2023-01-0924 Published 11 Apr 2023

Using Ethernet or a Wireless Harness and Named Data Networking in Autonomous Tractor-Trailer Communication

Ahmed Elhadeedy and Jeremy Daily Colorado State University

Citation: Elhadeedy, A. and Daily, J., "Using Ethernet or a Wireless Harness and Named Data Networking in Autonomous Tractor-Trailer Communication," SAE Technical Paper 2023-01-0924, 2023, doi:10.4271/2023-01-0924.

Received: 15 Nov 2022 Revised: 29 Jan 2023 Accepted: 01 Feb 2023

Abstract

Autonomous truck and trailer configurations face challenges when operating in reverse due to the lack of sensing on the trailer. It is anticipated that sensor packages will be installed on existing trailers to extend autonomous operations while operating in reverse in uncontrolled environments, like a customer's loading dock. Power Line Communication (PLC) between the trailer and the tractor cannot support high bandwidth and low latency communication. This paper explores the impact of using Ethernet or a wireless medium for commercial trailer-tractor communication on the lifecycle and operation of trailer electronic control units (ECUs) from a Systems Engineering perspective to address system requirements, integration, and security. Additionally, content-based and host-based networking approaches for in-vehicle communication, such as Named Data Networking (NDN) and IP-based networking are compared. Implementation, testing and evaluation of prototype trailer ECU communication with the tractor ECUs over Ethernet is shown by transmitting different data types simultaneously. The implementation is tested with two networking approaches, Named Data Networking, and Data Distribution Service (DDS) and the test indicated that NDN over TCP is an efficient approach that is capable of meeting automotive communication requirements. Using Ethernet or a wireless harness and NDN for commercial trailer Anti-Lock Braking System (ABS) ECU provides adequate resources for the operation of autonomous trucks and the expansion of its capabilities, and at the same time significantly reduces the complexities compared to when new features are added to legacy communication systems. Using a wireless medium for tractor-trailer communication will bring new cybersecurity challenges and requirements which requires new development and lifecycle considerations.

Introduction

Level 4 and 5 [1] autonomous trucks (AT) are designed to travel long distances without a human driver and the AT is subject to be in situations where it needs to drive in reverse, whether it is a maneuver on a public road or needs to park the trailer in delivery or pickup yards without human intervention. Autonomy sensors are currently being placed on the tractor itself and no sensors being placed on the trailer facing backward which makes autonomous driving in reverse a challenge. Some researchers have addressed autonomous truck reverse driving from an algorithm or vehicle control prospective [2, 3] but not from an ECU integration or systems engineering and the impact it would have on the lifecycle.

Truck native communication protocol between the trailer and the tractor such as Power Line Carrier (PLC) has a limited bitrate of $10kB/s$ which makes it unsuitable for autonomy applications, so adding autonomy sensors (e.g., LiDAR, camera or ultrasonic sensors) to the back of the trailer would require an additional trailer ECU for signal processing and communication with the network of the AT, which means having two separate ECUs on the trailer, the native and the newly added ECU. Additionally, AT L4/and L5 autonomy brings its own communication network, such as Ethernet and CAN FD channels on top of the native tractor network channels such as J1939, PLC or ISO11992, so integrating a second trailer ECU with all of the new and native communication channels will be complex.

In this paper, we will discuss vehicle intra-communication related literature and the impact of using Ethernet or a wireless harness and Named Data Networking (NDN) on the different aspects of the trailer ECU from a systems engineering prospective such as the impact on requirements, and security. A comparison between Named Data Networking, and IP-based Data Distribution Service (DDS) is included, in addition, to a test and evaluation of each approach when transferring multiple data types from one device to three other devices.

Related Literature

In this section, we discuss the related art in vehicle networks and ECU communication architecture, such as Wireless Sensor Networks, Wireless Harness and Wireless CAN, Automotive Protocol Conversion or Replacement with Ethernet, Named Data Networking (NDN) and Tractor-Trailer Communication.

A. Wireless Sensor Network The concept of wireless sensors network is primarily focused on using a wireless medium to transfer the data from the sensors to an ECU. The ECU itself is wired to the vehicle network and follows the traditional automotive architecture.

Parthasarathy et al. conducted an experiment to evaluate the performance of short-range IEEE 802.15.4-based wireless network on a heavy vehicle between the TPMS sensors and a main and an additional gateway ECUs [4]. Lin et al. evaluated the performance of wireless sensor network under Wi-Fi and Bluetooth interference where the sensors are wirelessly communicating with base stations that are hardwired to the ECU [5]. Potdar and Suyog proposed a zone-based wireless sensor network where ECUs are wired to a gateway that communicates wirelessly with different nodes or sensors [6]. Shaer et al. presented the concept of a wireless blind spot detection and embedded microcontroller using XBee DigiMesh [7].

