DISSERTATION

# AUTONOMOUS TRUCKS AS A SCALABLE SYSTEM OF SYSTEMS: DEVELOPMENT, CONSTITUENT SYSTEMS COMMUNICATION PROTOCOLS AND CYBERSECURITY

Submitted by

Ahmed Elhadeedy

Department of Systems Engineering

In partial fulfillment of the requirements

For the Degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Spring 2024

Doctoral Committee:

Advisor: Jeremy Daily

Edwin Chong
Christos Papadopoulos
Jie Luo

ABSTRACT

AUTONOMOUS TRUCKS AS A SCALABLE SYSTEM OF SYSTEMS: DEVELOPMENT, CONSTITUENT SYSTEMS COMMUNICATION PROTOCOLS AND CYBERSECURITY

Driverless vehicles are complex to develop due to the number of systems required for safe and secure autonomous operation. Autonomous vehicles embody the definition of a system of systems as they incorporate several systems to enable functions like perception, decision-making, vehicle controls, and external communication. Constituent systems are often developed by different vendors globally which introduces challenges during the development process. Additionally, as the fleet of autonomous vehicles scales, optimization of onboard and off-board communication between the constituent systems becomes critical. 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. Legacy communications use powerline carrier communications at 9600 baud, so upfitting existing trailers for autonomous operations will require adopting technologies like Ethernet or a wireless harness between the truck and the trailer. This would require additional security measures and architecture, especially when pairing a tractor with a trailer.

We proposed tailoring the system of systems Model for autonomous vehicles. The model serves as the governing framework for the development of constituent systems. It's

essential for the SoS model to accommodate various development approaches that are used for hardware, and software such as Agile, or Vee models. Additionally, a queuing model for certificates authentication compares the named certificate approach with the traditional approach. The model shows the potential benefits of named certificates when the autonomous vehicles are scaled. We also proposed using named J1939 signals to reduce complexities and integration efforts when multiple on-board or off-board systems request vehicle signals. We discuss the current challenges and threats on autonomous truck-trailer communication when Ethernet or a wireless harness is used, and the impact on the Electronic Control Unit (ECU) lifecycle. In addition to using Named Data Networking (NDN) to secure in-vehicle and cloud communication. Named Data Networking can reduce the complexity of the security of the in-vehicle communication networks where it provides a networking solution with security by design.

ACKNOWLEDGEMENTS

I am grateful to the committee chairman, Dr. Jeremy Daily, for his continuous advice, support, and guidance.

I would like to thank Dr. Christos Papadopoulos for his invaluable recommendations and inputs.

# DEDICATION

To my parents, wife, kids, and family who have unconditionally supported me throughout this long journey. Thank you so much for your patience and motivation!

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

# Chapter 1 Introduction

## 1.1 Background

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 as shown in Table 1.1. Autonomy sensors are currently being placed on the tractor itself and no sensors are 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 perspective [2] [3] but not from an ECU integration or systems engineering and the impact it would have on the lifecycle.

**Table 1.1:** Levels of autonomy as defined by the SAE **[1]**.

| SAE Level | What does the human in the driver's seat have to do? | What do these features do? | Example Features |
|---|---|---|---|
| Level 0 | You are driving whenever these driver support features are engaged - even if your feet are off the pedals and you are not steering | These features are limited to providing warnings and momentary assistance | • automatic emergency braking<br>• blind spot warning<br>• lane departure warning |
| Level 1 | You must constantly supervise these support features; you must steer, | These features provide steering OR | • lane centering OR<br>• adaptive cruise control |

