**Case Study Exploration: Bookout Vs Toyota**

Baby Vennela Kothakonda

Software Engineering Management (CSC-770)

Dakota State University

18th February 2024

**Contents**

[**Report on Toyota’s UA case of safety-critical system failure** 3](#_Toc159307624)

[***Key findings and conclusions from the NHTSA Technical Assessment of Toyota Electronic Throttle Control(ETC) systems report.*** 3](#_Toc159307625)

[***The methodologies used by NHTSA in their technical assessment and evaluate their effectiveness in determining the root causes of unintended acceleration in Toyota vehicles.*** 4](#_Toc159307626)

[***Barr Group Investigation Vs NHTSA findings*** 5](#_Toc159307627)

[***Significance of Michael Barr’s testimony in the Book out Vs Toyota court case and his role in understanding Toyota ETC and allegations:*** 6](#_Toc159307628)

[***Evaluation of Barr’s Credibility- based on qualification, experience, and evidence presented in the case.*** 7](#_Toc159307629)

[***Legal arguments put by Toyota's team refuting Barr's argument and their effectiveness*** 7](#_Toc159307630)

[***Impact of the Bookout Vs Toyota Case:*** 8](#_Toc159307631)

[***Recommendations for Toyota*** 8](#_Toc159307632)

[***Lessons learnt*** 9](#_Toc159307633)

[**References** 10](#_Toc159307634)

# **Report on Toyota’s UA case of safety-critical system failure**

# ***Key findings and conclusions from the NHTSA Technical Assessment of Toyota Electronic Throttle Control(ETC) systems report.***

NHTSA considered the report of NASA's evaluation of Toyota's ETC systems as well as performed its own data review and vehicle examination and determined that as such there is no design or implementation flaw in the system, that has any reasonable cause to create an unexpected Acceleration event in the system. The consumer complaints included allegations that there were large throttle openings. However, as such there are no large throttle openings possible as there are no design flaws in the system. However, on critical evaluation and study of the situation, NHTSA indicated that it is possible that by failure if there is a mimic valid accelerator pedal signal, it can induce a large throttle opening. However, for such a failure to happen, two failures in the precise resistance change must be necessary to create the exact circuit configuration in the correct time phase. However, the combination of all these possibilities in the consumer usage of vehicles is very remote. In case such failures happen outside of the narrow conditions, there is always a chance for the creation of a Diagnostic Trouble Code(DTC). But there is no evidence of such formation. Even the microanalysis performed by NHSTA indicated that the proximity of such failure is almost out of scope. Typical possible occurrences of latent resistive short-producing abnormal pedal sensor voltages were investigated, but they are not present. From all these key findings and evaluations, NHTSA's technical assessment indicated that no design flaw in the system can create a large throttle opening for Toyota.

# ***The methodologies used by NHTSA in their technical assessment and evaluate their effectiveness in determining the root causes of unintended acceleration in Toyota vehicles.***

There are multiple methods employed by NHTSA as part of their technical assessment, and it is found that as such there is no scope for technical failure, that can create a large throttle opening of Toyota ETS. The methodologies included the following, the effectiveness of each is presented below,

***Data analysis***: most of the data collected by Toyota is from the consumer complaint data and collection of the information from the real-time cases reported with UA. The large collection of data from this approach provided insights into what frequency, nature, and type of causes are creating the UA event. However, the actual effectiveness of the methodology is very much conditional. The accuracy of the information collected and shared will decide the effectiveness of the methodology and this is very much dependent on the quality as well as the quality of the data available as well.

***Physical examination of the vehicle***s: This is another approach employed by NHTSA. Through this approach, the physical examination of the Toyota vehicle's ETS is performed and the actual pedal sensor positions and resistive shorts are tested. Both the mechanical and electrical fault proximity and evidence of the failures are investigated. The approach is very impressive. However, the generalizability of the results can be limited by the number of observations that can be made through this approach.

***Collaborations***: With technical experts like NASA, NHTSA collaborated and leveraged its expertise in the systems, software, functional evaluation, and so forth. The findings provided further support for the NHTSA's technical assessment and the report. The findings were supported with substantial evidence from these technical insights and expertise of NASA. Collaboration enhanced the approach's effectiveness, extended the scope of investigation as well improved the reliability of the findings.