B. Wireless Harness and Wireless Controller Area Network The wireless harness concept is focused on replacing the wiring of in-vehicle ECU with a wireless medium such as Bluetooth, Wi-Fi, Ultra-Wideband (UWB) and the automotive 60GHz millimeter-wave. The primary focus is on the measurements, characterization of the wireless signal and the impact of different noise factors on the delay between a transmitter and receiver for in-vehicle communication. The existing art does not cover a wireless communication between the trailer and the tractor. Takayama and Kajiwara evaluated the performance of in-vehicle ECU-to-ECU mesh-networking using UWB-IR for various antenna locations [8] and suggested using ceiling reflection for millimeter-wave wireless harness between two ECUs [9]. Similar studies were conducted on ZigBee [10], IEEE 802.11ad [11] and IEEE 802.15.1 [12] for *in-vehicle* communication with positive results in the presence of interference.

Reddy et al. validated the concept of wireless CAN to Bluetooth gateway to enable wireless CAN transmission from an ECU to a CAN bus [13]. Lun Ng et al. presented the Wireless Controller Area Network (WCAN) using the Token Frame Scheme [14] where the ECUs are connected using a token ring topology and communicating using the CAN principles, however, the proposed solution is different from the standard automotive CAN specifications.

C. Automotive Protocol Conversion or Replacement with IP-Based Protocol and Ethernet The focus of the Ethernet-related literature is on replacing automotive protocols with Ethernet and Internet Protocol (IP) and on converting automotive protocols from and to Ethernet, where a single protocol will be wrapped in an Ethernet frame (e.g., CAN bus messages or FlexRay) but does not cover supporting heterogeneous automotive protocols in addition to sensors data over ethernet simultaneously for autonomous tractor trailer application.

Zuo et al. evaluated the concept of CAN/CANFD conversion and transmission to Scalable service-Oriented MiddlewarE over IP (SOME/IP) using a gateway that communicates with another ECU via an ethernet link [15]. The concept doesn't enable the ECU to communicate with the main vehicle bus but to another ADAS ECU and does not take other data formats and protocols into account. Nichiţelea and Unguritu proposed using a different Electric and Electronic architecture that is completely based on automotive Ethernet using SOME/IP [16]. Data Distribution Service (DDS) was also proposed for Automotive Software Architectures using IP [17]. Postolache et al. presented an implementation and testing of packing multiple CAN frames in an Ethernet frame using a CAN-Ethernet gateway [18]. Lee et al. also presented a design of a FlexRay/Ethernet Gateway to pack FlexRay messages in Ethernet packets [19]. Kim et al. proposed a gateway framework that supports message routing between two protocols, such as routing and converting messages from CAN to FlexRay or Ethernet. In addition, the gateway is capable of routing of Diagnostics over IP (DoIP) messages to Unified Diagnostic Services (UDS) on CAN or FlexRay, the message translation to another protocol is happening inside the gateway itself using pre-defined routing and translation tables using Automotive open system architecture (AUTOSAR) [20]. Ashjaei et al. addressed and presented an overview of Time-Sensitive Networking (TSN) in automotive applications [21] which includes current and future trends in vehicle networks such as Domain Controller Unit (DCU) that replaces legacy gateways with automotive Ethernet as a backbone for the vehicle network architecture [22, 23, 24]. Audio Video Transport Protocol (AVTP) is used to wrap automotive protocols frames or IEC 61883-compliant multimedia in IEEE 1722 Ethernet frames. This method requires the type of data that will be wrapped in the Ethernet frame to be the same in the Ethernet frame such as all CAN messages, all FlexRay or all IEC 61883-4 (i.e., MPEG2-TS Video) data [25, 26, 27, 28].

Some literature suggests replacing automotive protocols and architectures such as CAN or FlexRay with a completely different topology or networking protocol (i.e., all Ethernet) such as [21, 22, 23]. Kraus et al. proposed the replacement of automotive CAN with optical data communication using an optical bus and central processing unit that manages and monitors all the connected devices using Stream Control Transmission Protocol (SCTP) [29]. Nichiţelea and Unguritu proposed replacing standard serial protocols (i.e., CAN, FlexRay and LIN) with ethernet [30] using SOME/IP [31].

