

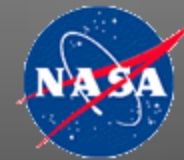
Assessment of ETC System (NASA support to NHTSA)



Mike Kirsch

NASA Engineering and Safety Center
(NESC)

Principal Engineer



Scope



- ▶ Determine if there are design and / or implementation vulnerabilities in the Toyota electronic throttle control (ETC) system that could realistically be expected to cause unintended acceleration (UA).

Goal



To Answer:

- ▶ What specific conditions are necessary for ETC failure to occur?
- ▶ Are those conditions evident in the reported cases to date?
- ▶ What physical or electronic evidence does the failure produce?
- ▶ What are the expected ranges in severity (throttle opening) and duration that could be caused by the failure?
- ▶ Could the failure have any effect on other interfaces, such as the braking system?

Team Organization



- ▶ **NASA Team Leverages Broad NASA Engineering and Safety Center Network of Experts**

- ▶ **Participants from:**
 - Ames Research Center, CA
 - Dryden Flight Research Center, CA
 - Goddard Space Flight Center, MD
 - Johnson Space Center, TX
 - Jet Propulsion Laboratories, CA
 - Kennedy Space Center, FL
 - Langley Research Center, VA
 - Marshall Space Flight Center, AL

- ▶ **Main themes of the Study**
 - System Engineering and Integration
 - Hardware
 - Software
 - Electromagnetic Compatibility
 - Human Factors



Points to Consider

- ▶ **Automotive troubleshooting is significantly different today than 10 years ago**
 - Hundreds of thousand of lines of software code
 - Much harder to trace symptoms to physical causes
- ▶ **NASA has developed a strong systems engineering culture over generations to manage mission success**
 - NASA Spacecraft needs to work the first time
- ▶ **NASA is applying this sound systems engineering approach to investigate possible ETC causes of unintended acceleration**
 - Similar to a failure investigation

Systems Engineering Approach



- ▶ Study complaint symptoms and history
- ▶ Develop understanding of how the design is supposed to work
- ▶ Develop understanding of how the design might fail
- ▶ Test for understanding
- ▶ Develop Event Sequence Diagrams
- ▶ Develop Fault Tree
- ▶ Test the vehicle ETC to evaluate scenarios derived from the Event Sequence Diagrams and the Fault Tree



Path to Vehicle Testing

- ▶ System, Hardware, and Software Engineering Analysis will lead to Test Scenarios for evaluation
- ▶ Test Scenarios to be evaluated and prioritized by feasibility of the failure and how well the failure behavior matches reported incident reports
- ▶ Test Scenarios to be conducted in the lab using bench top subsystem model (825)
- ▶ Test Scenarios to be conducted on “non-complaint” vehicle at GSFC
- ▶ Test Scenarios to be conducted in collaboration with DOTs Vehicle Research Test Center on other Model Years, and “complaint” vehicles