| SAE Level | What does the human in the driver's seat have to do? | What do these features do? | Example Features |
|---|---|---|---|
| | brake, or accelerate as needed to maintain safety | brake/acceleration support to the driver | |
| Level 2 | You are driving whenever these driver support features are engaged - even if your feet are off the pedals and you are not steering | These features provide steering AND brake/acceleration support to the driver | • lane centering AND<br>• adaptive cruise control at the same time |
| Level 3 | When the feature requests, you must drive | These features can drive the vehicle under limited conditions and will not operate unless all required conditions are met | • traffic jam chauffeur |
| Level 4 | These automated driving features will not require you to take over driving | These features can drive the vehicle under limited conditions and will not operate unless all required conditions are met | • local driverless taxi<br>• pedals/steering wheel may or may not be installed |
| Level 5 | You are not driving when these automated driving features are engaged - even if you are seated in the "driver's seat" | This feature can drive the vehicle under all conditions | • same as level 4, but feature can drive everywhere in all conditions |

Truck native communication protocol between the trailer and the tractor such as Power Line Carrier (PLC) has a limited bitrate of 10*kB/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.

Fully autonomous or self-driving trucks are expected to operate and travel long distances without human intervention. This includes the entire process such as coupling and uncoupling the trailer. In order to support various maneuvers including driving in reverse, additional autonomy sensors are needed to be mounted on the rear of the trailer. This will increase the bandwidth requirements due to the newly added sensors. The existing truck-trailer communication protocols such as Power Line Communication (PLC) and ISO11992-CAN have limited bandwidth which makes them incompatible with the new requirements. There have been proposals to use Ethernet between the tractor and the trailer. Additionally, there is a need to automate the process of physically coupling and uncoupling the trailer with a tractor. Moreover, a multi-layer cybersecurity implementation to secure the tractor and the trailer against new attacks due to the new features added.

## 1.2 Autonomous Truck Sensors and The Blind Spot

Autonomous trucks, such as level 5 autonomy, are expected to operate for extended periods and start and end missions without human interventions. This requires several autonomy sensors such as Radar, Lidar, cameras, and others, in addition to automation mechanisms. Autonomous trucks sensors are mounted on the tractor itself and no

autonomy sensors are considered for the trailer. This configuration creates a blind spot for the tractor virtual driver since there is no sensor on the back of the trailer. This limits the capability of driving in reverse and would require reliance on human assistance. To address this issue, a sensor could be added to the back of the trailer to enable reverse driving. This would require an update to the communication link between the truck and the trailer to provide higher bandwidth and enable sensor data transmission to the autonomous truck.

The communication between the truck and the trailer is currently using J1939, PLC, or ISO11992. The connector used for connection between the truck and the trailer is, for example, the J560 seven conductor electrical connector. Every time there is a trailer coupled or uncoupled, the connector needs to be plugged in or unplugged. This becomes a challenge for level 5 autonomous vehicles since human interventions are desired to be reduced. There are some solutions to automate the trailer hitching as well as the plugging in the electrical connections. Some proposals suggested placing the connectors in a precise location, so the two electrical connections mate when the tractor backs up and couples with the trailer. Another proposal is to use robotic arms in geo-fenced areas to automate the coupling without human intervention. In a scalable solution, a robotic arm is an expensive solution, especially if it needs to be mounted on each truck.

## 1.3 Research Questions

This dissertation seeks to address the following questions:

1. What systems engineering designs are essential for enabling level 4 and 5 autonomous trucks to effectively perform reverse driving and automate trailer coupling, with the aim of reducing complexity?

2. What considerations are necessary for the system lifecycle and cybersecurity in the context of the new design?

3. How can systems engineering principles and methodologies be leveraged to design and develop scalable communication systems for autonomous truck-trailer combinations, thereby improving their efficiency?