D. Named Data Networking (NDN) Automotive NDN literature is mainly focused on the connected vehicles and Vehicle-to-Everything (V2X) communication [32, 33, 34, 35, 36, 37] and there is a limited number of papers that addresses using NDN in intra-vehicle communication and the integration with existing automotive protocols. Papadopoulos et al. presented the concept of using NDN for in-vehicle communication with ECU experimentation as a future step suggesting that NDN is a better network approach

[38] and in [39], they presented Name-based secure communication architecture for in-vehicle communication suggesting that NDN is an improved IP alternative. Threet et al. demonstrated secure CAN communication using NDN between two Raspberry Pis with average latency for CAN Interest and Data packets of 73 milliseconds [40]. Some researchers have shown that NDN-based networks have better latency performance than IP-based networks [41] using ndnSIM to simulate internet network that connects multiple cities. The existing art was a motive for us to evaluate the performance of NDN when used in the context of autonomous vehicles with multiple ECUs intra-communicating with CAN and two sensors' data as shown in the test and evaluation section later in this paper.

E. Security and Tractor-Trailer Communication The existing art covers the topic of autonomous trucks driving in-reverse from an algorithm and controls perspective [42, 43] but not from a trailer ECU architecture, integration, or systems-thinking point of view. Non-Autonomous Tractor communication art includes different solutions such as combining CANopen and J1939 networks [44], and securing and encrypting the J1939 and diagnostics traffic on the tractor side as Daily et al. presented in [45, 46]. Power Line Carrier (PLC) is being used as a low-speed communication bus between the trailer and the tractor which is not suitable for AT applications due to the bitrate limitation in PLC, where the preamble bitrate is 8772 bits per second and the data body bitrate is 10,000 bits per second [47]. Recent research has shown that PLC communication is vulnerable to hacking and missing authentication on some critical functions as disclosed by National Motor Freight Traffic Association, Inc. (NMFTA) [48, 49] with countermeasures proposed. Additional autonomous and Heavy-duty Vehicles security vulnerabilities are discussed in [50, 51, 52, 53]. Goers and Kühne presented transmitting CAN and sensors data over automotive Ethernet to the truck Advanced Driver-Assistance System (ADAS) ECU [54]. Their long-term proposed solution is for the trailer ABS to have an Ethernet switch, Microcontroller Unit (MCU), ISO 11992 CAN and a multiplexer that communicates with the tractor over a coiled cable. Extending the ISO 11992 standard to include an additional physical layer such as Ethernet was also mentioned. Technology and Maintenance Council (TMC) presented the need for an automated tractor-trailer coupling process and the need for a higher data transmission speed between the trailer and the tractor [55]. They also mentioned controlling the trailer lights (e.g., stop light and turn signals) can be controlled over CAN instead of using separate electrical conductors.

Architecture

On the basis of the above reflections on the state of the field, we can understand that there is a need for a systems-thinking based solution that addresses the following gaps in the existing art:

1. Using the content-centric NDN protocol as a network protocol instead of the traditional host-centric IP for intra-communication, between the trailer ECU and the tractor.
2. Test, evaluation, and empirical data of NDN when used for autonomous vehicles intra-communication over Ethernet or a wireless medium.
3. Using a wireless medium as the only communication link between the trailer and the tractor and the impact on the lifecycle.
4. Upgrade of the trailer ABS architecture to meet the needs of L4/L5 ATs and adding Telematics, lights control and GPS to the trailer ABS ECU instead of having a separate ECUs or hardware module.

Ethernet-Based Trailer ABS

Similar to the solution presented in [54], we propose an enhanced architecture for the trailer ABS ECU to better fit the needs of the conventional trucks and SAE level 4 and 5 Autonomous Tractor and to combine all of the existing trailer features in one ECU instead of having separate hardware modules such as telematics and GPS. SAE Level 4 and 5 autonomy will bring additional communication buses to the tractor to meet timing and bandwidth requirements such as adding CAN FD and Ethernet on top of tractor platform and the trailer ECU is expected to communicate with the AT over these channels since it will be part of the autonomy hardware feeding sensors data to the self-driving software. Retrofitting an additional new trailer ECU will be complex and result in a big harness as shown in Figure 1. The proposed new trailer ABS architecture differs from the existing art as follows: adding telematics and GPS within the ABS, replacing the MCU with a SoC, removing the physical CAN from the trailer ECU, using a multi-Gig Ethernet, and adding several interfaces to the MCU at the tractor side as shown in Figure 1.

FIGURE 1 (Left) Retrofitting an autonomy ECU in the trailer to process rear sensors to accommodate level 4 and 5 autonomy needs. (Right) Proposed upgraded trailer ABS architecture that integrates with the existing autonomous tractor architecture.

