4910-59-M

DEPARTMENT OF TRANSPORTATION

National Highway Traffic Safety Administration

Docket No. NHTSA-2014-0108

Request for Comment on

Automotive Electronic Control Systems Safety and Security

AGENCY: National Highway Traffic Safety Administration (NHTSA), Department of Transportation (DOT).

ACTION: Request for comments.

SUMMARY: This notice presents the National Highway Traffic Safety Administration's research program on vehicle electronics and our progress on examining the need for safety standards with regard to electronic systems in passenger motor vehicles. The agency undertook this examination pursuant to the requirements of the Moving Ahead for Progress in the 21st Century Act (MAP-21) Division C, Title I, Subtitle D, Section 31402, Subsection (a). In addition, and in accordance with MAP-21, we are seeking comment (through this document) on various components of our examination of the need for safety standards in this area. As MAP-21 also requires this agency to report to Congress on our findings pursuant to this examination, we intend to submit a report to Congress based in part on our findings from this examination and public comments received in response to this document.

DATES: You should submit your comments early enough to ensure that Docket Management receives them no later than **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: Comments should refer to the docket number above and be submitted by one of the following methods:

- Federal Rulemaking Portal: http://www.regulations.gov. Follow the online instructions

for submitting comments.

- Mail: Docket Management Facility, U.S. Department of Transportation, 1200 New Jersey Avenue, S.E., West Building Ground Floor, Room W12–140, Washington, DC 20590-0001.
- Hand Delivery: 1200 New Jersey Avenue, S.E., West Building Ground Floor, Room W12–140, Washington, DC, between 9 a.m. and 5 p.m. ET, Monday through Friday, except Federal Holidays.
- *Instructions*: For detailed instructions on submitting comments and additional information on the rulemaking process, see the Public Participation heading of the SUPPLEMENTARY INFORMATION section of this document. Note that all comments received will be posted without change to http://www.regulations.gov, including any personal information provided.
- *Privacy Act*: Anyone is able to search the electronic form of all comments received into any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). You may review DOT's complete Privacy Act Statement in the Federal Register published on April 11, 2000 (65 FR 19477-78). For access to the docket to read background documents or comments received, go to http://www.regulations.gov or the street address listed above. Follow the online instructions for accessing the dockets.

FOR FURTHER INFORMATION CONTACT: For technical issues: Mr. David V. Freeman of NHTSA's Office of Vehicle Crash Avoidance & Electronic Controls Research at (202) 366–0168 or by email at *david.v.freeman@dot.gov*. For legal issues: Mr. Jesse Chang of NHTSA's Office of Chief Counsel at (202) 366-9874 or by email at *jesse.chang@dot.gov*.

SUPPLEMENTARY INFORMATION

In this document, the agency is presenting its progress in conducting an examination of the need for safety standards and seeking comments on its findings thus far. The agency is directed to conduct this examination and report its findings to Congress by the Moving Ahead for Progress in the 21st Century Act (MAP-21). [1]

I. MAP-21 and Examining the Need for Electronic System Safety Standards

In section 31402 of MAP-21, Congress directs this agency to "complete an examination of the need for safety standards with regard to electronic systems in passenger motor vehicles." [2] In conducting this examination, the Act directed the agency to consider various topics:

(1) electronic components;

(2) the interaction of electronic components;

(3) the security needs for those electronic components to prevent unauthorized access; and

(4) the effect of surrounding environments on the electronic systems.[3]

Finally, the Act also directed the agency to allow for public comment in conducting this examination.[4] Upon completing the examination, the Act also directs the agency to submit a report to Congress on the highest priority areas for safety with regard to the electronic systems.[5]

This document presents the agency's progress thus far in conducting the examination required in section 31402. We illustrate how we are examining each of the areas described by Congress in section 31402 and are seeking public comment on that examination. We intend to incorporate the comments received pursuant to this document in our report to Congress

[1] Moving Ahead for Progress in the 21st Century Act, Pub. L. No. 112-141 (Jul. 6, 2012), § 31402.
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *Id*.

identifying the need for safety standards.

II. Background

a. NHTSA's Safety Role

The National Highway Traffic Safety Administration (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 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. We identify and measure 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.

b. Growth in Automotive Electronics and their safety challenges

The use of electronics in the design of modern automobiles is a rapid ongoing progression. The first common use of automotive electronics[6] dates back to 1970s and by 2009 a typical automobile featured over 100 microprocessors, 50 electronic control units, five miles of wiring and 100 million lines of code.[7] Use of electronics is not new. It has enabled safer and more fuel-efficient vehicles for decades. Electric and hybrid vehicles could not have been

[6] Not including electronics use for radio purposes.
[7] "This car runs on code," R.N. Charette, 2009, http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code

developed and produced without the extensive use of electronics and proven safety technologies such as electronic stability control could not have been implemented. 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 concerns in the areas of reliability, security, and safety assurance of growingly networked vehicles leveraging electronics.

Electronics provide many safety, security, convenience, comfort, and efficiency functions for vehicle operators through interconnections and communications with other onboard electronics systems. Common communications networks and protocols allow for the exchange of information between sensors, actuators, and the electronic control units that execute software programs to accomplish specific functions. A vehicle will typically feature multiple networks. Those networks may be isolated from one another for a variety of reasons such as safety and security; however, in other cases different networks could be interconnected to enable exchange of information across a broader range of systems. Sharing data across multiple networks can be safeguarded against adverse influence over safety-critical systems; however, effectiveness of such approaches is only anecdotally known today. Growing system complexity and abundance of design variants even within one manufacturer over model years and across classes of vehicles pose general concerns over whether existing processes can ensure their functional safety. 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, and hence are difficult to investigate without a record of data from the electronic systems.