## 1.4 Contribution of the Study

This study contributes to the field of autonomous vehicles systems engineering as follows:

1. Autonomous vehicle as a System of systems and a tailored Vee model to improve the development and the design of a scalable communication system for autonomous truck constituent systems.
2. Autonomous truck-trailer high bandwidth communication over a wireless harness and automated pairing
3. Security of constituent systems communication and truck-trailer Ethernet or wireless harness-based communication when an unlimited number of trailers are considered for one truck.
4. Using Named Data Networking, named signals and NDNCERT for autonomous truck and trailer communication and digital certificates management and verification

## 1.5 Structure of the Dissertation

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 perspective such as the impact on requirements, and security. A comparison between Named Data Networking, and IP-based Data Distribution Service (DDS) and SOME/IP is included, in addition, to a test and evaluation of each approach when transferring multiple data types from one device to three other devices. This dissertation is organized into five chapters: Chapter 1 is the introduction; Chapter 2 reviews relevant literature on the related topics; Chapter 3 describes the autonomous tractor-trailer communication including wireless communication, security, and the impact on the lifecycle; Chapter 4 presents wireless pairing over a wireless medium; Chapter 5 presents the use, test and security of Named Data Networking; Chapter 6 introduces the concept of autonomous vehicles development as a system of systems using a V-model at that level and Chapter 5 is the conclusion.

# Chapter 2 Literature Review[1]

In this section, we discuss the related art of 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), tractor-trailer communication and autonomous vehicle systems engineering.

## 2.1 Wireless Sensor Network

The concept of a wireless sensor 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 a 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 networks 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].

[1] Contains content from [86]

## 2.2 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 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.

## 2.3 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 with another ADAS ECU and does not take other data formats and protocols into account. Nichițelea 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 the 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 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 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 a 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].

## 2.4 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 an 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 an 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.

## 2.5 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 the 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.

## 2.6 Autonomous Vehicle Systems Engineering

Level 4 and 5 autonomous vehicles (AV) [56] are engineered to operate for

extended periods without a human driver or driving controls in the vehicle. This is enabled by a variety of systems such as advanced computing, sensors, and machine learning. According to ISO/IEC/IEEE 15288, a System of Systems (SoS) is a System of Interest whose elements are themselves systems [57]. Autonomous vehicles embody a SoS concept since they incorporate numerous hardware and software systems to enable functions such as perception, decision-making, vehicle controls, and external communication. This renders the safe and secure development of the overall product a complex process due to the number of systems developed, internally to the vehicle or externally in the environment.

To address these challenges and development complexities, AV hardware and software development must include holistic SoS methodologies. Vehicle hardware and software development are challenging because of the number of stakeholders influencing the development and the distributed development of the vehicle systems. Often, the autonomous vehicle constituent systems are developed individually by different vendors globally with informal processes to coordinate the development efforts at a vehicle level. The AV SoS existing research mainly addresses vehicle operations, post-deployment, and connected vehicles as shown in

Table 2.1 with less focus on the hardware and the software development and the vehicle platform integration.

**Table 2.1:** SoS Related Art in Automotive, Autonomous Vehicles and Defense

| Category | Paper Scope |
|---|---|
| AV development, Operation and Post-deployment | Autonomous vehicles system of systems framework is proposed to enable autonomous vehicles to perform complex maneuvers on the highway [58]. |
| | Model land transportation, internet inspired reference model for autonomous driving and development acceleration [59] |
| | Autonomy operation after deployment and the interaction with the external systems. Architecting vehicles to be a constituent of the future transportation systems [60] |
| | Connected AVs from a system of systems perspective including Model-Based approach and use cases and behavior patterns [61] |
| | SoS approach to AV deployment, V2X and vehicle charging [62] |
| | SoS perspective for co-existence of automated vehicles and human driver vehicles and the interaction with the infrastructure [63] |
| | Modeling interactions between the constituent systems and Maneuvers Manager for Autonomous Vehicles [64] |
| AV SoS Model-Based System Engineering (MBSE) | Autonomous Vehicle SoS decomposition and architectural framework using MBSE [65] |
| | MBSE Approach for designing a resilient SoS using |

