An Overview of NHTSA's Electronics Reliability and Cybersecurity Research Programs

Authors(s): Arthur Carter, David Freeman, and Cem Hatipoglu

National Highway Traffic Safety Administration (NHTSA)

Paper ID 15-0454

Abstract

This paper provides an overview of the National Highway Traffic Safety Administration's (NHTSA) research programs in electronic control systems reliability and automotive cybersecurity. The agency's electronics reliability research covers methods and voluntary standards both inside and outside the automotive industry. The research looks for such standards and methods that assess, identify, and mitigate potential new hazards that may arise from the increasing use of electronics and electronic control systems in the design of modern automobiles. Cybersecurity, within the context of road vehicles, is the protection of vehicular electronic systems, communication networks, control algorithms, software, users, and underlying data from malicious attacks, damage, unauthorized access, or manipulation.

BACKGROUND

NHTSA's safety role

NHTSA is responsible for developing, setting, and enforcing regulations for motor vehicles and motor vehicle equipment. Many of the agency's regulations are Federal Motor Vehicle Safety Standards (FMVSSs) with which manufacturers must self-certify compliance when offering motor vehicles and motor vehicle equipment for sale in the United States. NHTSA also studies behaviors and attitudes in highway safety, focusing on drivers, passengers, pedestrians, and motorcyclists. Additionally, NHTSA identifies and measures behaviors involved in crashes or associated with injuries, and working with States and other partners develop and refine countermeasures to deter unsafe behaviors and promote safe alternatives. Further, the agency provides consumer information relevant to motor vehicle safety. For example, NHTSA's New Car Assessment Program (NCAP) provides comparative safety information for various vehicle models to aid consumers in their purchasing decisions (e.g., the 5-star crash test ratings). The purpose of the agency's programs is to reduce motor vehicle crashes and their attendant deaths, injuries, and property damage.

Progression of electronics use in vehicles

The first common use of automotive electronics dates back to 1970s and by 2009 a typical automobile featured over 100 microprocessors, 50 electronic control units, five miles of wiring and probably contains close to 100 million lines of code [1]. Use of electronics has enabled safer and more fuel-efficient vehicles for decades and also facilitated convenience functions demanded by the consumers. Electric and hybrid vehicles could not have been developed and produced without the extensive use of electronics. Other proven safety technologies such as electronic stability control could also not be implemented without electronics.

Over time, growth of electronics use has accelerated and this trend is expected to continue as the automotive industry develops and deploys even more advanced automated vehicle features. This trend

results in increased complexities in the design, testing, and validation of automotive systems. Those complexities also raise general challenges in the areas of reliability, security, and safety assurance of increasingly networked vehicles that leverage electronics within a distributed, embedded and real-time control system architecture.

Growing system complexity and abundance of design variants even within one manufacturer over model years and across classes of vehicles raise general questions over whether manufactures can ensure the functional safety of existing processes. Further, anomalies associated with electronic systems—including those related to software programming, intermittent electronics hardware malfunctions, and effects of electromagnetic disturbances—may not leave physical evidence. Thus, they are difficult to investigate without a record of data from the electronic systems. As a result, NHTSA, industry members, and other interested parties are actively researching this issue to better understand these potential new functional safety challenges and identity methods to help address them.

National Research Council Study

In 2010, the National Highway Traffic Safety Administration (NHTSA) funded a National Research Council (NRC) study on how the agency's regulatory, research, and defect investigation programs can be strengthened to help address the safety assurance and oversight challenges arising from the expanding functionality and use of automotive electronics. Proceedings of this research through the NRC appointed 16-member committee was published in the Transportation Research Board (TRB) Special Report 308 [7] by the National Academies of Sciences (NAS) in 2012. It identified five main challenges for the safety of future electronic control systems:

1) An increased amount of complex software that cannot be exhaustively tested;
2) The highly interactive nature of the electronic control system—more interactions exist among system components, and the outcome may be difficult to anticipate;
3) The growing importance of human factors consideration in automotive electronic control system design;
4) The potentially harmful interaction with the external environment including electromagnetic interference; and
5) The novel and rapidly changing technology.

