditions. As indicated earlier, vehicles today have embedded software comprising millions of lines of code in a wide variety of vehicle systems. It is well known that

[10] According to J. D. Power and Associates (2011), a study measuring problems experienced during the past 12 months by original owners of 3-year-old (2008 model year) vehicles indicates that owners are experiencing the lowest problem rate since the inception of the study in 1990. The study found that the greatest gains have been made in reducing problems associated with vehicle interiors, engines, transmissions, steering, and braking. However, the problem rate for some electronics systems, including entertainment and tire pressure monitoring systems, increased.

exhaustively testing large and complex software programs to simulate every possible state under real-world operating conditions is not physically possible. Accordingly, development of vehicle control strategies that are fail-safe (or "fail-soft") in the event of some unforeseen and potentially unsafe vehicle operating condition is a critical goal for automotive manufacturers. This will remain the case, since software in future vehicles can be expected to become even more complex. Of course, the growth in software size and complexity in the automotive industry is mirrored in other sectors of transportation and in other fields such as energy, chemical production, and manufacturing. The complexity is creating challenges in all domains and thus becoming the subject of much research.[11] In this regard, the automotive industry should benefit from the understanding gained in developing safety-critical software generally.

Another challenge of the electronics-intensive vehicle stems from the highly interactive nature of the electronic control systems on the vehicle. Increasingly, these systems share sensors and information to reduce cost and complexity and to increase system functionality. Thus, the systems could share incorrect information, which might lead to unintended consequences in vehicle operation. As in the case of software, understanding every possible unintended interaction among complex systems and implementing mitigation strategies as part of the vehicle validation process are difficult, and the difficulty will increase as systems are added and become dependent on one another. Meeting this challenge places a premium on monitoring the vehicle state in real time and on implementing strategies for fail-safe or fail-soft operation.

A further challenge in today's electronics-intensive vehicle relates to the interactions between the driver and the vehicle. As electronics-driven systems with new behaviors and interfaces are introduced at a faster pace, the driving experience can change, and some drivers may be surprised by certain vehicle behaviors that are normal for the new system. The unfamiliar driver may respond in a way that causes safety problems. Similarly, a startled or stressed driver may not react properly when faced with an unexpected condition. For example, the means for shutting off

[11] For example, in 2007, because of concerns about problems attributed to software for robotic spacecraft, the National Aeronautics and Space Administration conducted a study of "flight software complexity," and in 2009 the National Science Foundation initiated a research program on "cyber-physical systems" intended to "reveal cross-cutting fundamental scientific and engineering principles that underpin the integration of cyber and physical elements."

the engine while driving when a vehicle has a keyless ignition system (push button) has been suspected to be misunderstood by drivers accustomed to the traditional keyed ignition switch. Thus, human factors, which have always been important in the design of vehicles, will grow in significance as new systems affecting the driver's interfaces and interactions with the vehicle are introduced.[12]

The fundamental role of networked electronics in today's vehicles was discussed earlier in the chapter. These networks are crucial in the operation of the vehicle, and various strategies are being used by manufacturers to ensure that they are protected against and isolated from sources of environmental interference and malicious access. The strategies include testing, monitoring and diagnostics, fail-safe mechanisms, controlled network gateways, and the use of communications protocols. For example, manufacturers and suppliers test vehicles and components to ensure that electromagnetic fields from a variety of external and internal sources do not cause unexpected or errant system behaviors. Whether the nature and level of this testing have kept pace with the changing electromagnetic environment and increased safety assurance required for the expanding electronics content in vehicles has not been the subject of extensive research in the public domain. In addition, the effectiveness of controlled network gateways and firewalls is coming into question as a result of recent research and testing. Examples of hackers accessing secure computer systems in other domains are well known, and researchers have recently demonstrated that vehicle systems can be accessed in a multitude of ways through these networks, as described in Box 2-2. The researchers have also shown that this access can be used to alter and degrade safety-critical vehicle systems such as braking, exterior lighting, and speed control. Cybersecurity, in particular, is attracting increasing attention from automobile manufacturers and NHTSA.

Finally, advanced vehicle technologies are being developed, and in some cases deployed, that promise further changes in the safety landscape. Electric-drive vehicles are already in use that have regenerative braking and propulsion systems under more integrated control as well as torque characteristics that differ from traditional vehicles powered by

[12] Customized interfaces are already being introduced. For example, BMW and Mini recently announced their support for "iPod Out," a scheme whereby Apple media devices will be able to control a display on the car's console. Increased customization along these lines can have the advantage of tailoring an interface to the needs of each driver, but they may lead to greater interface variability and driver unfamiliarity.

BOX 2-2

Automotive Vulnerabilities to Cyberattack

Experiments have been conducted by researchers at the University of Washington and the University of California, San Diego, to examine cybersecurity vulnerabilities in modern automobiles. They have demonstrated how individuals with sufficient skill and malicious intent could access and compromise in-vehicle networks and computer control units, including those controlling safety-critical capabilities such as braking, exterior lighting, and engine operations. In the laboratory and in road tests, the researchers first demonstrated the ability to bridge internal networks and bypass what the researchers described as "rudimentary" network security protections to gain control over a number of automotive functions and ignore or override driver input, including disabling the brakes, shutting off the engine, and turning off all lights (Koscher et al. 2010). To do so, they extracted and reverse-engineered vehicle firmware to create messages that could be sent on the CAN through the OBD port to take control of these systems. This included the insertion of code in the control units to bridge across multiple CAN buses. In follow-up experiments, the researchers examined all external attack surfaces in the vehicle to demonstrate and assess the possibility of remote access to cause similar outcomes (Checkoway et al. 2011). The experiments indicated that such exploitation can occur through multiple avenues, including those requiring physical access to the vehicle (e.g., mechanics' tools, CD players) and those using remote means such as cell phones, other short-range wireless devices, and tire pressure monitoring systems.

The committee was briefed by the researchers, who described in more detail the many possible means by which an adversary could attack a vehicle in the manner outlined above and the implications for the safe operation of a vehicle.[1] In the briefing and published papers cited above, the researchers surmise that automotive manufacturers have designed their networks with-

Box 2-2 (*continued*) Automotive Vulnerabilities to Cyberattack

out giving sufficient attention to such cybersecurity vulnerabilities because automobiles have not faced adversarial pressures (unlike PCs connected to the Internet) and because of the incremental nature by which these networks have been expanded, interconnected, and opened to external communication channels. Recognizing that high levels of interconnectedness among vehicle control units are necessary for desired functionality, the researchers did not propose the creation of physically isolated networks. Instead, they proposed the hardening of remote interfaces and the underlying code platform, greater use of antiexploitation mitigations used elsewhere, and the use of secure (authenticated and reliable) software updates as part of automotive component design.

The committee notes that although the researchers did not give specific examples of a vehicle having been compromised by such an external attack, cyberattacks in the field have been reported. One such incident, in early 2010, involved a former employee of an automotive dealership alleged to have remotely hacked into systems that had been installed in purchased vehicles to track their whereabouts and gain access to them in the event of a bank repossession. About 100 private vehicles were targeted; their starters and GPS were deactivated and their horns were triggered. Many of the owners were stranded and incurred towing expenses, according to media reports.[2] Obviously, had such an attack compromised a vehicle's power train, braking, and other operating systems while being driven, the consequences could have been much more severe.

[1] Two of the researchers, Tadayoshi Kohno and Stefan Savage, briefed the committee on March 4, 2011.

[2] http://www.pcworld.com/article/191856/exemployee_wreaks_havoc_on_100_cars_wirelessly.html.

internal combustion engines. Continued growth in the EV fleet will place new safety assurance demands on industry and oversight responsibilities on NHTSA. Intelligent vehicle concepts that now appear to be far out on the horizon, such as V2V and V2I, may progress even faster than expected and add further to the safety assurance and oversight challenge.

The next chapter discusses how automobile manufacturers are attempting to meet these various safety and cybersecurity challenges through their product design, development, and production processes.

CHAPTER FINDINGS

Finding 2.1: *Electronics systems have become critical to the functioning of the modern automobile.* Enabled by advances in sensors, microprocessors, software, and networking capabilities, these systems are providing a rich and expanding array of vehicle features and applications for comfort, convenience, efficiency, operating performance, and safety. Almost all functions in today's automobile are mediated by computer-based electronics systems. Some of these systems have improved on capabilities once provided by mechanical, electromechanical, and hydraulic systems. In many other cases, electronics systems are enabling the introduction of new capabilities, including a growing number of applications intended to assist the driver in avoiding and surviving crashes.

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.* System interconnectivity and complexity are destined to grow as the capabilities and performance of electronics hardware, software, and networking continue to expand along with consumer demands for the benefits these interconnected systems confer. Networked electronics systems and software will continue to be the foundation for much of the innovation in automobiles and may lead to fundamental changes in how the responsibilities for driving tasks and vehicle control are shared among the driver, the vehicle, and the infrastructure.

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.* As systems share sensors and exchange data to expand functionality, an emerging safety assurance challenge is to prevent (*a*) the unintended coupling

of systems that can lead to incorrect information being shared and (*b*) unauthorized access to or modifications of vehicle control systems, both of which could lead to unintended and unsafe vehicle behaviors. A critical aspect of this challenge is to ensure that the complex software programs managing and integrating these electronics systems perform as expected and avoid unsafe interactions. Another is to ensure that the electronics hardware being embedded throughout the vehicle is compatible with the demanding automotive operating environment, including the electromagnetic environment, which may be changing as electronics devices and accessories are added to automobiles. Inasmuch as many problems in software and electromagnetic interference may leave no physical trace behind, detection and diagnosis of them can be more difficult.

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.* Although automotive manufacturers spend much time and effort in designing and testing their systems with users in mind, the creation of new vehicle capabilities may lead to responses by drivers that are not predicted and that may not become evident until a system is in widespread use. Drivers unfamiliar with the new system capabilities and interfaces may respond to or use them in unexpected and potentially unsafe ways. Thus, human factors expertise, which has always been important in vehicle design and development, is likely to become even more so in designing electronics systems that perform and are used safely.

Finding 2.5: *Electronics technology is enabling nearly all vehicles to be equipped with 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.* Access to data logged in EDRs can aid crash investigators, while diagnostics systems can facilitate vehicle repair and servicing and inform automotive manufacturers about possible system design, engineering, and production issues. Continued advances in electronics technology and their proliferation in vehicles can be expected both to necessitate and to enable more applications for monitoring state of health, performing self-diagnostics, implementing fail-safe strategies, and logging critical data in the event of crashes and unusual system and vehicle behaviors.

REFERENCES

Abbreviation

TRB Transportation Research Board

Charette, R. N. 2009. This Car Runs on Code. *IEEE Spectrum,* Feb. http://spectrum.ieee.org/green-tech/advanced-cars/this-car-runs-on-code.

Checkoway, S., D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. 2011. Comprehensive Experimental Analyses of Automotive Attack Surfaces. Presented at 20th Advanced Computing Systems Association Conference, San Francisco, Calif., Aug. 10–12. http://www.autosec.org/publications.html.

Cook, J. A., I. V. Kolmanovsky, D. McNamara, E. C. Nelson, and K. V. Prasad. 2007. Control, Computing and Communications: Technologies for the Twenty-First Century Model T. *Proceedings of the Institute of Electrical and Electronics Engineers,* Vol. 95, No. 2, Feb., pp. 334–355.

J. D. Power and Associates. 2011. U.S. Vehicle Dependability Study. Press release. http://www.jdpower.com/news/pressrelease.aspx?ID=2011029.

Koscher, K., A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. 2010. Experimental Security Analysis of a Modern Automobile. In *Institute of Electrical and Electronics Engineers Symposium on Security and Privacy* (D. Evans and G. Vigna, eds.), Institute of Electrical and Electronics Engineers Computer Society, May.

Krüger, A., B. Hardung, and T. Kölzow. 2009. Reuse of Software in Automotive Electronics. In *Automotive Embedded Systems Handbook* (N. Navet and F. Simonot-Lion, eds.), CRC Press, Boca Raton, Fla.

Navet, N., and F. Simonot-Lion. 2009. A Review of Embedded Automotive Protocols. In *Automotive Embedded Systems Handbook* (N. Navet and F. Simonot-Lion, eds.), CRC Press, Boca Raton, Fla.

Shladover, S. E. 1990. Roadway Automation Technology—Research Needs. In *Transportation Research Record 1283,* Transportation Research Board, National Research Council, Washington, D.C., pp. 158–167.

Simonot-Lion, F., and Y. Trinquet. 2009. Vehicle Functional Domains and Their Requirements. In *Automotive Embedded Systems Handbook* (N. Navet and F. Simonot-Lion, eds.), CRC Press, Boca Raton, Fla.

TRB. 1998. *Special Report 253: National Automated Highway System Research Program: A Review.* National Research Council, Washington, D.C. http://onlinepubs.trb.org/onlinepubs/sr/sr253.html.

3

Safety Assurance Processes for Automotive Electronics

The automotive industry is customer-driven, and each original equipment manufacturer (OEM) designs its new vehicles and their features to meet customer demands for various attributes such as comfort, styling, fuel economy, safety, and reliability. All product design and development decisions are also influenced by anticipated product development, manufacturing, and warranty costs and by the need to comply with federal emissions, fuel economy, and safety standards. Beyond these generalizations, the specifics of product development differ by automotive manufacturer. Each OEM and supplier views its product development processes as proprietary, giving it a competitive advantage by facilitating innovation, enabling smoother integration of procured components, managing costs, and increasing product reliability.

Despite the many differences in their product development practices, OEMs share similar philosophies on how to ensure the reliable performance of their products. For the most part, they follow processes during product design, engineering, and manufacturing intended to ensure that products perform as expected up to defined failure probabilities, and performance is verified through testing and analysis. As preparation for the possible failure of critical components, all manufacturers have established failure monitoring and diagnosis systems that are likewise tested. When a failure is detected, these systems are designed to implement predefined strategies to minimize the harm. For example, they may notify the driver through a malfunction dashboard light, shut off the failed

system if it is nonessential, or command a reduction in engine power to avoid stranding the motorist and to enable the vehicle to "limp home" for repair. Only certain safety-critical features, such as brakes, which must remain operational at all times, consist of independent redundant systems.[1]

The Federal Motor Vehicle Safety Standards (FMVSSs) administered by the National Highway Traffic Safety Administration (NHTSA) require that vehicles have certain safety features and characteristics, such as brakes, air bags, and crush resistance. Each manufacturer must certify their presence in the manufacturer's vehicles and their compliance with the minimum performance capabilities prescribed in each FMVSS. Some FMVSSs mandate redundancy—most notably for braking—but none specifies how any capability should be provided through specific system designs.

An overview of the FMVSSs is provided in Chapter 4. These regulations do not prescribe the coverage, content, or ordering of activities that manufacturers must follow in designing, engineering, and manufacturing their products, including any that are intended to meet an FMVSS. Thus, NHTSA does not prescribe or certify the use of specific design approaches, materials, safety analysis tools, testing protocols, or quality assurance methods to reduce the potential for failures or to minimize their impact—for example, by demanding the use of protective shielding, dual memory locations, corrosion resistance, or diagnostic and fail-safe strategies. Because automobile manufacturers have wide latitude to choose their own product designs, architectures, and materials, they are left with the responsibility to devise the most appropriate analysis, testing, monitoring, and fault response strategies.

The proprietary nature of automotive development, coupled with the large number of manufacturers selling vehicles in the United States,[2] leads to difficulty in assessing how each manufacturer seeks to ensure the safe performance of its electronics systems and how diligently each

[1] As discussed in Chapter 2, brake hydraulics are split so that typically the left front and right rear wheels use half the system and the right front and left rear wheels use the other half. If one system fails, the other will provide degraded but balanced braking.

[2] The following 17 OEMs and their major divisions sell an appreciable number of automobiles in North America: Toyota (Lexus, Scion), General Motors (Buick, Cadillac, Chevrolet, GMC), Chrysler (Chrysler, Dodge, Jeep, Ram), Volkswagen (Porsche, Audi, Bentley), Ford (Lincoln), Hyundai/Kia, Honda (Acura), Nissan (Infiniti), Fiat (Fiat, Lancia, Ferrari, Maserati), Suzuki, Subaru, Daimler (Mercedes-Benz, Smart, Orion), BMW (BMW, Mini, Rolls Royce), Mazda, Mitsubishi, Jaguar/Land Rover, and Volvo.

carries out these processes. Nevertheless, the committee's visits with four major OEMs and a top supplier, consultations with experts from the automotive industry, and literature reviews suggest that automotive manufacturers follow many similar processes intended to ensure a reliable and safe product. The common elements of the processes are described in the first section of this chapter.

After these assurance processes are described, consideration is given to industry-level standardization efforts that are intended to aid manufacturers in improving their assurance methods for meeting new and changing challenges arising from electronics systems. In particular, the pending International Organization for Standardization (ISO) Standard 26262 is discussed. This voluntary standard is intended to guide OEMs and their suppliers as they devise and follow their own processes for identifying, prioritizing, and minimizing risks associated with safety-related electronics systems. As of this writing, the final draft of ISO 26262 was being decided by ballot, and hence its use and influence remain uncertain. Automotive manufacturers already have much at stake in ensuring the safe and dependable performance of their products because of litigation, warranty claims, and loss of brand image and sales. The ISO standard is discussed because it demonstrates the apparent recognition within the automotive industry of the special assurance challenges arising from electronics systems. This standard-setting activity may also present an opportunity for NHTSA to gain a stronger understanding of the means by which automotive manufacturers seek to ensure the safe and secure performance of their vehicles.

The chapter concludes with a summary of key findings from the discussion, which are referred to later in the report to support the committee's recommendations to NHTSA.

SAFETY ASSURANCE PRACTICES IN THE AUTOMOTIVE INDUSTRY

The following description of how automotive manufacturers carry out safety assurance during product design, engineering, and manufacturing is not intended to be exhaustive. Most of the practices described are well known to practitioners, and more in-depth descriptions of each can be found in the cited literature. The purpose of the description is to inform those unfamiliar with the processes about the basic approaches

and strategies followed within the industry. The discussion explains how manufacturers (*a*) elicit and define product safety requirements; (*b*) design system architectures to include system monitoring, diagnostic, and fail-safe strategies; (*c*) use safety analysis tools during product design and engineering; (*d*) test and verify system and component designs; (*e*) validate system conformance to safety requirements; and (*f*) monitor for and learn from issues that arise in the field. Taken together, these approaches and strategies make up the product safety assurance processes that are referred to often in this report.

Eliciting and Defining Product Safety Requirements

All automotive manufacturers must comply with government regulations such as the FMVSSs. In addition, the manufacturers have internal product requirements that include the OEM's own quality and performance expectations. For example, an OEM will define the core requirements associated with each vehicle's make or product line. Many vehicle performance requirements, such as handling capabilities and ride quality attributes, differ by manufacturer and by product line, depending on the expectations of each vehicle's customer base. Other requirements, such as those related to safety, may be universally followed by manufacturers for all their products. Consistent application of certain requirements within a product line enables the OEM to maintain brand image and reuse assets across models. The diversity of demands and expectations across product lines, however, leads to thousands of safety, quality, reliability, and performance requirements that guide manufacturer decisions governing the design elements, engineering, and material choices for their vehicles and constituent systems.

Various manufacturer requirements relate to vehicle safety. First, nearly all products are subject to requirements ensuring that they will not inflict certain hazards on motorists and technicians, such as electric shock, fire, and toxicity. Some of these requirements are rooted in government regulation, such as rules demanding flame-resistant seat covers, while others are unique to the manufacturer. Second, certain vehicle systems are subject to additional requirements governing their ability to perform operational functions in a dependable manner. Among such systems are those allowing the driver to maintain visibility and vehicle control, such as wipers, brakes, steering, and external lighting. Government regulations often establish minimum performance capabilities for these safety-critical systems (for example, wipers being able to

remove a volume of water from a windshield at a certain rate). Even in these cases, the OEM will have internal requirements specifying each system's expected dependability in providing the function, such as wipers working with a given degree of reliability under a range of plausible operating conditions.

Finally, there are internal safety requirements concerning system interfaces and interactions with the driver. For the most part, government regulations do not prescribe design considerations such as the location of radio control buttons or the spacing of the brake and accelerator pedals. Accordingly, the manufacturer makes these design choices subject to its own safety requirements. For example, the manufacturer may have a standard requirement that a radio control knob be located to avoid causing the driver to glance away from the road for more than a predetermined number of seconds.

OEMs know that vehicles and systems that do not perform safely will become the subject of consumer complaints, warranty claims, lawsuits, and possibly safety actions by NHTSA. Eliciting and defining these requirements before the design process begins are therefore central to the safety assurance processes of all manufacturers. To guide the design of safety-critical vehicle systems such as braking and steering, the OEM must be thorough in specifying what these systems should and should not do to keep the vehicle in a safe mode for all foreseeable uses and environmental conditions. Because conformance will need to be evaluated and validated at all stages of product development, these expectations must be specific and well documented. The expectation that a system will *never* fail is generally avoided, since the ability of the system to meet this expectation cannot be verified.

A major challenge faced by automotive manufacturers in defining these requirements is in recognizing how the system will be used by and interact with the driver—that is, in identifying the human aspects of performance. For mature systems with an operational track record, knowledge of past uses and operating conditions can guide the specification of system safety requirements. For newer and more complex systems, such information must be obtained with assistance from other means, including simulation and modeling, workshops with users, field tests by drivers, and consultations with specialists from other vehicle domains and engineering fields having similar systems. Examples of human factors challenges associated with advancements in vehicle electronics are discussed in Box 3-1.

BOX 3-1

Human Factors in the Design of Electronics Systems

Even with the increasing role played by electronics and software in vehicle control functions, the driver remains the critical determinant of safe performance. Driver actions and inactions contribute to the majority of crashes and are most often labeled as the proximate causes. The label of driver error, however, can obscure the role that vehicle designs can play in crash causation if insufficient consideration is given to human capabilities and limits. The new capabilities of vehicle electronics promise to eliminate or mitigate some driver errors, but they risk introducing new ones if drivers are not properly considered as integral to the vehicle system.

The field of human factors engineering provides various standards, guidelines, and test procedures to aid in the design of systems that are less likely to induce driver errors. These practices apply to the physical layout of the vehicle to ensure that drivers can see, reach, and operate vehicle controls. For example, human factors practices guide the placement, width, and length of the brake and accelerator pedals to minimize pedal misapplication. Human factors practices also apply to the design of dashboard warning lights and control levers and buttons to ensure that drivers can easily interpret information and control critical vehicle systems. Traditional safety analysis tools such as failure mode and effects analyses (discussed below) help ensure that design choices are consistent with driver expectations and response tendencies.

Increasingly, automotive manufacturers apply techniques that have been developed to make other consumer products user-friendly, such as user-centered requirements generation and usability testing. Their applicability is growing as vehicle electronics assume greater control of the vehicle through such features as adaptive cruise control, collision warning systems, lane-keeping aids, and automated braking systems. These and similar "mixed initiative" systems could cause the driver to

Box 3-1 (*continued*) Human Factors in the Design of Electronics Systems

misunderstand and be startled by the electronics even when the system is operating as designed.

A major challenge for system designers is in understanding the long-term adaptation of the driver to the electronics and the degree to which the driver will assume that the vehicle is capable of certain control functions. For example, drivers might begin to believe that the vehicle carries out some control functions in a way that is inconsistent with the designers' intent. Advances in driving simulators and instrumented vehicles are thus being developed to give human factors engineers new tools to assess and model how the driver and automotive electronics will interact. In this sense, automotive vehicles exemplify the mass adoption of the assisting or operating "robot," partnering with humans to ease or even take over the human workload.

Diagnostics and Fail-Safe Strategies in Electronics Architecture

All OEMs and OEM suppliers view their system architectures as proprietary because the architectures provide the foundation for a multitude of design decisions that follow. For example, the vehicle's embedded electronics architecture, at a minimum, defines the electric components (power, sensors, controller units, actuators) on the vehicle. It maps every electronics-enabled feature to an electronic control unit or multiple units for distributed processing and establishes the communication protocols between the electronic components. These decisions are made with many requirements and constraints in mind, including the need to manage production costs, accommodate changes such as the addition or removal of features, and use the architecture across multiple product lines. In the case of the embedded electronics architecture, such requirements can influence decisions about whether to use central or distributed processing and where to locate controllers in relation to sensors and actuators.

Hence, during the development of this system architecture—when the basic system connections and relationships are established—important

decisions are made to ensure conformance with the defined safety requirements, including the strategies that will be used to monitor for and diagnose faults and to control their safety risks. Design and implementation of self-diagnostics strategies occur during this phase. Onboard diagnostics are required by the U.S. Environmental Protection Agency (EPA) to facilitate maintenance and servicing of emissions control systems. However, these are minimum requirements and pertain to emissions-related systems only. OEMs have added many other diagnostic capabilities into their electronics systems architectures for detecting, containing, and responding to faults in other systems, especially safety-related faults.

Because each OEM uses its own diagnostic strategies (apart from the EPA-mandated elements), there is no single industry self-checking or diagnostic standard. Instead, there are overarching similarities in the approaches used. Diagnostics are performed during vehicle start-up and operation, and the driver is often unaware of the checks being performed. In general, diagnostic systems are designed so that when an error is sensed, a diagnostic trouble code (DTC) is recorded. Some DTCs are intended to aid technicians in making necessary repairs and adjustments to the vehicle. Others serve a supervisory, or "watchdog," function that can force the system into a predefined state, such as causing the engine to shut down or operate at reduced power for limp-home capability. Usually if a detected error is not indicative of a condition affecting vehicle drivability or safety, a DTC will be stored for a limited number of ignition key cycles, during which time it can be retrieved by a repair technician. Detected errors that indicate a problem with vehicle drivability or certain safety-related functions, such as the condition of an air bag, will set a DTC and be accompanied by a dashboard malfunction indicator light to inform the driver that the function has been disabled or the vehicle needs to be serviced. Detected errors that can adversely affect the ability of the driver to operate the vehicle safely will trigger a DTC as well as an immediate containment and fail-safe action.

The exact methods used for detecting and diagnosing faults vary by manufacturer and system architecture and function. In the case of an electronic throttle control system (ETC), a common method for detecting faults or unusual behaviors is to use two independent sensors. A disagreement in the two sensor signals will trigger a DTC. Another frequently used method is to install a watchdog processor along with the main processor in a control unit. If the watchdog detects an abnormality

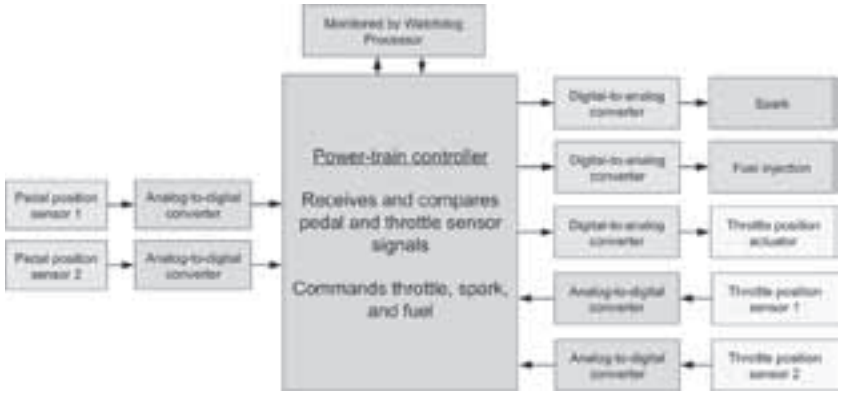


FIGURE 3-1 ETC input and output flows.

that escapes the main processor, it will set a DTC and force the system into a fail-safe mode.

Figure 3-1 shows a simplified diagram of the fault detection strategies defined in an ETC's architecture. The primary input to the ETC is the driver's depression of the accelerator pedal. Two sensors in the pedal assembly measure the pedal position and send analog signals to digital converters, which send digitized values to the main processor. In addition, the main processor receives signals from one or more sensors that measure the position of the throttle plate.[3] If the signals from the two pedal sensors are inconsistent, the processor will trigger a DTC. A DTC will also be triggered if the signal from the throttle plate sensor is inconsistent with the signals from the pedal sensors. Furthermore, incongruent actions by the main processor will cause the watchdog processor to trigger a DTC.

The system's response to detected faults is defined in the architecture. In the case of faults in the ETC, the response differs according to the perceived severity of the condition. Depending on the strategy used, a DTC may cause the control unit to limit power so that the vehicle can only be driven slowly. More restrictive responses may be to force idle or to shut down the throttle motor, cut off the fuel supply, or stop the spark plugs from firing to render the vehicle inoperable. System designers

[3] The throttle plate also contains two springs that automatically return it to a semiclosed position (sufficient for idle) when not commanded to be opened further.

must make determinations about the response strategy that is appropriate to the detected condition and its implications. Shutting off the engine, for example, may guarantee that the driver will tow the vehicle to a repair station, but it also can risk stranding a motorist, possibly in unsafe circumstances. Having carefully defined and well-articulated safety requirements can therefore guide developers of the ETC's architecture in making choices about the most appropriate system response to a failure.