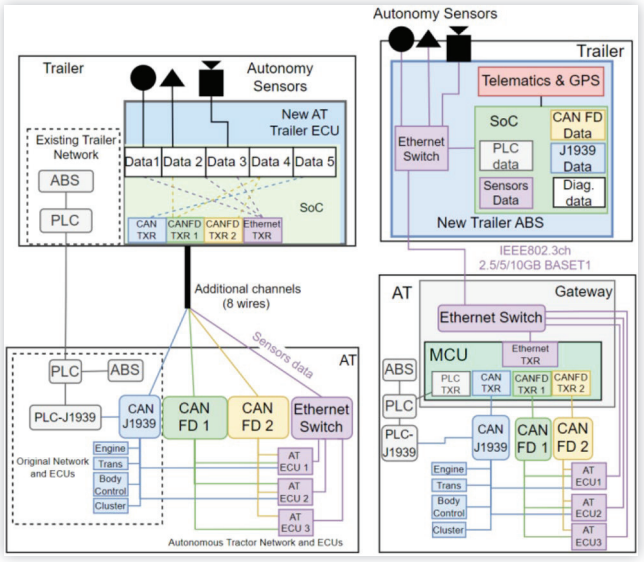
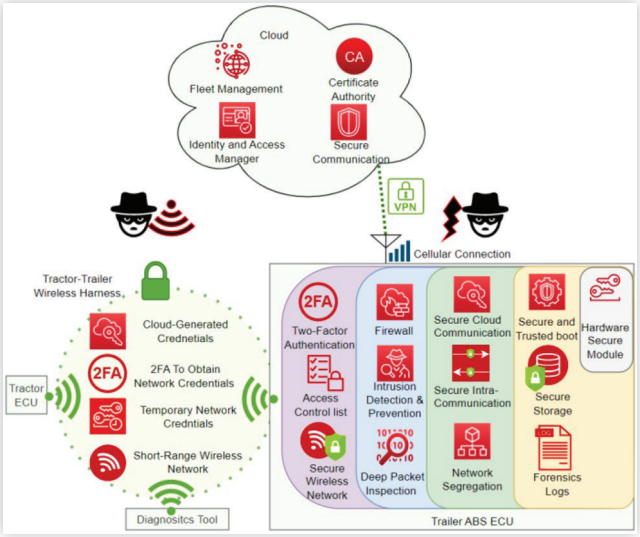


FIGURE 15 A Multi-layer security concept for the new trailer ABS ECU and the tractor ECU



in a message over Rich Communication Services (RCS) from the cloud to each ECU as shown in Figure 14. After the two ECUs are authenticated by the cloud over the VPN, for example, the cloud could send a code number to each ECU using a new different channel such as RCS which uses IP and encryption. When each ECU receive their OTP, they will send it again to the cloud over the VPN. Both of GPS and OTP could be used as part of a Multi-factor Authentication (MFA) process.

Impact on the ECUs Lifecycle The AT and the trailer ECUs will be subject to new attack vectors due to the use of new interfaces and features such as Ethernet or wireless harness and cellular connection which will have an impact on the lifecycle and requires new design considerations. Based on the proposed changes to the trailer ABS and as suggested by [50], NHTSA [51], SAE J3101 [61], and SAE J3061 [62] new design consideration, development and lifecycle process are needed for the trailer ECU, especially when it comes to security such as following Security Development Lifecycle (SDL). Figure 15 shows a multi-layer cybersecurity concept to protect against the new attacks on the ECU.

Table 7 shows the impact on the lifecycle of the ECU and the new activities that needs to be taken into consideration.

Identity And Access Management FMS will be responsible for access control of the wireless harness network where it regulates the level of access for each Wi-Fi credentials. FMS will be able to add and update the access control list (ACL) in each ECU to define the users and groups for each entity connecting to the wireless harness networking using the provided credentials. For example, doing diagnostics over the wireless harness will be possible for both AT and the trailer using DoIP and the Wi-Fi connection credentials for a technician with a diagnostic tool will have a different access level compared to the ECU pairing credentials. In both cases, credentials are managed and generated by FMS and stored and updated regularly within the ECU.