Further, the study offered recommendations to NHTSA on the actions that the agency could take to meet the six challenges they identified. These include:

1. Becoming 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
2. Convening a standing technical advisory panel; undertaking a comprehensive review of the capabilities that the agency will need in monitoring and investigating safety deficiencies in electronics-intensive vehicles
3. Ensuring that Event Data Recorders (EDRs) become commonplace in new vehicles
4. Conducting research on human factors issues informing manufacturers' system design decisions

5. Initiating a strategic planning effort that gives explicit consideration to the safety challenges resulting from vehicle electronics that give rise to an agenda for meeting them
6. Making the formulation of a strategic plan a top goal in NHTSA's overall priority plan

The program plans we outline in this paper primarily respond to the first NAS recommendation.

Electronics Systems Safety Research

Informed by the NRC study and other internal deliberations on this topic, NHTSA established the Electronic Systems Safety Research Division within the Office of Crash Avoidance and Electronic Controls Research. While our existing investigative and rulemaking processes do cover electronic system (they emphasize performance metrics that apply regardless of whether the vehicle uses a mechanical or electronic way of achieving the performance), we also recognize the increasing industry focus, and processes that govern the safety assurance associated with vehicle systems that are mostly electronic in nature. This type of research can help enhance our understanding of various functional safety issues, fail-safe operations, diagnostics, software reliability, hardware validation, on-board tamper-resistance enhancements, hacking, and malicious external control. Along these themes, NHTSA has developed and is conducting new research in the areas of electronics reliability and automotive cybersecurity (including how these topics affect vehicle automation research). Given the close relationship between electronics reliability, cybersecurity, vehicle automation, our Electronic Systems Safety Research Program are closely considers the relationship between all three topics.

In support of our efforts, NHTSA started building in-house applied electronics research capabilities at its testing facility at the Vehicle Research and Test Center (VRTC) in East Liberty, OH. The purpose of these capabilities is to support testing of electronic systems and potential countermeasures towards developing objective test procedures for electronics related standards, requirements, guidelines, principles, or best practices.

Further, the agency established a Council on "Vehicle Electronics, Vehicle Software, and Emerging Technologies" to coordinate and share information on a broad array of topics related to advanced vehicle electronics and emerging technologies. The Council is managed by senior NHTSA officials. Its mission is to (1) broaden, leverage, and expand the agency's expertise in motor vehicle electronics; (2) to continue ensuring that technologies enhance vehicle safety; (3) review and advise the research program on electronics topics.

The primary goals of the electronics reliability and automotive cybersecurity research programs are similar. The five primary goals are to

1. build a knowledge base to establish comprehensive research plans for automotive electronics reliability/cybersecurity and develop enabling tools for applied research in these areas
2. strengthen and facilitate the implementation of safety-effective voluntary industry-based standards for automotive electronics reliability / cybersecurity

3. foster the development of new system solutions for improving automotive electronics reliability / cybersecurity
4. identify potential minimum performance-based vehicle safety requirements and/or principles for electronics reliability / cybersecurity
5. create foundational materials for future potential NHTSA policy and regulatory decision activities

ELECTRONICS RELIABILITY PROGRAM

NHTSA's electronics reliability research program covers various safety-critical applications deployed on vehicles today, as well as those envisioned on future vehicles that may feature more advanced forms of automation and connectivity.
NHTSA's electronics reliability research activities in support of our five aforementioned primary goals include the following projects.