Safety Analysis During System Design and Development

Figure 3-2, adapted from a recent paper by General Motors engineers (Sundaram and Hartfelder 2011), shows how a number of analytic methods are used in an iterative manner by OEMs as part of the safety analysis conducted during product design, development, and production. There is no need to review each of the methods here, since the techniques are used widely in industry and are described thoroughly in the safety engineering literature. Nevertheless, because its use is noted elsewhere in this report, including the description of the analysis of Toyota's ETC by the National Aeronautics and Space Administration's (NASA's) engineering team in Chapter 5, one method warranting discussion for illustrative purposes is failure mode and effects analysis (FMEA).[4]

FMEA was originally developed for military applications. It requires the participation of experts from multiple engineering disciplines and vehicle domains with broad knowledge of the requirements, functions, interfaces, and user actions of the system being analyzed. These teams are tasked with identifying (*a*) each key system feature and its function; (*b*) possible modes of failure for each of the functions; (*c*) the adverse effects that can arise from the failure; (*d*) failure symptoms and methods of detecting them; and (*e*) the means by which the failure and its adverse effects are prevented or managed by the system design, including the use of fail-safe mechanisms. An example of an abbreviated FMEA output, developed by NASA to examine Toyota's ETC, can be found in Table 5-5 of Chapter 5.

An advantage of the FMEA process is that it enables the identification and cataloging of potential failure modes by likelihood and severity, allowing preventive actions to be taken early in the design process. A disadvantage is that it is not useful for examining multiple failure points

[4] A more detailed description of FMEA and other safety analysis techniques used in the automotive sector is given by Woltereck et al. (2004).

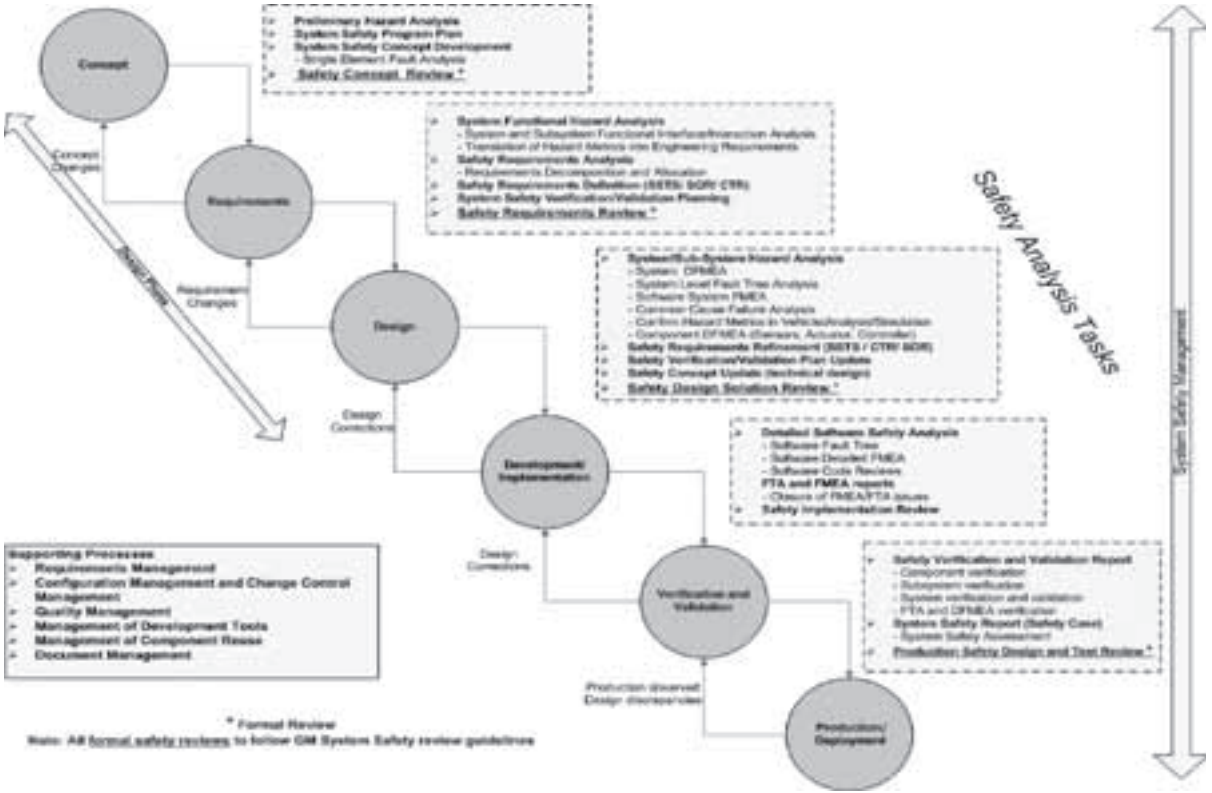


FIGURE 3-2 Safety analysis during vehicle design, development, and production.
(*Source:* Sundaram and Hartfelder 2011.)

and their effects at a system level. The statement of task for this study implicitly recognizes the challenges automotive manufacturers face in evaluating low-probability hazards by asking for a discussion of the "the limitations of testing in establishing the causes of rare events." Examples of these challenges are discussed below. The examples include exhaustively testing software for all conceivable anomalous behaviors and predicting failure scenarios that involve coincidental faults occurring among multiple interconnected electronics systems. While even very rare failure modes may arise in a fleet of tens of millions of vehicles operating under a wide range of conditions, anticipating and evaluating them is made more complicated by their intermittent nature and the potential for electronics-related faults to leave no physical trace of causes.

For the most part, techniques such as FMEA work best for failures caused by random, wear-out phenomena and for problems arising in the individual system components rather than in their interactions. Thus, manufacturers use many other techniques to model and analyze failure processes in different ways and in combinations that show the causes of a certain event. Fault tree analysis (FTA), for example, is used to analyze how resistant systems are to both single and multiple initiating faults. In addition, because more complex electronics-intensive systems raise the possibility of more unanticipated failure combinations and sequences, manufacturers are using other tools to inform their safety analyses. Among them are computer models of the architectural structure and simulations that include the driver to aid in early identification of a large number of possible failure modes that may arise from system interactions and to assess their consequences (Törngren et al. 2009).

Improving data and methodologies for evaluating and testing for rare events remains a challenge for automotive manufacturers, as it does for manufacturers in other industries. Ideas on collaborative research by NHTSA and industry to address this challenge are offered later in this report (Chapter 6).

Component Design and Verification Testing

The design and engineering work for most vehicle subsystems and components is conducted by major suppliers. The scale and scope of supplier procurements have compelled OEMs to convey their needs and demands to suppliers in a multitude of ways. Among them are visual depictions of conceptualized systems and detailed specifications of components contained in formal requests for proposals. The exact procedures depend on

the maturity and complexity of the products being procured and the relationship between the OEM and the suppliers. Like OEMs, suppliers want to keep their product architectures, designs, and development processes confidential to the extent possible, since they compete with other suppliers for OEM business. These transparency constraints can limit the depth of an OEM's knowledge of a supplied component or subsystem design. It is thus common for OEMs to have a generic list of verification requirements for all supplier content as well as additional requirements tailored to the specific product under procurement. The supplier is usually expected to provide a plan for verifying that its product conforms to all agreed-on specifications.

Testing is the most common method of verifying that OEM specifications have been met. Procurement contracts may identify hundreds of items requiring certain testing activities up to defined levels for different operating conditions and for various environmental stresses. For example, tests of resistance to dust, salt spray, water, thermal shock, and vibrations may be required. Durability test criteria for electronics hardware will usually simulate aging and associated degradation effects. OEMs and their suppliers also test for electromagnetic compatibility (EMC), as explained in Box 3-2. Many of the tests prescribed will reflect industry-wide and international standards [i.e., those of the Society of Automotive Engineers (SAE) and ISO], and others will be unique to the OEM. While suppliers are expected to do most of the testing, OEMs usually inspect and then check results through acceptance methods ranging from hardware-in-the-loop simulations to testing of prototype and sampled products in their laboratories and proving grounds. Because suppliers of vehicle electronics systems have come to rely on commercial off-the-shelf hardware that has already been tested and warranted for the demanding automotive environment, the need for additional supplier testing has been reduced in some cases. Indeed, the proliferation of standardized automotive hardware has made its supply much like that of a commodity, since all OEMs and suppliers have access to the same hardware components, from sensors and actuators to drive circuits and microprocessors.

In general, automotive software development follows the same path as that described for automotive systems and components generally (Törngren et al. 2009, 10-31). The establishment of software architecture, algorithms, and testing plans in accordance with the OEM's requirements is the primary responsibility of the supplier. Since most software

BOX 3-2

Automotive EMC Testing

EMC is commonly defined as the ability of equipment or a system to function satisfactorily in its electromagnetic environment without introducing intolerable electromagnetic disturbances to anything in that environment. There are two main aspects of the EMC challenge. The first, prevention, consists of controlling the generation of radiated and conducted electromagnetic emissions from electronic products and limiting disturbances produced by licensed transmitters. The second, referred to as EMC immunity, is to create products that can operate normally when they are exposed to anticipated electromagnetic environments.

The U.S. government does not require EMC immunity for most industrial products. Federal regulations focus instead on controlling emissions and regulating transmitters, mainly so that radio and cellular operations are not disturbed. The absence of federal regulations on product immunity does not preclude companies from establishing their own product emissions and immunity requirements. Automobile manufacturers have long had to address the effects of electromagnetic interference. For example, short-pulse currents flowing on wiring from the distributor to the spark plugs produced high-frequency electromagnetic fields that disturbed AM radio reception. The problem was alleviated by replacing copper wires with resistive wiring to reduce the level of current flowing.

Today's automobiles, of course, contain more electronics than radios, and thus many more systems and components that can both emit electromagnetic interference and be susceptible to it. In addition, the electromagnetic environment has changed, with more transmitters on board the vehicle (e.g., mobile phones) and located along the roadway. The automotive industry has come to rely substantially on company- and industry-level testing standards for electromagnetic influences, including industry standards from ISO and SAE. During the committee's visits to OEMs, it found significant uniformity in the way EMC testing is performed.

Box 3-2 (*continued*) Automotive EMC Testing

In all cases, the OEMs require suppliers to perform and document electromagnetic tests on components and subsystems before the equipment is accepted, and in some cases the OEMs recheck the testing. Most suppliers use standard ISO and SAE test methods, with some adaptations to meet the specific demands of OEMs. These tests appear to consist of both radiated and conducted testing, including use of reverberation chambers.

The OEMs require testing for both subsystems and complete vehicles, although typically the subsystem testing was at higher levels (approximately 30 V/m) than full vehicle testing. All perform radiated testing of complete vehicles in semianechoic (and sometimes reverberation) chambers, with antennas set up outside and near the vehicles to expose them to levels of electromagnetic fields across the frequency band (up to about 2.5 GHz). The tests are typically performed for both horizontal and vertical polarization of the fields using side and front exposure angles. Some testing was also performed in a strip line to test at the lower frequency range. In some cases an automobile was exposed to a radar-type pulse. Testing was also performed with an electrostatic discharge gun.

used in the vehicle is contained in these procured subsystems and components, most vehicle software is developed in modular fashion by the suppliers themselves.

Unlike hardware defects, all software deficiencies are by their nature design deficiencies rather than manufacturing flaws. Whereas various tools and techniques are used to check software for coding errors, defective coding is not the only possible source of software-related errors, many of which will not be revealed in software having nontrivial complexity even with the most exhaustive testing regime. For example, testing cannot reasonably be expected to reveal how complex software will behave under all conceivable conditions, such as the variability that can occur in execution paths and timing of messages to and from the electronic control units. The extent to which OEMs use effective software

engineering practices, such as requirements execution, model-driven design, model checking, and static analysis, is unclear, but such practices are increasingly warranted in light of the expanding role of embedded software.

Adding new functions and features to vehicles, which is usually accomplished by adding software, increases software design complexity and complicates efforts to verify software correctness. As is noted in the description of NASA's analysis of Toyota's ETC software given in Chapter 5, code structures can differ substantially in their ability to be inspected and verified as safe. For example, code that minimizes variable scope, the occurrence of cross-coupling, and intertask dependencies is more amenable to inspection and to obtaining assurance that implementation errors will be detected during execution. As automotive manufacturers integrate software developed during different time periods and by different suppliers, such verification can become even more important but more complicated and time-consuming. The challenges associated with software assurance are discussed further in Box 3-3.

Software can be customized to a higher degree than can hardware, but a higher degree of customization makes the software even less amenable to standardized testing, at least in the same manner as off-the-shelf hardware. Each OEM and supplier can choose to customize software as much as it sees fit, and hence there is likely to be significant variability in the amount of customization in the automotive industry. The testing challenge associated with customized and complex software is recognized by the automotive industry. A partnership of leading automotive suppliers and OEMs, known as the Automotive Open System Architecture (AUTOSAR), is pursuing the development of a methodology for software and software architecture intended to provide an open and standardized architecture. By rendering software designs more transparent and less proprietary, AUTOSAR is intended to facilitate at least some aspects of testing, such as performing tests for interoperability. Details cannot be given here on the objectives and progress of this partnership, but AUTOSAR is an example of how the automotive industry is cooperating to manage the growing complexity of electronics systems and the software underlying them.

Validating Conformance

Validation—determining what the hardware and software should do and that they are doing it correctly—is more difficult than verification

BOX 3-3

Challenges of Software Assurance

As described in Chapter 2, software is involved in monitoring and controlling most safety-critical vehicle components such as the brakes, engine, steering, and air bags, as well as in enabling many safety features such as lane departure warning and blind spot monitoring. Software is also used throughout the vehicle for non-safety-related systems. The array of software is responsible not only for providing expected functionality under nominal conditions but also for detecting abnormal or degraded behavior in hardware components and responding in a safe way. Software assurance, therefore, is intended to ensure that safety-critical systems (*a*) perform as expected under nominal conditions; (*b*) respond appropriately to hardware failures, both intermittent and permanent; and (*c*) do not exhibit unsafe behaviors under any circumstances.

In the field of software development, a number of industry-wide standards outline assurance processes to be followed during development, including standards specific to automotive software.[1] These standards describe various assurance activities and steps to be followed during development and for verification and validation. They cover reviews of requirements, architecture, and design; analyses of failure modes and effects; code inspections; and software-in-the-loop laboratory testing. However, even the most rigorous adherence to a process standard cannot guarantee software safety and dependability. Part of the problem is that the huge state space managed by software renders testing ineffective for providing confidence at high levels, since testing can cover only a small proportion of the scenarios that can arise in practice from complex software. Furthermore, because the software components of a complex electronics system are inevitably mutually dependent, a critical function may be undermined by the failure of a software component thought to be noncritical and thus not subject to the same testing and development processes called for in the standard.

(continued on next page)

Box 3-3 (*continued*) Challenges of Software Assurance

In recognition of these software assurance challenges, new analysis techniques intended to provide stronger evidence than does testing are under investigation. Two such techniques are formal methods, which involve the use of powerful algorithms to cover large state spaces more readily than does testing alone, and model-based design, in which software implementations are generated automatically from precise, high-level models. In addition, an approach to software assurance that is attracting attention (especially in Europe)—and that is recommended in a recent National Academies report (NRC 2007)—calls on the developer not only to follow development process standards but also to construct "assurance cases" that make explicit the argument that the system is dependable or safe and marshal evidence for software users in evaluating the safety argument objectively.

[1] Examples from the automotive software field are Motor Industry Software Reliability Association guidelines and the pending ISO 26262 functional safety standard. Examples from defense and aviation are RTCA-178B and MIL–Std-882C/D.

testing in many ways. Because supplier-provided subsystems and components may be in various stages of design, development, or maturity at any given time, the conduct of vehicle-level validations of systems in a timely manner can be difficult. Yet identifying problems late in vehicle development is undesirable, since such flaws can be costly to correct (though less costly than correcting problems arising in use). The committee could not confirm the validation techniques used within the industry generally and thus cannot know the extent to which OEMs exploit many new tools and processes, such as computer-aided software engineering tools. Use of these tools can allow validation through computer simulations rather than through physical prototype testing, which can lead to fewer costly problems that are discovered late in product development. Computer-aided hardware- and human-in-the-loop simulations, for example, allow for analysis of software–hardware compatibility and driver usability.

One problem that may be found during validation of supplier-provided software is that the software does not satisfy OEM-stipulated requirements and thus does not perform as intended. In view of this possibility, OEMs are often most interested in the quality of the software development process that was carried out, including the extent of adherence to development process standards as discussed in Box 3-3. Accordingly, the traditional method for validating software includes checking for conformance to standardized processes (e.g., through audits) and carrying out a complementary mix of evaluation methods.[5] One of these evaluation methods may be for the supplier to specify the assumptions about requirements and to present evidence that the software will behave in a manner that meets them, perhaps by the use of example application scenarios. Another issue that can arise is that the requirements themselves are incorrect or incomplete, so that even if the software functions as specified, the resultant actions may not be satisfactory or safe (Howard 2004). To ensure that requirements elicitation is sound, executable requirement models that enable automated code generation and requirements validation to occur concurrently are becoming available. However, the committee could not confirm the extent to which OEMs and suppliers use these methods.

All OEMs conduct testing of vehicles on test tracks and on public roads. Manufacturers often instrument vehicles to log more detailed information on the operation of the vehicle, including the interaction of the electronics systems in the vehicle. Objective and subjective data from such testing are gathered and analyzed for unexpected system and driver behaviors, which may reveal needed product changes. While such full vehicle evaluation is essential, it can occur too late to resolve major issues such as observed qualitative changes in the driving experience resulting from a new technology's interface or capability. The validation activities instituted earlier during product design and development, as described above, are intended to identify and resolve such issues long before they arise during road testing. Road tests can nevertheless clarify the need for incremental modifications to the product and enable system calibration (Conrad and Fey 2009, 11-2).

[5] A review of automotive software safety assurance processes and standards is given by Czerny et al. (2004).

Field Analysis

If safety or quality problems emerge in customer vehicles despite attempts to prevent them, surveillance and analysis of issues arising in the field are critical in resolving the problems quickly and preventing their recurrence in future designs. To facilitate such surveillance, OEMs have access to warranty repair, field report, and parts data obtained from dealers, including returned parts from warranty repairs. OEMs also log complaints from vehicle owners through their service centers and have access to NHTSA's consumer complaint data. All manufacturers are strongly motivated to support active field monitoring and analysis programs: they have an immediate interest in preventing costly litigation and recall campaigns and a longer-term interest in making product improvements and decreasing warranty expenses.

As discussed in Chapter 2, many OEMs have equipped their vehicles with electronic event data recorders (EDRs), originally for monitoring the effectiveness of air bag deployments in crashes. The data saved in these devices are not necessarily available to the OEM, since it does not own the crashed vehicle. Nevertheless, to obtain EDR data, NHTSA and other investigators can require the cooperation of the OEM if the technology for downloading and interpreting the saved data is only available to the manufacturer. Ownership of the data recorded in EDRs is a legal issue with considerable impact on the utility of EDRs for these investigative purposes. In a 2006 rulemaking that required certain common data elements in vehicles equipped with EDRs, NHTSA gave extensive consideration to the privacy issues associated with EDRs, acknowledging that the resolution of these issues will affect the value and practicality of mandating EDRs on all vehicles.[6] As discussed in Chapters 4 and 6, NHTSA is considering requiring EDRs on all new vehicles, although the privacy and data ownership issues are outside its regulatory purview.

INDUSTRY STANDARDS ACTIVITIES FOR ELECTRONICS SAFETY ASSURANCE

Compared with the United States, many other countries with large automotive industries give their manufacturers less leeway to define all aspects of their safety assurance processes. The European Union (EU),

[6] http://www.nhtsa.gov/DOT/NHTSA/Rulemaking/Rules/Associated%20Files/EDRFinalRule_Aug2006.pdf.

for example, requires that manufacturers selling automobiles in member countries demonstrate that they have performed certain tests and followed specified processes during vehicle design, development, and production. Compliance with EMC testing standards is part of the EU certification process.[7] EU regulators also require that manufacturers take certain steps during product development and design, such as conducting safety analyses by using FMEAs and FTAs. To have their vehicle types certified by a member EU country, the OEM must present evidence, usually to independent auditors, confirming that all such steps were satisfied.

Because government review and certification of product safety assurance are more common in Europe, various industry-led standards-setting bodies have developed guidance for manufacturers. In the area of electronics systems safety assurance, an influential standard is the International Electrotechnical Commission (IEC) standard IEC 61508 (Functional Safety of Electrical/Electronic/Programmable Electronic-Related Systems). It provides guidance on processes to ensure that safety-critical electronics work as intended. The standard calls on manufacturers who subscribe to it to take systematic steps to identify all possible ways in which the product could stop functioning as required to perform its safety-critical functions during its entire lifetime of use. Manufacturers who subscribe to the standard are expected to identify each potential hazard situation systematically and calculate its probability of occurrence with adverse consequences to assign a "system integrity level" (SIL). The higher the assigned SIL, the more rigorous the safety assurance measures that must be carried out to ensure that the risk of the adverse consequence does not exceed "tolerable" levels.

Since its introduction more than 10 years ago, IEC 61508 has induced the creation of a number of industry-specific standards for functional safety, including those for machinery, chemical processing, and nuclear power plants. Various guidance documents that are intended to help

[7] The EU and Japan impose certain safety assurance process requirements on automobile manufacturers as part of vehicle type certification. In the EU, Framework Directive 2007/46/EC for automotive type approval lists more than 50 separate topics for approval of the whole car, plus other requirements that apply to components. The directive requires OEMs to obtain third-party approval testing, certification, and production conformity assessments, such as for EMC. If the vehicle prototype passes the required tests and the production arrangements pass inspection, vehicles or components of the same type are approved for production and sale within the EU without further testing of individual vehicles. For more details see http://www.vca.gov.uk/vca/additional/files/vehicle-type-approval/vehicle-type-approval/vca004.pdf.

BOX 3-4

Functional Safety Methodology for Electromagnetic Influences

IEC 61508 requires that consideration be given to all of the environments that could result in an unsafe situation for the subject product. These environments may include shock, vibration, temperature, and electromagnetic fields and their induced voltages and currents. Industry testing standards for EMC are usually established for product reliability purposes. For example, the tests may be designed to ensure that the product will operate reliably 95 percent of the time for a given period. More sophisticated testing to ensure a lower incidence of failure over the entire product life cycle may be demanded for products having critical safety-related functions. Thus, IEC has offered guidance, in IEC 61000-1-2, on how to consider electromagnetic influences on functional safety. The guidance emphasizes that while electromagnetic testing remains important for functional safety, the design of the product to avoid electromagnetic influences is paramount. The standard also emphasizes the importance of the product being designed and tested to ensure that it operates safely during its entire life cycle, which is not required for standard (nonsafety) EMC applications. An additional IEC publication, IEC 61000-2-5 (Classification of the Electromagnetic Environment), provides a survey of the levels of various types of radiated and conducted electromagnetic disturbances present in different locations (including typical and worst case).

manufacturers meet the standard's requirements have been developed. Box 3-4 gives an example of the IEC-approved methodology for addressing EMC for functional safety.

Although automotive manufacturers can follow the guidance of IEC 61508, until recently they have not had an industry-specific standard for ensuring the functional safety of vehicle electronics. Such a standard is now pending, developed by the automotive industry through ISO.

ISO 26262, Road Vehicle Functional Safety, is intended to apply to all safety-related automotive systems, but with an emphasis on electronics. Industry interest in developing the standard originated from the recognition that the proliferation of electronics systems in vehicles was introducing greater complexity into both automotive systems and their development processes.

Developers of ISO 26262 expect that it will lead to manufacturer safety assurance practices that are more transparent and consistent in analytical rigor. Like the IEC standard it is modeled after, it calls for manufacturers to assign automotive safety integrity levels (ASILs) to vehicle systems or functions with corresponding rigor in the safety assurance steps followed. In so doing, it draws attention to the importance of using many of the safety assurance processes discussed earlier in this chapter. Among those processes are eliciting safety requirements, using safety analysis tools such as FMEAs and FTAs, and monitoring for safety performance in the field. To make safety assurance a prominent and transparent part of product development, ISO 26262 emphasizes formal management review of and sign-off on key safety-related decisions at all stages of product planning, development, verification, and validation. The general structure of ISO 26262 is outlined in Box 3-5.

Because of its pending approval status, whether all automotive manufacturers selling vehicles in the United States will subscribe to ISO 26262 in whole or in part is unknown. Many automotive manufacturers and suppliers have indicated their intention to follow the standard, including some that met with the committee. A U.S. member of the team responsible for drafting the standard explained to the committee that even companies that already carry out many of the safety assurance processes necessitated by the standard are likely to experience transitional challenges because of the implications for organizational structure and requirements for new work products and documentation.[8] From the standpoint of many proponents of ISO 26262, one of its early benefits may be to prompt organizational-level scrutiny of long-standing practices and processes through a review of their actual safety assurance contributions.

ISO 26262 merits discussion because it represents an industry-led effort to ensure that vehicle electronics systems continue to perform safely as

[8] Joseph D. Miller, Chief Engineer, Systems Safety, TRW, and Automotive Member of ISO TC22 SC3, Working Group 16, briefed the committee during its meeting on November 16, 2010.

BOX 3-5

General Structure of ISO 26262

Automotive manufacturers and suppliers from Europe, Asia, and North America have participated in the development of ISO 26262. The draft standard consists of 10 parts. Part 1 contains a vocabulary to describe the elements of a system and their relationships, and Part 2 contains overall guidance on safety management. The core parts of the standard consist of the following:

Part 3: Concept phase. This part contains guidance on (*a*) identifying items subject to the standard; (*b*) analyzing use situations and identifying potential hazards associated with each situation; (*c*) carrying out hazard classifications, including determining the ASIL associated with each item; and (*d*) determining safety requirements and goals.

Parts 4, 5, and 6: Product development at the system level and at the hardware and software levels. These parts contain guidance on (*a*) specifying the technical safety requirements at the system, hardware, and software levels; (*b*) defining the design and architecture metrics for each level; (*c*) evaluating and integrating testing; and (*d*) validating and confirming functional safety before release of the design for production. A standard "V" model is used to sequence the work products and reporting requirements for each activity.

Part 7: Production and operation. Because ISO 26262 is a life-cycle standard, this part provides guidance for ensuring that the functional safety is achieved during production through planning measures (e.g., implementation of traceability measures), maintenance and repair actions, and processes for field monitoring.

Parts 8, 9, and 10: Supporting processes. These parts include guidance on performing hazard analyses and risk assessments to determine ASILs [ASILs range from A (lowest) to D (highest)]. On the basis of these analyses, the manufacturer can tailor the necessary activities according to each item's ASIL.

Source: Briefings to the committee by Joseph D. Miller, TRW Automotive Member ISO TC22 SC3, Working Group 16.

they grow in complexity and functionality and because adherence to the standard may bring about greater confidence among safety regulators and the public. Whether the confidence will be justified on the basis of the standard's influence on industry practices and safety outcomes cannot be assessed at this time.

CHAPTER FINDINGS

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.* Each manufacturer is responsible for devising its own safety assurance approaches. Each is responsible for choosing the most appropriate risk and failure analysis techniques, material and manufacturing quality control processes, and means for verifying and validating performance to acceptable failure rates. In addition, each designs and verifies its strategies for safety in the event of a failure. Measures aimed at preventing faults may not succeed under all circumstances. Therefore, a common strategy for detecting and responding to their occurrence in ETCs is through the use of two independent pedal position sensors, two springs to return the throttle to semiclosed position, a second processor to supervise the actions of the main processor, and a series of programmed fail-safe responses that are triggered in the event of a failure, including shutdown of the engine or restriction of its power.

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.* Manufacturers and their suppliers seek to verify the proper performance of their electronics hardware at the component, system, and vehicle levels. Manufacturers reported recognition that even the most exhaustive software testing regimes and strict adherence to software development prescriptions cannot guarantee that complex software will behave safely under all plausible circumstances.

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.* All manufacturers visited reported that they engaged experts in human factors early in the design of their new electronics systems and throughout the later stages of product development and evaluation.

Finding 3.4: *Automotive manufacturers have been cooperating through ISO to develop a standard methodology for evaluating and establishing the functional safety requirements for their electronics systems.* The pending standard—ISO 26262, Road Vehicle Functional Safety—originated from recognition within the automotive industry that the proliferation of electronics systems in vehicles is introducing greater complexity into both automotive systems and their development processes. Final approval of the standard is pending but expected in early 2012. Whether all automotive manufacturers and suppliers selling vehicles and components in the United States will subscribe to ISO 26262 in whole or in part is unknown at this time; however, many companies have signaled their intention to follow the standard's guidance for safety assurance practices that are more transparent and consistent in analytical rigor.