| Category | Paper Scope |
|---|---|
| | deterministic and probabilistic modeling [66] |
| | Utilization of MBSE to document a SoS [67] |
| | SoS-based approach to develop autonomous driving Mobility-as-a-Service [68] |
| Cybersecurity | V2V Intrusion detection based on the principles of SoS [69] |
| | Framework to identify the most critical security vulnerabilities in cyber physical system of system [70] |
| | Developing security requirements early in the design and maintaining stringent standards for in-vehicle and external systems. [71] |
| | Cybersecurity consequences of the current uncoordinated evolution of these systems-of-systems [72] |
| | Security Engineering of Defense systems using the wave model [73] |
| Safety | SoS tailored analysis based on ISO26262 for platooning and V2V [74] |
| | Co-engineering of safety and security for embedded electronic systems [75] [76] |
| | Systems-Theoretic Accident Model and Processes (STAMP) for safety and security analysis in a vehicle platoon as an example [77] |

| Category | Paper Scope |
|---|---|
| | Safety Analysis process for a SoS [78] |
| System of Systems Engineering | System of systems V-model at the top layer and multiple V-models for the constituent systems at a lower layer [79] |
| | Defense SoS-VEE Model that is focused on early SoS Engineering activities and integrating the constituent systems, even if they are following different systems engineering models [80] |
| | Methods and challenges for building resilient and reliable SoS [81] |

Based on the existing art, we presented a tailored SoS V-model for the autonomous vehicle's hardware and software development. This model can serve as the governing framework for all development activities for the constituent systems with safety and security integrated. Furthermore, a networking solution between the constituent systems is presented using Named Data Networking (NDN) to address the challenges of scalability and to optimize communication between constituent systems. NDN is evaluated in comparison to Scalable service-Oriented MiddlewarE over IP (SOME/IP) when used in the same setup, in addition to a queuing model for cloud requests. Named J1939 signals are proposed using NDN to unify communication between on-board and off-board systems since they are not connected to the vehicle Controller Area Network (CAN) bus. This reduces the complexities and additional integration efforts and formats between the different systems requesting and receiving the data.

# Chapter 3 Autonomous Truck-Trailer Communication[2]

## 3.1 Architecture

Based on 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 the trailer ABS architecture to meet the needs of L4/L5 ATs and add Telematics, lights control, and GPS to the trailer ABS ECU instead of having a separate ECUs or hardware module.

[2] Contains content from [86] [104] [105]

### 3.1.1 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 the 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 3.1. 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 3.1.