Functional Safety Process and Requirements Research

This project focuses on examining ISO 26262 process standard and how it can improve the electronics reliability and security through encouraging design best practices at manufacturers. The scope of automotive functional safety, as defined within the ISO 26262 standard, only covers a portion of safety assurance activities associated with the design and manufacturing of a safe vehicle. More specifically, the ISO 26262 process addresses the safety related requirements necessary to meet the identified safety integrity levels of vehicle functions under electrical and electronic failures. While this process is only a piece of the overall vehicle safety assurance process, it is of great interest, because it adds a streamlined functional safety component to the standard systems engineering process that deals with the growingly complex portion of the vehicle architecture, namely the electronics, control system and software design. NHTSA continues to evaluate the ISO 26262 standard [8] and its process steps as well as other approaches used in the industry and those emerging in academic settings such as System Theoretic Process Analysis (STPA).

The agency has research underway that is applying the ISO 26262 standard in conjunction with STPA to safety critical automotive systems that directly govern the motion controls of a vehicle. More specifically, we are researching safety requirements associated with electronic throttle control (various propulsion system variations such as internal combustion engine, diesel, hybrid, electric), electronic brake control, electronic steering control (through electric power steering, pure steer-by-wire and differential braking), and rechargeable energy storage system controls.

Reliability Enhancing Systems Solutions

NHTSA is currently researching areas of advanced diagnostics and prognostics as they pertain to predicting impending system failures (prognostics) and logging critical fault code data (diagnostics) in safety-critical automotive electronic control systems. The agency is seeking to identify the safety improvement opportunities that may be gained from the development and use of enhanced diagnostics and prognostics in automotive applications.

NHTSA is also conducting an assessment of failure-response mechanisms that could help ensure that automotive, safety-critical, electronic control systems are (1) fail safe(i.e. allow driving in a safe-state to

mitigate loss or partial loss of functionality); (2) fail operational(i.e. allow normal driving with loss-of-function warning); and (3) fail secure i.e. disallow the vehicle to be used in the advent of a catastrophic failure. The agency is seeking to gain and provide insight into how automotive technologies address safety beyond system reliability practices (i.e. in addition to preventing the failure, how do systems react to failures?).

Another area of research is the human-factors challenges associated with driver interactions during system failures in safety-critical automotive electronic control systems. Driver notifications/warnings pertaining to an electronic control system failure would ideally be timely, appropriate, and effective.

AUTOMOTIVE CYBERSECURITY PROGRAM

As stated before, NHTSA established five primary goals, based on a systems engineering process, to address cybersecurity challenges associated with the secure operation of motor vehicles equipped with advanced electronic control systems.

Our automotive cybersecurity research activities in support of these goals include the following activities:

Establishing an Automotive Cybersecurity Knowledge-base

NHTSA has been actively researching cybersecurity standards, principles and best practices in automotive and other industries. A mature knowledge base in cybersecurity exists primarily in the information technology (IT) domain, which provides valuable insights for the protection of automotive electronic assets, however, principles adopted from IT security may not fully address the security and safety requirements of cyber-physical systems[1] (CPS) [4]. Because security risks can result in imminent safety concerns in case of CPS such as an automobile, risk tolerance associated with security vulnerabilities differ significantly -particularly for systems that govern the motion controls of a vehicle. As a result, we investigated various threat modeling approaches used in other industries and researched potential threat modeling and characterization methods that may apply to vehicle controls [3].

We also investigated design and quality control processes that focus on cybersecurity challenges throughout the lifecycle of a product. For instance we reviewed various National Institute of Standards and Technology (NIST) publications, and particularly studied NIST's Cybersecurity Risk Management Framework and how it may be applied to modern automobiles [2].

Industry Standards, Best Practices and Cybersecurity Initiatives

To facilitate security-by-design through quality assurance processes, the automotive manufacturers, suppliers, and other stakeholders are collaborating through SAE International to examine the emerging vehicle cybersecurity concerns and considering actions that could include the development of voluntary standards, guidelines, or best practices documents. NHTSA encourages these activities and provides feedback to SAE International Standards committees, such as the Vehicle Electrical System Security committee, and the Electrical Hardware Security committee.