REFERENCES

Conrad, M., and I. Fey. 2009. Testing Automotive Control Software. In *Automotive Embedded Systems Handbook* (N. Navet and F. Simonot-Lion, eds.), CRC Press, Boca Raton, Fla.

Czerny, B. J., J. G. D'Ambrosio, P. O. Jacob, B. T. Murray, and P. Sundaram. 2004. An Adaptable Software Safety Process for Automotive Safety-Critical Systems. SAE Paper 2004-01-1666. http://ja.delphi.com/pdf/techpapers/2004-01-1666.pdf.

Howard, J. 2004. Preserving System Safety Across the Boundary Between System Integrator and Software Contractor. SAE Paper 2004-01-1663. Presented at Society of Automotive Engineers World Congress and Exhibition, Detroit, Mich., March.

NRC. 2007. *Software for Dependable Systems: Sufficient Evidence?* Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences, National Academies Press, Washington, D.C. http://www.nap.edu/catalog.php?record_id=11923.

Sundaram, P., and D. Hartfelder. 2011. Rigor in Automotive Safety Critical System Development. Presented at 29th International System Safety Conference, Las Vegas, Nev., Aug. 8–12.

Törngren, M., D. Chen, D. Malvius, and J. Axelsson. 2009. Model-Based Development of Automotive Embedded Systems. In *Automotive Embedded Systems Handbook* (N. Navet and F. Simonot-Lion, eds.), CRC Press, Boca Raton, Fla.

Woltereck, M., C. Jung, and G. Reichart. 2004. How to Achieve Functional Safety and What Safety Standards and Risk Assessment Can Contribute. SAE Paper 2004-01-1662. Presented at Society of Automotive Engineers World Congress and Exhibition, Detroit, Mich., March.

National Highway Traffic Safety Administration Vehicle Safety Programs

In April 2011, the National Highway Traffic Safety Administration (NHTSA) reported that 32,788 people were killed during 2010 on U.S. roads in crashes, of which about 80 percent involved passenger cars and light trucks.[1] As in previous years, a number of risky driver behaviors and actions, such as alcohol use, inattention, fatigue, and speeding, were among the major causal factors.[2] Yet the 2010 data were widely acclaimed as providing further statistical evidence of a generally positive trend in traffic safety. About 18,000 fewer people died in motor vehicle crashes in 2010 than in 1980, even as vehicle travel almost doubled.[3] This substantial improvement resulted from a combination of factors, such as better design and control of highways, stricter laws governing seat belt use and penalizing drunk driving, and more responsive and protective motor vehicles.

The automotive industry deserves credit for responding to consumer and NHTSA demands to make vehicles inherently safer through innovations in automotive designs, materials, and engineering, including advancements in vehicle electronics. However, safer vehicles are widely recognized as providing only part of the solution to making driving safer. Since 1995, the number of people who have died on U.S. roadways has declined by about 20 percent. This decline is impressive, but during the same period traffic fatalities declined by 40 percent in the

[1] http://www-nrd.nhtsa.dot.gov/Pubs/811451.pdf.
[2] http://www-fars.nhtsa.dot.gov/People/PeopleDrivers.aspx.
[3] http://www.nhtsa.gov/PR/NHTSA-05-11.

United Kingdom and by more than 50 percent in France and 15 other high-income countries for which long-term traffic safety data are available (TRB 2011). In all of these countries, policy makers have emphasized changing high-risk driver behaviors, particularly speeding, drunk driving, and lax seat belt use, by means of stringent laws, intensive public communication and education, and a commitment to traffic enforcement.

Although NHTSA does not license drivers, design roads, or set and enforce traffic laws, the agency shares responsibility with the Federal Highway Administration for providing funding aid and technical assistance to state and local governments having these responsibilities. In collecting and analyzing the nation's traffic safety data, NHTSA has long reported that driver behavior and performance are the most significant factors in crashes. The most recent results of agency crash causation studies are summarized in Table 4-1. They indicate that crashes in which the driver was the proximate cause far outnumber those in which vehicle defects or roadway deficiencies were the most critical factors (NHTSA 2008). Thus, one of the challenges before NHTSA's Office of Vehicle Safety is to ensure that vehicles retain their high levels of safety performance while finding ways to make vehicles more effective in countering many of the unsafe driver behaviors. The focus of this report is on automotive electronics. However, as indicated by these crash causation data, NHTSA faces many safety-related challenges (and accompanying demands on its resources) in addition to those associated with overseeing the safe performance of automotive electronics.

The committee was asked to advise NHTSA on how the regulatory, research, and defect investigation activities carried out by the Office of Vehicle Safety can be improved to meet the safety assurance demands of the increasingly electronics-intensive automobile. This chapter describes the key responsibilities and capabilities of the office. The committee was not asked to examine all responsibilities of the office, and it is not in a position to advise on the priority that should be given to such improvements relative to other program interests and associated resource demands. Nevertheless, it became evident to the committee that the Office of Vehicle Safety is highly optimistic that vehicle electronics will play an important role in mitigating risky driver behaviors. In this regard, the office's interest in promoting the introduction of these electronics systems is intertwined with its interest in ensuring that they and all other electronics systems in the vehicle perform their functions safely and reliably.

The next section starts with an overview of the Office of Vehicle Safety and then reviews its regulatory, research, and defect investigation

TABLE 4-1 Critical Precrash Event Attributed to Vehicles, Drivers, and Roadway and Atmospheric Conditions

	Number of Crashes in Sample		
Key Reason for Critical Precrash Event	*Unweighted*	*Nationally Weighted*	*Weighted Percentage*
Key Reasons for Critical Precrash Event Attributed to Vehicles			
Tires failed or degraded; wheels failed	56	19,320	43.3
Brakes failed or degraded	39	11,144	25.0
Other vehicle failure or deficiency	17	9,298	20.8
Steering, suspension, transmission, or engine failed	16	4,669	10.5
Unknown	2	212	0.5
Total in category	130	44,643	100
Key Reasons for Critical Precrash Event Attributed to Drivers			
Recognition error (e.g., distraction, inattention)	2,094	828,308	40.6
Decision error (e.g., too fast, illegal maneuver)	1,752	695,516	34.1
Performance error (e.g., panic, overcompensation)	510	210,143	10.3
Nonperformance error (sleep, medical problem)	369	145,844	7.1
Other or unknown driver error	371	162,132	7.9
Total in category	5,096	2,041,943	100
Key Reasons for Critical Precrash Event Attributed to Roadway and Atmospheric Conditions			
Roadway			
Slick roads (e.g., ice, debris)	58	26,350	49.6
View obstructions	19	6,107	11.6
Signs and signals	5	1,452	2.7
Road design	3	745	1.4
Other highway-related condition	9	5,190	9.8
Subtotal	94	39,844	75.2
Atmospheric conditions			
Fog, rain, or snow	11	2,338	4.4
Other weather-related condition	6	2,147	4.0
Glare	24	8,709	16.4
Subtotal	41	13,194	24.8
Total in category	135	53,038	100

Note: Sample of 5,471 crashes investigated from July 3, 2005, to December 31, 2007. The "critical reason" is the immediate reason for the critical precrash event and is often the last failure in the causal chain. Numbers may not add up to total because of independent rounding.

Source: NHTSA 2008, Tables 9(a), 9(b), and 9(c).

programs in greater depth, with emphasis on the applicability of these programs to ensuring safe vehicle electronics. Consideration is then given to how NHTSA's oversight of vehicle electronics safety through its regulatory, research, and defect investigation programs compares with aspects of federal oversight of the design and manufacture of aircraft and medical devices.

VEHICLE SAFETY PROGRAM OVERVIEW

In 1966, the federal government took on a central role in promoting highway safety across the nation by enactment of both the National Traffic and Motor Vehicle Safety Act and the Highway Safety Act. Congress delegated responsibility for administering the provisions of these acts to the U.S. Department of Transportation (DOT), which was created in the same year. The first act established a federal role in prescribing minimum safety standards for motor vehicles, enforcing compliance, and monitoring the safety performance of vehicles on the road, and it included authority to order manufacturer recalls for noncompliance and for safety defects. The act also authorized a federal role in motor vehicle and highway safety research. The second act established a federal program for granting funds to states for the development of highway safety programs, including those intended to affect driver behavior. Since its creation within the U.S. DOT in 1970, NHTSA has held the responsibilities for promulgating and enforcing the Federal Motor Vehicle Safety Standards (FMVSSs) and for the monitoring and remediation of vehicle safety defects. Along with the Federal Highway Administration, NHTSA has responsibility for administering the state highway safety grants program and for carrying out research to support these activities.

Administrative responsibility for the motor vehicle safety regulatory program and the state highway safety grant program is divided within NHTSA offices. The focus of this study is on the activities of the Office of Vehicle Safety, which has responsibility for the former program. That program includes development and enforcement of the FMVSSs and the conduct of vehicle safety research (as opposed to research in support of highway safety programs such as driver education and traffic enforcement).

An organization chart for the Office of Vehicle Safety is shown in Figure 4-1. The rulemaking division is responsible for development of the

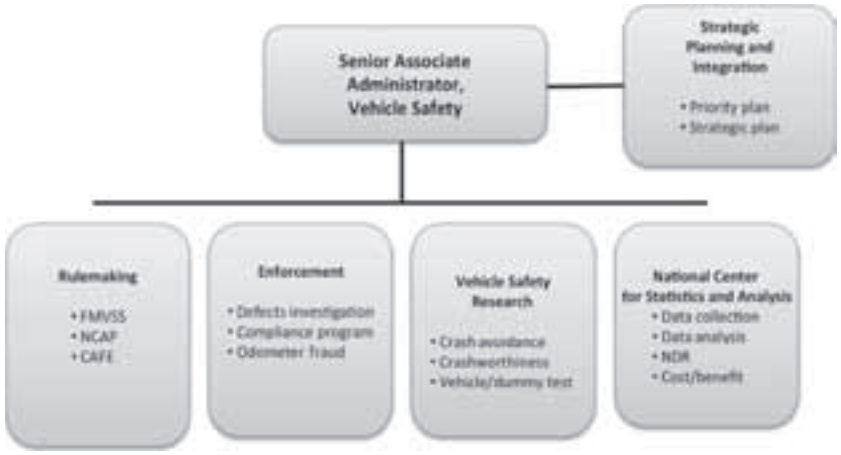


FIGURE 4-1 Organization chart, NHTSA's Office of Vehicle Safety (NDR = National Driver Register).

safety-related FMVSSs, as well as other activities such as the nonregulatory New Car Assessment Program (NCAP)[4] and the setting of corporate average fuel economy standards. The enforcement division includes the Office of Defects Investigation (ODI), which monitors for and investigates safety defects in the fleet, and the regulatory compliance program, which randomly tests vehicles in the marketplace for adherence to particular FMVSSs. The research division undertakes studies to inform and provide the basis for new safety regulations, including research on vehicle crashworthiness, human–vehicle performance, and advanced crash avoidance technologies.

Each of these three major programs is discussed below. Particular consideration is given to how they contribute to NHTSA's oversight and understanding of the safety opportunities and challenges arising from vehicle electronics. The other major division of the Office of Vehicle Safety, the National Center for Statistics and Analysis (NCSA), provides NHTSA with the information necessary for understanding

[4] In 1979, NHTSA created the NCAP to improve occupant safety by development of timely comparative safety information that encourages manufacturers to improve the safety of their vehicles voluntarily. Since that time, the agency added rating programs and offered information to consumers via the website, www.safercar.gov. The program is not regulatory but seeks to influence manufacturers to build vehicles that consistently achieve high ratings.

the nature and causes of traffic crashes nationally and for assessing agency regulatory activities. NCSA's activities, which include development of the National Motor Vehicle Crash Causation Survey (NMVCCS), are described in Box 4-1 but are not reviewed further in this chapter.

RULEMAKING

The FMVSSs are grouped into three main categories prescribing minimum vehicle capabilities for crash avoidance, crashworthiness, and postcrash integrity. The FMVSSs most pertinent to electronic vehicle control systems are the crash avoidance standards, since they cover vehicle capabilities and features such as braking, controls, and displays.

The FMVSSs covering crash avoidance are given in Table 4-2. These regulations, like all the FMVSSs, are written in terms of minimum safety performance requirements. Thus, the FMVSSs are intended to be design and technology neutral out of recognition that automotive technologies change over time and vary across manufacturers. The emphasis on prescribing performance, as opposed to specifying designs and interfaces, also has the advantage of making the FMVSSs more durable. This attribute can be especially important in view of the difficulty of amending federal regulations. The promulgation of the FMVSSs, like all federal regulations, is governed by federal rulemaking cost-effectiveness and procedural requirements[5] and by NHTSA's own statutory requirements that rules be practicable, meet a specific need for motor vehicle safety, and be stated in objective terms. Under these circumstances, the need to make frequent revisions to standards to accommodate changes in technology could inhibit innovation and prove difficult to administer.

FMVSS 124 offers an example of how and why the FMVSSs are performance oriented. The standard states that a vehicle's throttle must be capable of returning to the idle position when the driver removes the actuating force from the accelerator control mechanism and when there is a disconnection between this control mechanism and the throttle. The standard does not define how the connection should be made or how the capability to return to idle should be established. When the standard was promulgated 40 years ago, the connections were mechanical and included springs on the throttle plate to return it to idle. The chronology of FMVSS 124, as shown in Box 4-2, illustrates the challenge that NHTSA faces in

[5] The Administrative Procedure Act and executive orders governing cost-effectiveness assessment.

BOX 4-1

Overview of NCSA

NCSA supports NHTSA rulemaking and research programs by monitoring the magnitude of the traffic safety problem; seeking to understand the factors that influence highway safety; performing crash investigations; and collecting and analyzing incident data, including crash reports from state and local authorities. Some of these data are intended to be comprehensive, such as the Fatality Analysis Reporting System (FARS), and others are sample-based, such as the National Automotive Sampling System General Estimates System (NASS GES), the NASS Crashworthiness Data System (NASS CDS), and the more detailed Special Crash Investigations (SCI). FARS is a census of fatal crashes on public roads and contains information about various crash characteristics as obtained from police reports and augmented by examination of additional driver record and vehicle information. NASS GES has information for a stratified sample of police-reported crashes, allowing the agency to describe the general characteristics and incidence of motor vehicle crashes in the United States. NASS CDS also contains data on a stratified random sample of police-reported crashes. However, the number of cases is much smaller, and the police-reported data are augmented by in-depth investigations that attempt to reconstruct the critical factors leading to the presence or absence of injuries in the crash. SCI cases, like NASS CDS cases, include more in-depth investigations of the crashes but are selected not through a random sample but to help the agency develop scientific understanding of new or interesting vehicle technologies or high-profile crashes. For example, rarely occurring events like unintended acceleration are not adequately represented in standard databases. NCSA may conduct special investigations of episodes or crashes linked with such factors (as it has for unintended acceleration; see the discussion in Chapter 5). NCSA also periodically performs special studies that can inform rulemaking and other NHTSA activities such as the

(continued on next page)

Box 4-1 (*continued*) Overview of NCSA

NMVCCS,[1] which is a nationally representative survey of crashes providing information on the contribution of precrash human factors, vehicle factors, and environmental factors related to crashes. In the most recent NMVCCS, investigators interviewed drivers and witnesses, visited the crash location to examine the physical evidence, and inspected the vehicle and extracted information from the event data recorder if one was available.

[1]http://www-nrd.nhtsa.dot.gov/Pubs/811059.PDF.

TABLE 4-2 FMVSSs for Crash Avoidance

Standard No.	*Name*
101	Controls and Displays
102	Transmission Shift Lever Sequence, Starter Interlock, and Transmission Braking Effect
103	Windshield Defrosting and Defogging Systems
104	Windshield Wiping and Washing Systems
105	Hydraulic and Electric Brake Systems
106	Brake Hoses
108	Lamps, Reflective Devices, and Associated Equipment
109	New Pneumatic Tires for Passenger Cars
110	Tire Selection and Rims for Passenger Cars
111	Rearview Mirrors
113	Hood Latch System
114	Theft Protection and Rollaway Prevention
116	Motor Vehicle Brake Fluids
117	Retreaded Pneumatic Tires
118	Power-Operated Window, Partition, and Roof Panel Systems
119	New Pneumatic Tires for Vehicles Other Than Passenger Cars
120	Tire Selection and Rims for Motor Vehicles Other Than Passenger Cars
121	Air Brake Systems
122	Motorcycle Brake Systems
123	Motorcycle Controls and Displays
124	Accelerator Control Systems
125	Warning Devices
129	New Non-Pneumatic Tires for Passenger Cars—New Temporary Spare Non-Pneumatic Tires for Use on Passenger Cars
131	School Bus Pedestrian Safety Devices
135	Light Vehicle Brake Systems

BOX 4-2

Chronology of Major Activities for FMVSS 124, Accelerator Control Systems

Notice of Proposed Rulemaking (NPRM)
September 30, 1970, 35 *Federal Register* 15241
Proposed rule states that accelerator control system and automatic speed control systems (ASCs) would be required to have at least two independent energy sources (such as springs), each capable of returning the engine to idle on release of the actuating force. One of those energy sources must be able to return the engine to idle in case of disconnection of any element of the system. A design requirement of ASCs would be their deliberate activation by the driver. ASCs must also be capable of automatic deactivation when the driver takes certain actions, such as pushing on the brake. In addition, ASCs must automatically deactivate once specified failure modes occur.

Proposed effective date: October 1, 1972.

Final Rule
April 8, 1972, 37 *Federal Register* 7097
The final rule retains the proposed two independent energy sources. In the NPRM, the return to idle only had to occur when the actuating force was removed. In the final rule, in the case of a failure in the system, the engine must return to idle at the time of the failure (such as breakage) or removal of the actuating force. The final rule dropped coverage of ASCs because the agency could not find crashes caused by the ASC and manufacturers were found to be following Society of Automotive Engineers guidelines for those systems. On issuance of the final rule, NHTSA also issued an NPRM on the time required for the engine to return to idle.

NPRM
April 8, 1972, 37 *Federal Register* 7108
Proposal would add a ½-second limit in which the engine must return to idle once the actuating force is removed or a system failure occurs.

(continued on next page)

Box 4-2 (*continued*) Chronology of Major Activities for FMVSS 124, Accelerator Control Systems

Response to Petitions to Reconsideration and Final Rule on time limit
September 23, 1972, 37 *Federal Register* 20033
Notice amends the standard to set a time limit for the system to return to idle. Under conditions of extreme cold (ambient air of 0°F or colder), the system is allowed 3 seconds to return to idle. At temperatures above 0°F, the maximum allowable return to idle time is reduced to 2 seconds for vehicles with a gross vehicle weight rating (GVWR) exceeding 10,000 pounds and to 1 second for all vehicles with a GVWR of 10,000 pounds or less.

Request for comments
December 4, 1995, 60 *Federal Register* 62061
NHTSA noted that the original standard was issued when only mechanical systems were commonly used in vehicles. The agency set out a series of questions to help it make a decision on amending the standard to address electronic accelerator control systems. NHTSA said that while it has attempted to address the issue of electronic accelerator control systems through interpretation letters, the volume of requests has continued. To address this issue, the agency indicated that "instead of answering these questions by drawing analogies between traditional mechanical components and new electronic systems, it amended the Standard to include provisions and language specifically tailored to electronic systems."

The agency identified the following failure modes of electronics systems and asked for comments on whether any other modes warranted consideration: the mechanical linkage and return springs between the pedal and the accelerator position sensor (APS); the electrical connections between the APS and the engine control processor; the electrical connections between the engine control processor and fuel or air metering devices that determine engine speed; power to the engine control processor; the APS and critical sensor; and the integrity of the engine control processor, APS, and other critical sensors.

Box 4-2 (*continued*) Chronology of Major Activities for FMVSS 124, Accelerator Control Systems

Public Technical Workshop
May 20, 1997
NHTSA held a workshop with participants from the Truck Manufacturers Association and the American Automobile Manufacturers Association to discuss how electronics systems work and how to apply FMVSS 124 to these systems. Both organizations "emphasized that there had been no safety-related developments concerning electronic accelerator controls to justify applying Standard No. 124 to such systems."

NPRM on electronic control systems
July 23, 2002, 67 *Federal Register* 48117
NHTSA reported that "where the present standard applies only to single-point severances or disconnections such as the disconnection of one end of a throttle cable, the proposed standard also is limited to single-point severances and disconnections such as unhooking one electrical connector or cutting a conductor at one location. The proposal does not attempt to make the requirements more stringent by requiring fail-safe performance when multiple severances or disconnections occur simultaneously." NHTSA also proposed several new test procedures, one of which would measure the engine speed under different load on a chassis dynamometer. NHTSA commented that this particular test was "technology-neutral" and could be used instead of other proposed tests. The other procedures were technology-specific. One was essentially the air throttle plate position test of the existing standard. Another was measurement of fuel flow rate in diesel engines, and the other was measuring input current to a drive motor, such as would be found in an electric vehicle.

Withdrawal of Proposed Electronic Rule
November 10, 2004, 69 *Federal Register* 65126
NHTSA indicated that it was withdrawing its proposal "while it conducts further research on issues relating to chassis dynamometer-based test procedures for accelerator controls."

(continued on next page)

Box 4-2 (*continued*) Chronology of Major Activities for FMVSS 124, Accelerator Control Systems

2011–2013 Vehicle Safety and Fuel Economy Rulemaking and Research Priority Plan
March 2011
NHTSA indicated that it is considering updating the accelerator control standard (FMVSS 124) by adding test procedures for vehicles with electronically controlled throttles and requiring a brake–throttle override system on some vehicles.

trying to write or amend rules to address major technological changes—in this case the advent of electronic throttle control systems (ETCs) to replace the long-standing mechanical control mechanisms.

In 1995, when automotive manufacturers began designing ETCs, NHTSA published a notice in the *Federal Register* posing a series of questions to help it determine whether amendments to the original standard were warranted to take into account the imminent introduction of ETCs. Manufacturers had repeatedly asked NHTSA for interpretations of FMVSS 124 to accommodate the design of compliant ETCs. NHTSA considered whether a change in the rule was needed to clarify the performance and testing criteria, partly to satisfy manufacturers but also to ensure that potential safety issues associated with this new form of throttle control were fully vetted. NHTSA had difficulty in revising the rule in ways that would accommodate all technological variability, and the agency eventually elected to withdraw all proposed changes to the regulation. Therefore, FMVSS 124 remains essentially unchanged since its creation 40 years ago. NHTSA simply interprets a "disconnection" to cover not only separations in cables and other physical linkages but also separations of electrical connectors and conductors linking the accelerator pedal with the engine control unit and the control unit with the throttle actuator.[6]

NHTSA does not know how an FMVSS performance requirement will ultimately be met through alternative product designs, materials, and technologies. Therefore, the agency is not in a position to demand that manufacturers use specific tests on their products, such as for corrosion

[6] Information provided to the committee in briefing by Nathaniel Beuse, Chief, Crash Avoidance Standards, NHTSA, June 30, 2010.

resistance, electromagnetic compatibility, or resistance to cracking. An FMVSS-required performance test for a penetration-resistant windshield, for example, can be specific in defining the impact forces and testing methods that must be used in demonstrating compliance. However, the rule does not specify the treatments that must be used or how the manufacturer should test for resistance to aging, temperature extremes, and other product properties. As explained in Chapter 3, the agency leaves these decisions to the automotive manufacturers, whose products are nevertheless required to be safe. A vehicle that complies with all FMVSSs may still contain a safety-related defect and be subject to a NHTSA-ordered recall. For example, if a compliant windshield is found to shatter spontaneously in significant numbers from extreme summer heat, NHTSA may consider this to be a safety defect and order a recall.

In the same vein, manufacturers are not required to apply for approval from NHTSA when they introduce a new vehicle system or component pertinent to an FMVSS. The manufacturer may request interpretations of the performance standard as it relates to a new technology or design, as occurred in the case of the ETC. However, NHTSA does not examine each product design and certify regulatory compliance. Automotive manufacturers are required to self-certify that their vehicles are in full compliance with the regulatory provisions when they deliver each vehicle to the dealer for sale to the public. NHTSA has various means by which it monitors and enforces adherence, which are discussed next, but compliance rests substantially on the diligence of the manufacturer.

ENFORCEMENT AND DEFECT INVESTIGATION

Complaint monitoring and investigation are the main means by which the Office of Vehicle Safety ensures that vehicles in the fleet are free of safety defects. This function is performed through ODI.

Defect Surveillance and Assessment

ODI's Defects Assessment Division, which consists of a staff of nine screeners and analysts,[7] is responsible for monitoring the fleet for vehicle safety defects. It does this primarily through screening of safety-related

[7] NHTSA informed the committee that the defect assessment staff consists of four mechanical engineers, one electrical engineer, one chemical engineer, and three automotive specialists with expertise obtained from working in the automobile industry.

data submitted by manufacturers [Early Warning Reporting (EWR) system discussed below], the technical service bulletins issued by manufacturers, and consumer complaints submitted through an online or hotline Vehicle Owner's Questionnaire (VOQ).[8]

The VOQs are especially important to this process. ODI informed the committee that the Defects Assessment Division screens more than 30,000 VOQs each year. The complaints are stored in a database that is available (in redacted form) to the public but are reviewed individually by screeners as they are submitted. As discussed below, the complaints vary in detail but are intended to contain information on the complainant, information on the identity of the vehicle, and a description of the event and the vehicle behavior conveyed in a narrative section by the motorist. On the basis of the professional judgment of the screeners and analysts, the vehicle owner may be contacted for more detailed information on the nature and sequence of the event, police reports, and the vehicle's repair records and history of symptoms.

According to ODI, its defect assessment analysts depend on the VOQ narratives and any follow-up interviews to gather much of the critical information about the episode, vehicle conditions and behaviors, and possible causes.[9] Analysts must use their professional judgment to make decisions about the existence of a safety hazard. They consider whether a trend can be discerned, such as in complaints involving issues closely spaced in time, similar consequences (fires, crashes, injuries), and similar circumstances (e.g., during parking, highway travel, low-speed driving). Consideration is also given to whether ODI has a history of complaints involving similar conditions and behaviors. Box 4-3 lists the types of questions that analysts raise when they conduct a defect assessment—in this case when they examine complaints involving forms of unintended acceleration.

Because the VOQ database is available to the public online, consumers may also review all complaints and file a petition with ODI to investigate a suspect defect trend or pattern. In such cases, ODI may open an inquiry to assess the merits of undertaking a defect investigation. Examples of inquiries involving concerns about unintended acceleration in Toyota vehicles are provided in Chapter 5 (see Table 5-1). Usually these

[8] According to ODI, more than 90 percent of consumer complaints are submitted online (56 percent) or through a telephone hotline (37 percent).

[9] Briefing by Gregory Magno, Defects Assessment Division Chief, ODI, October 12, 2010.

BOX 4-3

Example Questions Asked by ODI Investigators of Unintended Acceleration Cases

Throttle Questions

Did the engine power increase from idle or did it fail to decrease after the accelerator pedal was released?
Engine power level (high or low, fixed or changing)?
Duration (short surge or sustained increase)?
Initiation speed?
Environmental conditions (ambient temperature, moisture)?
Engine conditions (cold or warm)?
Cruise control status?
What equipment was being operated?
Postincident inspection or repairs of throttle system?
Throttle system service history?

Brake Questions

What was the vehicle response to brake application?
Did the engine power increase begin when the brake was applied? Did the engine power change with braking force?
Did the engine power change after brake release (in "P" or "N")?
Was the brake system inspected after the incident? Were any problems found?
Did the brake components display signs of overheating?
Did the driver apply the brake pedal more than once during the event?
Were there any brake system service issues before or after the incident?

Source: Briefing by Jeffrey Quandt, Vehicle Control Division Chief, ODI, October 12, 2010.

inquiries include an examination of complaint rates for the subject vehicle and comparisons with peer vehicles as well as follow-up interviews with and surveys of complainants.

One simple means of sorting the VOQs is by the vehicle component code that the motorist assigns as being the suspected source of the defect. The motorist can choose from more than two dozen component codes such as service brakes, electrical system, power train, fuel system, steering, tires, and vehicle speed control. However, sorting by these codes to identify complaint rates is unreliable for many vehicle behaviors and conditions, since the code selections depend on the judgment of the vehicle's owner with regard to the component involved in the event. As discussed in the next chapter, for example, unintended acceleration could be categorized under the code for the service brake, speed control, power train, or a number of other components. Similarly, conditions that have little to do with unintended acceleration, such as stalling or hesitation due to transmission problems, may be categorized under the code vehicle speed control. Accordingly, ODI analysts do not routinely sort complaints on component codes when they assess complaints for suspect defects. Instead, they review the consumer narrative section, since it can convey more information on vehicle behaviors, conditions, and event circumstances.