While there are challenges, progressively introduced safety technologies, such as Automatic Emergency Braking (AEB), have the potential to significantly reduce the many thousands of fatalities and injuries that occur each year as a result of motor vehicle crashes. Further, continued innovation into more advanced forms of vehicle automation could address other types of crashes where human driver error plays a role. In May 2013, NHTSA released a preliminary statement of policy[8] concerning automated vehicles where the agency outlined its planned research into emerging technologies. Given the complexity of these new systems in terms of the additional electronics software and hardware needed, electronic control systems safety will continue to grow in importance as these systems become more commonplace in production vehicles.

Along these lines, the Transportation Research Board (TRB) Special Report 308[9] by the National Academies of Sciences (NAS) in 2012 identified five challenges for the safety of future electronic control systems:

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

[8] http://www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf
[9] The Safety Promise and Challenge of Automotive Electronics, insights from unintended acceleration, National Research Council of the National Academies, ISBN 978-0-309-22304-1, 2012.

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

- 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;
- convening a standing technical advisory panel; undertaking a comprehensive review of the capabilities that the agency will need in monitoring for and investigating safety deficiencies in electronics-intensive vehicles;
- ensuring that Event Data Recorders (EDRs) become commonplace in new vehicles;
- conducting research on human factors issues informing manufacturers' system design decisions;
- 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; and
- making the formulation of a strategic plan a top goal in NHTSA's overall priority plan.

In addition to the challenges regarding electronic components and their ability to function reliably in spite of their complex interactions, NHTSA believes there are also challenges with regard to the ability of these systems to remain free of unauthorized access or malicious attacks. While documented demonstrations[10,11,12] of vehicle hacking to date have required some form of

[10] "Experimental Security Analysis of a Modern Automobile," K. Koscher et. al., IEEE Symposium on Security and Privacy, Oakland, CA, 2010.
[11] "Comprehensive Experimental Analyses of Automotive Attack Surfaces," S. Checkoway et.al., USENIX Security, 2011.
[12] "Adventures in Automotive Networks and Control Units," C. Miller, C. Valasek, DEF CON 21, Las Vegas, NV, 2013.

long-term physical access to the vehicle and our review has not identified any reported field incidents resulting in a safety concern, we recognize that lack of occurrence does not imply impossibility. As further discussed in this document, NHTSA is interested in gathering and evaluating information from the public (as part of its examination pursuant to MAP-21) to determine what additional work is needed in this area.

c. Industry's Existing Safety Assurance Processes

Notwithstanding the increased difficulty in the safety assurance of growingly more complex systems, the automotive industry uses a number of safety and quality assurance practices in the design of safety critical systems, which are not unique to but also cover electronic systems. As documented in a number of publications and also summarized in the NAS Report, these approaches include the:

- establishment of system safety requirements;
- assessment of design hazards and risks at component, function, system, manufacturing and process levels such as by the use of failure mode and effects analysis[13] (FMEA) and fault tree analysis[14] (FTA);
- quality management systems such as ISO/TS 16949[15], advanced product quality planning (APQP), and Design for Six Sigma (DFSS);
- design validation and verification testing such as electrical, environmental, lab, test track and limited field trials;
- variants of production part approval process (PPAP); and
- post deployment field data analysis.

[13] IEC 60812 standard covers the process for conducting FMEA analysis.
[14] IEC 61025 standard covers the process for conducting FTA analysis.
[15] ISO/TS 16949:2002 covers particular requirements for the application of ISO 9001:2000 for automotive production and relevant service part organizations.

Further, many automotive original equipment manufacturers (OEM) were actively engaged in the development and revision of the ISO 26262[16] standard and some have already started to follow its principles. As further discussed in this document, NHTSA is interested in gathering and evaluating information from the public (as part of its examination pursuant to MAP-21) to determine whether there are emerging gaps in the functional safety assurance processes of motor vehicles.

d. Existing Safety Process Standards Research Overview

Sectors of the automotive industry currently consider electronics safety and cybersecurity as part of their design and quality control processes. Three process standards from the broader transportation industry are frequently mentioned as suitable and preferred methods also used in the design of road vehicles usually complementing existing safety assurance practices: ISO 26262, MIL-STD-882E, and DO-178C.

ISO 26262 is the first automotive industry specific standard[17] that addresses safety-related systems comprised of electrical, electronic, and software elements providing safety-related functions in the design of road vehicles. It is an adaptation to the International Electrotechnical Commission (IEC) 61508[18] standard to road vehicles. The first publication of ISO 26262 was in November 2011. This standard seeks to address various important challenges facing today's road vehicle technologies including:

- the safety of new electrical, electronic, and software functionality in vehicles;
- the trend of increasing system complexity, software content, and use of

[16] International Organization for Standardization (ISO) standard for Road vehicles – Functional safety.
[17] Van Eikema Hommes, Q., "Review and Assessment of the ISO 26262 Draft Road Vehicle - Functional Safety," SAE Technical Paper 2012-01-0025, 2012, doi:10.4271/2012-01-0025.
[18] IEC 61508 is an international standard for functional safety of electrical/electronic/programmable electronic safety-related systems. This standard considers all of the environments that could result in an unsafe situation for the subject product, including shock, vibration, temperature, and electromagnetic fields and their induced voltages and currents.

electromechanical components; and

- the risk from both systematic failure and random hardware failure.