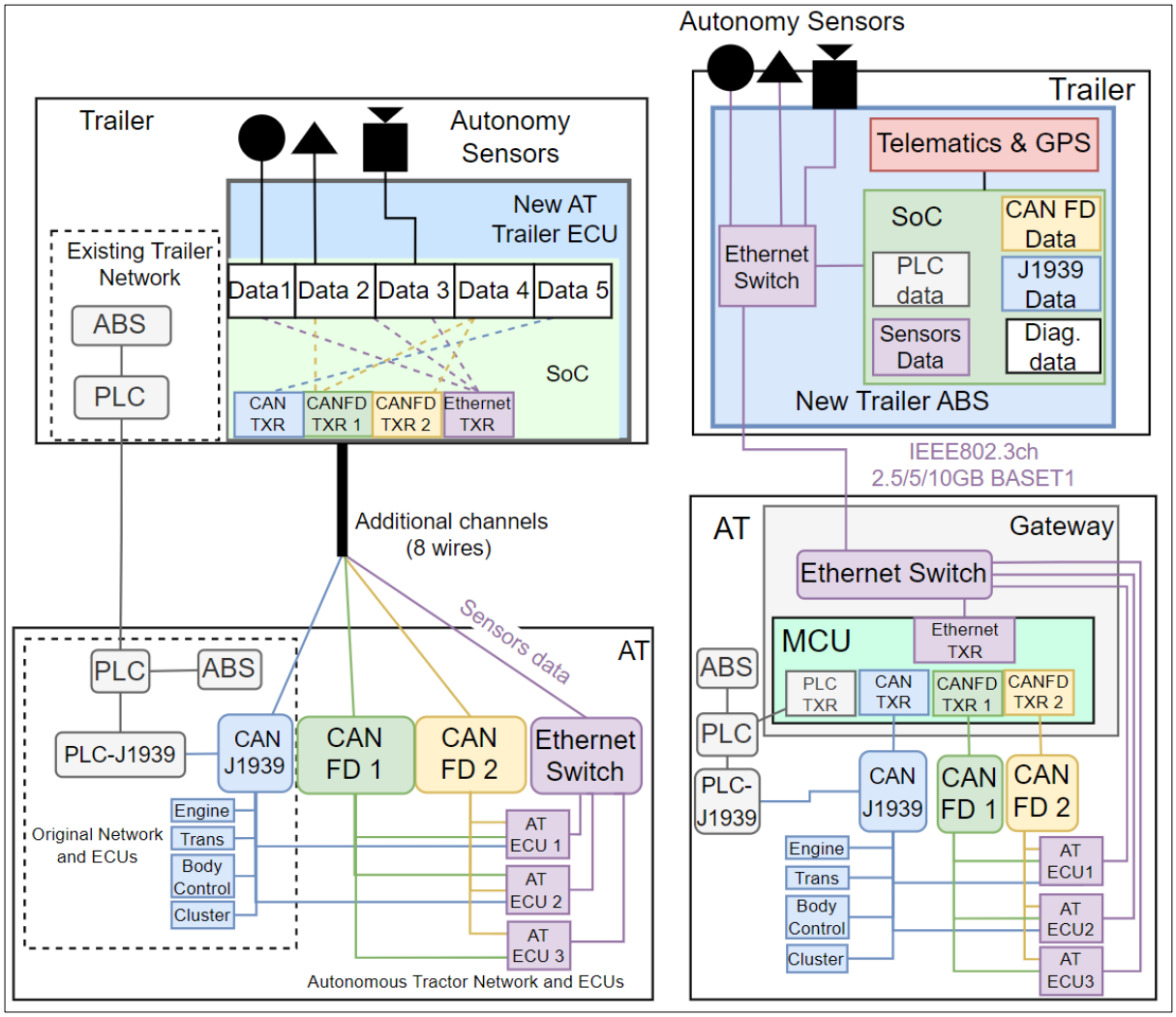


**Figure 3.1:** (Left) Retrofitting an autonomy ECU in the trailer to process rear sensors to accommodate level 4 and 5 autonomy needs. (Right) Proposed upgraded trailer ABS architecture that integrates with the existing autonomous tractor architecture.

### 3.1.2 Wireless Trailer ABS

We propose replacing the physical data cables between the trailer and the tractor with a wireless medium. Wireless Trailer ABS architecture will be similar to the Ethernet-based architecture except for the physical link between the trailer and the tractor. The wireless harness concept for *in-vehicle* ECU communication has been previously proposed and tested using different wireless mediums such as Ultra-wideband [8] ,

millimeter-waves [9], and 60 GHz Wi-Fi [11] with positive results such as achieving a data rate of 600 to 700 *Mbps* in the case of the using IEEE 802.11ad. The wireless harness has not been addressed or proposed when used between the trailer and the tractor as a communication link. The wireless harness (e.g., IEEE 802.11ad) supports multi-gig data rate and could be leveraged in the communication between the tractor and trailer ABS ECU to enable automatic pairing and eliminate the need for plugging a cable for conventional trucks or autonomous trucks, especially if the process of coupling and uncoupling a trailer and a tractor needs to be automated without human intervention. The wireless trailer ABS can contain any functionalities needed on the trailer side such as braking, traction control, trailer monitoring and diagnostics, lights control, telematics, or any additional functionalities to reduce the number of ECUs or hardware modules needed. The wireless harness as shown in Figure 3.2, using 60 GHz Wi-Fi for example, could have a standardized range for truck-trailer communication only to avoid interference with other applications.