Another source of data available to ODI for defect surveillance is the EWR system. Automotive manufacturers are required by the 2000 Transportation Recall Enhancement, Accountability, and Documentation (TREAD) Act to provide NHTSA with reports, mostly on a quarterly basis, of vehicle production counts, warranty claims, consumer complaints, dealer and nondealer field reports, property damage claims, and fatality and injury claims and notices. The TREAD Act also expanded NHTSA's staffing and budgetary resources and called for improvements in ODI's computer systems to make use of the newly required early warning data.

ODI analysts explained to the committee that they use various methods to filter and analyze these aggregated data to identify high counts and high rates, increasing trends, and outliers.[10] Analysts sort some of the data, such as the warranty claims, by the same component codes as contained in the VOQ. As in the case of the VOQs, two dozen component codes can lack the specificity needed to identify defect trends. If the

[10] Briefing to the committee by Christina Morgan, EWR Division Chief, October 12, 2010.

vehicle behavior is not the result of a clearly identifiable component defect, the EWR data may not be helpful in alerting ODI to the problem's occurrence.

In briefings to the committee, ODI analysts noted that the EWR data lack the detail needed to be the primary source for monitoring the fleet for safety defects and that the main use of these data (especially the field reports) has been to support defect monitoring and investigations by supplementing traditional ODI data.[11]

Defect Investigations

ODI's investigative unit consists of specialists in crash avoidance, crashworthiness, and heavy-vehicle (truck and bus) defects. The specialists are usually asked to initiate an investigation in response to a referral from the Defects Assessment Division. These investigations typically consist of two phases. The first is a preliminary evaluation, and the second is an engineering analysis. During the preliminary phase, investigators send an information request letter to the manufacturer to obtain data on complaints, crashes, injuries, warranty claims, modifications, part sales, and service bulletins. The manufacturer can present its views with regard to the suspected defect in a response to the letter. Preliminary evaluations are expected to be completed within three months of the date they are opened. A preliminary evaluation may be closed on the basis of a determination that a more in-depth investigation is not warranted or because the manufacturer has decided to conduct a recall in response.

If a recall is not forthcoming and investigators believe that further analysis is warranted, the preliminary evaluation is upgraded to an engineering analysis, during which ODI investigators conduct a more detailed analysis of the nature and scope of the suspected defect. Although investigators consult the information collected during the preliminary evaluation, such as analyses of VOQs and EWR data, they usually require more detailed supplemental information. They obtain it through inspections, tests, surveys, and additional information from the manufacturer and suppliers, such as returned parts, parts sales data, information on design changes, and more details on warranty claims. Engineering analyses may involve the examination of specific vehicles, but ODI informed the committee that it does not have the staffing or resources to examine

[11] Briefing to the committee by Christina Morgan, EWR Division Chief, October 12, 2010.

large numbers of vehicles or conduct full crash investigations.[12] ODI may therefore seek assistance from NCSA's Special Crash Investigations unit. ODI can also use the Vehicle Research and Test Center for testing and engineering analysis if a preliminary evaluation has not resolved the concern raised by the complaints. More examples of how these resources were deployed to investigate concerns about unintended acceleration and the possibility of electronics vulnerabilities are given in Chapter 5.

If investigators conclude that the evidence indicates the existence of a safety-related defect, they prepare a briefing for a multidisciplinary review panel (a panel of experts from throughout the agency) for critical assessment. ODI evaluates the recommendations of the panel and decides whether to send a recall request letter to the manufacturers. Manufacturers rarely let a situation progress to this point. A recent report (GAO 2011) indicated that since 2000 not a single recall has been ordered by NHTSA for passenger cars; manufacturers have undertaken recalls voluntarily, either in advance of a NHTSA investigation or in response to an ongoing one, long before issuance of a recall request letter. Under the law,[13] ODI may require a manufacturer to conduct a recall only if the agency can establish that a defect exists and is "related to motor vehicle safety." To demonstrate the existence of a defect, ODI must be able to show the potential for a significant number of failures. To establish that the defect pertains to safety, ODI must be able to show that the defect presents an unreasonable risk of a crash, injury, or death. According to ODI, one of the main challenges investigators face in ordering a recall is in proving a safety defect's existence when the defect has yet to exhibit a safety consequence. Therefore, establishing legal proof of defect can be challenging, and ODI's "influencing" of voluntary recalls—which is the norm—is viewed as permitting a more effective and practical enforcement program.

Box 4-4 gives an example of a recent ODI investigation of an electronics system exhibiting a defect. The number of complaints received, the warranty claims data consulted, and the types of testing undertaken by ODI are shown. In this case, the manufacturer issued a voluntary recall that was influenced by the ODI investigation.

[12] Information submission by NHTSA to committee on December 7, 2010.
[13] Chapter 301, Title 49, United States Code.

BOX 4-4

Example of an ODI Electronics Investigation and Recall

Investigation: EA09-002 *Manufacturer recall*: 10V-172

Alleged defect

Electronic stability control malfunction
Fretting corrosion of steering wheel position sensor connector

Safety consequences

Inappropriate electronic stability control activation
Inappropriate braking with no brake lights
Risk of lane departure from braking "pull"

Vehicle population: 40,028
Complaints: 58
Crashes: 4
Warranty claims: 2,424 (steering wheel position sensor connector repairs)

Testing to simulate fault condition

Fault detection normally occurs in less than 1 second (electronic stability control deactivated)
Fault injection produced range of sensor voltages where fault detection may be delayed by several seconds

Source: Briefing by Jeffrey Quandt, Vehicle Control Division Chief, ODI, October 10, 2010.

Recall Monitoring

ODI's Recall Management Division oversees recalls to ensure compliance with statutory and regulatory requirements and to track progress in implementing defects remedies. Manufacturers are required to describe the population of vehicles subject to the recall, the nature of the defect and its consequences (e.g., number of reported accidents, injuries, fatalities, and warranty claims), and the remedial actions planned as part of

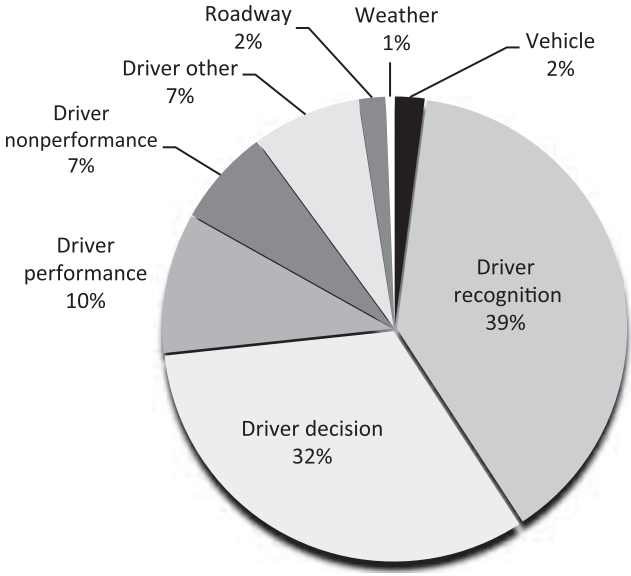


FIGURE 4-2 Key reasons for critical precrash event, percent share by the vehicle, driver, roadway, and weather. See Table 4-1 for data.
(*Source:* NHTSA 2008.)

the recall campaign. Manufacturers are required to furnish a chronological summary of all the principal events that were the basis for the determination of the defect to the Recall Management Division. NHTSA is required to approve the recall plan, and the agency imposes fines on manufacturers for violations of requirements relating to the recall process, including defect notification and campaign timeliness.[14]

VEHICLE SAFETY RESEARCH

Figure 4-2 shows NMVCCS estimates of the share of all crashes for which the critical precrash event can be attributed to the vehicle, the driver, the roadway, and weather conditions. The figure shows the dominant influ-

[14] For example, in 2010, the agency twice imposed the maximum penalty of $16.375 million on Toyota for failing to notify the agency of defects involving accelerator pedals in a timely manner.

ence of the driver on traffic safety. Although vehicle, weather, and roadway factors are often contributing factors to crashes, they are the critical reason for a crash only 5 percent of the time, as determined by NHTSA.

From the standpoint of NHTSA's research programs, the large proportion of crashes attributed to driver errors is grounds for focusing research and development on technological (including vehicle-based) and nontechnological means of improving driving safety performance. The former is the responsibility of NHTSA's Office of Vehicle Safety Research (OVSR), which has a budget of about $33 million annually for research on vehicle safety systems (e.g., occupant restraint and protection) (about $8 million), biomechanics (about $11 million), heavy-duty vehicles (about $2 million), alternative fuel safety (about $4 million), and crash avoidance (about $8 million).

Crash avoidance technologies in particular are viewed as a promising means of mitigating driver errors, and OVSR conducts research to evaluate the developmental status and effectiveness of these technologies and how drivers are likely to use and respond to them. Crash avoidance research includes the following:

- Evaluations of human factors issues, such as the best way for vehicle-based safety systems to provide hazard notifications and warnings to drivers, modify unsafe driving behaviors (e.g., distraction and alcohol impairment), and mitigate unintended side effects on drivers (e.g., ensure that systems do not lead to a loss of driver vigilance or situation awareness);
- Development of methodologies for estimating the potential safety benefits of existing and emerging crash avoidance technologies, such as those that increase driver awareness and vehicle visibility, decrease alcohol involvement in crashes, and decrease intersection collisions and rollovers;
- Development of performance standards and tests for technology-based crash avoidance capabilities, including support for the agency's considerations of FMVSS rulemakings to require certain capabilities in vehicles (e.g., performance standards and tests for electronic stability control); and
- Monitoring of the state of technology development of emerging and more advanced (or "intelligent") technologies for driving assistance (warning and control systems), driver monitoring, and vehicle-to-

vehicle communications. What technologies are becoming available? In what situations do they promise to work? What is their potential safety effectiveness?

Some of these research activities are performed by outside contractors, and others are conducted and administered by research personnel at the Vehicle Research and Test Center. According to committee briefings from OVSR, much of the research is performed in collaboration with research institutes, universities, automotive manufacturers, and other U.S. DOT agencies such as the Research and Innovative Technology Administration and the Federal Highway Administration. One example of such collaboration, as described by OVSR to the committee, is a research activity being undertaken by NHTSA in cooperation with the Automotive Coalition for Traffic Safety (which includes automotive manufacturers). This multiyear research program, known as the Driver Alcohol Detection System for Safety Program, is intended to develop and test prototypes of noninvasive technologies for measuring driver blood alcohol levels.[15] NHTSA described these efforts as intended to support a nonregulatory, market-based approach for preventing crashes caused by drunk driving.

According to OVSR, crash avoidance research activities are "data driven." They are intended to be guided by where the agency's crash database indicates that research can be helpful in mitigating safety problems, such as drunk driving, rear-end collisions, and unsafe lane changes, as well as other concerns pertaining to vulnerable populations such as children and the elderly. The intent of the research planning is to prioritize resource allocations on the basis of the potential for realizing reductions in traffic fatalities and injuries. Allocations are also affected by programmatic requirements (e.g., responsibility for heavy-duty vehicle and alternative energy safety research) and events that may arise and warrant immediate research attention (e.g., unintended acceleration concerns). Because of the emphasis on research results that can be applied to known safety problems, much of the program's research is designed to support agency decisions such as whether and how to promulgate a performance-oriented FMVSS mandating a vehicle safety capability made possible by advancements in vehicle technology.

[15] For more information on the Driver Alcohol Detection System for Safety Program, see http://www.nhtsa.gov/DOT/NHTSA/NVS/Public%20Meetings/Presentations/2010%20Meetings/HyundaiDADSS.pdf.

Mostly through the activities and facilities of the Vehicle Research and Test Center, OVSR also provides engineering analysis and testing support for ODI's surveillance and investigation activities. For the most part, however, this research activity consists of testing and engineering analyses of suspected defects in vehicles in response to a request by ODI investigators. NHTSA officials informed the committee that OVSR does not conduct significant research in areas such as fail-safe and diagnostic strategies, software design and validation, or cybersecurity.

During committee briefings, OVSR presented a framework for how it sees its research helping NHTSA achieve the agency's dual mission of reducing the incidence and severity of motor vehicle crashes and ensuring that vehicles perform safely. The framework, shown in Figure 4-3, divides agency research activities into the traditional crash avoidance and crashworthiness stages and further divides them into the "normal driving," "crash imminent," "crash event," and "postcrash" phases. Examples of NHTSA research to further the role of electronics systems in each of these four crash phases are given. Missing from these listed activities, as acknowledged by OVSR, is research to address the safety assurance challenges that these advanced systems may present. As shown in the bottom shaded rows of Figure 4-3, OVSR is beginning to venture into these research areas, particularly in view of the emphasis placed by the agency on electronics systems as possible solutions to traffic safety problems.

In the next section, the strategic and priority planning activities of OVSR are described. Through these activities, OVSR will presumably make determinations about whether it should devote more

Crash Avoidance		**Crashworthiness**	
Normal Driving	**Crash Imminent**	**Crash Event**	**Postcrash**
Driver distraction	Forward crash avoidance	Adaptive restraints	Crash notification
Alcohol detection	Lane-departure warning	Child side impact	Event data recorders
Driver support systems	Crash-imminent braking	Oblique offset/frontal	Advanced crash notification
Drowsy driver detection	Lane-keeping		
Blind spot surveillance	Vehicle-to-vehicle, vehicle-to-infrastructure		
	Advanced air bags		
New Topics			
Fail-safe strategies		**Advanced event data recorders**	
Software reliability			
Fault detection and diagnosis methods			

FIGURE 4-3 NHTSA vehicle safety research topics.

research attention to the safety assurance needs of the electronics-intensive vehicle.

STRATEGIC AND PRIORITY PLANNING FOR RESEARCH AND RULEMAKING

The purpose of NHTSA's most recent *Vehicle Safety and Fuel Economy Rulemaking and Research Priority Plan* (NHTSA 2011), according to the agency, is to describe the projects that the agency intends to work on in the rulemaking and research areas that are priorities or that will take significant agency resources. The document is intended not only to be an internal management tool but also to communicate NHTSA's highest priorities to the public. It lays out the rationale for why the identified projects are considered priorities. Emphasis is given to their relevance to specific safety problems as identified from analyses of crash data. The plan states that the priorities are based on their potential for large safety benefits. Priority is also given to projects that can address special safety hazards, such as those related to vulnerable populations (for example, children and the elderly). The plan acknowledges that Congress and the White House may request that the agency address other areas, which can affect priorities during the planning time frame.

An important element of the plan is that all identified projects, including research initiatives, be accompanied by a time frame for a decision. For example, projects in the research stage are noted with milestones indicating when NHTSA expects to decide whether the initiative is ready to move from the research to the rulemaking stage. The emphasis on agency decision making, particularly for research, reflects the focus of the agency's vehicle safety research program on supporting specific rulemaking initiatives.

The plan lists a number of projects for evaluating electronics systems as countermeasures for problems such as rear-end collisions, lane departures, and blind spot detection. Several other projects relevant to electronics safety assurance are as follows:

- Event data recorder requirement—plans for a proposed rulemaking to mandate the installation of event data recorders on all light-duty vehicles and a proposal to consider enhancements to their capabilities and applicability;

- Update of FMVSS 124 on accelerator control—revision of the test procedure for vehicles with ETCs and the addition of systems that would override the throttle on application of the brake; and
- Update of FMVSS 114 pertaining to keyless ignitions—revision of the standard to consider ways of ensuring the ability of drivers to turn off the engine in the event of an on-road emergency.[16]

These three priorities, as well as planned research to examine pedal placement and spacing, appear to have resulted from the recent experience with unintended acceleration, for reasons discussed further in Chapter 5.

The earlier discussion of NHTSA's vehicle safety research programs noted that the agency is considering whether to support research to inform the automotive industry's efforts to address cybersecurity and improve fail-safe and fault detection strategies for complex vehicle electronics. The priority plan does not list these areas as candidates for agency research. Whether such research, if undertaken, would be viewed as supporting prospective regulatory decisions was not made clear to the committee. NHTSA regulations in these areas, however, would be unprecedented, as pointed out earlier.

The plan does not communicate strategic decisions, such as whether consideration is being given to changes in the agency's regulatory approach in response to the safety challenges associated with vehicle electronics. However, as noted at the outset of the plan, "NHTSA is also currently in the process of developing a longer-term motor vehicle safety strategic plan that would encompass the period 2014 to 2020" (NHTSA 2011, 1). While this planning effort may be where such decisions will be made, no additional details on its purpose or progress were offered by NHTSA officials during the course of this study.

SAFETY ASSURANCE AND OVERSIGHT IN OTHER INDUSTRIES

NHTSA's vehicle safety activities represent one approach to overseeing the safety of a transportation activity and vehicle. Within the U.S. DOT, several agencies have transportation safety regulatory and oversight

[16] On December 12, 2011, NHTSA issued a Notice of Proposed Rulemaking to address safety issues arising from keyless ignition controls and their operation (Docket No. NHTSA-2011-0174). *Federal Register,* Vol. 76, No. 238.

responsibilities and differ in how they implement them. Among such agencies are the Federal Railroad Administration, the Federal Motor Carrier Safety Administration, and the Federal Aviation Administration (FAA). FAA's approach in overseeing the design and production of aircraft is reviewed briefly, since this transportation industry—perhaps more than any other—is highly safety conscious and technologically complex. In addition, consideration is given to a regulatory and oversight approach from outside the transportation sector by reviewing aspects of the Food and Drug Administration's (FDA's) safety responsibility for medical devices. Although in-depth reviews are not provided, the comparisons make the earlier distinctions about NHTSA's regulatory and defect surveillance approach more concrete.

FAA and Aircraft Safety

In developing its airframe and engine airworthiness regulations,[17] FAA is authorized by law to set minimum standards for the design, materials, construction, quality of work, and performance of aircraft and their engines. Despite its legal authority to prescribe the details of product design and construction, FAA has elected to place greater emphasis on ensuring that aviation equipment performs safely rather than on establishing specific design and construction standards for products. In this important respect, the FAA regulations are comparable with the performance-oriented FMVSSs promulgated by NHTSA—the details of the design and development process are left to the manufacturer. In many other respects, the scope and depth of the regulatory roles of FAA and NHTSA differ significantly. These differences have many origins, not the least of which is the fact that aircraft are far more expensive to develop and build than automobiles and their systems must maintain airworthiness and operability in flight.[18]

Aircraft manufacturers must apply to FAA for approval and certification to develop and build a new aircraft type. In contrast, automotive manufacturers do not need approval from NHTSA to develop and build a new type of automobile. FAA's certification process covers all product development phases, from initial planning to flight testing. Each manufacturer applicant must present a certification plan that sets out the safety

[17] 14 CFR Parts 21 through 49.

[18] For example, in the event of a fault, aircraft, unlike automobiles, cannot implement fail-safe defenses that shut down the engines in flight. Thus, they require extensive redundancy and preventive measures for faults in safety-critical systems.

assurance processes it will use through all development and production stages, including specification of procedures for hazard assessment, safety analysis, testing, inspection, design change proposal, hardware and software development and integration, and manufacturing quality control. On receipt of the application, FAA exercises a prominent role in the approval of these plans: FAA must review and approve the safety assurance plans before the applicant can even proceed to the next phase of product development. Even at the final stages of aircraft and engine development, FAA must approve the battery of tests and evaluations that are conducted in preparation for the aircraft or engine to be placed in service. Before it grants certification, FAA audits all of the procedures followed by the manufacturer as well as the results of tests.

Although FAA reviews manufacturer safety assurance plans and processes intensely, the burden of proving the soundness of the safety assurance system is on the manufacturer. To facilitate compliance, FAA advises manufacturers to follow certain preapproved processes for product development. In particular, the agency publishes advisory circulars (ACs) that define acceptable means of conforming to specific airworthiness regulations. For example, one AC (AC 25.1309-1 draft) establishes the means by which manufacturers are to determine the levels of risk tolerance for various functional capabilities of the aircraft. Manufacturers are advised to designate design assurance levels (DALs) for their safety-critical systems, not unlike the automotive safety integrity levels prescribed in ISO 26262 for automotive electronics systems as explained in Chapter 3. Manufacturers are thus expected to implement safety assurance measures compatible with the DAL for each system. FAA does not specify how applicants must conduct DAL classifications, but it advises on the use of specific industry-developed standards (e.g., SAE ARP4754 and ARP4761) for analytic rigor and requires manufacturers to demonstrate the use of rigorous analytic processes (e.g., failure mode and effects analyses and fault tree analyses, both of which are discussed in Chapter 3). Specifically with respect to safety-critical software, FAA advises manufacturers to follow the industry-developed standard RTCA-178B, which prescribes steps to be followed during software development.[19] Aircraft and engine manufacturers are not compelled to follow the standards

[19] The Radio Technical Commission for Aeronautics is a federal advisory committee. Its participants come from industry and academia. Box 3-3 in Chapter 3 provides more information on software development standards for functional safety.

referenced in ACs, but FAA's demanding requirements for the approval of alternative processes mean that the aviation industry almost universally subscribes to the processes preapproved in circulars.[20]

FAA's hands-on approach to safety oversight can make fulfillment of its requirements costly and time-consuming. Although FAA designates senior engineers from manufacturers to carry out many of the detailed document reviews and inspections that make up the certification process, FAA staff must review the most significant process elements. FAA has a major unit, the Aircraft Certification Service, dedicated to this function and housed in more than two dozen offices across the country and abroad. Although FAA issues a handful of new aircraft-type certificates per year, the Aircraft Certification Service requires a large cadre of test pilots, manufacturing inspectors, safety engineers, and technical specialists in key disciplines such as flight loads, nondestructive evaluation, flight management, and human factors.

FDA and Class III Medical Devices

Manufacturers of the most safety-critical (Class III) medical devices must receive approval from FDA before the devices can be marketed for public use.[21] FDA's and NHTSA's safety oversight processes are comparable in that they combine safety requirements as a condition for approval with postmarketing monitoring to detect and remedy product safety deficiencies in the field.

FDA's postmarket surveillance uses mandatory reporting of adverse events by manufacturers and voluntary reporting by health professionals and consumers. In 2002, FDA supplemented these sources of surveillance information with a new approach. It established a voluntary network of clinicians and hospitals to provide a two-way channel of communication to support surveillance and more in-depth investigations of medical device safety performance.[22] The Medical Product Safety Network, known as MedSun, now has about 350 participating user facilities. Each participating facility has trained liaisons, who are instructed to report issues of interest to FDA electronically. According

[20] A comparison of safety assurance processes for safety-critical electronics in the automotive and aerospace domains is given by Benz et al. (2004).

[21] FDA regulates three classes of medical devices. The most intensely regulated, designated as Class III, are those supporting or sustaining human life, such as pacemakers, pulse generators, and implanted defibrillators.

[22] http://www.fda.gov/MedicalDevices/Safety/MedSunMedicalProductSafetyNetwork/default.htm.

to FDA officials who briefed the committee, agency epidemiologists can query MedSun participants for specific information on the performance of devices under investigation, and participants regularly submit device performance information to FDA's surveillance program, including reports on safety-related "close calls."

MedSun represents a small part of FDA's postmarket surveillance system. It is discussed here because it demonstrates a collaborative approach that may have application in the automotive sector. MedSun's effectiveness for defects surveillance could not be examined in this study. A recent report by the Institute of Medicine (IOM), however, found that FDA's MedSun and certain other collaborative initiatives for postmarket surveillance are "scientifically promising" provided they are resourced adequately (IOM 2011, 143–144).[23]

Conceptually, FDA's MedSun resembles NHTSA's Crash Injury Research Engineering Network (CIREN). CIREN was created by the agency in 1996 for detailed investigation of vehicle crashes. The program brings together experts from medicine, academia, industry, and government to perform analyses of the injuries sustained in specific collision modes such as front, side, and rollover crashes. The participating trauma centers are among the nation's largest, and the engineering centers are based at academic laboratories with extensive experience in vehicle crash and human injury research. Each trauma and engineering center collects detailed medical and crash data on approximately 50 crashes per year, and these data are shared among participating centers through a computer network that is also accessible to NHTSA researchers. While CIREN does not collect information on the performance and functioning of vehicle electronics systems, it demonstrates the value of such collaborative forums and how NHTSA can play a role in supporting them.

CHAPTER FINDINGS

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*

[23] The IOM report found: "The FDA has postmarketing surveillance programs—such as MedSun, MD EpiNet, and the Sentinel Initiative—that are scientifically promising, but achieving their full promise will require a commitment to provide stable, adequate resources and will require resolution of various technical issues, such as unique device identifiers."

their functions as intended and do not prompt other unsafe driver actions and behaviors. Alcohol-impaired driving, speeding, distraction, and failure to use seat belts represent long-standing driver behaviors that contribute to many crashes and their consequences. Advancements in vehicle electronics could reduce crashes and their severity through alerts, crash-imminent actions, and automated control. Such benefits will depend on drivers accepting the technologies and using them appropriately. In addition, industry and NHTSA have an interest in ensuring that new safety technologies do not have the unintended effects of confusing or startling drivers or causing them to become too dependent on the technologies themselves for safe driving.

Finding 4.2: *NHTSA's FMVSSs 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.* In being primarily performance-oriented, the standards are intended to be design- and technology-neutral, in recognition that automotive technologies evolve and vary across manufacturers. Hence, automotive manufacturers are not required to seek NHTSA approval when they develop and introduce a new vehicle system, even if it pertains to an FMVSS-required safety capability or feature. NHTSA may offer an interpretation of a new technology's conformance to an FMVSS performance requirement, but it does not advise on specific design strategies or testing methods carried out by the manufacturer, such as means by which corrosion resistance, electromagnetic compatibility, software reliability, and diagnostic and fail-safe properties are designed and verified. Automotive manufacturers are required to self-certify that their vehicles comply with the performance requirements when they deliver each vehicle to the dealer.

Finding 4.3: *Through ODI, NHTSA enforces the statutory requirement that vehicles in consumer use not exhibit defects that adversely affect safe vehicle performance.* ODI analysts monitor the fleet for indications of vehicle safety defects primarily through the screening and analysis of consumer complaints, supplemented with information submitted by manufacturers in compliance with the EWR system. By law, to demonstrate the existence of a safety defect, ODI investigators must be able to show a potential for a significant number of failures as a result of the defect and that such failures present an unreasonable risk of a crash, injury, or death. The defect may pertain to any vehicle component that can adversely affect

the safe performance of the vehicle, regardless of whether it pertains to a capability required in a specific FMVSS. ODI inquiries and investigations seldom lead to manufacturers being ordered to undertake a safety recall to remedy a defect. However, ODI investigative actions often prompt the manufacturer to issue a voluntary recall, even in instances where there is uncertainty about whether the defect meets the statutory definition of presenting an unreasonable safety risk.

Finding 4.4: *NHTSA refers to its vehicle safety research program as being "data driven" and decision-oriented, guided by analyses of traffic crash data indicating where focused research can further the introduction of new regulations and vehicle capabilities aimed at mitigating known safety problems.* In particular, electronics systems that can aid in crash avoidance are viewed as promising ways to mitigate driver errors. The agency's crash avoidance research thus includes evaluations of human factors issues, methodologies for estimating the potential safety benefits of existing and emerging crash avoidance technologies, performance standards and tests that can be established for technology-based crash avoidance capabilities, the state of development of emerging and more advanced technologies for driving assistance, driver monitoring, and vehicle-to-vehicle communications.

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.* NHTSA has indicated that such a forward-looking strategic plan is being developed, but its purpose and the progress on it have not been made clear. For example, NHTSA does not undertake significant research in support of industry efforts to make improvements in areas such as fail-safe and diagnostic strategies, means for detecting dual and intermittent faults, electromagnetic compatibility, software safety assurance, or cybersecurity. Nor does the agency undertake significant research in support of improvements in the processes and data capabilities of ODI in monitoring for and investigating the fleet for electronics-related defects. Such defects may become more common (owing to the growth in electronics systems) and more difficult to identify and assess because their occurrence does not always leave a physical trace. Whether such an expansion of research emphasis is warranted is a strategic consideration and a candidate for coverage in the pending strategic plan.

Finding 4.6: *FAA's regulations for aircraft safety are comparable with the performance-oriented FMVSSs 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.* Aircraft manufacturers must apply to FAA for approval and certification to develop and build a new aircraft type. FAA's certification process covers all product development phases; FAA reviews and approves all manufacturer safety assurance plans. In contrast, under NHTSA's approach, these responsibilities are left to manufacturers. For NHTSA to engage in comprehensive, aviation industry–type regulatory oversight of manufacturer assurance plans and processes would represent a fundamental change in the agency's regulatory approach that would require substantial justification and resources, and possibly new statutory authority. 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, however, such a profound change in the way NHTSA regulates automotive safety does not appear to be a near-term prospect.

Finding 4.7: *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.* MedSun represents a small part of FDA's postmarket surveillance system. This network is discussed here because it demonstrates a government–industry collaborative approach that may have application for automotive safety. NHTSA's CIREN program is conceptually similar to the FDA network for medical devices, demonstrating NHTSA's potential for supporting such collaborative surveillance activities.