Typical concerns associated with the ISO 26262 standard may include that the

- standard could be laborious to apply;
- hardware portions of the standard's coverage may be very similar to existing industry practices with limited incremental benefits;
- software portions of the standard may primarily recommend good systems engineering practices for software safety; and
- assessment of the automotive safety integrity levels (ASIL) may vary due to subjectivity in the process.

Due to some of these limitations, existing practices and ISO 262626 are sometimes augmented with more mature system engineering approaches that are outlined in MIL-STD-882E and DO-178C, particularly on the software engineering side.

MIL-STD-882E is the U.S. Department of Defense's systems engineering approach for eliminating hazards, where possible, and minimizing risks where those hazards cannot be eliminated. By taking a systems approach, this standard considers hazards in the entire lifecycle of systems, products, equipment, and infrastructure including design, development, test, production, use, and disposal stages. The principle of this standard is that system safety should follow the system engineering process, and is the responsibility of all functional disciplines, not just the system safety professionals. This standard has gone through a number of revisions in order to adapt to changes in technology and lessons learned through experience.

In the aviation industry, DO-178C[19] is an accepted guidance for software development.

[19] DO-178C: Software considerations in airborne systems and equipment certification.

Conformance to this standard means the software satisfies airworthiness[20] requirements with an acceptable level of confidence. As part of the airworthiness certification process, DO-178C provides guidelines to produce the software lifecycle data needed in order to support the certification process (e.g. plans for software development, verification, configuration management, and quality assurance). It also provides a comprehensive list of considerations in order to avoid errors and mistakes that could be introduced into software. DO-178C considers system software development as a subset of the overall system development process. It assumes that safety-critical requirements for software systems are defined in the higher-level system engineering activities and are given at the beginning of the software development process. Some automotive companies indicated that the principles outlined in this more mature standard complement the software standard described in ISO 26262 Part 6,[21] which is still evolving.

As we discuss further in this document, NHTSA continues to investigate functional safety approaches for the automotive industry that may effectively address emerging concerns from the increased use of electronics and software in the design of automobiles.

e. Available Data[22] Sources Research Overview

For purposes of determining the capabilities of various datasets to categorize and rank vehicle electronics safety issues, we considered vehicle recall data, vehicle owner's questionnaire (VOQ) data, early warning reporting (EWR) data, and data from our field crash investigation databases such as National Automotive Sampling System (NASS), Fatality Analysis Reporting System (FARS), and Special Crash Investigation (SCI) database. Further, we considered event data recorder (EDR) capabilities. We briefly describe our findings on these

[20] Airworthiness of an aircraft refers to meeting established standards for safe flight.
[21] ISO 26262-6:2011-Road vehicles; Functional safety; Part 6: Product development at the software level.
[22] Data for purposes of examining the need for safety standards with regard to automotive electronic systems does not include personally identifiable information about the operators.

various data sources in this section. While we believe that the sources of information available to NHTSA in this regard are useful in helping the agency begin to identify the highest priority areas with regard to electronic components (and their interactions), we also believe that they have certain limitations in ranking safety issues associated with vehicle electronics. This limitation is mostly driven from the lack of detailed information regarding specific electronic system failure types. Hence, in section V. we seek comment from the public as to what other sources of information and data are available.

The vehicle recall database is a publicly available resource that documents safety defects or failures to meet minimum performance standards set by the Federal Motor Vehicle Safety Standards (FMVSS) in a motor vehicle or item of motor vehicle equipment. When manufacturers decide a safety defect or a noncompliance exists in a motor vehicle or item of motor vehicle equipment they manufactured, they are required to notify NHTSA and furnish a report with particular information about the defect or noncompliance, the products involved, and additional information including the manufacturer's plan to remedy for free the defect or noncompliance (See U.S.C. § 30118 and 49 CFR 573.6).

Defect and noncompliance notifications and information reports are reviewed by NHTSA analysts who enter them in the recall database. The database includes summaries of the defect description, consequences, and remedy for each recall. The number of vehicle recalls has increased significantly in the past 20 years, nearly tripling from 1993 (222) to 2013 (654). While the vehicle recall database contains a large amount of useful information, the database and underlying defect reports were not intended for detailed or precise statistical analyses of recalls by typology or root cause related to motor vehicle electronic systems. Any such analysis requires a manual review and classification process. However, this work can be limited by the

amount of detail contained in the defect information reports, which normally provide more general descriptions of the defect condition and potential safety consequences.

Vehicle Owner Questionnaires (VOQs) are voluntarily submitted by consumers to NHTSA to report a complaint in a vehicle or related equipment item. Each complaint (which is stored in a database and made available to the public redacted of personal identifiers) identifies the vehicle type, incident specifics, and includes a free form narrative to describe details. Complaint content and trends are helpful for general screening purposes but follow-up is sometimes necessary to verify and clarify complaints and incident specifics. Approximately 50,000 VOQs were filed in 2013.

Another source of data is the EWR system. Several data types are regularly reported to NHTSA by manufacturers. The data include non-dealer field reports (documents), listings of death/injury claims (records), and aggregated counts of certain claim types. The quarterly reporting interval, high level component coding of aggregate figures, and variability in manufacturer reporting are factors that are considered when analyzing certain EWR data sets to study safety critical embedded control systems. Field reports are the only EWR data sets available for evaluating specific defect conditions, including incidents in which the problem is intermittent or cannot be duplicated.