Future actions and collaboration: Investigating future actions and planning based on the expert evidence collected, and expertise information collected, helps the NHTSA to keep updated with the existing data and to draw in inferences for better technical decisions in the future for design and other functional systems implementation for ETC as well as for other related sub-systems. The effectiveness once again is dependent on the organizational functioning and is reliant on the number of data aspects collected and their utility as well in the future.

# ***Barr Group Investigation Vs NHTSA findings***

NHTSA mainly confined its findings to ETC as well as on the pedal systems and worked from multiple aspects like system, software, and so forth, to determine the effectiveness of these systems and their potential capability in meeting the requirements of the functionality and their possible contribution to the Unintended Acceleration events of Toyota vehicle. NHTSA findings more or less are distinct from the findings of the Barr group. Barr Group investigation has reported that there is likely a systematic software malfunction in the main CPU of the vehicle system. This is working by itself to open the throttle without the actual intention of the operator. Further, it is working to properly control the fuel injection as well as the injection aspects. Hence basically the domain of suspicion and subsequent investigation performed by NHTSA is different from that of the Barr group and the allegations from each side are also different. While NHTSA did not critique anything about the design or the performance of the Toyota ETC system, Barr's group pointed out the error in the software system, which makes up for critical safety failure. Further, the consequences of the findings are also different for both systems. From NHTSA and the Barr group investigation, the recommendations and the set of remedial actions suggested also are going to be different, based on variations in their findings. Since the approach is different there is scope for discrepancies, for instance, the Toyota system's forensic investigation of the vehicle might lead different set of vulnerabilities and flaws that are not identified by NHTSA.

# ***Significance of Michael Barr’s testimony in the Book out Vs Toyota court case and his role in understanding Toyota ETC and allegations:***

Barr is having extensive technical expertise and his understanding of ETC and failure modes etc. is instrumental in dissecting the complexities of Toyota's ETCs. He did perform forensic analysis critically and comprehensively of the software code employed in Toyota's ETCS. His expertise in software engineering contributed to detailed scrutiny of the code and helped him to identify the flaws that are responsible for the throttle function failure in the Toyota system. When there was no identified design flaw, existing in Toyota's ETC, Michael Barr, identified that the bugs, software flaws, and sensor malfunctionalities all contributed to the failure of the system. He played a key role in educating the jury about the nuances and complexities involved in the case. From nowhere, he managed to provide a compiling and convincing testimony to the court about the possible reasons for the failure of the ETCS. These factors made the jury make informed decisions about the case and helped them to make decisions with better insights into the actual technical aspects of the case. The expert opinion of Michael Barr, helped the jury to make in right decisions in the case. His credentials as well as the findings from his very detailed and microscopic investigation into the factors responsible for the failure of the throttle, helped the jury to safeguard the accountability in the case. Some key findings like Toyota not using standard OS, for example, Toyota's Rx-OSEK850, is not compatible with OSEK. MISRA C-rules were not followed comprehensively by Toyota. Internal coding standards follow-up failure is a major breach by Toyota, as per an investigation by Barr.

# ***Evaluation of Barr’s Credibility- based on qualification, experience, and evidence presented in the case.***

Michael Barr is an expert in the embedded system and he has several years of experience in the domain. He has a bachelor's and master's in electrical and computer-related departments from the premier institutions of the United States of America. His professional experience is indeed valuable and proven and this supports his credibility as an expert in the current context. As an expert witness, with evidence from past instances, he made an excellent presentation of the possible technical failures due to the flaws in the software. He stood firm and convincingly presented his opinions, for the counterarguments of the legal attorneys from the other party. Barr also constructively worked to present compelling evidence from past events. Apart from the evidence presented for supporting his testimony in the case CJ-2008-7969, which all worked to enhance the credibility of Barr in the current case(Finch,2009).