REFERENCES

Abbreviations

GAO	Government Accountability Office
IOM	Institute of Medicine
NHTSA	National Highway Traffic Safety Administration
TRB	Transportation Research Board

Benz, S., E. Dilger, W. Dieterle, and K. D. Müller-Glaser. 2004. A Design Methodology for Safety-Relevant Automotive Electronic Systems. SAE Paper 2004-01-1665. Presented at Society of Automotive Engineers World Congress and Exhibition, Detroit, Mich., March.

GAO. 2011. *NHTSA Has Options to Improve the Safety Defect Recall Process.* GAO-11-603. June. http://www.gao.gov/new.items/d11603.pdf.

IOM. 2011. *Medical Devices and the Public's Health: The FDA 510(k) Clearance Process at 35 Years.* National Academies Press, Washington, D.C.

NHTSA. 2008. *National Motor Vehicle Crash Causation Survey: Report to Congress.* DOT HS 811 059. July. http://www-nrd.nhtsa.dot.gov/Pubs/811059.PDF.

NHTSA. 2011. *NHTSA Vehicle Safety and Fuel Economy Rulemaking and Research Priority Plan, 2011–2013.* March. http://www.nhtsa.gov/staticfiles/rulemaking/pdf/2011-2013_Vehicle_Safety-Fuel_Economy_Rulemaking-Research_Priority_Plan.pdf.

TRB. 2011. *Special Report 300: Achieving Traffic Safety Goals in the United States: Lessons from Other Nations.* National Academies, Washington, D.C.

5

Review of National Highway Traffic Safety Administration Initiatives on Unintended Acceleration

The statement of task for this study requests "an independent review of past and ongoing industry and NHTSA [National Highway Traffic Safety Administration] analyses to identify possible causes of unintended acceleration." As noted in Chapter 1, NHTSA's Office of Defects Investigation (ODI) has investigated driver complaints of unintended acceleration for more than 40 years, and these complaints have encompassed a wide range of reported vehicle behaviors. Some complaints have involved moving vehicles that do not slow down as expected when pressure on the accelerator pedal is released. Others have involved vehicles that speed up abruptly with high engine power from a stopped position or while moving slowly. At other times the complainants describe fluctuations in engine idling, hesitation, shuddering during gear change, fluctuation of cruise control speeds around their set values, or delayed deceleration when brakes are applied on an uneven road surface. Degraded or failed braking is often asserted along with the unintended acceleration. Some complainants report having brought the vehicle to a dealer or other repair facility after the episode only to learn that no vehicle-related causes could be found or to receive an unsatisfactory explanation of possible causes.[1]

The committee is not charged with determining which of these vehicle behaviors constitute unintended acceleration or with examining alternative theories of the causes of such behaviors. The charge is to review the

[1] The committee read the narratives of hundreds of complaints submitted to NHTSA and downloaded from the agency's website to make these characterizations.

investigations conducted and supported by ODI on the basis of its definition of unintended acceleration and its purposes in conducting the investigations. ODI informed the committee that it investigates consumer complaints to determine whether the conditions and behaviors reported result from a vehicle-related deficiency that presents a public safety risk.[2] The agency's investigations inform decisions about whether specific follow-up steps are warranted, such as influencing or ordering a manufacturer safety recall, amending a Federal Motor Vehicle Safety Standard (FMVSS), or sponsoring research to identify vehicle- and human-related factors that may be causing or contributing to an evident safety deficiency. The emphasis of this chapter is on reviewing ODI investigations of unintended acceleration with regard to their use in informing such agency decisions. As a consequence, the chapter does not assess ODI's investigations with regard to reasons unconnected to agency decision making—for example, whether the investigations are suited to exploring all conceivable means by which electronics systems could fail and lead to unsafe vehicle conditions or behaviors. The committee understands that ODI's investigations are intended to identify defects that present a demonstrable safety hazard.[3]

For years, ODI's Defects Assessment Division has sorted the complaints it receives on unintended acceleration according to certain signature characteristics that it associates with driver pedal misapplication. By doing so, ODI believes that it can make more effective use of its investigative resources and better identify complaints involving unintended acceleration in which pedal misapplication was not the likely cause. The criteria that ODI uses for this sorting are derived from the report *An Examination of Sudden Acceleration* (Pollard and Sussman 1989), which was produced by the U.S. Department of Transportation's (DOT's) Transportation Systems Center (TSC). The committee was asked to review

[2] Title 49, United States Code, Chapter 301, Subchapter 1, Section 30101. To demonstrate the existence of a safety defect, NHTSA needs to show that a defect exists and that it is safety-related. Accordingly, the agency must prove both that substantial numbers of failures attributable to the defect have occurred or are likely to occur and that the failures pose an unreasonable risk to safety.

[3] One could argue that NHTSA should examine electronics systems to assess any vulnerabilities that could plausibly lead to unsafe behaviors in the field and then perhaps look for evidence of such behaviors in the fleet. However, NHTSA does not view "prove out" as part of its mission, and therefore ODI's investigations are not designed for this purpose. As noted in Chapter 1, NHTSA describes the purpose of its initiatives on unintended acceleration as "intended to provide NHTSA with the information it needed to determine what additional steps may be necessary to identify the causes of unintended acceleration in Toyota vehicles and determine whether a previously unknown electronic defect may be present in those vehicles and warrant a defect investigation" (NHTSA 2011, 12).

and comment on the continued relevance of the criteria derived from that report, which is often referred to as the Silver Book.

More recently, questions have arisen about whether vulnerabilities in electronic throttle control systems (ETCs) have caused or contributed to an increase in consumer complaints alleging unintended acceleration, particularly by drivers of Toyota vehicles, which experienced a notable increase in these complaints in recent years. In February 2011, NHTSA released its most comprehensive report on unintended acceleration since sponsoring the Silver Book more than 20 years ago. The report, *Technical Assessment of Toyota Electronic Throttle Control Systems* (NHTSA 2011), recounts ODI's investigations of unintended acceleration complaints involving Toyota vehicles over the past decade, analyzes the entire consumer complaint database for all reported incidents involving forms of unintended acceleration, reports on agency analyses of warranty data and crash investigations, and draws conclusions from a NHTSA-commissioned study (NASA 2011) by the National Aeronautics and Space Administration (NASA) of potential design and implementation vulnerabilities in the Toyota ETC. NASA's study results are not detailed in this chapter (since the study is available on the Internet),[4] but ODI's conclusions about the candidate causes of unintended acceleration as informed by the NASA results are examined.

Finally, ODI's investigative actions and processes are not considered with regard to matters such as their documentability or compliance with administrative and statutory requirements.[5] The committee was not constituted to perform such auditlike functions. The U.S. DOT Office of Inspector General (OIG) did undertake such an audit (OIG 2011) and has made several recommendations to NHTSA for improving related aspects of its defect surveillance and investigation programs.

The emphasis of the chapter is on describing how ODI has monitored for and investigated the potential causes of unintended acceleration. The purpose is to obtain insight into where changes in NHTSA's regulatory, research, and defect investigation approaches may be needed, given that other electronics systems could be suspected in reports of vehicle control problems and other unintended behaviors in the same manner as Toyota's ETC.

[4] http://www.nhtsa.gov/UA.

[5] For example, the committee did not review the grounds for NHTSA assessing a civil penalty against Toyota for recall timeliness.

PAST NHTSA INITIATIVES ON UNINTENDED ACCELERATION

As indicated in Chapter 1, two major investigations of unintended acceleration were commissioned by NHTSA during the 1980s. The first (Walter et al. 1988) was undertaken in response to incidents involving the Audi 5000. The second, which led to the Silver Book (Pollard and Sussman 1989), involved more vehicle makes and models and focused on incidents involving vehicles that had been stopped or moving slowly before accelerating suddenly.

Audi 5000 Investigation

During the mid-1980s, ODI received a large number of consumer complaints by owners of the Audi 5000 reporting episodes of unintended acceleration. In analyzing complaints for all vehicle makes and models spanning Model Years 1978 to 1986, ODI calculated an exceptionally high rate of complaints against the Audi 5000: an estimated 556 per 100,000 vehicles produced compared with a fleetwide average of 28 per 100,000.[6] The complaint rate remained high even after the vehicle had been the subject of earlier recalls intended to fix the perceived problem. In 1982, for example, Volkswagen (the Audi importer) had issued a recall to modify the shape of the accelerator pedal to prevent interference by the floor mat. In 1983, the company issued a recall to attach a plate to the brake pedal to elevate it relative to the accelerator pedal.

Even before commencing its Audi investigation, ODI had conducted dozens of investigations of complaints alleging unintended acceleration involving scores of vehicle makes and models. Some of the complaints involved prolonged, high-speed events, and others involved abrupt, short-lived acceleration often ending with a crash. The investigations prompted a number of recalls to repair various problems, including pedal entrapment, throttle icing, broken or ill-fitting parts in the throttle assembly, and bound accelerator cables that had caused the throttle to remain open even when the driver's foot was removed from the accelerator pedal. In all of these cases, physical evidence could be identified to determine the source of the problem, but in a large majority of other cases no vehicle-related

[6] The Audi complaint rates were calculated by NHTSA in October 1988. As noted in Chapter 1, media attention contributed to the rate of complaint reporting by Audi drivers. For example, a November 1986 broadcast of the CBS show *60 Minutes* portrayed the Audi as "out of control" (the title of the broadcast).

deficiency was found. The latter cases tended to involve vehicles that were accelerating abruptly from a stopped or parked position or from a low travel speed, often accompanied by a reported loss of braking. It was also common for the driver to claim that the acceleration started at the same time as brake application. Unable to find physical evidence of brake failure or the kinds of mechanical problems listed above, ODI usually attributed these incidents to drivers pressing the accelerator pedal instead of, or in addition to, the brake pedal.

The large number of reports of unintended acceleration involving the Audi 5000 caused ODI to enlist TSC to conduct a more thorough investigation of why the phenomenon was being reported much more frequently among owners of this vehicle (Walter et al. 1988). The TSC investigators analyzed the vehicle's major mechanical, electronics, and electromechanical systems to determine the conditions under which they could create high engine power; measured the dimensions and examined the design of the Audi driver compartment to determine whether the features of the compartment and driving controls might increase the probability of pedal misapplication; and studied the age and other characteristics of Audi drivers to determine whether they were more likely than the drivers of other vehicles to be exposed to situations in which unintended acceleration could occur.

In examining the Audi complaints, the TSC investigators found that a large proportion of the incidents involved reports of unintended acceleration and brake failure occurring at the same moment. The investigators were unable to identify any combination of failures that could create simultaneous failures of these two systems without leaving any physical evidence and concluded that pedal misapplication had to be the cause. The investigators therefore sought to explain why the accelerator pedal was being misapplied more often by drivers of the Audi than by drivers of other vehicles. They observed that the pedal and seating arrangements of the Audi differed from those of peer domestic vehicles, and they noted that many of the drivers reporting unintended acceleration had owned the vehicle for a short period of time. The investigators surmised that the higher incidence of pedal misapplication may have resulted from drivers' unfamiliarity with the vehicle's seating and pedal layout.

Another feature of the Audi 5000 that TSC investigators suspected may have contributed to pedal misapplication was the vehicle's idle stabilizer. After Model Year 1983, Audi incorporated an electronically controlled idle stabilizer to regulate engine speed according to the demands

of engine load. The system, composed of an electronic control unit and an electromechanical air valve, was prone to defects that caused a high idle speed and periodic engine surging.[7] The TSC team noted that because of their intermittent nature, these behaviors may not have been detected during premarket testing of the Audi or in postcrash investigations by ODI and others. Volkswagen had recalled the idle stabilizer valve because of the surging problem. While the surges were not accompanied by a large throttle opening and were not found to be consistent with consumer complaints of high-power acceleration, the TSC team speculated that the vehicle behavior could have startled some drivers and led some to press the accelerator pedal when they intended to apply the brake.

Silver Book

After the Audi 5000 investigation, TSC was enlisted again by ODI to conduct a more broadly based review of unintended acceleration complaints. The focus of this follow-up study was on incidents in which the acceleration began while the vehicle was stopped or moving slowly. ODI recognized the occurrence of other types of unintended acceleration incidents such as those starting from higher speeds but wanted to obtain a better understanding of this more common class of incidents. These sudden acceleration incidents were also troubling because they tended to be accompanied by reports of complete brake loss. The product of this second TSC investigation, *An Examination of Sudden Acceleration,* has come to be known as the Silver Book (Pollard and Sussman 1989).

In carrying out its investigation, the TSC team reviewed hundreds of complaints submitted by drivers alleging unintended acceleration during the previous decade. The investigators also reviewed relevant literature and case documentation; interviewed drivers who had filed complaints; and studied the fuel systems, brakes, cruise control systems, power trains, and pedal and gearshift lever layouts of 10 vehicle makes, some of which were selected because of their above-average complaint rates. The team's methods and results were subjected to peer review by a group of experts in various safety and engineering disciplines.

In a manner similar to the Audi 5000 investigation, the TSC investigators examined possible mechanical causes. They focused on the potential

[7] The idle speed control systems of the time would more appropriately be called idle stabilization systems, since they only provided a "trimming function" around the normal operating point to help achieve smoother idle quality.

for a sticking throttle caused by problems such as frayed or kinked cables, broken springs, and stuck pedals. They concluded that such mechanical faults were not likely to be causes of unexplained cases of unintended acceleration since their origins would be evident during postevent inspection of the vehicle. Transmission and idle speed stabilizer systems were also examined for conditions that might lead to unintended acceleration. Because it had no influence on throttle actuation, the transmission was dismissed as a possible cause. The TSC team concluded that the idle speed stabilizer was incapable of causing the simultaneous high levels of fuel and air flow needed to produce the reported high-power acceleration.

Cruise control modules had often been suspected as a source of unintended acceleration, and they were tested to assess whether they could create and sustain a large throttle opening.[8] Modules were thus placed in an environmental chamber and subjected to variations in power supply, temperature, and electromagnetic interference over a period of months.[9] The TSC team did not find any significant or sustained malfunctions of the modules as a result of any of the environmental conditions tested. Whereas the electromagnetic interference tests caused system malfunctions, they were found to be momentary. In examining the possible transient conditions that might cause intermittent problems, the TSC team concluded that the low probability of simultaneous failures of more than one component, coupled with the many redundant mechanical and electrical fail-safe mechanisms for disabling the servo (including light tapping of the brake), ruled out the cruise control as a plausible cause of wide-open throttle.

Once again, the TSC investigators found that complete loss of braking was common among driver complaints of unintended acceleration occurring in a stopped or slow-moving vehicle. The team could not identify any credible mechanisms by which brakes could fail fully but then recover normal function with no signs of physical damage. In addition, the team pointed to tests indicating that brake application, even if it is

[8] Cruise control systems of the time consisted of control switches, an electronic control module (typically using a microprocessor or custom integrated circuit), a speed sensor typically mounted in the transmission or in the speedometer cable, a servo that mechanically pulled on the throttle lever, and electric or vacuum dump valves that would release the vacuum in the actuator when the brake pedal was depressed.

[9] The electromagnetic interference test simulated a transient of an air conditioning clutch engaging and disengaging (which produces a large electrical transient on the power line), and the radio frequency interference units were subjected to a signal from a high-power citizens band antenna located close to the module and a simulated electrostatic discharge.

assumed to be delayed somewhat to simulate a driver's emergency response to the onset of acceleration, will quickly stop a vehicle accelerating from a stationary position or low travel speed.[10]

Unintended acceleration accompanied by unexplained brake loss had long been associated with pedal misapplication.[11,12] The TSC investigators knew this and questioned whether certain vehicle-related factors could be responsible for drivers applying the wrong pedal after being startled by a vehicle-related condition or behavior. They surmised that phenomena such as engine surging, high idling, or even unexpected noises could induce this effect, especially among drivers unfamiliar with the vehicle, its operating characteristics, and its control layout. Noting that many incidents had involved motorists operating new vehicles, the team surmised that such patterns could be indicative of the driver lacking familiarity with the gearshift lever and pedals. The Silver Book therefore recommended that NHTSA undertake more research to determine whether such vehicle-related factors may have contributed to pedal misapplication, including research to examine the effect of pedal layouts and configurations. NHTSA subsequently sponsored research by the Texas Transportation Institute (Brackett et al. 1989) to advise on pedal designs and layouts that might be less susceptible to misapplication.

In the decade following the release of the Silver Book (and before the introduction of ETCs), NHTSA continued to receive complaints involving unintended acceleration across vehicle makes and models. ODI's investigations of these complaints led to many of the same conclusions reached in the Silver Book: most incidents were caused by drivers mistakenly pressing the accelerator pedal, while the remainder resulted from mechan-

[10] The Silver Book's Appendix E refers to brake force and performance tests conducted at NHTSA's test center by R. G. Mortimer, L. Segal, and R. W. Murphy: "Brake Force Requirements: Driver–Vehicle Braking Performance as a Function of Brake System Design Variables."

[11] The TSC investigators were not the first to associate pedal misapplication with unintended acceleration. ODI had concluded that pedal misapplication was the cause of many episodes of unintended acceleration during the previous 20 years of case investigations. Pedal misapplication had also received attention in the human factors literature (Schmidt 1989; Rogers and Wierwille 1988; Vernoy and Tomerlin 1989).

[12] Pedal misapplication is also now known to be a source of unintended acceleration by operators of commercial vehicles. In a study of unintended acceleration involving school buses and other heavy vehicles, the National Transportation Safety Board (NTSB) reported that the drivers in these occurrences all reported a loss of braking, but the investigators did not find physical evidence of brake damage. NTSB concluded that the brakes did not fail; instead, the drivers had applied the accelerator pedal when they had intended to apply the brake (NTSB 2009).

ical problems (e.g., stuck pedals and accelerator cables) and pedal obstructions (such as floor mat entrapment). During this period, pedal misapplication was found to be more common among vehicles with automatic transmissions that lacked brake transmission shift interlocks. Although these devices were not required at the time by federal regulation, many manufacturers began installing them during the 1980s and 1990s. The interlock requires the driver to press the brake pedal to shift out of park and is designed to keep the driver from shifting into drive or reverse while the accelerator pedal is mistakenly depressed. The increased use of the interlock during the 1990s substantially lowered the number of reports of unintended acceleration involving vehicles maneuvering in parking lots and driveways (Reinhart 1994).[13]

Much of the history of ODI's investigations of unintended acceleration during the 1990s can be found in an April 2000 notice issued by NHTSA in the *Federal Register*.[14] During that period, ODI often referred to the Silver Book's findings as grounds for determining when a reported incident had the hallmarks of pedal misapplication and when it did not. As the design of power trains and cruise controls changed during the 1990s, the test results reported in the Silver Book lost their relevance and were no longer cited by ODI when it investigated unintended acceleration incidents involving later model vehicles. Nevertheless, ODI investigators continued to refer to the Silver Book's characterization of pedal misapplication incidents as a way to sort complaints of unintended acceleration. The advent of ETCs did not change the relationship between the brakes and the throttle control systems, which continue to remain independent of one another.

INVESTIGATIONS OF TOYOTA COMPLAINTS

According to a recent report by the U.S. DOT OIG, ODI conducted 24 investigations of unintended acceleration involving numerous vehicle makes and models from 2002 through 2010. The investigations led to

[13] The brake shift interlock is not always fail-safe. In a notable case from 1998, ODI investigated a case of unintended acceleration by a police officer in Minneapolis, Minnesota. ODI concluded that the cause was pedal misapplication but found that the functioning of the brake transmission shift interlock had been compromised by an aftermarket device causing the cruiser's brake lights to flash when the dome light was energized (NHTSA File Number MF99-002, March 18, 1999).

[14] April 28, 2000 (Vol. 65, No. 83, pp. 25026–25037).

15 recalls affecting 13 manufacturers (OIG 2011, 5).[15] Eight of the investigations involved Toyota vehicles and led to two manufacturer recalls. ODI made several other preinvestigation inquiries of unintended acceleration in Toyota vehicles; two of them resulted in Toyota issuing recalls before ODI had opened a formal investigation. During the same period, ODI investigated Ford four times, General Motors three times, and Chrysler twice for reports of unintended acceleration (OIG 2011, 11). Nine other automotive manufacturers were the subject of investigations and inquiries.[16] ODI concluded that in all of these cases pedal misapplication or mechanical factors such as floor mats impeding the pedal, throttle valve sticking, and bound cables were the sources of the behavior.

OIG's audit assessed the effectiveness of ODI's processes for identifying and addressing safety defects and compared the processes with those followed by automotive safety authorities in other countries. OIG concluded that ODI had followed established procedures in conducting its investigations of unintended acceleration complaints and in monitoring resulting safety recalls. Although it did not question ODI's conclusions about the causes of the investigated cases of unintended acceleration, OIG recommended that ODI improve its documentation of preinvestigation activities and communications with manufacturers, establish a systematic process for seeking third-party assistance with investigations, and set and adhere to timelines for completing investigations.[17]

Early Toyota Investigations

A summary of the Toyota investigations and inquiries is provided in Table 5-1. It indicates how the consumer complaint data were used both by ODI and by consumers to identify, analyze, and investigate occurrences of unintended acceleration. The four earliest investigations, occurring from 2003 to 2006, were initiated in response to petitions by consumers

[15] The OIG report also contains tabulations of unintended acceleration complaints across the industry by manufacturer. These complaints were identified through broad searches of the Vehicle Owner's Questionnaire database using the component code "vehicle speed control." The OIG report notes that using this component code to sort complaints will exclude some complaints that may have involved unintended acceleration if the complaint was filed by using a different component code such as "service brakes." In addition, some complaints coded for "vehicle speed control" may involve issues unrelated to acceleration, such as transmission behaviors. The committee's own sampling of the Vehicle Owner's Questionnaire data found numerous instances of both shortcomings.

[16] Honda, Audi, Daimler, Buell, MacNeill Auto Products, Electronic Mobility, Jonway, CTS, and Kia were each investigated once.

[17] The OIG report is available at http://www.oig.dot.gov/sites/dot/files/ODI%20Final%20Report%2010-06-11.pdf.

TABLE 5-1 Summary of ODI Investigations and Inquiries on Unintended Acceleration Involving Toyota Vehicles, 2003–2010

Vehicles Involved (Toyota and Lexus Makes)	*ODI Investigation or Inquiry*	*Findings and Conclusions*	*Action*
Lexus GS and LS (Model Years 1997–2000) Petition assessment opened 2003	*Response to a consumer petition:* A petitioner to ODI reported experiencing multiple events of unintended acceleration, one that led to a rear-end collision. In each case, no vehicle-related cause was identified by the dealer. After reviewing other VOQs, the petitioner cited a high percentage of complaints in which the component code "vehicle speed control" had been marked in the complaints filed for this vehicle model. ODI interviewed the petitioner, inspected a Model Year 1999 Lexus LS 400, examined past complaints involving reports of unintended acceleration involving the same vehicle model, and compared complaint rates of peer vehicles made by other manufacturers.	After normalization to account for vehicle production data, ODI did not find the Lexus complaint rate to be higher than that of peer vehicles. In the interview, the petitioner reported applying the brake before the crash. ODI cited findings from earlier work (the 1989 Silver Book) indicating that the driver probably applied the accelerator pedal when the intent was to apply the brake pedal.	Assessment closed
Camry and Lexus ES 300 (Model Years 2002–2003) Investigation opened 2004	*Response to a consumer petition:* A petitioner reported that her Lexus accelerated unintentionally, causing a low-speed crash in a parking lot. The petitioner reported that she applied the brakes but that they were ineffective. In scanning complaints, ODI found 20 reports alleging unintended acceleration involving these vehicle makes and model years.	After conducting an analysis of past complaints, conducting driver interviews, and performing vehicle inspections, ODI concluded that the reported incidents involved acceleration coincidental with brake application during low-speed maneuvering with no evidence of failed components. The agency cited earlier investigations involving similar circumstances (low initiation speeds and acceleration and reported brake failure occurring coincidentally), suggesting that the likely cause was pedal misapplication.	Investigation closed, no recall

(continued on next page)

TABLE 5-1 (*continued*) **Summary of ODI Investigations and Inquiries on Unintended Acceleration Involving Toyota Vehicles, 2003–2010**

Vehicles Involved (Toyota and Lexus Makes)	*ODI Investigation or Inquiry*	*Findings and Conclusions*	*Action*
Camry and Lexus ES 300 (Model Years 2002–2005) Petition assessment opened 2005	*Response to consumer petition:* ODI received a petition citing complaint data alleging unintended acceleration involving these vehicles. The petitioner suspected that the ETC could be the source of the problem. ODI visited the petitioner and inspected the vehicle, reviewed the complaints, interviewed drivers, inspected other vehicles, and sent an information letter request to Toyota.	The prevalence of low initiation speed incidents and reported brake failure caused ODI to conclude that pedal misapplication was the likely cause rather than an electronics-related problem.	Assessment closed
Camry and Solara (Model Years 2002–2006) Petition assessment opened 2006	*Response to consumer petition:* ODI received a petition from a driver reporting unintended acceleration, many citing other complaints found in the VOQ database to support the petition, and questioned whether a malfunctioning ETC was the cause. ODI reviewed the VOQs, visited the petitioners, obtained parts, interviewed drivers, inspected vehicles, and sent an information letter request to Toyota seeking warranty claim data.	The lack of significant warranty claims and prevalence of low initiation speed incidents and reported brake failure caused ODI to conclude that pedal misapplication was the likely cause rather than an electronics problem.	Assessment closed
Camry and Lexus ES 350 (Model Years 2007–2008) Investigation opened 2007	*ODI review of consumer complaints:* In monitoring complaint reports, ODI found five reports by drivers alleging unintended acceleration involving these vehicles. Analysts noticed that the complaints involved unintended acceleration occurring at high initiation speeds, in contrast to earlier complaints. ODI interviewed the drivers and inspected vehicles. Through the Vehicle Research and Test Center, ODI surveyed vehicle owners. Six hundred owners responded, and 35 reported problems with floor mat interference with the accelerator pedal.	The interviewed drivers reported that the accelerator pedal would not return to its rest position after it was released. ODI inspectors observed the prevalence of unsecured all-weather floor mats in vehicles and suspected that the cause was pedal entrapment. The rubber floor mats were found to be unsecured because they were placed over the secured carpet floor mat.	Toyota issued a recall of the accessory rubber floor mat, prompting ODI to close its investigation.

Sienna (Model Year 2004) Investigation opened 2008	*ODI review of complaint data:* ODI's Early Warning Division recommended a review of the Model Year 2004 Sienna because the Early Warning Reporting data showed an unexplained trend of pedal interference in owner complaints made to Toyota. On further review of the VOQ complaint data, ODI found an additional complaint and Toyota field report involving this vehicle suggestive of pedal interference.	Vehicle inspections by ODI and Toyota found that the trim panel on the center console could obstruct the accelerator pedal.	Toyota issued a recall to fix the panel component, prompting ODI to close its investigation.
Tacoma (Model Years 2006–2007) Petition assessment opened 2008	*Response to consumer petition:* A petitioner reported experiencing two unintended acceleration events at low speed in a 2-hour period. The petitioner cited other complaints of unintended acceleration involving the same vehicle. ODI examined the complaint database for similar reports and interviewed the petitioner and more than 60 other drivers reporting similar incidents. ODI also tested consumer vehicles and queried Toyota for more information.	ODI reported finding no evidence supporting a vehicle defect but could not identify a likely cause for the reports of unintended acceleration.	Assessment closed
Lexus ES 300 (Model Years 2002–2003) and ES 350 (Model Year 2007) Petition assessment opened 2009	*Response to consumer petition:* The petitioner reported experiencing prolonged unintended acceleration while driving at highway speeds. The brakes were reported to have slowed the vehicle but became increasingly ineffective after prolonged use. The driver reported that he stopped the vehicle by shifting to neutral and shutting off the engine. The dealer did not find a vehicle defect but noted that the driver-side floor mat was out of position.	ODI interviewed the driver and examined complaints for the vehicle make and model. ODI obtained a Lexus ES 350 for examination at the agency's testing center. ODI reported that the tests did not reveal a potential electronics-related source of unintended acceleration. ODI noted that the vehicle involved was already covered by the earlier recall for pedal entrapment by floor mats.	Assessment closed

(continued on next page)

TABLE 5-1 (*continued*) **Summary of ODI Investigations and Inquiries on Unintended Acceleration Involving Toyota Vehicles, 2003–2010**

Vehicles Involved (Toyota and Lexus Makes)	*ODI Investigation or Inquiry*	*Findings and Conclusions*	*Action*
Multiple Toyota models and years Inquiry made in 2009–2010 (manufacturer issued a recall before the investigation was opened)	*ODI response to a crash investigation:* The fatal crash of a Lexus ES 350 in San Diego, California, which was found by the local police to be caused by a floor mat (designed for another vehicle model) entrapping the accelerator pedal, prompted ODI to reassess the adequacy of the earlier floor mat recall. The driver was unsuccessful in efforts to shut off the engine by using the on–off button for the keyless ignition system.	Toyota issued a second recall of the vehicles more prone to floor mat entrapment to reshape their pedals. For vehicles with keyless ignition systems, ODI advised Toyota to install systems in which application of the brake would override accelerator control.	Toyota issued a recall to reshape pedals on all vehicles and to install brake override software on vehicles equipped with keyless ignition systems.
Multiple Toyota models and years Inquiry made in 2009 (manufacturer issued a recall before the investigation was opened)	*ODI complaint analysis:* ODI examined a complaint in which the driver reported that the released accelerator pedal returned slowly to its rest position as opposed to remaining stuck in the depressed position, which is characteristic of floor mat entrapment. ODI also found evidence of similar pedal malfunctions in subsequent screening of warranty repair data submitted by Toyota.	Toyota contacted ODI and identified the specific pedal component defect that could cause excess friction in some pedal assemblies.	Toyota issued a recall to replace the affected pedal component.