Summary/Conclusions

For SAE level 4 and 5 autonomous tractors to drive in reverse, it needs additional autonomy sensors on the back of the trailer and current trailer ABS ECU cannot support autonomous tractor networking or have autonomy sensors connected due to the limitation in the computation, networking and architecture. We proposed a new trailer ABS ECU architecture that contain all of the existing features such as telematics, lights and GPS and uses automotive Ethernet or a wireless harness as the only communication link with the autonomous tractor in addition to using Named Data Networking. NDN is a new and promising networking architecture that could be standardized in the automotive industry to reduce complexity and have security by default in the data and interest packets. We discussed NDN and evaluated it against Data Distribution Service (DDS) and the experiment had positive results. The test shows the NDN over TCP is an efficient protocol that is capable of meeting automotive communication requirements. We presented an automated tractor-trailer pairing method in addition to the security measures to authenticate each of them before pairing, in addition to the impact on different aspects of the lifecycle. Using Ethernet or a wireless harness and NDN for commercial trailer ABS ECU provides adequate resources for the operation of autonomous trucks and the expansion of its capabilities, and at the same time significantly reduces the complexities compared to when new features are added to legacy communication systems. Future work will include the networking and security specification for Named Data Networking when used between the trailer and the tractor and test and evaluation of the proposed system using twisted-pair automotive Ethernet and automotive ECUs and evaluation of the wireless harness concept.

TABLE 6 Summary of PC (the transmitter) CPU consumption percentage for per script per each protocol

Mean CPU %	DDS	NDN over UDP	NDN over TCP	NDN over UDP (Bytes)	NDN over TCP (Bytes)
Lidar script	50.7%	44.4%	44.6%	33.6%	32.8%
CAN script	3.7%	8.8%	8.6%	12.3%	11.6%
Cam script	15.2%	20.8%	20.9%	5.9%	5.6%
NFD	-	4.4%	5.8%	8.3%	13.1%

TABLE 7 Main impact of the new features and interfaces on the trailer ABS lifecycle phases and technical processes per the V-model and INCOSE [63]

Technical Process	Phase Impact
System Requirements Definition	• ABS Hardware and software security and performance requirements • Security requirements for the new communication channels (e.g., in-vehicle and cloud), hardware and software such as authorization, authentication, and data integrity and confidentiality. • Wireless connections requirements such as the wireless harness and the cellular connection performance and bandwidth • Design and cybersecurity risk assessment of adding Wi-Fi and cellular to the ABS. • Distributed development in the case of the tractor and the trailer from two different OEMs. • Requirements from different stakeholders (tractor and trailer OEMs)
System Design	• Design and security specification and the architecture of the new system including deployment, software, hardware, and cloud architecture. • System analysis including cost, technical risks, and effectiveness analysis • Cybersecurity analysis to configure the proper cybersecurity level for the system • Safety and cybersecurity by design
Implementation and Integration	• Secure hardware and software implementation • Integration, configuration, and testing of software and hardware components • Secure IT infrastructure • New procedures and training
Verification, Validation and Testing	• Scanning for vulnerabilities in the software and the hardware • Reverse Engineering, Fuzzing, and penetration testing • Conformance testing of the security functions and implementation • Testing of the wireless harness under different conditions including end-to-end data gatewaying • Features and cybersecurity integration testing • Software and hardware integration testing
Production, Operation, Maintenance and Updates	• Refined security assessment • Personnel Training and cybersecurity culture • Diagnostics over the wireless harness and the impact on the tools and protocols used. • Software updates process such as Over-the-air or over-the-wireless-harness updates • Fleet monitoring for security incidents and incident response • Pairing credentials handling and management
Disposal	• Disposal procedure and strategy • Secure disposal of the system and the data it contains

References

1. SAE International, "Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles," no. J3016_202104.
2. Nyberg, P., "Stabilization, Sensor Fusion and Path Following for Autonomous Reversing of a Full-scale Truck and Trailer System," Linköping University, 2016.
3. Josef, V., "Trailer Parking Assistant," in *Proceedings of the 16th International Conference on Mechatronics - Mechatronika 2014*, 2014.
4. Parthasarathy, D., Whiton, R., Hagerskans, J., and Gustafsson, T., "An In-Vehicle Wireless Sensor Network for Heavy Vehicles," in *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*, 1-8, 2016.
5. Lin, J.-R., Talty, T., and Tonguz, O.K., "An Empirical Performance Study of Intra-Vehicular Wireless Sensor Networks under WiFi and Bluetooth Interference," in *2013 IEEE Global Communications Conference (GLOBECOM)*, 581-586, 2013.
6. Potdar, M. and Wani, S., "Wireless Sensor Network in Vehicles," SAE Technical Paper 2015-01-0241, 2015, https://doi.org/2015-01-0241.
7. Shaer, B., Marcum, D.L., Becker, C., Gressett, G. et al., "Wireless Blind Spot Detection and Embedded Microcontroller," *Advances in Security, Networks, and Internet of Things* (2021): 717-730.
8. Kajiwara, I.T.a.A., "Intra-Vehicle Wireless Harness with Mesh-Networking," in *2016 IEEE-APS Topical Conference on Antennas and Propagation in Wireless Communications (APWC)*, 146-149, 2016.
9. Yamada, R. and Kajiwara, A., "Automotive Millimeter-Wave," *IEICE Communications Express* 1 (2021): 1-6.
10. Reddy, A.D.G., "Simulation Studies on ZigBee Network for In-Vehicle Wireless Communications," in *2014 International Conference on Computer Communication and Informatics*, 1-6, 2014.
11. Nino, R., Nishio, T. and Murase, T., "IEEE 802.11ad Communication Quality Measurement in In-vehicle Wireless Communication with Real Machines," in *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 0700-0706, 2020.