Separately, regarding our national crash databases, the National Automotive Sampling System (NASS)[23] is composed of two systems - the Crashworthiness Data System (CDS) and the General Estimates System (GES). These are based on cases selected from a sample of police crash reports. CDS data focus on passenger vehicle crashes, and are used to investigate crash circumstances, vehicle crash response and occupant injury and identify potential improvements in vehicle design. The GES database contains crash statistics on police-reported crashes

[23] http://www.nhtsa.gov/NASS

involving all types of vehicles. The information comes from samples of police reports of the estimated six million crashes that occur annually. Each NASS database is weighted to characterize a nationally representative sample. Each crash must involve at least one motor vehicle traveling on a traffic way, which results in property damage, injury, or death, and it must be obtained from a police report.

The Fatality Analysis Reporting System (FARS)[24] is a nationwide census database on crashes involving fatalities containing similar information to NASS-GES. These two crash databases consist of approximately 120 data elements that describe the crash, which are derived from review of police crash reports by trained data entry personnel; however, similar to the case with VOQs, there may be challenges in using these databases to perform detailed analyses for purposes of ranking emerging electronics concerns because data elements were not established with this specific purpose in mind. In combination with other datasets, analysis of GES and FARS can still provide confirming or augmenting evidence in identifying potential priority areas in electronics reliability.

The Crash Injury Research and Engineering Network (CIREN) database consists of over 1,000 discrete fields of data concerning severe motor vehicle crashes, including crash reconstruction and medical injury profiles extending back to 1996. CIREN cases feature detailed data on occupant injury, vehicle damage and restraint technology and crash environment, as well as technical or human factors that are related to injury causation in motor vehicle crashes. Each CIREN case is reviewed together by both medical and engineering professionals, along with the crash investigator, to determine injury causation and data accuracy.

The Special Crash Investigations (SCI)[25] database contains a range of data collected from

[24] http://www.nhtsa.gov/FARS
[25] http://www.nhtsa.gov/SCI

basic data contained in routine police and insurance crash reports to comprehensive data from special reports by professional crash investigation teams. Hundreds of data elements relevant to the vehicle, occupants, injury mechanisms, roadway, and safety systems are collected for each of the over 100 crashes designated for study annually. SCI cases are intended to be an anecdotal data set useful for examining special crash circumstances or outcomes from an engineering perspective. The SCI program's flexibility allows for investigations of new emerging technologies related to automotive safety.

Finally, Event Data Recorders[26] (EDRs) are devices that may be installed in a motor vehicle to record technical vehicle information for a few seconds leading up to the crash. For instance, EDRs may record vehicle speed, engine throttle position, brake use, driver safety belt status, and air bag warning lamp status. NHTSA has been using EDRs to support its crash investigation program for several years and EDR data is routinely incorporated into NHTSA's crash databases. This type of data could potentially play a role in finding when safety critical automotive electronics were not functioning properly.

III. Our Examination of the Areas Identified in MAP-21 to Date

NHTSA has been actively engaged in research (both internally and with outside parties) in automotive electronics reliability, cybersecurity, and emerging technologies in advanced vehicle automation for the past two years. The agency has established, per MAP-21,[27] 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

[26] In 2006, NHTSA published a final rule creating a regulation (49 CFR Part 563, Event Data Recorders (Part 563)) that specifies the minimum data set that should be collected if a manufacturer decides to voluntarily install an EDR in their vehicle, along with requirements for the range and accuracy of EDR data, as well as requirements for storage and retrieval. Part 563 applies to vehicles manufactured on or after September 1, 2012. In December 2012, NHTSA proposed a standard that would mandate EDRs on all vehicles required to have frontal air bags. (77 FR 74144). No final rule publication date has been established.

[27] Moving Ahead for Progress in the 21st Century Act, Pub. L. No. 112-141 (Jul. 6, 2012), § 31401(a).

technologies. The Council is governed by senior NHTSA management and the mission of the group is to broaden, leverage, and expand the agency's expertise in motor vehicle electronics to continue ensuring that technologies enhance vehicle safety and review and advise on the research program established over electronics reliability, cybersecurity and automation topics.

With input from the Council, NHTSA has identified and funded initial research into the following areas:

- Hazard analyses of safety-critical electronic vehicle control systems, applying Hazard and Operability (HazOp) process referenced within the ISO 26262 standard as well as System Theoretic Process Analysis (STPA);
- Examination of process oriented functional safety and security standards for automotive electronics design and development;
- Automotive cybersecurity concerns, threats, and vulnerabilities, and potential countermeasures;
- Best practices in safeguarding against cybersecurity risks in related but in non-automotive industries; and
- Human factors and other emerging concerns associated with highly automated vehicles.

Because the agency was already investigating vehicle electronics as a new and emerging research area for vehicle safety prior to the passage of MAP-21, the agency has already completed some research and analyses that address some of the items listed by Congress in section 31402 of MAP-21. Research reports are available on the agency's website[28] and we

[28] Office of Vehicle Crash Avoidance & Electronic Control Research technical publications are posted on the NHTSA website at http://www.nhtsa.gov/Research/Crash+Avoidance/Office+of+Crash+Avoidance+Research+Technical+Publications

expect to publish more reports as projects are completed over the 2015-16 timeframe. It should be noted that the research described in this notice represents research already underway and future research that the agency anticipates undertaking as resources permit. This section shows our initial progress on the areas that Congress directed the agency to consider in the examination required under section 31402. We further request comments on our research thus far and request specific comments on the issues identified in the following sections.

a. Electronics Components and the Interaction of Electronic Components

To examine the potential safety concerns associated with electronic components and interactions of electronic components, we initiated research in developing potential approaches to analyzing the automotive electronic control system architecture and their interconnections. In conjunction, we reviewed data sources available to NHTSA to assess datasets that would be useful to analyze for purposes of this initiative (as documented in section II.e.). Further, we initiated systematic hazard analyses on select safety-critical automotive control systems to better understand the vehicle level safety risks. In the following paragraphs, we provide further details on these research topics that enable us to begin examining the first two areas stated in MAP-21 systematically.