[1] Cyber-physical systems (CPS) are engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components. [National Science Foundation's definition of CPS]

Another industry activity that NHTSA strongly encourages is the recent joint effort undertaken by Alliance of Automotive Manufacturers and the Association of Global Automakers with the goal of establishing a voluntary information sharing and analysis center (ISAC) or other comparable program for the automobile industry sector.

NHTSA studied the ISAC model [5] for safeguarding against cybersecurity risks and threats in other industries such as financial services, information technology, and communications. Our analyses indicate that an automotive sector specific information sharing forum, such as an ISAC, is beneficial to pursue. It could advance the cybersecurity awareness and countermeasure development effectiveness among public and private stakeholders. ISACs have a unique capability to provide comprehensive inter- and intra-sector coverage to share critical information pertaining to sector analysis, alert and intelligence sharing, and incident management and response.

Our research across other industries indicates that the *complete prevention* of cyber-threats is unlikely. This fact and the successful use of ISACs in other industry sectors, suggest that it might also be effective for the auto industry to have mechanisms in place to expeditiously exchange information related to cyber-threats, vulnerabilities, and countermeasures among industry stakeholders when threats occur. Such a mechanism would enhance the ability of the automotive sector to prepare for, respond to, and recover from cybersecurity

System Solutions for Automotive Cybersecurity

In terms of system solutions, here are four major pieces to the agency's research approach.

6. *Preventive solutions*: This group of techniques helps to harden the design of automotive electronic systems and networks such that it would be difficult for malicious attacks to take place. Using structured security process standards could help identify vulnerabilities such that necessary design improvements can be identified and implemented during the design phase of the product. These vulnerabilities include possible entry points through accessible physical interfaces (such as the OBD-II port, USB ports, CD/DVD players), short range wireless interfaces, (such as Bluetooth, Wi-Fi, or Dedicated Short Range Communications (DSRC)), and long-range wireless interfaces such as cellular or satellite-based connectivity to the vehicle). Examples of design improvements could include the use of:

    a. encryption and/or authentication of messages on communication networks;
    b. different communication approaches, architectures or protocols;
    c. segmentation/isolation of safety-critical system control networks;
    d. redundant communications , direct measurements and/or message authentication or source validation for safety critical system inputs that can influence the motion controls of a vehicle;
    e. strong authentication controls for remote access vectors to vehicles;
    f. gateway controls and firewalls between interfaced vehicle networks;

g. formal methods for the specification, development and validation of embedded systems; etc.

The primary intents of this category of activities are (1) to significantly reduce the probability of cyber risks; and (2) to limit the impacts of a potential cybersecurity breach (e.g. one part of one vehicle or just one vehicle as opposed to an entire fleet).

7. *Real-time intrusion detection methods*: As a complement to the preventative measures, detecting intrusions into the system would help provide more comprehensive protection. A cybersecurity breach would likely take place on or through a communication network. From an intrusion detection perspective, vehicular network communications are considered fairly predictable and may be well-suited for real-time monitoring to detect anomalous activity with respect to nominal expected message flows. We are initiating research in 2015into real-time monitoring technologies targeted for use in the automotive sector.

8. *Real-time response methods*: Once a potential intrusion is detected, having practical strategies in place would help mitigate potential harmful impacts. Depending on the potential risks and level of intrusion detection confidence, the vehicle architecture could be designed to take a variety of actions such as: (1) temporarily or permanently shutting down the communication network(s) (at the potential cost of disabling various safety functions); (2) informing the driver; (3) recording and transmitting before-and-after trigger point data for further analysis; (4) and counter-measure development, etc. The purpose of this category of cybersecurity defense is to mitigate the potential harmful consequences of detected anomalous activity on the vehicle experiencing the potential breach.