12. Akingbehin, K., "Hybrid Wireless Harness for Low Mass Vehicular Applications," in *2012 21st International Conference on Computer Communications and Networks (ICCCN)*, 1-5, 2012.
13. Reddy, A., Dhadyalla, G., and Kumari, N., "Experimental Validation of CAN to Bluetooth Gateway for In-Vehicle Wireless Networks," in *2013 International Conference on Emerging Trends in Communication, Control, Signal Processing and Computing Applications (C2SPCA)*, 1-5, 2013.
14. Ng, W.L., Ng, C.K., Noordin, N.K., and Ali, B.M., "Performance Analysis of Wireless Control Area Network (WCAN) Using Token Frame Scheme," in *2012 Third International Conference on Intelligent Systems Modelling and Simulation*, 695-699, 2012.
15. Zuo, Z., Yang, S., Ma, B., Zou, B. et al., "Design of a CANFD to SOME/IP Gateway Considering Security for In-Vehicle Networks," *Sensors* (2021): 23.
16. Nichiţelea, T.-C. and Unguritu, M.-G., "Automotive Ethernet Applications Using Scalable Service-Oriented Middleware over IP: Service Discovery," in *2019 24th International Conference on Methods and Models in Automation and Robotics (MMAR)*, 576-581, 2019.
17. Kugele, S., Hettler, D., and Peter, J., "Data-Centric Communication and Containerization for Future Automotive Software Architectures," in *2018 IEEE International Conference on Software Architecture (ICSA)*, 65-6509, 2018.
18. Postolache, M., Neamtu, G., and Trofin, S.D., "CAN - Ethernet Gateway for Automotive Applications," in *2013 17th International Conference on System Theory, Control and Computing (ICSTCC)*, 422-427, 2013.
19. Lee, T.-Y., Lin, I.-A., and Liao, R.-H., "Design of a FlexRay/ Ethernet Gateway and Security Mechanism for In-Vehicle Networks," *Sensors* (2020): 641.
20. Kim, J.H., Seo, S.-H., Hai, N.-T., Cheon, B.M. et al., "Gateway Framework for In-Vehicle Networks Based on CAN, FlexRay, and Ethernet," *IEEE Transactions on Vehicular Technology* 64, no. 10 (2015): 4472-4486.
21. Ashjaei, M., Lo Bello, L., Daneshtalab, M., Patti, G. et al., "Time-Sensitive Networking in Automotive Embedded Systems: State of the Art and Research Opportunities," *Journal of Systems Architecture* 117 (2021).
22. Xie, G., Li, Y., Han, Y., Xie, Y. et al., "Recent Advances and Future Trends for Automotive Functional Safety Design Methodologies," *IEEE Transactions on Industrial Informatics* 16 (2020): 5629-5642.
23. Zinner, H., Brand, J., and Hopf, D., "Automotive E/E Architecture Evolution and the Impact on the Network," March 2019. [Online]. Available: https://ieee802.org/1/files/public/docs2019/dg-zinner-automotive-architecture-evolution-0319-v02.pdf.
24. Alparslan, O., Arakawa, S., and Murata, M., "Next Generation Intra-Vehicle Backbone Network Architectures," in *2021 IEEE 22nd International Conference on High Performance Switching and Routing (HPSR)*, 1-7, 2021.
25. Mihalache, R., "Automotive Gateways (Bridge & Gateway from FlexRay/CAN/LIN to AVB Networks)," 2014. [Online]. Available: https://avnu.org/wp-content/uploads/2014/05/AVnu-AAA2C_Automotive-Gateways_Bridge-Gateway-from-FlexRayCANLIN-to-AVB-Networks_Razvan-Mihalache.pdf.
26. Olsen, D., "Audio Video Transport Protocol (AVTP)," 2014. [Online]. Available: https://avnu.org/wp-content/uploads/2014/05/AVnu-AAA2C_Audio-Video-Transport-Protocol-AVTP_Dave-Olsen.pdf.
27. "IEEE Standard for a Transport Protocol for Time-Sensitive Applications in Bridged Local Area Networks," IEEE 1722-2016, 2016.
28. Carlson, B., "The Rise and Evolution of Gateways and Vehicle Network Processing," June 2019. [Online]. Available: https://www.nxp.com/docs/en/training-reference-material/THE-RISE-AND-EVOLUTION-OF-GATEWAYS-AND-VEHICLE-NETWORK-PROCESSING.pdf.
29. Kraus, D., Leitgeb, E., Plank, T. and Löschnigg, M., "Replacement of the Controller Area Network (CAN) Protocol for Future Automotive Bus System Solutions by Substitution via Optical Networks," in *2016 18th International Conference on Transparent Optical Networks (ICTON)*, 1-8, 2016.
30. Nichiţelea, T.-C. and Unguritu, M.-G., "Automotive Ethernet Applications Using Scalable Service-Oriented Middleware over IP: Service Discovery," in *2019 24th International Conference on Methods and Models in Automation and Robotics (MMAR)*, 576-581, 2019.
31. AUTOSAR, "Example for a Serialization Protocol (SOME/IP)," [Online]. Available: https://some-ip.com/papers/cache/AUTOSAR_TR_SomeIpExample_4.2.1.pdf.
32. Rawat, D.B., Doku, R., Adebayo, A., Bajracharya, C. et al., "Blockchain Enabled Named Data Networking for Secure Vehicle-to-Everything Communications," *IEEE Network* 34, no. 5 (2020): 185-189.
33. Hou, R., Zhou, S., Cui, M., Zhou, L. et al., "Data Forwarding Scheme for Vehicle Tracking in Named Data Networking," *IEEE Transactions on Vehicular Technology* 70, no. 7 (2021): 6684-6695.
34. Saxena, D., Raychoudhury, V., Suri, N., Becker, C. et al., "Named Data Networking: A survey," *Computer Science Review* (2016): 15-55.
35. Kerrche, C.A., Ahmad, F., Elhoseny, M., Adnane, A., Ahmad, Z., and Nour, B., "Internet of Vehicles over Named Data Networking: Current Status and Future Challenges," in *Emerging Technologies for Connected Internet of Vehicles and Intelligent Transportation System Networks*, 2019.
36. Chen, M., Mau, D.O., Zhang, Y., Taleb, T. et al., "VENDNET: VEhicular Named Data NETwork," *Vehicular Communications* 1, no. 4 (2014): 208-213.
37. Wang, A., Chen, T., Chen, H., Ji, X. et al., "NDNVIC: Named Data Networking for Vehicle Infrastructure Cooperation," *IEEE Access* 7 (2019): 62231-62239.
38. Papadopoulos, C., Shannigrahi, S., and Afanaseyv, A., "In-Vehicle Networking with NDN," in *Proceedings of the 8th ACM Conference on Information-Centric Networking*, 127-129, 2021.
39. Papadopoulos, C., Afanasyev, A., and Shannigrahi, S., "A Name-Based Secure Communications Architecture for Vehicular Networks," in *2021 IEEE Vehicular Networking Conference (VNC)*, 178-181, 2021.
40. Threet, Z., Papadopoulos, C., Poddar, P., Afanasyev, A., William Lambert, H.B., Ghafoor, S., and Shannigrahi, S., "Demo: In-Vehicle Communication Using Named," in *Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2022*, 2022.