NHTSA is also conducting research to develop an electronics-related failure-typology.[29] As part of this research, we are evaluating the various sources of data described in section II. e. (defect data, crash databases, etc.) to determine if suitable data exists at this time to effectively utilize a detailed failure typology that would describe and categorize the hazards and causes of automotive electronic control system failures. Through such analysis, the agency would like to

[29] Establishing a failure typology refers to developing categories and data elements that can help the agency (and others) organize the types of failures relating to electronic control systems in vehicles. Establishing the typology is an important step in helping to create a structure to help analyze potential safety problems relating to electronics in vehicles.

understand how trends in the underlying data for the chosen dataset change over time as a function of increased use of electronics. We expect to publish our failure-typology research in 2015 and continue our research on appropriate datasets into 2016.

Another approach we are taking is to study the automotive electronic system architecture. Functional safety assurance of modern automobiles requires a thorough understanding of electronic control systems' design under a variety of scenarios. These circumstances include systems' behavior under nominal conditions and also during failure conditions. Equally important are state-of-the-art capabilities in detecting failures (diagnostic/prognostic) and fault-tolerant and/or fail-safe strategies that can prevent errors from resulting in safety hazards. To this end, NHTSA funded initial research to perform hazard analyses in select safety-critical automotive control system areas, such as Accelerator Control Systems (ACS)/Electronic Throttle Control (ETC), Rechargeable Energy Storage Systems (RESS), and steering and braking control systems within the context of automatic lane centering function. These studies apply the Hazard and Operability (HazOp) process referenced within the ISO 26262 standard as well as System Theoretic Process Analysis (STPA) approach to identify the system level hazards associated with potential failures in the subject control systems. The purpose of these studies is to better understand the critical automotive system functions, failures, and risks and identify safety goals and requirements. Further, another purpose is to compare and contrast results obtained from existing hazard analyses techniques. We are currently prioritizing our hazard analysis research to cover electronic throttle control, steering control, braking control and motive power areas. We expect to publish a series of research reports on hazard analyses starting in 2015.

A typical automotive electronic control system primarily relies on the following to perform its intended purposes:

- Sensors (measurements);
- Interpretation of sensed signals (e.g. conversion, configuration, classification);
- Estimations of parameters (when direct sensing may not be available, e.g., vehicle speed);
- Actuators (to carry out the intended motive);
- Communication networks (that facilitate electronic exchange of information between sensors, controllers and actuators);
- Design and programming of the control algorithm (conditions and respective actions) including:
    a. design and software coding that implement:
        i. the intended functions; and
        ii. system monitoring and malfunction detection logic; and
    b. supervisory logic that arbitrates between multiple, potentially conflicting, subsystem commands; and
- Availability of motive power.

Interactions between electronic components (and distributed embedded systems) are facilitated primarily by communication networks and shared use of sensors, software logic and actuators. Prioritization of competing requests from the various control subsystems and the driver for safety-critical functions is a potential area of anticipated future research due to continued proliferation of safety and convenience functions.

Comments Requested

1) NHTSA currently has research underway that is evaluating the hazards associated with electronic control systems that could impact a vehicle's steering, throttle, braking and motive

power first because they can impact the fundamental control functions that a driver performs (such as providing lateral (via steering) and longitudinal (throttle, braking) control for the vehicle). This means, we would research safety hazards associated with other automotive electronic control systems (e.g. safety restraint systems control, power door lock control, lighting control) later. We seek comment on this approach from a need for standards research priority stand-point.

a) Should the agency pursue alternative approaches to categorize and prioritize potential electronic control system hazards and impacts to support new standards?
b) For hazard analysis research, the agency is currently pursuing HazOp and STPA. What other hazard analysis methods should the agency also consider and why?
c) What other automotive electronics should we consider in our research that could affect the electronics in the safety critical systems we identified (steering, throttle, brakes, etc.)?

2) NHTSA currently has research underway that is evaluating system performance requirements for critical safety systems. We seek comment on automotive electronic component and system performance requirements for control systems that impact throttle, braking, steering, and motive power management:

a) What performance-based tests, methods, and processes are now available for safety assurance of these types of automotive electronic control systems?
b) What series of performance-based tests should the agency consider to ensure safe functionality of these types of automotive electronic control systems under all real-world conditions (e.g. nominal, expected, non-nominal, and failure conditions)?
c) Performance tests would ideally be applicable regardless of any specific design choices. We surmise that electronic components may have a wider variety of manufacturer

specific tuning and implementation variations. What types of challenges does this create for designing performance tests for electronic components? What methods are available for addressing those challenges?