Source: Derived from NHTSA 2011 and original ODI investigation reports.

who had experienced unintended acceleration and subsequently reviewed the consumer complaint data [Vehicle Owner's Questionnaire (VOQ)] to identify reports from drivers who experienced similar episodes. In response to the petitions, ODI also consulted the VOQ data to look for similar reports involving the same vehicle makes and models, to identify drivers to interview and complainant vehicles to inspect, and to compare complaint rates among peer vehicles. Some of the consumers who filed the petitions speculated on the possibility of malfunctioning ETCs as the cause. However, the prevalence of low initiation speeds and reports by drivers of applying the brakes to no effect coincidental with the occurrence of the unintended acceleration led ODI to conclude that pedal misapplication was the likely cause in all four investigations.

Pedal Entrapment Investigations and Recalls

In 2007, ODI analysts observed that a number of consumer complaints with regard to Toyota vehicles involved unintended acceleration occurring at high travel speeds and for prolonged periods, in contrast to more common complaints in which the acceleration occurred at low initiation speeds and was short-lived. In these later cases, drivers often reported conditions suggesting that the throttle had remained stuck in an open position rather than going quickly from idle to wide open, as typically occurs in cases where the driver presses firmly on the accelerator pedal believing it is the brake. The drivers also reported having trouble slowing the vehicle in response to the unintended acceleration, since prolonged or repeated brake application became increasingly ineffective. After interviewing drivers and inspecting vehicles associated with these complaints, ODI investigators noted the common use of an unsecured rubber floor mat placed on top of the carpeted mat. The investigators concluded that the rubber mat, which was designed with a raised lip on the front edge, was susceptible to slipping under the accelerator pedal, potentially preventing the pedal from returning to its rest position when the driver released it.

ODI notified Toyota of the identified problems. In response, the manufacturer issued recalls to install redesigned floor mats and alert dealers and vehicle owners to the risk of unsecured floor mats as well as evasive actions that should be taken in the event of pedal entrapment. In subsequent reviews of the VOQ data, ODI investigators identified another possible means by which the trim panel in the center console of a particular Toyota model (2004 Sienna) could cause pedal entrapment. Toyota was notified and issued a fix for the console.

During the floor mat investigations, ODI mailed a survey to more than 1,800 owners of the 2007 Lexus ES 350 requesting information on occurrences of unintended acceleration. Of the approximately 600 owners who responded, 10 percent stated that they had experienced unintended acceleration, and 6 percent complained of occasional pedal interference from floor mats. The survey also indicated that many owners were unfamiliar with how to press the start–stop button to turn off the engine in an emergency while the vehicle is in motion.

ODI also obtained a Lexus ES 350 from a complainant to perform an engineering analysis of possible vehicle-related causes of the unintended acceleration and difficulties associated with regaining control of the vehicle.[18] These tests, conducted at the Vehicle Research and Test Center (VRTC),[19] indicated that the accelerator pedal was capable of being entrapped by the lip of the unsecured rubber floor mat. The tests also indicated that when the vehicle's throttle is kept open by an entrapped pedal or other means, the vacuum power assist in the braking system will become depleted if the driver repeatedly presses the brakes to slow the vehicle. The loss of vacuum power assist caused braking to be much less effective and to demand significantly more pedal force.

ODI was called to investigate a highly publicized crash involving a Lexus ES 350 on a highway in the city of Santee in San Diego County, California, during August 2009. This crash, involving four deaths, brought renewed public and media attention to the occurrence of unintended acceleration in Toyota vehicles. Both ODI and San Diego County sheriff's investigators[20] determined that the cause of the crash was entrapment of the accelerator pedal caused by a floor mat that had been designed for another vehicle. The floor mat was found in the vehicle under the accelerator pedal. It was evident that the driver had tried to slow and regain control of the vehicle by repeatedly applying the brakes, which led to the brakes losing vacuum and overheating. There was also evidence that the driver, who was operating a dealer-loaned vehicle, was unable or unprepared to respond by moving the gearshift lever out of drive or by turning the engine off by holding down the ignition start–stop button.

---

[18] VRTC Memorandum Report EA07-010-VRTC-DCD7113, 2007 Lexus ES 350 Unintended Acceleration. http://www-odi.nhtsa.dot.gov/acms/docservlet/Artemis/Public/Pursuits/2007/EA/INFR-EA07010-28888.pdf.

[19] VRTC, in East Liberty, Ohio, is a federal facility that conducts research in support of NHTSA. It supports ODI's testing needs.

[20] San Diego County Sheriff's Department Incident Report concerning August 2009 crash in Santee, California (Case No. 09056454).

The involvement of the Lexus ES 350, which had been among the Toyota models subject to the earlier floor mat recall, in the Santee crash prompted ODI to question whether Toyota's recall plan was adequate and whether other precautions were needed to prevent a recurrence of such outcomes.[21] Toyota responded by issuing a second recall to reshape the accelerator pedal to reduce the potential for floor mat entrapment. For recalled vehicles equipped with the start–stop button, Toyota also installed software that would cause application of the brake to override the throttle in the event of entrapment.[22]

Pedal Sticking Recall

In late 2009, after the issuance of Toyota's second recall associated with floor mats, ODI observed that some owners of Toyota vehicles were complaining about the need to press harder than normal on the accelerator pedal to increase vehicle speed, and some were also finding that the pedal was slow to return to a rest position after it was released. ODI subsequently received several field reports from Toyota indicating similar circumstances, although none of the cases appeared to have produced wide-open throttle. ODI met with Toyota in January 2010 to review the source of the problem, which Toyota concluded had been caused by excessive friction in a defective pedal component. That month Toyota issued a recall of the component and devised an interim remedy that involved altering the pedal component while a supplier manufactured a replacement part for the affected vehicles.

Concerns About the Role of the ETC

As noted, during the course of many of these earlier Toyota inquiries and investigations, ODI was asked by petitioners to investigate the possibility of the ETC being the source of the unintended acceleration. These electronics systems had been introduced in some Toyota vehicles during the late 1990s and in the Camry and Lexus ES in Model Year 2002. In its aforementioned VRTC testing of the Lexus ES 350, ODI had performed some limited electronics-related tests, including the introduction of multiple electrical signals into the vehicle's electrical system to assess susceptibility to electrical interference. In addition, testers placed a strong magnet near the throttle body and the accelerator pedal sensors. The tests caused

[21] The recall plan included notification of dealers and consumers with regard to the potential dangers of using floor mats not designed for the vehicle.

[22] The brake override software only works if the driver is applying the brake and thus would have no effect on cases involving misapplication of the accelerator pedal.

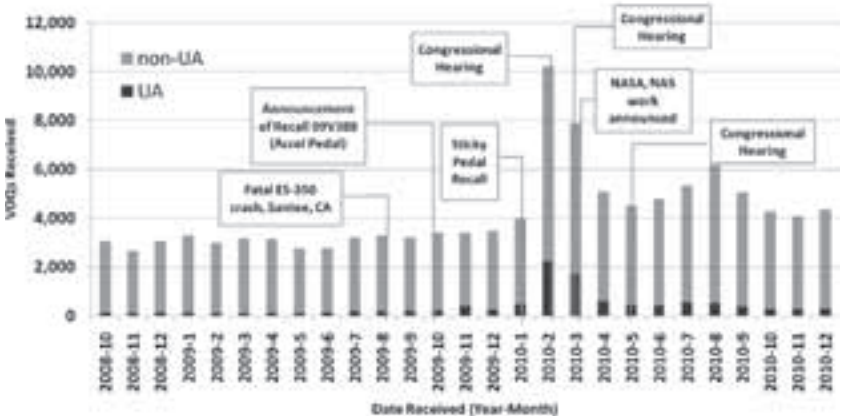


FIGURE 5-1 Consumer complaints of unintended acceleration (UA) in relation to publicized events, as reported by NHTSA. Total VOQ traffic versus those matching UA keyword search, October 2008 through December 2010. Keyword search is overinclusive and complaints are unconfirmed (Accel = accelerator). (*Source:* NHTSA 2011, Figure 2, page 18.)

an increase in engine idle speed (up to approximately 1,000 revolutions per minute), but ODI investigators could find no evidence of susceptibility to creation of a large throttle opening.

ODI believed that it had already determined the pedal-related causes of unintended acceleration by Toyota vehicles, and it had not found any evidence of relevant problems with the ETC in its VRTC testing or through its reviews of warranty repair data submitted by Toyota. However, public concerns about the possible role of this electronics system persisted. In congressional hearings during early 2010, NHTSA was also questioned about its technical capacity to investigate and test for electronics problems.[23] NHTSA's initiatives in response to these concerns are discussed below.

The publicity from the Toyota recalls, the fatal Santee crash, and the ensuing congressional hearings prompted more drivers, particularly owners of Toyota vehicles subject to the recalls for pedal entrapment and sticking, to lodge complaints of unintended acceleration with NHTSA. Figure 5-1 shows the fluctuations in complaints in proximity to these

[23] Hearings before the Oversight and Government Reform Committee, U.S. House of Representatives, February 24, 2010.

publicized events as well as NHTSA's announcement of its intention to commission studies by NASA and the National Research Council [referred to as the National Academy of Sciences (NAS) in the figure].

RECENT NHTSA INITIATIVES ON UNINTENDED ACCELERATION

Reexamination of All Consumer Complaints of Unintended Acceleration

In early 2010, ODI embarked on a review of its entire VOQ database for the period January 1, 2000, to March 5, 2010, to identify and characterize reported incidents involving Model Year 1998 to 2010 vehicles that could be viewed as having involved unintended acceleration. In so doing, ODI noted that the VOQ form does not contain any condition-related code that consumers can use consistently to report the occurrence of unintended acceleration.[24] Accordingly, ODI analysts had to undertake a keyword text search[25] of the narratives of the more than 400,000 complaints lodged during the 10-year period to identify complaints alleging the broadest possible range of conditions that could be construed as involving unintended acceleration.

Results of the VOQ analysis, shown in Table 5-2, were released in the agency's comprehensive report (NHTSA 2011). ODI found roughly 19,000 complaints containing key words that could be associated with forms of unintended acceleration. A manual reading of the narratives of these 19,000 complaints revealed 9,701 in which some form of unintended acceleration was reported, representing about 2 percent of total complaints filed during the period.[26]

---

[24] Consumers are asked in the questionnaire to identify the vehicle component (or components) that they believe is associated with the problem being reported. One component option is "vehicle speed control." Sorting on this component is sometimes done to identify complaints in the VOQ data that involve unintended acceleration, but such component characterizations are made inconsistently by consumers. Thus, relying on "vehicle speed control" as a sorting mechanism may help in identifying some reports of unintended acceleration, but it will lead to other relevant reports being missed (i.e., those categorized under a different vehicle component such as electrical, engine, power train, and service brakes) and other reports that do not involve unintended acceleration being included.

[25] Keyword search overview and terms are available in Report No. NHTSA-NVS-2011-ETC-SR01.

[26] The USDOT OIG (2011, 6) performed a text search on all complaints submitted to NHTSA between 2002 and 2009 and estimated that about 4 percent per year, or 13,778, involve allegations of some degree of unintended acceleration. The OIG did not manually review the identified complaints, as ODI did in arriving at the 2 percent figure.

TABLE 5-2 Unintended Acceleration Consumer Complaints Received by NHTSA, 2000–2010

Item	*Number*
Total consumer complaints (January 1, 2000, to March 5, 2010)	426,911
Complaints identified by key words associated with unintended acceleration	19,269
Complaints after manual review of narratives (Model Year 1998–2010 vehicles only)	9,701
Complaints deemed to have sufficient information to infer incident circumstances, conditions, and driver actions	5,512

Source: NHTSA 2011, Table 2.

The 9,701 complaints were further examined for certain objective information about incident circumstances and conditions, such as whether a crash occurred, the speed at which the incident began, and the actions of the driver. The complaints were examined for other information helpful for inferring these details, such as whether the incident occurred in a parking lot or driveway. A total of 5,512 complaints of the 9,701 were deemed to contain sufficient information to identify or infer incident circumstances. On the basis of this information, the ODI analysts were able to group the complaints into initiation speed ranges—that is, the speed at which the onset of unintended acceleration occurred. The results of these grouping are shown in Table 5-3. More than two-thirds of the complaints (and more than 80 percent of the complaints involving crashes) involved unintended acceleration that started from a stationary position or low speed (less than 15 mph). ODI reported that many of these incidents (40 percent of complaints and 64 percent of complaints involving crashes) took place while the vehicle was in a parking lot and where the driver reported immediate ineffective braking.

TABLE 5-3 Share of All Consumer Complaints of Unintended Acceleration by Initiation Speed (All Manufacturers)

Initiation Speed	*Percentage of Total Complaints (N = 5,512)*	*Percentage of Complaints Involving Crashes (N = 2,039)*
Stationary	36	33
Low speed (<15 mph)	33	51
Medium speed (15–45 mph)	12	9
High speed (>45 mph)	19	7

Source: NHTSA 2011, Table 3.

ODI concluded that the low initiation speed incidents are highly suggestive of pedal misapplication for the reasons explained in the earlier discussion of the Silver Book. ODI further concluded that many of the incidents involving vehicles in which the onset of acceleration occurred at medium and higher speeds (31 percent of complaints) also were likely the result of pedal misapplication. This was particularly the case if the driver reported experiencing the acceleration at the same moment as reported application of the brake—for example, when the driver was trying to brake while approaching an intersection, an exit ramp, or stopped traffic. However, ODI also concluded that some of the higher-speed incidents were caused by pedal entrapment, including the incidents already identified as having involved entrapped floor mats.

ODI's complaint analysis focused further on the ETC-equipped Toyota Camrys from Model Years 2002 to 2006. This analysis also indicated that the large majority (74 percent) of complaints involved high-power acceleration beginning when the vehicle was standing or moving slowly, as shown in Table 5-4. In a large percentage of these complaints, the driver

TABLE 5-4 Share of Toyota Camry Consumer Complaints of Unintended Acceleration by Initiation Speed and Driver Actions

		Complaints (%)		
Initiation Speed	*Scenario*	*Model Year 1998–2001 Without ETC (N = 110)*	*Model Year 2002–2006 with ETC (N = 544)*	*Model Year 2007–2010 with ETC (N = 304)*
Low speed (<15 mph)	Apply brake pedal	48	69	25
	Apply accelerator pedal	12	4	4
	Release accelerator pedal	5		
	Idle or normal operations	3	1	3
Roadway speed (≥15 mph)	Apply brake pedal	7	6	7
	Apply accelerator pedal			0.3
	Release accelerator pedal	12	3	23
	Cruise control		1	5
	Drivability problem	1	7	23[a]
	Other or unknown	1		1
Unknown speed	Unknown intent	12	10	10

Note: Columns may not add to 100 percent because of rounding.

[a] The higher number of complaints involving drivability concerns was a result of a transmission-related defect.

Source: NHTSA 2011, Table 6.

claimed to have applied the brakes. The analysis also indicated a number of cases in which the acceleration began at highway speeds; they occurred among the Model Year 2007 to 2010 vehicles that had been subject to the floor mat recalls. In addition, the analysis uncovered a number of complaints reporting vehicle hesitation and lurching, mostly among the Model Year 2007 to 2010 vehicles. ODI concluded that the latter incidents did not involve high-power acceleration and were attributable to transmission problems, consistent with Toyota technical service bulletins.

Crash Investigations Using Toyota Camry Event Data Recorder Data

During 2010, NHTSA conducted field investigations of 58 crashes involving Toyota Camrys equipped with ETCs and documented the results (NHTSA 2011). Unintended acceleration had been reported or suspected in all 58 crashes.[27] Twenty years earlier, investigators only had vehicle inspections and documentation, physical evidence at the crash scene, and testimony from vehicle occupants and witnesses to rely on. In contrast, the ODI investigators in 2010 could obtain additional objective evidence from the event data recorders (EDRs) in the crash vehicles. Indeed, the 58 crashes were selected because of the expected availability of EDR data.

EDR data were not available in five of the 58 crashes; the devices did not record data because of low crash forces. In one other case, the EDR data were not used because the recorded values were clearly erroneous. ODI removed these six crashes from the study. Of the remaining 52, ODI concluded that 12 involved circumstances that were not characteristic of unintended acceleration. Those 12 crashed vehicles had been driven off the road or struck objects with no EDR evidence of either acceleration or braking, suggesting factors such as driver inattention or falling asleep at the wheel.

Of the remaining 40 crashes, the investigators confirmed with physical evidence that one involved pedal entrapment by a floor mat. Among the remaining 39, investigators concluded that the most likely cause of all the crashes was pedal misapplication. The EDR data proved especially helpful in reaching this conclusion. In 29 of the 39 crashes, the EDR showed no brake pedal application at all, since the brake light switch had never transitioned from "off" to "on." EDR readings from an additional six cases

[27] The 58 cases were identified by ODI by reviewing consumer complaints, police records, Toyota records, insurance company records, and media reports.

showed that the brake had been applied late in the crash, indicated by the brake light switch transitioning to "on" either 1 second before or at the time of the crash. The significantly delayed brake pedal application (suggesting a late driver correction after application of the wrong pedal) was considered insufficient to have any meaningful effect on slowing the vehicle before the crash. The EDR also recorded the accelerator pedal position, which was used by ODI investigators to better account for the location of the drivers' feet. In 35 of the 39 incidents, the pedal position data indicated either sustained or increasing pressure on the accelerator pedal.

Other EDR and investigation data indicated that in 28 of the 39 cases the driver began to experience acceleration when the vehicle was traveling at speeds of 15 mph or less. All but one of the 28 crashes took place in a confined space, mostly residential driveways and commercial parking lots. The nine cases in which acceleration began when the vehicle was moving at faster speeds (>15 mph) consisted of traffic circumstances in which the driver would likely have been trying to apply the brake to slow the vehicle (for example, in approaching a stoplight). In addition, the investigators found that 24 of the 39 crashes involved drivers aged 65 or older. The finding of a high proportion of older drivers was consistent with ODI's earlier observation from investigations of unintended acceleration that older drivers are overinvolved in these cases.

According to ODI's summary assessment, the 58 crash investigations did not reveal any new candidate causes, such as failure of the ETC, for unintended acceleration.

Examinations and Measurements of Toyota Camrys

In its report (NHTSA 2011), ODI explained how it had obtained 20 drivable Model Year 2001 to 2009 Toyota Camrys to permit more extensive examination and measurement of vehicle braking and ergonomic characteristics. Eleven of the 20 vehicles, including two Model Year 2001 vehicles that were not equipped with ETCs, had not been involved in reported unintended acceleration events. The other nine consisted of "complaint" vehicles that had been involved in alleged unintended acceleration events. In selecting the nine complaint vehicles, any vehicles that had been involved in confirmed cases of entrapped or sticking pedals were excluded.

Examination of Braking Characteristics

In testing the Camry vehicles, ODI measured the effect of open-throttle acceleration on the performance of brake systems. Each vehicle underwent

acceleration and brake performance testing to quantify braking effectiveness with and without power assistance. Tests included baseline acceleration and then a series of acceleration tests while applying pressure to the brake pedal by using the forces required for testing to comply with NHTSA's brake performance regulation (FMVSS 135). Additional brake tests were conducted by using similar forces to measure the stopping distances of each vehicle. Braking tests were conducted with no acceleration, full acceleration with vacuum assist, and full acceleration without vacuum assist.

ODI concluded that the subject braking systems were more than adequate to halt acceleration initiated at low speed, including instances involving wide-open throttle. Even without vacuum assist, the brakes demonstrated the ability to overcome the engine torque, although the brake pedal force necessary to do so increased substantially. The tests indicated that a large throttle opening maintained for a longer period, as occurred in some pedal entrapment cases, could prompt drivers to pump the brakes repeatedly to cause loss of vacuum assist and overheating of the brakes from prolonged application.

ODI stated that these findings are consistent with its earlier conclusion that reports of total and immediate brake failure coincidental with the onset of acceleration, as alleged in many low initiation speed incidents, are implausible and indicative of pedal misapplication. The findings of brake fade and vacuum depletion provided further evidence of why brakes sometimes became difficult to use and eventually ineffective during pedal entrapment cases occurring at highway speeds and when the driver applied the brakes repeatedly.

Gearshift Lever Ease of Use

An assessment of whether the gearshift lever could be used to disengage the engine quickly and simply in the event of unintended acceleration was made. The Camry shift pattern and required movements to achieve drive, neutral, reverse, and park were examined, along with any extra effort that might be required to move the lever, such as pressing a button on the shifter. The tests did not reveal any ease-of-use issues for the standard shifter used in the Camry when compared with measurements taken from other vehicles. In all cases, shifting to park or reverse caused the transmission to go to neutral.[28]

[28] The testers did find, however, that a serpentine design on the "autostick" shifter of the highest-trim models could increase the chances of a driver not being able to shift quickly out of drive when under duress.

Pedal Layout and Driver Interface

The orientation, location, and operation of the accelerator and brake pedals in the Camrys were tested and measured. NHTSA reported that these measurements did not provide any basis for concluding that pedal misapplication was more likely in the Camry than in other vehicles (NHTSA 2011, 54). However, the testers observed that the accelerator pedal used for the ETC-equipped vehicles presented a "feel" different from that of the pedal in Camrys not having ETCs. Compared with the Model Year 2001 vehicles (which have cables linking the pedal to the throttle), depressing the pedal in the ETC-equipped Camrys caused the engine to produce power at a different rate and with a different level of operator effort. The testers also noted that the accelerator pedal force-versus-displacement effort in the 2002 ETC-equipped Camry was somewhat similar to the vehicle's brake pedal force-versus-displacement effort. The testers speculated that this pedal similarity could make it more difficult for a driver to discern the difference between the two pedals by their feel (NHTSA 2011, 53).

NASA Investigation of the Toyota ETC

In early 2010, NHTSA commissioned NASA's Engineering and Safety Center (NESC) to investigate whether vulnerabilities exist in the Camry ETC and whether any of them could be a plausible source of reported occurrences of unintended acceleration. By enlisting NASA, NHTSA was able to draw on specialized testing capabilities and engineering disciplines, including expertise in software analysis, electronics engineering, systems safety, and electromagnetic compatibility. NASA's report was released in February 2011.

NASA Study Approach and Key Results

NASA's investigation was multiphased. After identifying the critical functions of the ETC, the NESC team examined how the electronics system is designed and implemented to guard against failures and to respond safely when failures occur. The team then looked for vulnerabilities in these designs and their implementation. After it identified potential vulnerabilities, the team looked for evidence from the fleet of any of them having caused unintended acceleration characteristic of a large throttle opening. Vulnerabilities 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 in the fleet, the NESC team reviewed consumer complaints for hallmarks of the failures and tested vehicles and components previously used by drivers alleging unintended acceleration.

On the basis of its vulnerability analysis, the NESC team identified the following 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 accelerator command. The two scenarios are shown in Table 5-5, which is an abbreviated version of the failure mode and effects analysis (FMEA) performed by the NESC team during its vulnerability analysis.

To test the plausibility of the first scenario, NESC investigators used multiple tools to analyze software logic paths and to examine the programming code for paths that might lead to unintended acceleration. These extensive testing and analytic efforts did not uncover any evidence of problems, but the team pointed out that no practical amount of testing and analysis can guarantee that software is free of faults. The NESC software analysts reported that certain characteristics of the subject software (from a 2005 Camry) hindered the testing. For example, they found that the code structure relied on the use of a single large memory space shared among all tasks with unrestricted access (in contrast to designs where each task is given private memory inaccessible to other tasks). This lack of modularity reportedly precluded automated analysis and required more time-consuming manual inspection by analysts (NASA 2011, Appendix A, Section A.8.2). Thus, the NESC team's technical description of its analysis suggested a concern that the software was not structured to facilitate assessments of dependability to a high degree of confidence.

To examine the second scenario, the team tested numerous potential software and hardware failure modes by using bench-top simulators and by testing vehicles involved in reported cases of unintended acceleration. The vehicles were inspected for signs of electrical faults. They were also subjected to electromagnetic interference by using radiated and conducted levels in excess of those required for type certification by the European Union.[29] The electromagnetic interference tests did not produce

[29] As explained in Chapter 3, the European Union requires automobile manufacturers to subject their vehicles and systems to electromagnetic compatibility testing, whereas the United States does not.

TABLE 5-5 Abbreviated FMEA of Toyota ETC by NASA

Electronics Component	*Conditions Necessary for Failure to Occur, Failure Mode*	*Failure Condition and Symptoms Found in Real World*	*Physical or Electronic Evidence, Failure Detection*	*Range of Throttle Opening*	*Failure Effect Braking?*	*System Failure Response: Fail-Safe Modes Applied*	*System-Level Prevention*
Functional Area: Pedal Command							
Pedal sensors	Position sensor fail high, low, intermediate values	Pedal sensor failures in warranty data. NESC engineered test	DTC for high, low, outside operational lane. None if pedal sensor fails within lane and a DTC is set	Throttle does not open with single failure.		Limp-home mode—throttle limited to <15°. If neither sensor is operable then idle mode. Under certain conditions involving potentiometer sensors, limp-home mode is not limited and may jump depending on the rate at which the pedal is applied.	Idle mode fuel cut. Fuel cut limits <2,500 revolutions per minute when accelerator pedal released.
	Incorrect learned value. Dual failure to specific voltages that result in voltages within operational range	No evidence in warranty data. NESC engineered test	Engineered fault in lane. Valid pedal signal escapes detection, no DTC set. Electrical failures should leave trace.	Small opening, <10° max between normal sensor values and DTC limit		None. Dual failures look like valid pedal signal cannot be detected, but 10° opening max.	
	Dual failures that result in voltages within operational range	No signs of dual resistive failures. NESC engineered test	Engineered fault in lane. Valid pedal signal escapes detection, no DTC set. Electrical failures should leave trace.	Wide-open throttle is conceptually possible, but no real-world evidence.	>35° opening could deplete vacuum assist if brakes are pumped.	None. Dual failures that emulate or look like a valid pedal signal cannot be detected.	*None possible* for multiple failures that look valid

(continued on next page)

TABLE 5-5 (*continued*) **Abbreviated FMEA of Toyota ETC by NASA**

Electronics Component	*Conditions Necessary for Failure to Occur, Failure Mode*	*Failure Condition and Symptoms Found in Real World*	*Physical or Electronic Evidence, Failure Detection*	*Range of Throttle Opening*	*Failure Effect Braking?*	*System Failure Response: Fail-Safe Modes Applied*	*System-Level Prevention*
Functional Area: Throttle Control Computer							
Main CPU	Faulty power, memory failure	ECM failures in warranty data. NESC engineered test	DTC set for bad power, memory fault, consistent data	None		Engine turned off	Engine turned off
Sub-CPU	Faulty power, memory failure	ECM failures in warranty data. NESC engineered test	DTC set for bad power, memory fault, consistent data	None		Engine turned off	Engine turned off
Main CPU software	Software unilaterally opens throttle with pedal released, idle fuel cut not active, watchdog serviced, no EDAC error, sub-CPU does not detect failure.	Cannot engineer a test. No place found in software where a single memory/variable corruption results in unintended acceleration.	Theoretical fault escapes detection.	Wide-open throttle is conceptually possible, but no real-world evidence.	>35° opening could deplete vacuum assist if brakes are pumped.	Engineered fault escapes detection.	*None possible,* malfunctioning computer opens throttle and appears normal without DTC, watchdog timeout, limp-home mode, or other errors.

Note: CPU = central processing unit; ECM = error-correcting memory; EDAC = error detection and correction. Shaded cells indicate scenarios that can theoretically lead to an uncommanded large throttle opening.

Source: NASA 2011, Table 6.5.2.2-1, page 77.

acceleration indicative of a large throttle opening, but some produced engine slowing and stalling.