41. Syambas, N.R., Tatimma, H., Mustafa, A., and Pratama, F., "Performance Comparison of Named Data and IP-Based Network—Case Study on the Indonesia Higher Education Network," *Journal of Communications* 13, no. 10 (2018).
42. Nyberg, P., "Stabilization, Sensor Fusion and Path Following for Autonomous Reversing of a Full-scale Truck and Trailer System," 2016.
43. Josef, V., "Trailer Parking Assistant," in *Proceedings of the 16th International Conference on Mechatronics - Mechatronika 2014*, 677-682, 2014.
44. Koppe, U., "Combining CANopen and SAE J1939 Networks," in *1st international Mobile Machine Control (MMC)*, 7-11, 2013.
45. Daily, J.S. and Kulkarni, P., "Secure Heavy Vehicle Diagnostics," in *2020 NDIA Ground Vehicle Systems Engineering and Technology*, 2020.
46. Daily, J., Nnaji, D., and Ettlinger, B., "Securing CAN Traffic on J1939 Networks," in *Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2021*, 2021.
47. J2497 JUL2012, "Power Line Carrier Communications for Commercial, Surface Vehicle Recommended Practice," SAE International, Truck and Bus Low Speed Communication Network Committee, 2012.
48. Gardiner, B., "NMFTA Letter - Disclosure of Confirmed Remote Write," March 3, 2022. [Online]. Available: http://www.nmfta.org/documents/ctsrp/Disclosure_of_Confirmed_Remote_Write_v4_DIST.pdf?v=1.
49. Gardiner, B., "PowerLine Truck Hacking 2TOOLS4PLC4TRUCKS," DEF CON Safe Mode ICS Village, 2020.
50. Wolf, M. and Lambert, R., "Hacking Trucks - Cybersecurity Risks and Effective Cybersecurity Protection for Heavy Duty Vehicles," Dencker, P., Klenk, H., Keller, H.B. and Plödererder, E. (Hrsg.), in *Automotive - Safety & Security 2017 - Sicherheit und Zuverlässigkeit für automobile Informationstechnik*, 45-60, 2017.
51. Stachowski, S., Bielawski, R. and Weimerskirch, A., "Cybersecurity Research Considerations for Heavy Vehicles," in *National Highway Traffic Safety Administration*, Report No. DOT HS 812 636, 2018.
52. Gao, C., Wang, G., Shi, W., Wang, Z. et al., "Autonomous Driving Security: State of the Art and Challenges," *IEEE Internet of Things Journal* 9, no. 10 (2022).
53. Dadam S.R., Zhu D., Ravi V.K.a.V. and Palukuru V.S.S., "Onboard Cybersecurity Diagnostic System for Connected Vehicles," SAE International, 2021.
54. Goers, A. and Kühne, S., "CAN over Automotive Ethernet for Trailer Interface," Bertram, T. (eds) in *Fahrerassistenzsysteme 2018. Proceedings*, 2019.
55. Force, Future Chassis & Brake Systems Task, "Recommendations Regarding Future TractorTrailer Coupling Technology," in *Technology & Maintenance Council's (TMC)*, 2021.
56. Zhang, L., Claffy, K., Crowley, P., Papadopoulos, C. et al., "Named Data Networking," *ACM SIGCOMM Computer Communication Review* 44, no. 3 (2014).
57. NFD Team, "NFD Developer's Guide," August 2021. [Online]. Available: https://named-data.net/wp-content/uploads/2021/07/ndn-0021-11-nfd-guide.pdf.
58. Zhang, Z., Yu, Y., Zhang, H., Newberry, E. et al., "An Overview of Security Support in Named Data Networking," *IEEE Communications Magazine* (2018).
59. "An NDN Client Library with AsyncIO Support in Python 3." [Online]. Available: https://github.com/named-data/python-ndn.
60. Real-Time Innovations (RTI), "RTI Connector for Python." [Online]. Available: https://github.com/rticommunity/rticonnextdds-connector-py.
61. SAE International, "Hardware Protected Security for Ground Vehicles," no. J3101, February 2020.
62. SAE International, "J3061® Cybersecurity Guidebook for Cyber-Physical Vehicle Systems," JAN2016.
63. Walden, D.D., Roedler, G.J., Forsberg, K.J., Hamelin, R.D. et al., *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*, 4th ed. (2015)