3) NHTSA currently has research underway that is evaluating diagnostics and prognostics for critical safety systems. We seek comment on vehicle health monitoring, diagnostics, and prognostics capabilities and fault-tolerant design alternatives for automotive safety applications.
   a) What methods are effective in identifying potential anomalous behavior associated with electronic components, systems, and communications reliably and quickly?
   b) What strategies do current vehicles have for activating a "fail-safe" mode when critical problems are detected? What types of problems are classified as "critical" and how does the vehicle detect these problems?
   c) What state-of-the-art detection and fail-safe response methods should the agency be aware of and further assess?
4) NHTSA currently has research underway that is evaluating various process standards and their applicability to critical safety systems. We seek comment on testing, validation, certification, and regulation alternatives for vehicle electronics to these process standards:
   a) What are the pros and cons of utilizing a process - certification method (e.g., ISO 26262) where the manufacturer is asked to identify, categorize, and consider potential remedies for electronics safety problems?
      i) What approaches should be considered for manufacturers to demonstrate conformity with voluntary industry process standards such as ISO 26262?

ii) How does one evaluate conformity to a process standard that uses an engineer's best judgment to identify, categorize, and consider potential remedies to electronics safety problems?

iii) What verification steps may be appropriate to ensure that potential standards are met?

b. Security Needs to Prevent Unauthorized Access to Electronic Components

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.

NHTSA has been actively researching existing cybersecurity standards and best practices in automotive and other industries. In reviewing the practices of other industries in dealing with cybersecurity issues, NHTSA has identified two general process-oriented approaches to addressing cybersecurity concerns. The first is design and quality control processes that focus on cybersecurity issues throughout the lifecycle of a product. The second is dealing with cybersecurity issues through establishing robust information sharing forums such as an Information Sharing and Analysis Center (ISAC). This section discusses the agency's findings regarding each of these strategies.

In regards to security design and 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.

While there may be no readily-available automotive cybersecurity standards at this time, NHTSA's research identified general cybersecurity safeguarding approaches that can potentially be examined and adapted for use in the automotive industry. For example, the cybersecurity

framework[30] developed and published by the National Institute of Standards and Technology (NIST) treats cybersecurity as a process integrated into the system, component, and device lifecycle. The guidelines referenced in this framework could allow the automotive industry to develop a security program for modern-day automobiles analogous to information security programs in place for information technology (IT) systems in general. Similarly, system security engineering could potentially be incorporated into the design process in a way similar to system safety engineering as specified in ISO 26262 and "E-safety vehicle intrusion protected applications (EVITA)."[31]

In regards to information sharing mechanisms, NHTSA studied[32] the ISAC model for safeguarding against cybersecurity risks and threats in other industries such as financial services, information technology, and communications. Our initial 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 prevention of cyber-threats would be impractical if not impossible. 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

---

[30] "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.0, NIST, 2014. Accessible at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

[31] EVITA is a project co-funded by the European Union that aims to design, verify, and prototype architecture for automotive on-board networks where security-relevant components are protected against tampering and sensitive data are protected against compromise (http://www.evita-project.org/).

[32] The study report "An assessment of the information sharing and analysis center (ISAC) model" can be accessed at the "Automotive Cybersecurity Topics and Publications" docket: NHTSA-2014-0071.

stakeholders. Such a mechanism would enhance the ability of the automotive sector to prepare for, respond to, and recover from cyber threats, vulnerabilities and incidents. Related to the sector-wide cybersecurity information sharing topic, the Alliance of Automotive Manufacturers (Alliance) and the Association of Global Automakers (Global Automakers) wrote[33] to NHTSA in July 2014 to inform about the new cybersecurity initiative they are undertaking with the goal of establishing a voluntary automobile industry sector information sharing and analysis center or other comparable program. In response[34], NHTSA encouraged Alliance and Global Automakers (as well as automotive original equipment manufacturers) to proceed expeditiously with the outlined process and expressed Agency's hope that their plan would target a date in 2015 for an automotive industry ISAC to become operational.

Security process standards and information sharing forums fit in a larger, more comprehensive automotive cybersecurity assurance approach. In general terms, there are four major pieces to the agency's research approach:

1. Preventive methods and techniques: This group of techniques would seek to harden the design of automotive electronic systems and networks such that it would be difficult for malicious attacks to take place in newer generation systems. Deployment and use of structured security process standards could help identify vulnerabilities such that necessary design improvements can be identified and implemented. 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

[33] Correspondence related to this initiative can be viewed in the "Automotive Cybersecurity Topics and Publications" docket: NHTSA-2014-0071.
[34] *Id.*

include potential use of:

a. encryption and/or authentication on communication networks;

b. different communication approaches or protocols; segmentation/isolation of safety-critical system control networks;

c. strong authentication controls for remote access to vehicles;

d. gateway controls between interfaced vehicle networks; etc.

Other approaches in the field of prevention research include methods such as those investigated in the Defense Advanced Research Projects Agency's (DARPA) high-assurance cyber military systems (HACMS)[35] program. The primary intents of this category of activities are 1) to significantly reduce the probability of cyber risks; and 2) to limit the impact of a potential cybersecurity breach (e.g. one vehicle as opposed to an entire fleet). NHTSA initiated applied research into vulnerability assessment and preventive type measures in 2014 and expects to publish reports starting in 2016.

2. Real-time intrusion detection methods: Total security through preventive measures may not be realistically achievable. Thus, as a complement to the preventative measures, detecting intrusions into the system through communications networks would provide additional protection. A cybersecurity breach would take place on or through a communication network. From an intrusion detection perspective, vehicular network communications are considered fairly predictable and well-suited for real-time monitoring to detect anomalous activity with respect to nominal expected message flows. We are initiating research into this type of technologies in the automotive sector.

3. Real-time response methods: Once a potential intrusion is detected, the strategies to mitigate its potential harmful impacts would also need to be designed in a practical manner.

[35] http://www.darpa.mil/Our_Work/I2O/Programs/High-Assurance_Cyber_Military_Systems_(HACMS).aspx

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: temporarily or permanently shut down the communication network(s) (at the potential cost of disabling various safety functions); inform the driver; record and transmit data before-and-after trigger point for further analysis 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. We expect to develop further research into this category of methods in 2016.

