U.S. Department
of Transportation

National Highway
Traffic Safety
Administration

Peer Review of NHTSA and NASA Test Plan into Toyota Unintended Acceleration

February 2011

DISCLAIMER

This publication is distributed by the U.S. Department of Transportation, National Highway Traffic Safety Administration, in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof. If trade or manufacturers' names or products are mentioned, it is because they are considered essential to the object of the publication and should not be construed as an endorsement. The United States Government does not endorse products or manufacturers.

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
NHTSA-NVS-2011-ETC-SR14		

4. Title and Subtitle	5. Report Date
Peer Review of NHTSA and NASA Test Plan into Toyota Unintended Acceleration	February 2011
	6. Performing Organization Code: NVS
7. Author(s)	8. Performing Organization Report No.: NHTSA-NVS-2011-ETC-SR14
9. Performing Organization Name and Address: U.S. Department of Transportation National Highway Traffic Safety Administration 1200 New Jersey Ave., S.E. Washington, DC 20590	10. Work Unit No. (TRAIS)
	11. Contract or Grant No.
12. Sponsoring Agency Name and Address: National Highway Traffic Safety Administration 1200 New Jersey Ave., S.E. Washington, DC 20590	13. Type of Report and Period Covered
	14. Sponsoring Agency Code

15. Supplementary Notes

This report provides supplementary information to NHTSA Report No. NHTSA-NVS-2011-ETC, "Technical Assessment of Toyota Electronic Throttle Control (ETC) Systems," January 2011.

16. Abstract

17. Key Words	18. Distribution Statement		
Sudden acceleration, unintended acceleration, electronic throttle control, "Silver Book,"			
19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages	22. Price

Form DOT F 1700.7 (8-72)

TABLE OF CONTENTS

LIST OF TABLES

1.0 PEER REVIEW OF NHTSA AND NASA TEST PLAN INTO TOYOTA UNINTENDED ACCELERATION

To provide an additional level of independent examination of the approach being taken by the National Highway Traffic Safety Administration (NHTSA) and the National Aeronautics and Space Administration's (NASA) study of Toyota unintended acceleration (UA), NHTSA tasked the John A. Volpe National Transportation Systems Center (Volpe Center) to conduct a peer review of the test plans developed by NASA and NHTSA's Vehicle Research and Test Center (VRTC). The Volpe Center put together a panel of experts to help conduct this review. NHTSA determined that the test plan could be considered a highly influential scientific document as defined by the Office of Management and Budget (OMB) because it is of significant public interest. Therefore, the peer review of this report complied with requirements of both Sections II and III of the OMB's "Final Information Quality Bulletin for Peer Review." In addition, the selection of peer reviewers complied with The National Academies' "Policy on Committee Composition and Balance and Conflicts of Interest for Committees Used in the Development of Reports."

1.1 Review Process

Expertise was the most important factor in selecting reviewers, and the Volpe Center needed to ensure that the selected reviewers had the knowledge, experience, and skills necessary to perform the review. According to The National Academies' guidelines, the group of peer reviewers needed to be "balanced in terms of the subtleties and complexities of the particular scientific, technical, and other issues to be addressed." To achieve a balanced peer review, the Volpe Center was tasked with selecting one electrical engineer, one mechanical engineer, one software engineer, one systems engineer, and one physicist, all with expertise in automotive applications or ground vehicles. Furthermore, none of the five peer reviewers were to share the same organizational or institutional affiliation. The peer reviewers also needed to be independent of NHTSA, any automaker or supplier, and any litigants or attorneys involved in related litigation and could not possess any conflicts of interest. The table below lists the disciplines and areas of expertise sought for each expert, knowing that it might be necessary for some disciplines to be replaced with others if they met the areas of automotive expertise.

It was anticipated that the initial test plans would be developed by the end of April 2010, with peer review starting immediately afterward and results reported back to NHTSA and NASA in one month. A need for subsequent additional test plan revisions was also expected so that the peer review would conduct additional and specific reviews of the test plan as it evolved.

Table 1 - Disciplines and Areas of Expertise

Areas of Automotive Expertise	Disciplines				
	Electrical Engineer	Mechanical Engineer	Software Engineer	Systems Engineer	Physicist
Electronics: analog, digital, power, flash memory, ASIC	X				
Electrical: wiring, harness, grounding	X			X	
Electro-mechanical: parts, materials, processes, mechanisms	X	X			
Materials, structures, thermal		X			X
Ergonomics		X			
Quality assurance, high reliability software standards, static analysis			X	X	
Failure modes/effects, fault tolerance, reliability, robustness	X	X	X	X	
Electromagnetics interference/compatibility, single event upsets	X			X	X
Electrical and mechanical interface controls	X	X		X	
Automotive systems	X	X	X	X	X
Testing	X	X	X	X	