Contact Information

Ahmed Elhadeedy
aelhadee@gmail.com

Jeremy Daily
Jeremy.Daily@colostate.edu

Definitions/Abbreviations

AT - Autonomous Tractor or Truck
ECU - Electronic Control Unit
NDN - Named Data Networking
NFD - Named Data Networking Forwarding Daemon
DDS - Data Distribution Service
CAN - Controller Area Network
CAN FD - Controller Area Network Flexible Data
SoC - System-on-Chip
MCU - Microcontroller
TCP - Transmission Control Protocol
UDP - User Datagram Protocol
RTPS - Real-Time Publish Subscribe protocol
ACK - Acknowledgement
ABS - Anti-Lock Braking System
GPS - Global Positioning System
CPU - Central Processing Unit
PLC - Power Line Carrier
AVB - Audio Video Bridging
TSN - Time-Sensitive Networking
SOME/IP - Scalable service-Oriented MiddlewarE over IP
ADAS - Advanced Driver-Assistance System
UWB - Ultra-wideband
DoIP - Diagnostics over IP
UDS - Unified Diagnostic Services
AUTOSAR - Automotive open system architecture
DCU - Domain Controller Unit
NMFTA - National Motor Freight Traffic Association, Inc.
RCS - Rich Communication Service
OTP - One-Time Passcode
ACL - Access Control List

FMS - Fleet Management System
SAE - Society of Automotive Engineers
VPN - Virtual Private Network
NHTSA - National Highway Traffic Safety Administration
SDL - Security Development Lifecycle
CSR - Certificate Signing Request

ISSN 0148-7191