4. Treatment methods: While the previous paragraph discussed response methods (deal with ensuring 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 the compromise may be experienced by them. Treatment methods involve timely information extraction from impacted parties, their analysis, development of countermeasures and timely dissemination to all relevant stakeholders (such as through an ISAC). This approach allows for design of stronger preventive methods in future generations of electronics. As outlined earlier, automotive industry (through Alliance and Global Automakers) is actively exploring information sharing alternatives related to automotive cybersecurity and NHTSA is closely monitoring activities related to this initiative.

Comments requested

1) We seek comment on any technical areas of automotive cybersecurity that the agency could focus on in its further research.
    a) Specifically, are there particularly vulnerable or strong design architectures that the agency should further examine?

b) What additional types of techniques (either in real world occurrences or as a part of research) have persons used to gain unauthorized access to vehicle systems? What types of systems were such persons able to gain access to?

c) What is the public's view on the differences in cybersecurity risks associated with an intrusion that requires use of in-cab physical interfaces (e.g. OBD-II port) versus close-proximity wireless interfaces (e.g. Bluetooth) versus long-range wireless means (e.g. cellular/satellite links)?

2) We seek comment on security process standards.

a) What security process standard alternatives are available? How do these standards differ and are there standards that are more suitable for application to the automotive industry versus others?

b) Could security assurance be handled within a modified framework of existing safety process standards (such as FMEAs, FTAs, ISO 26262) or does "design for security" require its own process?

3) We seek comments on security performance standards. In contrast to the process standards (that establish methods for considering cybersecurity risks during product design), we use the term "performance standard" to mean standards that evaluate the cybersecurity performance (or resilience) of a system after production of the final product.

a) What types of metrics are available to test a vehicle's ability to withstand a cyber-attack?

b) Are there any common design characteristics that help ensure a minimum level of security from unauthorized access to a vehicle's electronic control systems?

c) What performance-based tests, methods, and processes are available for security assurance of automotive electronic control systems?

d) Are there hardware, software, watchdog algorithm, etc. requirements or criteria that would help differentiate algorithm designs that are more secure against cyber-attack?

c. Effects of the Surrounding Environment on Electronic Component Performance

In addition to malicious interference that may be artificially introduced (as covered under cybersecurity in section III.b.), the surrounding natural environment could affect the electronic components and systems in three primary ways:

1. By creating conditions that could cause electronic components to fail prematurely;
2. By creating conditions that could result in electronic control systems to act in unintended ways; and
3. By creating conditions for electronic sensors or systems to perceive the environment differently than reality.

Effects of the environment potentially causing electronic components to fail prematurely, such as through moisture, heat and corrosion, are typically handled by fail-safe strategies. Monitoring algorithms can detect sensors and components that fail and operate outside of the intended range and inform control algorithms to operate in fail-safe mode. Manufacturers take placement and environmental exposure into account in the design of electromechanical components.

Examples of the environment potentially causing electronic control systems to act in unintended ways are electromagnetic interference (EMI) and potential build-up of low-resistance paths on a circuit-board, such as a tin whisker.[36] OEMs very commonly perform electromagnetic compatibility (EMC) testing on their platforms in accordance with SAE International[37] and ISO[38] standards. NHTSA has investigated EMI effects on an electronic control system in a recent

[36] A crystalline, hair-like structure of tin that can form on a tin-finished surface. (taken from NAS Report)
[37] SAE J551, SAE J1113
[38] ISO 7637, ISO 10605, ISO 11451, ISO 11452

investigation. In 2010, NHTSA and National Aeronautics and Space Administration (NASA) conducted EMC testing as part of the inquiry into whether Unintended Acceleration (UA) was related to the electronic throttle control system in Toyota vehicles. In this study, EMC testing at exposure levels well above existing certification standards did not produce open throttle.[39]

Among the risks with EMI is for the electronic control unit's memory settings to be altered unintentionally. This could change the way the system behaves especially if the EMI's influence is not detected. Manufacturers utilize various methods to prevent unintended EMI influence, such as by retaining safety critical system parameters in more than one memory location (such that a random alteration could be detected and system shut down with warning). Formation of conductive tin whiskers on a circuit board could potentially result in low resistance paths and unintended system behavior, particularly if they cause a short between circuits resulting in unintended activation of an actuator. Most such issues result in electrical faults and safe shut-down of corresponding functions. Manufacturers use various techniques to mitigate the concern including changes to the manufacturing process, addition of elements like copper and nickel, and the use of surface coatings. Further, circuit board design takes into account the possibility of circuit-board shorts in trace placement.

Another possibility is for the environment to impact the advanced sensors (such as radar, lidar, cameras, GPS, etc.) on a contemporary vehicle in a way that could result in unintended engagement or non-operational status of system functions. To mitigate this risk, manufacturers utilize various forms of sensor fusion technologies to reduce reliance on any single sensor signal for safety-critical functions.

---

[39] "Technical Support to the National Highway Traffic Safety Administration (NHTSA) on the Reported Toyota Motor Corporation (TMC) Unintended Acceleration (UA) Investigation", 2011, NASA. Section 6.8 of this report discusses the EMC testing and the full report can be accessed at http://www.nhtsa.gov/staticfiles/nvs/pdf/NASA-UA_report.pdf.

Related to 5.9 GHz DSRC, NHTSA is initiating research into analyzing potential communication interference impacts of devices that operate on and in neighboring spectrums of the DSRC band[40]. NHTSA expects to complete this study in 2015.

