BOSCH

July 29, 2019

Robert Bosch LLC
38000 Hills Tech Dr.
Farmington Hills, MI 48331
www.bosch.us

Michael Huntley
Division Chief, Vehicle & Roadside Operations
Office of Carrier, Driver, & Vehicle Safety
Federal Motor Carrier Safety Administration
US Department of Transportation
1200 New Jersey Avenue, S.E.
Washington, DC 20590

Re: Advanced Notice of Proposed Rulemaking - Safe Integration of Automated Driving Systems-Equipped Commercial Motor Vehicles
Docket No. FMCSA-2018-0037

Dear Mr. Huntley,

Robert Bosch LLC (Bosch) appreciates this opportunity to provide its perspective concerning FMCSA's examination of topics that require consideration in light of the emergence of Automated Driving Systems (ADS)-Equipped Commercial Motor Vehicles. Bosch applauds the Agency's ongoing efforts to stimulate dialogue with the industry and other relevant stakeholders. Bosch was grateful to participate in one of the public workshops convened by FMCSA in 2018 and believes that such events have helped to bring forth a better understanding of the benefits offered and challenges posed by Automated Driving Systems.

The topic of cybersecurity is tightly intertwined with the emergence of increasingly automated and connected vehicles and it is a priority for Bosch. Bosch has been working for several years to develop robust and comprehensive solutions for our customers. Bosch strongly supports a layered approach to vehicle cybersecurity, with a central gateway[1] serving as a critical component in the protection strategy for the vehicle. Please see Attachment A for a graphic explaining this approach. We have espoused this principle in the development of our own products and in our engagement with customers. Understanding the importance of industry cooperation and engagement in addressing potential threats and developing best practices, Bosch joined the Automotive Information Sharing and Analysis Center (Auto-ISAC) in 2016.

[1] A central gateway is defined in the Society of Automotive Engineers (SAE) J1939-31 Standard "Network Layer".

Bosch has welcomed the Department of Transportation's consistent focus on the importance of cybersecurity which has served, and continues to be, one of the key elements recommended for the Voluntary Safety Self Assessments outlined in the Department's Automated Vehicle Guidance 2.0 and Automated Vehicle Guidance 3.0. In reviewing the ANPRM, Bosch welcomed FMCSA's discussion of this critical topic and the statement that "FMCSA and NHTSA are focused on strong cybersecurity to ensure these systems work as intended and are built to mitigate safety and security risks" (page 24456).

Bosch strongly supports the NHTSA Cybersecurity Best Practices[2]. We would respectfully request that FMCSA closely examine the following sections of the document which we feel carry a strong relevance for commercial vehicles:
6.7 Fundamental Vehicle Cybersecurity Protections
6.7.7 Use Segmentation and Isolation techniques in Vehicle Architecture Design

Bosch also wishes to highlight the recent work done by NHTSA in the context of the December 2018 report Cybersecurity Research Considerations for Heavy Vehicles[3] Bosch views the Section 1.2 conclusions in the report to be of significant importance. Two excerpts are included below for reference:

- "MD/HD trucks applying J1939 appear slightly more vulnerable than automobiles with proprietary CAN architectures. In addition, MD/HD trucks are more vulnerable to attack because of the exposed trailer wiring and extensive use of third-party telematics solutions that are linked to the vehicle CAN."[4]
- "Increased cybersecurity risk is present in MD/HD trucks due to these vehicles employing similar fleet management and telematics technologies. This business practice increases scalability risk with respect to a potential vulnerability."[5]

---

[2] National Highway Traffic Safety Administration; Cybersecurity Best Practices for Modern Vehicles (2016, October); Report No. DOT HS 812 333.
[3] Stachowski, S., Bielawski, R., & Weimerskirch, A. (2018, December). Cybersecurity Research Considerations for Heavy Vehicles; Report No. DOT HS 812 636; Washington, DC: National Highway Traffic Safety Administration.
[4] Stachowski, S., Bielawski, R., & Weimerskirch, A. (2018, December). Cybersecurity Research Considerations for Heavy Vehicles; Report No. DOT HS 812 636; Washington, DC: National Highway Traffic Safety Administration.
[5] Stachowski, S., Bielawski, R., & Weimerskirch, A. (2018, December). Cybersecurity Research Considerations for Heavy Vehicles; Report No. DOT HS 812 636; Washington, DC: National Highway Traffic Safety Administration.

In alignment with the report issued by the Motor Carrier Safety Advisory Committee (MCSAC) on October 16, 2018, Bosch would like to echo the following recommendations:

- "FMCSA should require some minimal level of cybersecurity to prevent HACVs from being hacked and weaponized."[6]
- "FMCSA should require HACVs to record safety-critical events for operation on public roads." [7] Bosch would note that it may also be beneficial for such systems to have the ability to log cybersecurity-specific data.

Bosch notes that the MCSAC report also mentioned voluntary consensus standards. Bosch wishes to highlight a few current and emerging industry voluntary standards that we view as being fundamental to the overall discussion surrounding cybersecurity. They are listed below.

- SAE J1939-71 DA – Digital Annex: addition of Imposter PGN Alert (PGN 61839)
- SAE J1939-91 (not yet published) - cybersecurity recommendations for J1939
- SAE/ISO 21434 (when available/published – the standard is expected to be released at the end of 2019 or early 2020)

Closing:

Bosch appreciates the opportunity to respond to this notice. We look forward to continuing to work with FMCSA, the Department of Transportation and other important stakeholders to help bring ADS-equipped vehicles to the market and to help realize the significant benefits of this transformative technology.

We would be pleased to address any questions or to provide additional information on this topic. Please do not hesitate to contact Ana Meuwissen at 202/815-7645 or at Ana.Meuwissen@us.bosch.com with any inquiries.

Yours sincerely,

[6] Motor Carrier Safety Advisory Committee; MCSAC Task 17-1 Report (October 16, 2018).

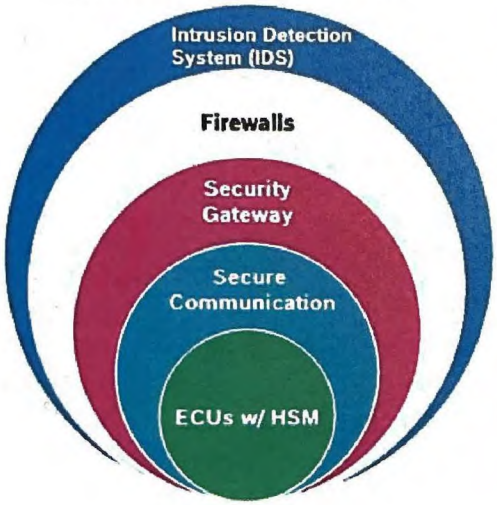
[7] Motor Carrier Safety Advisory Committee; MCSAC Task 17-1 Report (October 16, 2018).

David Sziraki
Vice President and Regional Business Unit Leader
Bosch Automotive Electronics
Robert Bosch LLC

Ana M. Meuwissen
Director, Federal Government Affairs
Robert Bosch LLC

Attachment A

Layered Security Approach



Solutions for CGW

- Intrusion Detection System
- On-Vehicle Firewall
  CAN, CAN-FD, Ethernet, Diagnostics
- **Security Gateway**: Domain separation, routing between domains/busses
- Not specified
- HSM (Hardware Security Module)
- Crypto Primitives
- Key management
- Secure Flashing
- Secure Boot
- Secure Storage
- Secure Diagnostics

CGW = Central Gateway