1.2 Results

The peer review process proved to be more difficult to accomplish than had been originally envisioned. There were several reasons for this:

- The NASA plan for evaluating vulnerabilities in the electronic throttle control was a top down systems view focusing on system level functions and system level fail safes to identify where built in failure tolerance was defeated. Thus, the document developed for peer review was a technical strategy for identifying system functional vulnerabilities rather than a specific technical plan. Peer reviewer feedback was philosophical rather than a critique of technical procedures.
- The test strategy was dependent on access to Toyota proprietary design details such as schematics, wiring, diagrams, circuit board layouts, and software source code. It took

some time to develop and implement administrative controls to manage the exchange and protection of the proprietary information, and it was early May before controls were fully implemented. This resulted in the test strategy being released in late June (a setback of nearly two months) when the NHTSA test plans and NASA test strategy were provided to the peer review panel along with a briefing overview.

- The Toyota Electronic Throttle Control (ETC) was far more complex than expected involving hundreds of thousands of lines of software code. This resulted in considerable time being spent running tests to validate the operation of the system and how it could fail. Test scenarios were then developed to understand the limitations of the system fail safes, if they could be defeated, and the overall system effect of the hypothetical failures. Test scenarios evolved from the understanding of the system and were provided for peer review following the initial test plan/strategy documents. Technical evaluation of the test scenarios required a detailed understanding of the ETC, and given the rapid progression of the work, there was insufficient schedule allocated for explaining the design of the ETC and the origin of the test scenarios to the peer review panel. This left the test scenarios and the test strategies vague for independent interpretation.

Nevertheless, despite this less than ideal situation, general and technical comments received from the peer reviewers were very helpful to ensure that the strategy being pursued by NASA enveloped various theories and potential software/hardware failure mechanisms in the ETC that could potentially result in UA.

There were also some requests for additional information from the panelists. NHTSA and NASA made a joint assessment and determined that the requests for additional information either reflected a detail matter rather than process review, and/or were for specific technical information/materials that would not be available until completion of the analysis. Therefore, these requests were not fulfilled since it was believed that delivery of the products would not facilitate the peer review intent.

Given this, an assessment was made on how the project could best benefit and utilize the expertise of the peer review panelists. Since the test work was nearly completed by this time, it was determined that an in-person debriefing of the NASA approach and findings would be the best alternative without causing additional delay in completion of the project final report. Such a

meeting was held in late October 2010 with all five peer review panelists, the Volpe Center coordinator, core members of the NASA team, and NHTSA staff. NASA provided a presentation that included a detailed overview of their approach (a top-down systems study) and a summary that included their findings, recommendations, and observations. The remainder of the day was devoted to questions by the peer review panel members and open discussion. The peer review panel members were generally satisfied with NASA's approach to thoroughly understanding the Toyota ETC system functionality, identification of potential vulnerabilities in the ETC that could result in UA, technical diligence in enveloping the various theories that have been postulated as potential causes of UA, and the findings. Various suggestions were offered to further strengthen the report as follows:

- Approach:
  - A clear explanation should be included on assumptions made in establishing the approach, as well as other assumptions made and alternative approaches that were not taken. Specifically, the top down systems view approach taken focusing on system level functions and system level fail safes assumes a design fault as opposed to manufacturing flaws.
  - Consideration should be given to inclusion of a probabilistic risk analysis/assessment. It was felt that such an analysis would support the approach taken since some alternatives would not be feasible even given an infinite amount of time.
  - It should be pointed out that the study relied in part on reverse engineering of the ETC system.
  - The report should contain a direct response to each of the outside "theories" about unintended acceleration and clearly show how the test results either prove or disprove these theories.
  - Discussion should be included to describe system, engine, and component changes across the various model years of interest.
- Complaint Data Analysis:
  - A clear description should be given of the process used to sort consumer complaint data (Vehicle Owner Questionnaires or VOQ's) into different "bins" of complaint types and how those bins relate to degree of throttle opening.

- Good traceability should be provided from VOQs and warranty data to the specific vehicle systems being investigated.
- Complaint data analysis should include an assessment of identical vehicles (or as close as possible – both Toyota and peer vehicles) that only differ in electronic versus mechanical throttle control.
- Discussion on the vagueness of the information in owners' complaints and the human factors issues associated with them.

· Technical Matters:

- A command related to speed of throttle closing may need to be added to the functional system design.
- There should be confirmation that in the Toyota model tested the "CHECK ENGINE" light is not a "SERICE ENGINE SOON" indicator.
- Potential "timing" errors of signal exchange among the different subsystems and components should be examined.
- The impact of integrated circuit device manufacturing failure rates on possible unintended acceleration should be discussed.

In summation, the debriefing and discussions with the peer review panel proved most beneficial. The suggestions offered were all taken under advisement by NHTSA and NASA in completing the work and report preparations.