Comments requested

1) NHTSA has reviewed the state-of-the art with respect to environmental conditions and vehicle electronics. What other ways can the environment impact electronic system performance other than the ways that we have considered, above?
2) NHTSA has done some testing on interference issues. We seek comment in the area of EMI/EMC.
    a) What could the agency do to further assess the electromagnetic interference (EMI) susceptibility impacts of growing use of electronics on automotive system safety and assess the adequacy of existing voluntary standards?
    b) Are there known EMI susceptibility differences in vehicles designed and sold in the U.S. versus in regions where EMC may be explicitly regulated?
3) We seek comment in the area of the environment's potential impact on advanced automotive sensors.
    a) Are any particular sensing technologies more susceptible or less susceptible to such effects (including EMC and other environmental effects such as moisture, corrosion, etc.)?

IV. Additional Comments Requested

In addition to the comments requested in regards to the specific topics discussed above, we are also seeking comment on other general issues relating to electronic component safety and

[40] DSRC band: 5.850 – 5.925 GHz.

cybersecurity.

1) One issue that we seek comment is the potential for voluntary safety process standards to help address challenges introduced by expanding use of electronics in automotive applications. In section II.d. above, we discuss the various design and quality control processes that the industry already uses to assess the safety and cybersecurity of their electronic components (e.g., ISO 26262).
    a) We seek public comment on the degree to which this type of safety process standard can provide an adequate level of protection from electronic component failures or potential cybersecurity breaches.
        i) What voluntary industry standards are best able to address safety assurance of electronics control system design for motor vehicles?
        ii) Specifically, what elements of the voluntary industry standards are best able to address electronics control systems and cybersecurity issues in motor vehicles?
        iii) What other standards than those described in this document are relevant for the agency to consider?
    b) What types of concerns with regard to electronic components safety and cybersecurity would <u>not</u> be addressed by voluntary safety process standards?
        i) What other standards are available that could address this type of safety concern?
        ii) What software development, validation and safety assurance methods and processes are suitable for safety critical automotive control systems?
    c) Are existing process standards such as ISO 26262, IEC 60812, IEC 61025, etc, suitable to address electronic control system design challenges for more advanced forms of vehicle automation?

2) Another issue that we seek comment on is in regards to the available information and data sources for identifying and understanding the issues related to electronic component reliability and cybersecurity. We recognize that much of the data available to the agency captures retrospective data. Thus, the traditional sources of information available to the agency have various limitations in this rapidly-developing area of automotive technology. Information that shows historic data on electronic component issues may not necessarily give an accurate prediction of what future electronic component reliability and cybersecurity issues can be. We seek comment on the data sources that are identified for potential consideration in the categorization of priority focus areas for electronics reliability.
    a) We are especially interested in identifying any potential data sources that could assist the agency in identifying potential emerging electronic component failures in vehicles in a timely manner.
    b) Has the agency considered all the relevant data on this subject? What additional sources of information could the agency consider?
3) We seek comment on what other information sources or strategies are available that can enhance the ability to detect potential electronics system related concerns in a timely fashion. What methods are available to improve traceability of potential electronic control system malfunctions?

V. Public Participation

How do I prepare and submit comments?

Your comments must be written and in English. To ensure that your comments are filed correctly in the docket, please include the docket number of this document in your comments.

Your comments must not be more than 15 pages long (49 CFR 553.21). NHTSA established this limit to encourage you to write your primary comments in a concise fashion.

However, you may attach necessary additional documents to your comments. There is no limit on the length of the attachments.

Please submit one copy (two copies if submitting by mail or hand delivery) of your comments, including the attachments, to the docket following the instructions given above under ADDRESSES. Please note, if you are submitting comments electronically as a PDF (Adobe) file, we ask that the documents submitted be scanned using an Optical Character Recognition (OCR) process, thus allowing the agency to search and copy certain portions of your submissions.

How do I submit confidential business information?

If you wish to submit any information under a claim of confidentiality, you should submit three copies of your complete submission, including the information you claim to be confidential business information, to the Office of the Chief Counsel, NHTSA, at the address given above under FOR FURTHER INFORMATION CONTACT. In addition, you may submit a copy (two copies if submitting by mail or hand delivery), from which you have deleted the claimed confidential business information, to the docket by one of the methods given above under ADDRESSES. When you send a comment containing information claimed to be confidential business information, you should include a cover letter setting forth the information specified in NHTSA's confidential business information regulation (49 CFR Part 512).

Will the agency consider late comments?

NHTSA will consider all comments received before the close of business on the comment closing date indicated above under DATES. To the extent possible, the agency will also consider comments received after that date.

How can I read the comments submitted by other people?

You may read the comments received at the address given above under COMMENTS. The hours of the docket are indicated above in the same location. You may also see the comments on the Internet, identified by the docket number at the heading of this notice, at http://www.regulations.gov.

Please note that, even after the comment closing date, NHTSA will continue to file relevant information in the docket as it becomes available. Further, some people may submit late comments. Accordingly, the agency recommends that you periodically check the docket for new material.

Anyone is able to search the electronic form of all comments received into any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). You may review DOT's complete Privacy Act Statement in the Federal Register published on April 11, 2000 (65 FR 19477-78) or you may visit http://www.dot.gov/privacy.html.

Authority: Sec. 31402, Pub. L. 112-141.

Issued in Washington, DC on _____ under authority delegated in 49 CFR part 1.95.

_____

Nathaniel Beuse
Associate Administrator for Vehicle Safety Research

[FR Doc. 2014-23805 Filed 10/06/2014 at 8:45 am; Publication Date: 10/07/2014]