9. *Treatment methods*: While the previous paragraph discussed response methods (dealing with fail-safe operation of the vehicle where an intrusion is detected), treatment methods deal with distributing information related to the subject risk to other potential vulnerable entities even before cybersecurity threat reaches them. Treatment methods involve timely information extraction from impacted parties, their analysis, development of countermeasures, and timely dissemination of that countermeasure to all relevant stakeholders (such as through an ISAC).

Applied Cybersecurity Research

NHTSA's primary objective through the cybersecurity program is to develop cybersecurity performance requirements, principles, best practices, and objective tests to assess conformance with such standards.

In support of this goal, NHTSA has been building applied cybersecurity testing capabilities and a cybersecurity laboratory at its Vehicle Research and Testing Center (VRTC) in East Liberty, OH. Current capabilities support communication bus and RF monitoring, CAN and GPS spoofing, firmware analysis and limited ECU penetration-testing. Planned future capabilities include RF disruption research, which will explore robustness associated with LTE, DSRC, GPS and Radar signals.

SUMMARY

The growth in electronics and software use in the design of automobiles is likely to continue because they support advanced

safety, efficiency, and convenience features. Along with this trend, come the challenges associated with managing safety and security of growingly complex automotive electrical architectures and networks.

NHTSA is continuing to conduct research on safety-critical automotive electronic control systems and collaborating with public and private sector stakeholders to advance its safety mission. The security for safety critical control systems remain a major area of interest for the Agency. Our main goal is to develop facts-based safety and security requirements or guidance for safety assurance of critical automotive systems.

In response to the Moving Ahead for Progress in the 21st Century Act (MAP-21) [6], NHTSA published a Federal Register notice outlining its examination of the need for safety standards with regard to electronic systems in passenger motor vehicles [9] in October 2014 and received public comments. We are in the process of writing a report to Congress, as required by MAP-21, which will also incorporate the received comments.

We have plans to extend ongoing electronics reliability research and cybersecurity research into emerging technologies that offer varying levels of vehicle automation as outlined in NHTSA's Preliminary Statement of Policy Concerning Automated Vehicles [10]. We are conscious of the increased role that electronic systems will play in the driving task in these future vehicles. Thus, NHTSA continues to design its research plans accordingly.

REFERENCES

1) Charette, R.N. (2009). This car runs on code. IEEE Spectrum.
2) McCarthy, C., & Harnett, K. (2014, October). National Institute of Standards and Technology Cybersecurity Risk Management Framework Applied to Modern Vehicle. (Report No. DOT HS 812 073). Washington, DC: National Highway Traffic Safety Administration.
3) McCarthy, C., Harnett, K., & Carter, A. (2014, October). Characterization of potential security threats in modern automobiles: A composite modeling approach. (Report No. DOT HS 812 074). Washington, DC: National Highway Traffic Safety Administration.
4) McCarthy, C., Harnett, K., & Carter, A. (2014, October). A summary of cybersecurity best practices. (Report No. DOT HS 812 075). Washington, DC: National Highway Traffic Safety Administration.
5) McCarthy, C., Harnett, K., Carter, A., & Hatipoglu C. (2014, October). Assessment of the Information Sharing and Analysis Center Model, (Report No. DOT HS 812 076). Washington, DC: National Highway Traffic Safety Administration.
6) Moving Ahead for Progress in the 21st Century Act, Public Law 112-141 (Jul. 6, 2012), § 31402.
7) National Research Council of the National Academies. (2012). The Safety Promise and Challenge of Automotive Electronics, insights from unintended acceleration, (ISBN 978-0-309-22304-1).
8) Van Eikema Hommes, Q.. (2012). Review and Assessment of the ISO 26262 Draft Road Vehicle—Functional

Safety. (SAE Technical Paper: 2012-01-0025)
9) NHTSA. (2014). Federal Register Notice: Automotive Electronic Control Systems Safety and Security. (NHTSA-2014-0108)
10) NHTSA. (2012). Preliminary Statement of Policy Concerning Automated Vehicles.