After contacting a consumer who had complained about unusual accelerator pedal responses, ODI recovered the vehicle's accelerator pedal assembly, which it turned over to the NESC team for analysis. The faulty assembly was found to contain a low-resistance path, which was determined to have been caused by an electrically conductive tin whisker (a crystalline, hairlike structure of tin that can form on a tin-finished surface) that had formed between signal outputs from the potentiometer pedal position sensors.[30]

Consideration was given to whether low-resistance paths in the pedal position sensing system—whether created by tin whiskers or other means[31]—could have produced unintended acceleration indicative of a large throttle opening. The NESC 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. However, for a vulnerability to be created, the two fault conditions would need to escape detection by meeting restrictive criteria consisting of a specific resistance range as needed to create the exact circuit configuration in a correct time phase. If the two faults did not meet these criteria, they would be detected and trigger a diagnostic trouble code (DTC) and a system fail-safe response such as reduced engine power.

To gain a better understanding of the probability of the two fault conditions occurring in the field, the NESC team examined Camry warranty repair data and consumer complaints of high-power unintended acceleration. The team posited that for every instance in which two undetected faults had led to an episode of unintended acceleration, numerous pedal repairs associated with single detected faults would be expected, since they would be much more likely than two faults having highly restrictive resistance ranges, circuit configurations, and timing phases.

In May 2010, ODI had requested warranty claim data from Toyota on all vehicles equipped with ETCs sold in the United States. In particular, ODI asked for details on any warranty claim involving an ETC hardware

[30] As discussed in Chapter 3, these sensors provide a voltage output to the engine control module that is proportional to the pedal's displacement when it is pressed by the driver. The engine control module uses the pedal position sensing information, along with information provided by other sensors, to adjust the throttle plate.

[31] Although the NESC team found evidence of tin whiskers, low-resistance paths can also be produced by the presence of moisture, salt spray, and other contaminants.

component, the engine control module, the throttle actuator, the accelerator pedal, any related wiring or harness connectors, and any DTCs that could be associated with a failure of the ETC. In reviewing the warranty data generally, ODI had determined that claim rates for the Camry components (per vehicle sold) were much lower than the claim rates typically found for defective components in other vehicle systems that had been the subject of safety recalls and were thus not suggestive of a defect trend in the Camry ETC.

The NESC team also reviewed the Camry warranty repair data for DTCs and repair items indicative of problems in the relevant accelerator pedal sensors and circuitry (NASA 2011, 37–41). The team found *fewer* warranty repair items than driver reports of high-power unintended acceleration and concluded that the warranty repair data "does not support an observable failure signature of pedal-induced DTCs" (NASA 2011, 16). In short, the warranty data indicated that the postulated dual-fault scenario involving the Camry pedal sensor system was an implausible source of the high-power unintended acceleration reported in consumer complaints.

Finally, the NESC team reported that its testing revealed ways in which a single-failure mode could cause relatively small throttle openings leading to controllable engine behaviors such as high idle speed, hesitation, and "jumpiness." The team noted that while some of these conditions did not trigger a DTC during testing, they were eliminated by releasing the accelerator pedal or could be overridden by applying the brakes. These controllable behaviors were inconsistent with reports of high-power unintended acceleration. The NASA investigators thus concluded that its testing and analysis "did not find that [the Toyota ETC] electronics are a likely cause of throttle openings as described in the VOQs" (NASA 2011, 17).

NHTSA's Response to NASA Results

On the basis of the NESC team's study, NHTSA has concluded "that the Toyota ETC system does not have design or implementation flaws that could reasonably be expected to cause UA [unintended acceleration] events involving large throttle openings as described in consumer complaints to NHTSA" (NHTSA 2011, 62). Specifically with respect to the postulated dual-fault scenario in the ETC's pedal position sensing system, NHTSA concurred that the absence of significant numbers of warranty repairs for more likely single faults is indicative of a hypothetical scenario

and not one "occurring in the real world" (NHTSA 2011, 63). NHTSA likewise concurred that the other forms of unintended acceleration created by single faults do not create large throttle openings and are likely to be rare and controllable; in NHTSA's view, they do not present a safety hazard. NHTSA acknowledged that Toyota's fail-safe strategy for the ETC studied can be characterized as imperfect because it does not respond to all theoretical failure pathways but concluded that "there is currently no evidence of a real-world safety risk produced by this phenomenon" (NHTSA 2011, 63).

NHTSA also noted that the NESC team's study did not reveal any ETC failure mode that could affect the vehicle's braking system (NHTSA 2011, 64), and hence any lack of braking effectiveness reported by a driver experiencing unintended acceleration could not be attributed to a shortcoming in the ETC.

On the basis of NASA's study and its own series of analyses and investigations, NHTSA outlined several steps that it planned to take in response to the findings, some of which were discussed in Chapter 4. It indicated that it will consider initiating new rulemakings to require (*a*) installation of systems that cause the brake to override the throttle, to prevent or mitigate unintended acceleration incidents (e.g., in the case of pedal entrapment); (*b*) measures to ensure that keyless ignition systems can be turned off by drivers during an on-road emergency; and (*c*) installation of EDRs on all new vehicles. NHTSA also indicated that it would consider research on the layout and spacing of accelerator and brake pedals, the utility of DTCs in conveying safety-critical information to drivers, and robust software development processes and fail-safe strategies to protect against multifault scenarios. The committee comments on some of these proposed initiatives in the next chapter.

CHAPTER FINDINGS

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.* The two main types of unintended acceleration incidents involving a large throttle opening are those in which rapid acceleration occurs suddenly when the vehicle is in a stopped position, moving slowly, or in the process of slowing down and those in which a moving vehicle maintains or increases its speed after

the driver releases the accelerator pedal. Degraded or failed braking is often asserted along with both of these forms of unintended acceleration. A range of other vehicle behaviors, from high engine idling to surging and transmission hesitations, are sometimes characterized as unintended acceleration. They are controllable and do not present the same safety hazard as acceleration involving a large throttle opening unless the vehicle behavior prompts an unsafe response by the driver, such as accidentally applying the accelerator pedal instead of the brake.

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.* Other commonly identified problems include malfunctioning mechanical components in the throttle control system, such as frozen and broken throttle plates, and frayed and trapped connector cables. NHTSA attributes forms of unintended acceleration involving a large throttle opening occurring in stopped and slow-moving vehicles to pedal misapplication, unless there is a credible explanation of why the vehicle's brakes were not applied or why they failed to stop and control the engine torque if they were applied. Braking action may not control unintended acceleration occurring in vehicles traveling at faster speeds under limited circumstances. Such incidents are investigated for other potential causes, including pedal entrapment and sticking and malfunctioning throttle control systems, and for evidence of brake damage caused by prolonged brake application.

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.* Reports of braking ineffectiveness in controlling a vehicle experiencing the onset of unintended acceleration from a stopped position or when moving slowly require an explanation for the ineffectiveness, such as physical evidence of damage to the brake system. Under these circumstances, investigating for phenomena other than pedal misapplication absent an explanation for the ineffectiveness of brakes, which are independent of the throttle control system and are designed to dominate engine torque, is not likely to be useful. Full consideration of the causes of pedal misapplication requires that vehicle design and operational conditions that can affect a driver's actions to control the vehicle be taken into account.

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.* In its investigations of such cases, NHTSA has usually concluded that the acceleration was caused by faulty mechanical components or the accelerator pedal becoming stuck or entrapped, often by a floor mat. NHTSA did not have a prior technical basis for suspecting the ETC as an alternative cause of such unintended acceleration events reported by owners of Toyota vehicles. Nevertheless, NHTSA commissioned a team of engineering specialists from NASA to investigate the potential for Toyota's ETC to produce unintended acceleration.

Finding 5.5: *NHTSA's decision to close its investigation of Toyota's 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 NASA.* In its initial investigations of complaints and examinations of warranty repair data, NHTSA did not find evidence implicating the ETC as a cause of unintended acceleration reported by drivers of Toyota vehicles. It confirmed the occurrence of pedal entrapment and sticking in some reported cases and the signature characteristics of pedal misapplication in others. The subsequent NASA investigation did not yield evidence contradicting these conclusions. NASA identified means by which vulnerabilities in the ETC could produce unintended acceleration but could not find evidence that these means offered a plausible explanation for any occurrences of high-power unintended acceleration observed in the fleet.

Finding 5.6: *The VOQ 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 pedal misapplication, and to aid investigators in identifying pedal entrapment by floor mats as the likely cause.* Other data available to ODI for monitoring the fleet for defects, including warranty repair information submitted quarterly by Toyota as part of the Early Warning Reporting system, were consulted in response to the suspicious VOQ patterns. These data did not provide indications of malfunctioning ETCs

or any other vehicle defects as possible causes. Unintended acceleration resulting from pedal entrapment or pedal misapplication would not be expected to be revealed by warranty repair data; thus, in this sense the absence of suspect patterns in the warranty data corroborated ODI's conclusions that floor mat entrapment was the cause of the increase in the Toyota complaints uncharacteristic of pedal misapplication.

Finding 5.7: *ODI's investigation of unintended acceleration in Toyota vehicles indicated how data saved in EDRs can be retrieved from vehicles involved in crashes to supplement and assess other information, including circumstantial evidence, in determining causal and contributing factors.* In this instance, the EDR data corroborated investigator findings of unintended acceleration occurring through pedal misapplication.

REFERENCES

Abbreviations

NASA	National Aeronautics and Space Administration
NHTSA	National Highway Traffic Safety Administration
NTSB	National Transportation Safety Board
OIG	Office of Inspector General, U.S. Department of Transportation

Brackett, R. Q., V. J. Pezoldt, M. G. Sherrod, and L. Roush. 1989. *Human Factors Analysis of Automotive Foot Pedals.* DOT-HS-807-512. National Highway Traffic Safety Administration, Washington, D.C.

NASA. 2011. *National Highway Traffic Safety Administration Toyota Unintended Acceleration Investigation: Technical Support to the National Highway Traffic Safety Administration (NHTSA) on the Reported Toyota Motor Corporation (TMC) Unintended Acceleration (UA) Investigation.* Jan. 18. http://www.nhtsa.gov/staticfiles/nvs/pdf/NASA-UA_report.pdf.

NHTSA. 2011. *Technical Assessment of Toyota Electronic Throttle Control (ETC) Systems.* Feb. http://www.nhtsa.gov/staticfiles/nvs/pdf/NHTSA-UA_report.pdf.

NTSB. 2009. *Highway Special Investigation Report: Pedal Misapplication in Heavy Vehicles.* http://www.ntsb.gov/doclib/safetystudies/SIR0902.pdf.

OIG. 2011. *Process Improvements Are Needed for Identifying and Addressing Vehicle Safety Defects.* Report MH-2012-001. Oct. 6.

Pollard, J., and E. D. Sussman. 1989. *An Examination of Sudden Acceleration.* Report DOT-HS-807-367. Transportation Systems Center, U.S. Department of Transportation.

Reinhart, W. 1994. The Effect of Countermeasures to Reduce the Incidence of Unintended Acceleration Accidents. Paper 94 S5 O 07. *Proc., 14th International Technical Conference on Enhanced Safety of Vehicles,* Washington, D.C., Vol. 1, pp. 821–845.

Rogers, S. B., and W. W. Wierwille. 1988. The Occurrence of Accelerator and Brake Pedal Actuation Errors During Simulated Driving. *Human Factors,* Vol. 31, No. 1, pp. 71–81.

Schmidt, R. A. 1989. Unintended Acceleration: A Review of Human Factors Contributions. *Human Factors,* Vol. 31, No. 3, pp. 345–364.

Vernoy, M. W., and J. Tomerlin. 1989. Pedal Error and Misperceived Centerline in Eight Different Automobiles. *Human Factors,* Vol. 31, No. 4, pp. 369–375.

Walter, R., G. Carr, H. Weinstock, E. D. Sussman, and J. Pollard. 1988. *Study of Mechanical and Driver-Related Systems of the Audi 5000 Capable of Producing Uncontrolled Sudden Acceleration Incidents.* Report DOT-TSC-NHTSA-88-4. Transportation Systems Center, U.S. Department of Transportation.

Recommendations to National Highway Traffic Safety Administration on Preparing for the Electronics-Intensive Vehicle

This report describes how

- Increasingly software-intensive electronics systems are being used in automobiles to provide capabilities that are both related and unrelated to vehicle safety (Chapter 2);
- Automotive manufacturers seek to ensure the performance of these electronics systems through preventive and fail-safe measures implemented during product design, development, and manufacturing as well as through lessons learned from postproduction surveillance (Chapter 3); and
- The National Highway Traffic Safety Administration's (NHTSA's) regulatory, research, and defect surveillance and investigation programs are oriented and applied to oversee the performance of vehicles and their constituent electronics systems (Chapter 4).

In reviewing NHTSA's response to reports of unintended acceleration, Chapter 5 provides a concrete example of much of the subject matter of these earlier chapters. It discusses how NHTSA has sought to address concerns about whether one electronics system, Toyota's electronic throttle control system (ETC), has performed safely. The discussion provides insight into the agency's defect surveillance and investigation processes and an example of how one automotive manufacturer has sought to ensure the performance of a safety-critical electronics system. The public apprehension and controversy that have surrounded Toyota's

ETC suggest the potential for other electronics systems to become implicated in safety concerns, particularly as electronics systems assume more vehicle safety and control functions.

In requesting these reviews, NHTSA tasked the committee with making recommendations on how the agency's regulatory, research, and defect investigation activities can be strengthened to meet the safety assurance challenges associated with the increasing use of electronics systems. The various findings from Chapters 2 through 5, which are summarized in Box 6-1, are synthesized in the following discussion and provide the basis for several recommendations to NHTSA.

NHTSA's CURRENT ROLE WITH RESPECT TO VEHICLE ELECTRONICS

NHTSA recognizes that electronics systems are transforming the automobile and in the process giving rise to opportunities for making driving safer and to new demands for ensuring that vehicles operate in a safe manner. For example, NHTSA now requires that new vehicles possess certain safety-enhancing capabilities that only electronics can provide, such as electronic stability control intended to aid in rollover prevention. Similar safety regulations may be promulgated in the future as agency researchers evaluate and monitor the development status of other technologies for crash avoidance, such as automatic lane-keeping, crash-imminent braking, alcohol detection, and blind spot surveillance. Because of the use of electronics systems in managing and controlling more vehicle functions, NHTSA's Office of Defects Investigation (ODI) is observing more manufacturer recalls that involve software reprogramming and other fixes to electronics systems. This is to be expected as software-intensive electronics supplant more mechanical, electromechanical, and hydraulic systems.

The growth of electronics systems in vehicles is thus influencing all aspects of NHTSA's regulatory, research, and investigation activities. That influence will almost certainly grow and place new demands on all of these activities. Public apprehension about Toyota's ETC and its role in unintended acceleration revealed these changing demands in stark fashion. The ETC is a simple technology compared with the newer systems being introduced and envisioned for motor vehicles. As these electronics systems become more complex, capable, and interconnected

BOX 6-1

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.

(continued on next page)

Box 6-1 (*continued*) Summary of Findings

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 (FMVSSs) 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 of traffic crash data indicating where focused research can fur-

Box 6-1 (*continued*) Summary of Findings

ther the introduction of new regulations and vehicle capabilities aimed at mitigating known safety problems.

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 FMVSSs 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.

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

(continued on next page)

Box 6-1 (*continued*) Summary of Findings

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 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 National Aeronautics and Space Administration's examination of the Toyota ETC.

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 pedal misapplication, and to aid investigators in identifying pedal entrapment by floor mats as the likely cause.

Finding 5.7: ODI's investigation of unintended acceleration in Toyota vehicles indicated how data saved in EDRs can be retrieved from vehicles involved in crashes to supplement and assess other information, including circumstantial evidence, in determining causal and contributing factors.

with one another, not only will safety assurance demands grow but so too will the challenge of building and maintaining public confidence in their safe performance (see Finding 4.1).

NHTSA does not regulate vehicle electronics directly. Through its Federal Motor Vehicle Safety Standards (FMVSSs), the agency requires that vehicles have certain safety-critical features and capabilities and that they perform to certain levels (see Finding 4.2). The regulatory emphasis on system performance rather than design is evidenced by the fact that the throttle control system in some vehicles might still rely on mechanical links from the accelerator pedal to the throttle, whereas others may make this connection through an ETC consisting of sensors, wires, computers, and motorized actuators. Since NHTSA does not require a specific design, it does not require, advise on, or evaluate the methods used by automotive manufacturers in design-specific areas such as corrosion testing, electromagnetic compatibility, resistance to vibrations, or software integrity. For the most part, NHTSA's FMVSSs do not address such aspects of product assurance, which are left to the manufacturer to decide.

Furthermore, the FMVSSs do not cover the vast majority of systems that are in today's vehicles, much less all electronics systems. Only a fraction of the electronics systems in the modern automobile are intended to provide an FMVSS-regulated safety capability. The manufacturer, therefore, is responsible for ensuring that these other systems do not create safety hazards through their design or interaction with safety-critical vehicle systems. For example, the FMVSSs require that certain vehicle control mechanisms, such as the gearshift lever, be located within safe reach of the driver, but the regulations are silent about similar controls for nonsafety features such as the radio and navigation system. NHTSA does not provide specific guidance or standards for the design of these unregulated systems with regard to safety. Similarly, the FMVSSs do not prescribe how electronics and other systems must be designed to avoid interfering with the functioning of systems that are intended to meet an FMVSS, such as keeping an entertainment system from interfering with the required performance of wipers.

NHTSA enforces the use of safe system designs and compels effective safety assurance by manufacturers through its compliance testing program and defect surveillance and investigation activities (see Finding 4.3). Moreover, ODI's scope of interest is much wider than enforcing compliance with FMVSSs; it can monitor, investigate, and seek remedies for any vehicle-related deficiency considered to be harmful to public safety. ODI's

investigation of floor mats as a possible cause of unintended acceleration and its influence over Toyota in recalling millions of its vehicles for pedal entrapment demonstrate ODI's wider scope of interest and authority.

NHTSA's vehicle safety research programs are focused on supporting agency decision making, particularly regulatory decisions (see Finding 4.4). This emphasis is consistent with the agency's mission of addressing known traffic safety problems while it avoids entanglement in the specific technological means by which automotive manufacturers meet the FMVSSs. Agency researchers do not generally develop technologies.[1] Instead, they examine emerging technologies to advise regulators on whether new safety-enhancing vehicle capabilities are technically feasible and could thus be required. The agency assumes that manufacturers will undertake the requisite research to obtain the design and engineering knowledge to establish appropriate safety precautions for their products.

KEEPING PACE WITH THE SAFETY ASSURANCE CHALLENGES ARISING FROM VEHICLE ELECTRONICS

As electronics systems proliferate in vehicles, it is reasonable to ask whether NHTSA's oversight and regulatory approach will need to be adjusted to keep pace with the safety assurance challenges these systems present. The ETC experience may be a harbinger of the demands to come. The fact that NHTSA was subjected to and could not respond convincingly to public concerns about Toyota's ETC and needed to enlist the technical expertise of the National Aeronautics and Space Administration indicates how demands on the agency's programs are changing.

The committee cannot predict the extent to which NHTSA's vehicle safety programs will need to be supplemented over time with new resources, competencies, and infrastructure as electronics continue to take over more vehicle controls. The findings in this study suggest that NHTSA will need to know more about how manufacturers design safety and security into electronics systems, monitor vehicles for evidence of safety deficiencies that may have new hallmarks, and investigate and test for problems in systems that may leave little physical evidence from

[1] NHTSA research has led to the development of some technologies used by the automotive industry, such as instrumented crash-test dummies used by automotive manufacturers during vehicle development and testing.

which to assess their cause. The remainder of this section discusses the implications of the proliferation of electronics systems for NHTSA oversight and engagement.

The controversy over whether ETCs caused unintended acceleration and the general trend toward increasing use of electronics systems for vehicle controls have raised questions about whether NHTSA should exert more influence over the safety assurance processes followed by industry.[2] Although it is not an immediate option, NHTSA could move to regulate these processes by establishing or approving testing methods used for electronic control systems and their components, such as testing for resistance to electromagnetic disturbances or software coding integrity. Such in-depth oversight appears to be unlikely. It is difficult to see how NHTSA could obtain the capacity for identifying suitable testing methods in light of the wide variability in the way manufacturers design and engineer vehicle systems. A more foreseeable option is for NHTSA to require that automobile manufacturers provide evidence that they have followed rigorous safety assurance processes during the design, development, and manufacture of electronics systems having implications for vehicle safety.

Chapter 3 reviews how automotive manufacturers seek to ensure the safe performance of their electronics systems. This study could not assess the quality of these processes or how well they are executed. Nevertheless, Chapter 3's review suggests that automotive manufacturers use many of the same fundamental processes for safety assurance and that they are systematic and carefully thought through (see Findings 3.1, 3.2, and 3.3). The processes consist of measures intended to guard against failures up to defined risk probabilities and to detect and respond to failures that do occur. Their design relevance and the system-level structure of these processes suggest the futility of NHTSA (or any other regulator) prescribing specific testing methods, preventive measures, fail-safe strategies, or other assurance processes.

The closest example of a regulatory agency having such hands-on safety assurance responsibility in the U.S. Department of Transportation is the Federal Aviation Administration's (FAA's) oversight of aircraft development and manufacturing. Even FAA recognizes the impracticality of prescribing specific design and testing processes. Instead, the agency's emphasis is on requiring manufacturers to demonstrate that they

[2] See "Response by Toyota and NHTSA to Incidents of Sudden Unintended Acceleration." Hearing before the U.S. House of Representatives Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, February 23, 2010.

have established robust and carefully followed safety assurance systems. These assurance systems can be examined in depth by FAA because aircraft manufacturers must apply to the regulatory agency for approval to build a new aircraft type. Accordingly, FAA verifies and certifies that aircraft manufacturers have instituted sound safety assurance systems through preapproval of plans and reviews of their implementation. To facilitate compliance, FAA advises manufacturers to follow certain preapproved processes for aspects of product development, including safety assurance standards developed by industry.

FAA's approach to safety oversight requires significant resources and authorities (see Finding 4.6). Although the agency designates senior engineers from aircraft manufacturers to fulfill many of the detailed document reviews and inspections that make up the certification process, FAA staff must review the most significant process elements. As discussed in Chapter 4, FAA has a major unit, the Aircraft Certification Service, dedicated to this function and housed in more than two dozen offices across the country and abroad. The Aircraft Certification Service requires a large cadre of test pilots, manufacturing inspectors, safety engineers, and technical specialists in key disciplines such as flight loads, nondestructive evaluation, flight management, and human factors.

For NHTSA to engage in similar regulatory oversight would represent a fundamental change in the agency's regulatory approach and would require justification and substantial resources. The introduction of autonomous vehicles, as envisioned in some intelligent vehicle concepts, could one day provide the grounds for NHTSA to adopt an oversight approach with elements modeled after those of FAA. At the moment, the justification for such a fundamental change in the way NHTSA regulates automotive safety is not evident, nor is such a change in regulatory direction a foreseeable prospect.

The near-term prospect is an effort to establish a consensus standard through the International Organization for Standardization (ISO) intended to guide automotive manufacturers as they develop their safety assurance processes, particularly for electronics systems affecting vehicle safety and control functions (see Finding 3.4). The pending standard, ISO 26262, will not prescribe the specific content of each manufacturer's safety assurance regime. However, it will compel subscribers to follow steps ensuring that the safety implications of electronics systems are well identified, analyzed for risks, and the subject of appropriate risk management actions. How influential this voluntary standard will become is not yet known,

but many manufacturers selling vehicles and automotive equipment in the United States appear to be intent on following its guidance in whole or in large part.

Whether widespread industry adherence to a process-based standard like ISO 26262 will lead to safer-performing vehicle electronics will depend to a large extent on the adequacy of existing manufacturer assurance processes and the degree to which manufacturers change their processes in response to the standard's guidance. The industry's apparent intention to follow ISO 26262 may give NHTSA greater confidence that manufacturers are striving to keep abreast of the challenges associated with electronics. Even if the agency does not endorse or require adherence to the standard, NHTSA will have a keen interest in ensuring the standard's safety effectiveness if many automotive manufacturers choose to follow it.

As a general matter, **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 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.

The introduction of ISO 26262 represents a potential opportunity for NHTSA to engage and collaborate with industry. As manufacturers reassess and adjust their safety assurance processes in response to the ISO standard and other industry-level guidance, many will undoubtedly need more information and analysis. Some will have research needs that NHTSA may be able to help meet. In the committee's view, support for this industry research can be a practical means by which NHTSA engineers and other personnel can increase their familiarity with industry safety assurance processes. Box 6-2 gives examples of where collaborative research and analysis supported by NHTSA may contribute to the strengthening of industry safety assurance processes and to the agency's own technical knowledge and competencies.

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

BOX 6-2

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 (e.g., levels, frequency range), and probability of occurrence of electromagnetic environments produced by other vehicles (e.g., radar transmitters), on-board consumer devices (both emissions and intentional transmissions), and other electromagnetic sources in the vicinity of the roadway (e.g., commercial radio stations, military radar systems). Study the potential operating impacts of these exposures on safety-critical vehicle electronics by consulting with experts in electromagnetic compatibility and by seeking their advice on design, testing, and control strategies relating to functional safety.
- 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. Review ways of reducing these vulnerabilities. Among the possibilities to examine are means to isolate safety-critical components, to restrict network access, and to use security engineering approaches such as improving code robustness and scheduling authenticated software updates.

Box 6-2 (*continued*) Candidate Research and Analysis to Inform Industry Safety Assurance Processes

- Examine the implications of electronics systems for the means by which automotive manufacturers are complying with the intent of the FMVSSs, 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.
- 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. Vehicle electronics that take the initiative in monitoring the roadway and controlling the vehicle might fundamentally change the demands placed on the driver and driver expectations with regard to vehicle behavior. Such studies should address the potential for multiple sources of information and warnings to distract and overload drivers, as well as the tendency for increasingly sophisticated vehicle automation to lead drivers to entrust more responsibility for driving to the vehicle than the designers intend.
- Collaborate with the automotive industry in developing effective methods for communicating the operational status of vehicle electronics to the driver. Examine how drivers interpret dashboard indicator icons and their suitability for conveying the operational status of more complex vehicle systems, such as indicating changes in vehicle behavior associated with the "limp home." While advances in display media, such as liquid crystal displays, are allowing the use of more elaborate warning icons and messages to communicate vehicle status, research can help develop a common "language" to ensure that drivers understand the intended message.

view, because NHTSA cannot be expected 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).**

STRENGTHENING CAPABILITIES FOR DEFECT SURVEILLANCE AND INVESTIGATION

ODI's role in monitoring the fleet for safety defects and ensuring that automotive manufacturers correct them quickly and effectively is an important part of NHTSA's safety mission (see Finding 4.3). As noted earlier, ODI's defect surveillance and investigation authorities go well beyond identifying deficiencies that pertain to the specific requirements of FMVSSs. ODI has authority to monitor, investigate, and seek remedies for any vehicle-related deficiency considered to be harmful to public safety. This postmarket safety monitoring capability has always been important to NHTSA, since it cannot assess all of the preventive and fail-safe measures that manufacturers implement during system design and manufacturing. Such measures will likely become even more complex as electronics functions grow.

Access to timely information on the behaviors and conditions exhibited by vehicles is vital to ODI's ability to monitor for safety deficiencies, identify vehicles warranting further investigation, and assess the prevalence and consequences of a vehicle safety deficiency (see Finding 4.3). The main data available to ODI for these purposes are the safety complaints lodged on an ongoing basis through the agency's Internet- and telephone-based Vehicle Owner's Questionnaire (VOQ).

Among the challenges ODI's analysts face in examining VOQs is that much of the information vital for assessing vehicle conditions and their causes can be found only in the narrative section of the form, if the infor-

mation is conveyed at all. Because the VOQ does not have a field in which consumers can choose from a common set of vehicle behaviors such as hesitation, high idling, and degraded braking, ODI analysts must review and manually categorize the relevant information conveyed in each complaint narrative. Even when they are aided by computer text searches, such manual analyses can be time-consuming and overlook trends and relationships that more quantitative analytic methods might detect.

ODI investigators also reported to the committee that the proliferation of electronics systems in vehicles is creating new challenges for "trouble shooting" the vehicle behaviors that are detected through consumer complaints and other means. Among the other data ODI has at its disposal for defect analysis and investigation are the quarterly submissions by manufacturers on warranty repairs, vehicles produced, claim notices, consumer complaints, and field investigation reports as required by the Early Warning Reporting (EWR) provisions of the Transportation Recall Enhancement, Accountability, and Documentation Act of 2000.[3] These data were originally intended to aid ODI with defect surveillance. Because the reports are submitted by manufacturers only four times per year, they may not provide the desired early information for detecting safety problems in their incipiency.[4] However, once a vehicle defect or safety problem is suspected through complaints analysis or other means, the EWR data can serve a supplemental or corroborating role (for example, by enabling investigators to check for indications of problems by consulting warranty repair data) (see Finding 5.6). To obtain more in-depth information such as more detailed warranty and parts records, ODI can query the manufacturer, as it did when it examined Toyota's ETC.