# ***Legal arguments put by Toyota's team refuting Barr's argument and their effectiveness***

The legal arguments put before by Toyota's legal team against Michael Barr's testimony mainly is about the reliability of Toyota's ETC, as per the investigation performed by NHTSA and NASA approaches. The validation of the system and the inferences drawn by NHTSA and NASA are projected reliable and counter-arguments mainly were drawn to prove the possible external factors that contributed to the failure of the ETS. They argued from the practical observations and argued to prove the faults of the evidence. However, Barr argued the vagueness there in the NHTSA and NASA reports, as their scope of investigation is limited and constrained to other aspects, and did not consider the possible software flaws. Evidentially Barr argued and demonstrated the faults in the software and convincingly indicated the reasons why the ETC might have failed. Evidence from the past presented strong present support for this insight(Anderson,2016).

# ***Impact of the Bookout Vs Toyota Case:***

Negative publicity is gathered by Toyota in the current case. The consumer trust in the legacy safety compliance and procedures followed by Toyota are now subjected to scrutiny and became the subject of debate in the aftermath of the case coming to public notice. There were callbacks following this legal case. Also, Toyota faced financial loss in terms of compensations and claim settlements in the aftermath of finding the flaws in the manufacturer's software solution offered to control ETC. The unintended UA is attributed to Toyota's manufacturing defect in terms of the software flaws and the company became subject to mistrust in the aftermath of the case. Also, the case triggered cautionary actions from other organizations like GM. Honda for handling GM ignition switches and the Honda Hybrid SW UA. The outcomes of the case started making consumers a bit more cautious and vigilant, blind acceptance of the safety critical systems is at least averted in the consumers who are safety conscious now. The case outcome, made the customer lose some confidence in the safety systems of Toyota, however, Toyota has taken up corrective actions to boost customer confidence (Kane et al.,2010).

# ***Recommendations for Toyota***

It is recommended that Toyota need to take immediate measures to regulate the correct flaws in the Toyota Systems. Also, it should work to improve the current state of operations in Toyota, along with a focus on improving the system continuously to make the vehicles safer. Data analytics-based knowledge collection needs to be employed for analysis of the vehicle conditions and should work to improve their safety standards continuously. Crate risk management, by increasing safety controls and ensuring advanced testing and validation before release of the new models. Also should work for better diagnostics and investigations in place. Compliance with standards both for hardware and software is mandatory and industry standards are enforced from time to time.

Based on Michael Barr's testimony, the software source code of the ETC monitoring systems needs to be re-tested and should be corrected for flaws. Rigorous safety testing is mandated. All standard protocols are to be followed in software coding(Lee,2020).

# ***Lessons learnt***

A key lesson is that overlooking the investigation is a grave mistake. A comprehensive investigation is mandatory to find out a more reliable root cause of the challenges.

Continuous improvement, regulatory compliance, etc. are necessary. Also, Toyota-like organizations must ensure user confidence by making their developments and measures revealed from time to time to keep up the trust. Specifically, in the context of ETC, thorough testing and re-implementing the right and reliable solution is an immediate requirement. Regulatory compliances and standard protocol follow-up are mandatory. These are some of the key lessons learned from the current case experience in general and for automakers in particular in the context of UA prevention.

# **References**

Anderson, A. F. (2016). Case study: NHTSA's denial of Dr.Rashaan’s petition to investigate sudden acceleration in Toyota vehicles fitted with electronic throttles. *IEEE Access*, *4*, 1417-1433. https://ieeexplore.ieee.org/iel7/6287639/6514899/07439741.pdf

Finch, J. (2009). Toyota sudden acceleration: a case study of the national highway traffic safety administration-recalls for change. *Loy. Consumer L. Rev.*, *22*, 472. <https://lawecommons.luc.edu/cgi/viewcontent.cgi?article=1055&context=lclr>

Kane, S., Liberman, E., DiViesti, T., & Click, F. (2010). Toyota's sudden unintended acceleration. *Safety Research & Strategies*. <https://www.safetyresearch.net/Library/ToyotaSUA020510FINAL.pdf>

Lee, Y. (2020). Analysis of unintended acceleration through physical interference of accelerator. *Forensic science international: reports*, *2*, 100079. https://www.sciencedirect.com/science/article/pii/S2665910720300256