As discussed in Chapter 4, the U.S. Food and Drug Administration (FDA) needs detailed data for monitoring and investigating the safety performance of medical devices. FDA has established a network of hospital administrators and clinicians who volunteer more detailed information on device performance. According to FDA officials who met with the committee, the network is designed to provide timely and detailed information for both safety surveillance and more thorough defect investigations. The agency can query network participants for information on the performance of devices under investigation, and

[3] Public Law 106-414. The law also requires manufacturers to make a report to NHTSA within 5 days of the time a safety defect is identified and a recall initiated.

[4] ODI briefing to committee, June 30, 2010.

participants regularly submit device performance information to FDA's surveillance program, including reports on safety-related "close calls." This industry-assisted monitoring network may provide a model for NHTSA to follow in obtaining more detailed information on the safety performance of electronics (see Finding 4.7).

During the Toyota ETC investigation, ODI was substantially aided by the availability of information on the actions of the driver and the status of the vehicle obtained from vehicle event data recorders (EDRs) (see Findings 2.5 and 5.5). These data, including recordings of the brake status and accelerator pedal position, were used to supplement and corroborate other information obtained during crash investigations, such as eyewitness accounts, the driver's stated actions, vehicle inspections, and physical evidence from the crash scene.

Because most new vehicles are equipped with EDRs, their utility for crash investigations is likely to grow, and they may be helpful in assessing whether new electronics systems have mitigated or contributed to a crash.[5] However, most EDRs only save data in the event of a crash that triggers an air bag deployment or vehicle accelerations in multiple directions. EDR data are thus not available for the investigation of less serious crashes or the thousands of consumer complaints alleging unsafe vehicle behaviors, including most cases of unintended acceleration, that do not result in crashes. To aid investigations into these cases, a recorder would need to log data continually and capture more aspects of the vehicle's subsystem states and network traffic, and perhaps save the data in response to a detected unusual vehicle condition or behavior or even on request by the driver.

The committee believes that ODI will need to seek ways to strengthen its capabilities and processes for defect monitoring, analysis, and investigation in response to the increasing use of electronics systems in automobiles. Accordingly, **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**

[5] The utility of EDR data for crash investigations will also be affected by legal issues governing investigator access to the stored data.

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).

In keeping with this recommendation, the committee believes that NHTSA should consider dedicating research to support improvements in ODI's surveillance and investigative processes and capabilities. Research to identify ways to improve the quality and timeliness of consumer complaint data; the tools and methods used by ODI to analyze these data; and the skill sets and testing infrastructure needed by analysts and investigators to support defect surveillance, analysis, and assessment should be considered. Several candidate research and analysis topics for these purposes are given in Box 6-3.

REACTION TO NHTSA's PROPOSED NEXT STEPS

NHTSA (2011) 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 consider the following:

- A rulemaking that would mandate the installation of EDRs on all light-duty vehicles and a proposal to consider future enhancements of EDR capabilities and applicability,
- An update of the accelerator control standard (FMVSS 124) examining revisions of performance test procedures for ETC-equipped vehicles and a requirement that systems be installed that can override the throttle through brake application,
- An update of the standard governing keyless ignitions (FMVSS 114) examining revisions that may be needed to ensure that drivers are able to turn off the engine in the event of an on-road emergency,[6] and
- Pedal-related research that would examine pedal placement and spacing practices to prevent entrapment or misapplication.

[6] On December 12, 2011, NHTSA issued a Notice of Proposed Rulemaking to address safety issues arising from keyless ignition controls and their operation (Docket No. NHTSA-2011-0174) (*Federal Register,* Vol. 76, No. 238).

BOX 6-3

Candidate Research and Analysis to Support ODI Capabilities and Functions

- Examine modifications to the VOQ 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. Consideration might be given to new features in the online questionnaire, such as drop-down menus with condition choices or uploading capabilities, that can make the questionnaire easier to complete and provide drivers more opportunity to convey details on the vehicle and its condition and behavior.
- In collaboration with manufacturers, 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. The examination should seek to identify weaknesses in these processes and means by which they have been strengthened.
- Investigate and make recommendations on ways to obtain more timely and detailed EWR-type data for defect surveillance and investigation. For example, consideration might be given to the creation of a voluntary network of automotive dealers and major repair centers to which ODI can turn for more timely and detailed vehicle servicing, repair, and parts data for defect monitoring and investigation. FDA's network for obtaining safety performance data on medical devices might serve as a model. To the extent that NHTSA can make use of current dealer–original equipment manufacturer networks for this data-gathering purpose, the inflexibilities associated with mandated data reporting systems such as the EWR could be reduced. NHTSA's Crash Injury Research Engineering Network program for collecting data for research on crash injuries offers another potential conceptual model for a collaborative forum.

Box 6-3 (*continued*) Candidate Research and Analysis to Support ODI Capabilities and Functions

- Examine how the data from consumer complaints of unsafe experiences in the field can be mined through electronic means and how the complaints might offer insight into safety issues that arise from human–systems interactions. Explore how these issues may be changing with the introduction and expansion of vehicle electronics systems.

The committee is not in a position to know where these initiatives should rank among NHTSA's research and rulemaking priorities. Nevertheless, **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 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 of failures. 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. In the committee's view, the utility and feasibility of equipping vehicles with more advanced data-recording systems that can log a wider range of data warrant further study and are thus among the candidate research topics identified in Box 6-2.

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). A number of examples of research that could be pursued through such a program are given in Box 6-2.

STRATEGIC PLANNING TO GUIDE FUTURE DECISIONS AND PRIORITIES

The four priority items above represent specific agency responses to the events surrounding unintended acceleration. The next priority plan may list more such items, some in response to newly arising safety concerns. Asked to advise NHTSA on its rulemaking, research, and resource priorities, the committee questions the wisdom of recommending the addition to this list of more narrowly construed initiatives and whether doing so would be at odds with the agency developing an effective longer-term strategy for meeting the safety demands arising from vehicle electronics. The committee notes that the current priority plan describes the Office of Vehicle Safety as being "currently in the process of developing a longer-term motor vehicle safety strategic plan that would encompass the period 2014 to 2020" (NHTSA 2011, 1). Presumably, this strategic plan could provide a road map for NHTSA's decisions with regard to the safety oversight challenges arising from the electronics-intensive vehicle; however, the plan's status and purpose have 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 Box 6-4. 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

BOX 6-4

Elements of a Strategic Planning Process

In the committee's view, the following are fundamental to strategic planning:

- Involved and supportive management led by senior staff,
- Cross-functional participation from throughout the organization,
- Third-party facilitation and other influential outside participants,
- The expectation that the process will take time and effort and not be completed in one or two meetings, and
- Regular updates made available to the public and decision makers.

The following are key process elements:

- Define the agency mission and principal agency activities
- State goals and desired outcomes
- Assess the external environment. The following are example considerations:
  - Who are the prime "customers" of the agency?
  - What are their expectations, and are they changing?
  - How is the technology of the automobile changing fundamentally, and how is this affecting the agency in fulfilling its mission or role?
  - How will technology continue to change?
  - Which external organizations have a major impact on the agency's functioning, and what is the agency's relationship with them?
  - What data are important in executing the agency's role effectively?

(continued on next page)

Box 6-4 (*continued*) Elements of a Strategic Planning Process

  - How can technology changes, such as the Internet and its instant communications, be expected to affect the agency, positively and negatively?
  - How might adversaries utilize the vehicle fleet for harm? What can be done about it?
- Assess the agency. The following are example considerations:
  - What are the agency's strengths and weaknesses (unit by unit)?
  - Has the agency's role changed over the years? Has the agency adapted to those changes? How?
  - Is the agency's staffing of the various functions consistent with the needed activity level in those functions? Is it consistent with the technology level?
  - What are the strengths and weaknesses of the databases used by the agency in conducting its work? For example, what do the databases indicate in terms of changing reasons for recalls and changing corrective actions?
  - Is the agency using the technology of the Internet and modern information technology in general to enhance performance of its role?
  - What are the strengths and weaknesses of the agency's relationship with the industry it monitors and regulates?
  - What are the strengths and weaknesses of the FMVSSs in terms of the automotive technology of today and the future?
  - What are the strengths and weaknesses of agency research programs, including research staff levels and capabilities?
  - How does the agency compare with FAA and FDA with respect to staffing, relationship with the industry regulated, and effectiveness?
  - What have been the greatest agency successes and its greatest failures?
  - What does the agency consider to be critical factors for its success?

Box 6-4 (*continued*) Elements of a Strategic Planning Process

- Articulate the agency's key strategies and objectives going forward:
  - The agency's role and responsibilities redefined or reiterated clearly
  - An explicit strategy developed for how to adapt to the expected changes in technology
  - Goals set for the size, nature, and content of the research programs in support of agency goals
  - Goals set for the size and capabilities of the staff in its various units such as ODI
  - Improvement objectives established for the databases used in the work of the agency
  - Metrics defined to indicate the agency's performance of its defined roles and responsibilities

guiding critical decisions concerning matters such as the most appropriate agency regulatory approaches and associated research and resource requirements.

The strategic planning process will put NHTSA in a better position to address and make decisions about matters such as the following:

- Whether the agency's regulatory role should be modified to take into account the safety assurance processes followed by automotive manufacturers during product development. For example, the advantages and disadvantages of urging or requiring manufacturers to demonstrate that they are implementing rigorous safety assurance as part of the design, development, and manufacturing of electronics systems that affect safety-critical functions should be examined.
- How NHTSA's research can be broadened to go beyond the provision of mostly technical support for regulatory decisions to (*a*) provide similar support for ODI as it seeks to strengthen its safety surveillance, investigation, and data availability and analysis capabilities and (*b*) help meet the shared research needs of automotive manufacturers

as they seek to improve their safety assurance processes. Such strategic planning would provide an opportunity for NHTSA to consider the nature of the research it undertakes, what should be encompassed by its research in the future, and the methods that are used to identify key research needs.

- The most appropriate means by which NHTSA can consult and interact more effectively with automotive manufacturers to (*a*) identify the safety assurance challenges arising from vehicle electronics, (*b*) understand how industry is working to meet these challenges, and (*c*) facilitate collaboration and cooperation among manufacturers and NHTSA.

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).

The long-term importance of strategic planning is obvious: the technological transformation of the automobile will continue, and being prepared for more safety concerns that arise rather than reacting to them will become increasingly important. As electronics systems proliferate, NHTSA will be called on to investigate suspected safety deficiencies in them, but it can ill afford to explore potential vulnerabilities in the same extraordinary manner that it did for Toyota's ETC.

The committee observes that NHTSA researchers are working with the automotive industry, universities, and other government agencies to examine future crash avoidance concepts such as vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications systems. These systems will enable even greater vehicle autonomy and necessitate advancements in vehicle electronics that will go well beyond any systems now being deployed. In the same vein, changes in the division of functions between the driver and the vehicle will (*a*) present new demands for and interpretations of FMVSSs; (*b*) heighten the need for safety assurance processes that instill high levels of driver confidence in these systems; and (*c*) place new demands on ODI's defect surveillance, analysis, and investigation activities.

The technical and economic feasibility of V2V, V2I, and other intelligent transportation systems are not considered in this study. However, it is difficult to imagine NHTSA accommodating their introduction without adapting its regulatory, research, and investigation processes. The strategic planning recommended here is not of a scope that would allow the agency to prepare for the many implications associated with conceived future systems such as V2V and V2I. However, by engaging in strategic planning on an ongoing basis, NHTSA will be in a better position to meet the safety demands that such technological advancements are likely to bring. The recommendations to NHTSA in this report are contained in Box 6-5.

BOX 6-5

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

(continued on next page)

Box 6-5 (*continued*) Recommendations to NHTSA

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.

REFERENCE

Abbreviation

NHTSA National Highway Traffic Safety Administration

NHTSA. 2011. *NHTSA Vehicle Safety and Fuel Economy Rulemaking and Research Priority Plan, 2011–2013.* March. http://www.nhtsa.gov/staticfiles/rulemaking/pdf/2011-2013_Vehicle_Safety-Fuel_Economy_Rulemaking-Research_Priority_Plan.pdf.

Study Committee Biographical Information

Louis J. Lanzerotti, *Chair,* is Distinguished Research Professor in the Department of Physics at the New Jersey Institute of Technology. Dr. Lanzerotti is a member of the National Academy of Engineering. He is retired Distinguished Member of Technical Staff of Lucent Technologies, where his responsibilities included supervision of laboratories and research and development. His principal research interests include space plasmas, geophysics, and engineering problems related to the impacts of atmospheric and space processes and the space environment on space and terrestrial technologies. He has served as chair of a number of National Research Council (NRC) boards and committees, including the Space Studies Board, the Committee for the Assessment of Options for Extending the Life of the Hubble Space Telescope, and the Army Research Laboratory Technical Assessment Board. He has been principal investigator (PI) on National Aeronautics and Space Administration (NASA) and commercial space satellite missions and is currently PI for instruments on the NASA dual spacecraft Radiation Belt Storm Probes mission, which is scheduled for launch in May 2012. Dr. Lanzerotti holds a BS in engineering physics from the University of Illinois and master's and doctoral degrees in physics from Harvard University.

Dennis C. Bley is President of Buttonwood Consulting, Inc., a Managing Partner in the WreathWood Group, and a member of the Advisory Committee on Reactor Safeguards at the U.S. Nuclear Regulatory Commission. He has more than 40 years of experience in nuclear and electrical

engineering, plant and human modeling for probabilistic risk assessment, and expert elicitation. He conducts research in human reliability analysis, probabilistic risk assessment of technological systems, and modeling uncertainties. Dr. Bley has a PhD in nuclear engineering from Massachusetts Institute of Technology (MIT) and a BSEE from the University of Cincinnati. He is recognized for developing and applying probabilistic risk assessment to a wide range of engineered facilities and has lectured at universities, industries, and government on all aspects of risk assessment. He has also authored many papers and reports on risk assessment techniques and methods. He has served on NRC and government committees evaluating such diverse topics as railroad safety, nuclear energy systems, disposal of chemical weapons in the Army's stockpile, airport operations, the space shuttle, and chemical facilities.

Raymond M. Brach is a consultant in the field of accident reconstruction and a professor emeritus of the Department of Aerospace and Mechanical Engineering, University of Notre Dame. He is a Fellow of the Society of Automotive Engineers (SAE). Other professional memberships include the American Society of Mechanical Engineers (ASME), the Acoustical Society of America, the Institution of Noise Control Engineers, and the National Association of Professional Accident Reconstruction Specialists. He was granted a PhD in engineering mechanics from the University of Wisconsin, Madison, and BS and MS degrees in mechanical engineering from Illinois Institute of Technology, Chicago. His specialized areas of teaching and research include mechanical design, mechanics, vibrations, acoustics, applications of statistics and quality control, vehicle dynamics, accident reconstruction, and microparticle dynamics. He is a licensed professional engineer in the state of Indiana. In addition to more than 100 research papers and numerous invited lectures, he has authored *Mechanical Impact Dynamics,* which was published by Wiley Interscience in 1991, and is a coauthor of *Uncertainty Analysis for Forensic Science,* Lawyers and Judges Publishing Company, 2004, and *Vehicle Accident Analysis and Reconstruction Methods,* published by SAE, 2005.

Daniel L. Dvorak is a Chief Technologist in the Systems and Software Division at the Jet Propulsion Laboratory, California Institute of Technology. Dr. Dvorak leads NASA's Software Architecture Review Board for real-time embedded flight software, he led the NASA study of flight software complexity, and he contributed to a NASA study of fault management practices in mission-critical systems and software. Before 1996

he worked at Bell Laboratories. Dr. Dvorak's interests include model-centric engineering, control architectures for robotic systems, human-rated automation, and verification and validation. Dr. Dvorak holds a PhD in computer science from the University of Texas at Austin, an MS in computer engineering from Stanford University, and a BS in electrical engineering from Rose-Hulman Institute of Technology.

David Gerard is an Associate Professor of Economics at Lawrence University. He was previously Executive Director of the Center for the Study and Improvement of Regulation in the Department of Engineering and Public Policy at Carnegie Mellon University. His area of expertise is risk regulation and focuses on the interrelationships between regulation and technological change. His current research includes the regulation of vehicle safety, transportation fuels, automobile emissions, and carbon capture and sequestration. He earned a BA from Grinnell College and an MS and a PhD in economics from the University of Illinois.

Deepak K. Goel is President and founder of the automotive electronics consulting company TechuServe LLC. He provides expertise in diverse areas such as "Best in World EE" designs; supplier development; low-cost sourcing; and profitable automotive electronic business growth, automotive part cost reduction, and product cost management. Before joining TechuServe, he held senior management and executive positions at Ford Motor Company. Since receiving his doctorate from Syracuse University, Dr. Goel has held several senior management, business leadership, and technical management positions in Dearborn, Michigan, at Ford Motor and Visteon; Ford Microelectronics in Colorado Springs, Colorado; Wang Laboratories in Lowell, Massachusetts; and IT&T in Shelton, Connecticut. He was an adjunct professor at the University of Colorado and Bridgeport University. He managed the design and launch of several electronic subsystems for all North American Ford vehicle programs at more than 20 North American assembly plants. In this capacity, while working with suppliers from the United States, Europe, China, and India, he had a unique opportunity to mentor the global supply base on how to meet the original equipment manufacturer cost, quality, and launch support needs. He spent more than 14 years in product development examining EE subsystem designs for defect avoidance and prevention.

Daniel Jackson is Professor of Computer Science at MIT and a MacVicar Teaching Fellow. He is the lead designer of the Alloy modeling language

and the author of *Software Abstractions: Logic, Language, and Analysis* (MIT Press, 2006), and he was recently chair of the committee that produced a National Academies report titled *Software for Dependable Systems: Sufficient Evidence?* (May 2007). He received his MA from Oxford University in physics and his SM and PhD from MIT in computer science. He has been a software engineer for Logica (United Kingdom) and Assistant Professor of Computer Science at Carnegie Mellon University. He has broad interests in many areas of software engineering, especially in specification and design, critical systems, and formal methods.

Linos J. Jacovides retired as Director, Delphi Research Laboratories, a position he held from 1998 to 2007. Dr. Jacovides joined General Motors (GM) Research and Development in 1967 and became department head of electrical engineering in 1985. His areas of research were the interactions between power electronics and electrical machines in electric vehicles and locomotives. He later transitioned to Delphi with a group of researchers from GM to set up the Delphi Research Laboratories. He is a Fellow of the Institute of Electrical and Electronics Engineers (IEEE) and was President of the Industry Applications Society of IEEE in 1990. He received a BS in electrical engineering and an MS in machine theory from the University of Glasgow, Scotland. He received a PhD in generator control systems from the Imperial College, University of London. Dr. Jacovides is a member of the National Academy of Engineering.

Pradeep Lall is the Thomas Walter Professor in the Auburn University Department of Mechanical Engineering, with a joint appointment in the Department of Finance. He is the Director of the National Science Foundation Center for Advanced Vehicle and Extreme Environment Electronics at Auburn University. His research areas are in electronic reliability, prognostics, material constitutive behavior, nanocomposites, failure mechanisms, life prediction models, and explicit dynamics. He is author or coauthor of two books, 11 chapters, and more than 250 journal and conference papers in the field of electronics packaging, with emphasis on design, modeling, and predictive techniques. He is a Fellow of ASME, recipient of the Samuel Ginn College of Engineering Senior Faculty Research Award, and a Six Sigma Black Belt in Statistics. He is the recipient of three Motorola Outstanding Innovation Awards and five Motorola Engineering Awards. Dr. Lall is an associate editor of ASME's *Journal of Electronic Packaging* and two IEEE journals, *Transactions on Components and Packaging Technologies* and *Transactions on Electronics Packaging*

Manufacturing. He earned a BE from the University of Delhi, an MS and a PhD from the University of Maryland, and an MBA from the Kellogg School of Management at Northwestern University.

John D. Lee is the Emerson Professor in the Department of Industrial and Systems Engineering at the University of Wisconsin, Madison. Previously he was with the University of Iowa and was the director of human factors research at the National Advanced Driving Simulator. Before moving to the University of Iowa, he was a research scientist at the Battelle Human Factors Transportation Center for 6 years. He is a coauthor of the textbook *An Introduction to Human Factors Engineering* and the author or coauthor of 170 articles. He recently helped edit the book *Driver Distraction: Theory, Effects, and Mitigation.* He received the Ely Award for best paper in the journal *Human Factors* (2002) and the best paper award from the journal *Ergonomics* (2005). He served as a member of the NRC Committee on Human–Systems Integration and has served on several other NRC committees. Dr. Lee serves on the editorial board of *Cognitive Engineering and Decision Making; Cognition, Technology, and Work;* and *International Journal of Human Factors Modeling and Simulation.* He is associate editor for the journals *Human Factors* and *IEEE Transactions on Systems, Man, and Cybernetics.* His research focuses on the safety and acceptance of complex human–machine systems by considering how technology mediates attention. Research interests include trust in technology, advanced driver assistance systems, and driver distraction.

Adrian K. Lund is President of the Insurance Institute for Highway Safety and the affiliated Highway Loss Data Institute (HLDI). Before becoming president in January 2006, Dr. Lund held numerous positions at the institutes. Trained initially as a psychologist, Dr. Lund has been involved in health-related research since 1975. He joined the institute in 1981 as a behavioral scientist and became senior vice president for research in 1993, chief operating officer of the institute and HLDI in 2001, and president in 2006. Dr. Lund is a highway safety expert and is consulted frequently by print and electronic media reporters. He appears regularly on television news magazine shows and on network news programs. He is the author of numerous scientific papers and has served on the boards and committees of many highway safety groups.

Michael J. Oliver is Vice President for Electrical/Electromagnetic Compatibility (EMC) Engineering at MAJR Products Corporation. An expert

in electromagnetic interference and radio frequency interference shielding technology, military shelter electrical EMC systems, and high-power antenna–radar dome (radome) design, Mr. Oliver has more than 20 years of experience in EMC and electromagnetic environmental effects in both military and commercial applications. Mr. Oliver holds three patents on EMC shielding and thermal management devices, and he has performed open and anechoic chamber radiated tests to military standards by utilizing various radiated test systems. He is the author of numerous publications and white papers on electromagnetic shielding products and military antenna–radome test methodology standards. A senior member of IEEE, Mr. Oliver currently serves on the board of directors of the IEEE EMC Society; as Chairman of the IEEE EMC Pittsburgh, Pennsylvania, chapter; and as Cochairman of the SAE EMC Committee. He serves as Chairman of the 2012 IEEE EMC Symposium, Pittsburgh, and is a member of the IEEE EMC Standards Advisory Coordination Committee and the dB Society.

William A. Radasky is Founder, President, and Managing Engineer of Metatech Corporation, which provides engineering solutions to problems in the areas of electromagnetic environmental effects, including electromagnetic interference and compatibility, nuclear and lightning electromagnetic pulse, and electrostatic discharge. He began his career in 1968 at the Air Force Weapons Laboratory, where he worked with the early high-altitude electromagnetic pulse codes. He founded Metatech Corporation in 1984. At Metatech, he has managed a series of projects to develop electromagnetic hardening measures and test methods to verify their performance. He has also been active in the development of commercial EMC standards with the International Electrotechnical Commission (IEC) to protect commercial systems from all types of electromagnetic threats. He served on the International Organization for Standardization (ISO) technical committee dealing with automotive EMC (ISO TC22/SC3/WG3) as a liaison between the ISO EMC automotive engineers and the IEC TC 77 committee, which develops basic EMC test standards for electronics equipment. In 2004, he was awarded the Lord Kelvin Medal by IEC for exceptional service in the development of international standards. He is a Fellow of IEEE and serves as Chairman of TC-5 (High-Power Electromagnetics) for the IEEE EMC Society. He has authored more than 400 publications on EMC subjects. He holds a BS from the U.S. Air Force Academy, an MS from the University of New Mexico, and

a PhD in electrical engineering from the University of California at Santa Barbara.

Nadine B. Sarter is Associate Professor in the Department of Industrial and Operations Engineering and the Center for Ergonomics at the University of Michigan. She teaches courses in cognitive ergonomics and human factors. She was previously on the faculty in the Department of Industrial, Systems, and Welding Engineering and the Institute for Ergonomics at Ohio State University. Before moving to Ohio State, she served on the faculty of the Institute of Aviation at the University of Illinois at Urbana–Champaign, where she held coappointments with the Departments of Psychology, Mechanical and Industrial Engineering, and the Beckman Institute. Her research interests include human–automation communication and coordination (primarily in high-risk, event-driven domains such as aviation), multimodal human–machine interfaces and interaction, error prevention and management, and attention and interruption management. Her research is conducted in application domains such as aviation, military operations, medicine, and automobiles. She is associate editor for *Human Factors; IEEE Transactions on Systems, Man, and Cybernetics;* and *IEEE Transactions on Intelligent Transportation Systems.* She is also a member of the editorial board for the *Journal of Experimental Psychology.* She has served on several NRC committees, including the Committee on Federal Aviation Administration (FAA) Aviation Safety Inspector Standards, the Committee for Evaluating Shipboard Display of Automated Identification Systems, and the Committee for a Review of the Federal Railroad Administration R&D Programs. She earned a BS in psychology and an MS in applied and experimental psychology from the University of Hamburg. She earned a PhD in industrial and systems engineering from Ohio State University.

James W. Sturges retired in 2009 from Lockheed Martin Corporation, where he had been Director, Engineering Processes, and Director, Mission Assurance. Before that he was Vice President, Engineering and Total Quality, at Loral Air Traffic Control/Lockheed Martin Air Traffic Management, and C3I Strategic Business Area Director for Loral Tactical Defense Systems, Arizona. He also had been a naval aviator and antisubmarine warfare officer for the U.S. Navy. He has a BFA from the University of North Carolina and an MS in aeronautics from the Naval Postgraduate School at Monterey, California. He is an Associate Fellow and member of the Standards Executive Council and past chair of the

Systems Engineering Technical Committee of the American Institute of Aeronautics and Astronautics.

Dennis F. Wilkie is Senior Vice President in the Management Consulting Division of Compass Group, Ltd. Before joining Compass Group, he was Corporate Vice President and Chief of Staff for the Integrated Electronic Systems Sector at Motorola, Inc. He spent most of his career at Ford Motor Company, where he retired as Corporate Vice President for Business Development. His work over the years focused on the application of control theory and systems engineering to automobiles and the field of transportation. He worked on infrastructure issues, such as automated highways, automated transportation systems, and intelligent transportation systems. In recent years, he has focused on the utilization of electronics and wireless technology for bringing new levels of convenience, safety, and information to the vehicle. He was elected to the National Academy of Engineering in 2000 and is a Fellow of SAE. He holds BS and MS degrees in electrical engineering from Wayne State University, a PhD in electrical engineering from the University of Illinois, and an MS in management (Sloan Fellow) from MIT.

The Safety Challenge and Promise of Automotive Electronics

INSIGHTS FROM UNINTENDED ACCELERATION

During 2009 and 2010, the national media reported drivers' claims that their cars had accelerated unintentionally; some blamed faulty vehicle electronics. The National Highway Traffic Safety Administration (NHTSA) asked the National Research Council to convene an expert committee to review investigations of unintended acceleration and to recommend ways to strengthen NHTSA's safety oversight of automotive electronics systems.

This report examines the safety agency's investigations of unintended acceleration over the past 25 years, including recent investigations of complaints by drivers of vehicles equipped with electronic throttle control systems. NHTSA investigators have not found evidence that faulty electronics have caused unintended acceleration; they attribute most cases to an obstruction of the accelerator pedal or to the driver mistakenly pressing the accelerator pedal instead of the brakes.

The study committee notes, however, that increasingly interconnected and complex automotive electronics are creating many new demands on the automotive industry for product safety assurance and on NHTSA for effective safety oversight. Meeting these emerging demands is critical, as advances in vehicle electronics offer consumers many benefits, including safety features. The report recommends that NHTSA take several actions to prepare for the electronics-intensive vehicle of the future and to meet the related safety challenges.

Also of Interest

Vehicle Safety: Truck, Bus, and Motorcycle
Transportation Research Record: Journal of the Transportation Research Board, No. 2194, ISBN 978-0-309-16070-4, 114 pages, 8.5 × 11, paperback, 2010, $59.00

Buckling Up: Technologies to Increase Seat Belt Use
TRB Special Report 278, ISBN 0-309-08593-4, 103 pages, 6 × 9, paperback, 2004, $22.00

An Assessment of the National Highway Traffic Safety Administration's Rating System for Rollover Resistance
TRB Special Report 265, ISBN 0-309-07249-2, 135 pages, 6 × 9, paperback, 2002, $21.00

Shopping for Safety: Providing Customer Automotive Safety Information
TRB Special Report 248, ISBN 0-309-06209-8, 160 pages, 6 × 9, paperback, 1996, $20.00

THE NATIONAL ACADEMIES™
Advisers to the Nation on Science, Engineering, and Medicine

The nation turns to the National Academies—National Academy of Sciences, National Academy of Engineering, Institute of Medicine, and National Research Council—for independent, objective advice on issues that affect people's lives worldwide.
www.national-academies.org

ISBN 978-0-309-22304-1
90000
9 780309 223041