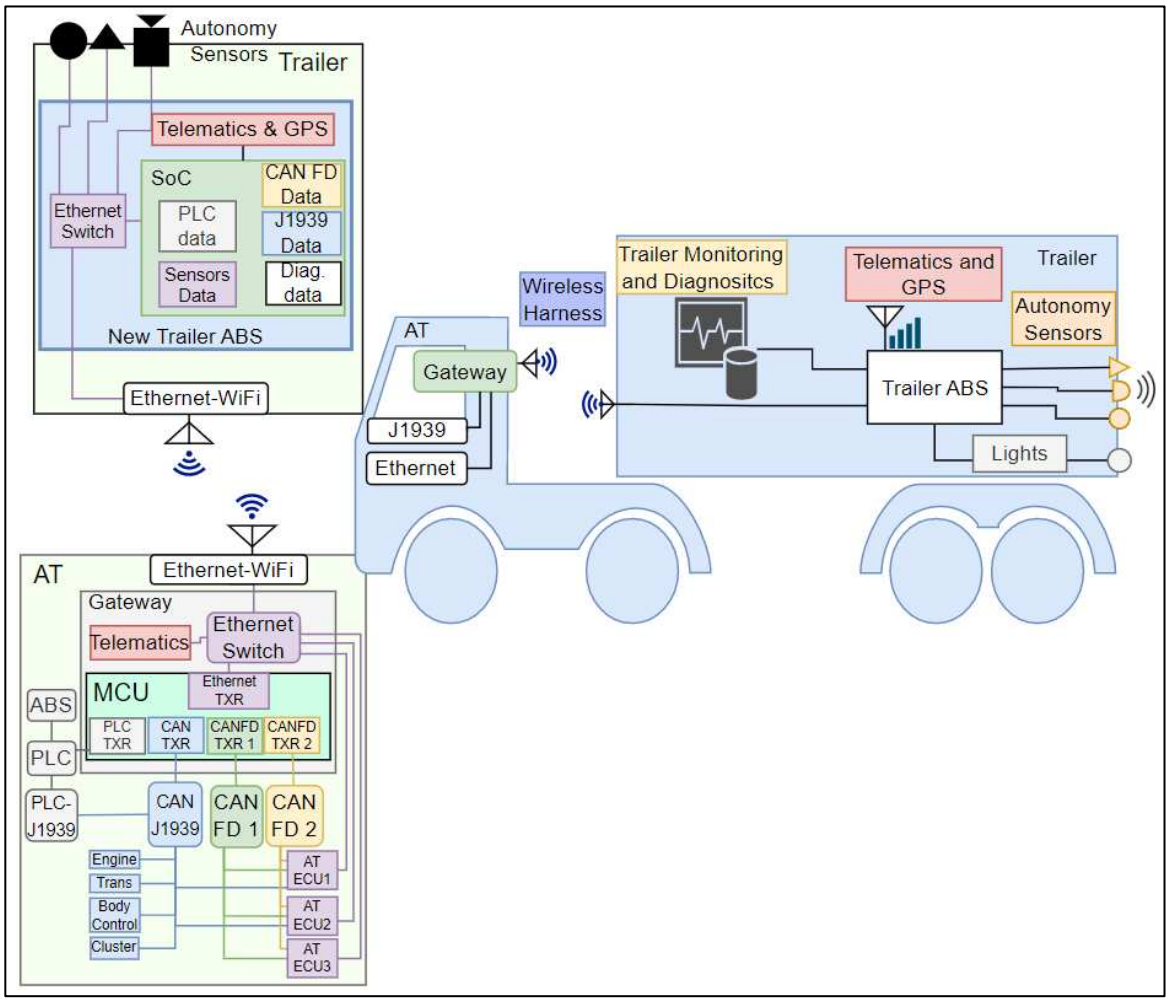


**Figure 3.2:** Proposed wireless trailer ABS ECU using a wireless harness and with more features combined such as telematics, GPS, and sensors data processing.

As discussed in the related literature section, the future in-vehicle network includes DCU and Ethernet as a backbone, so for conventional trucks, a future network concept for conventional trucks is shown in Figure 3.3.

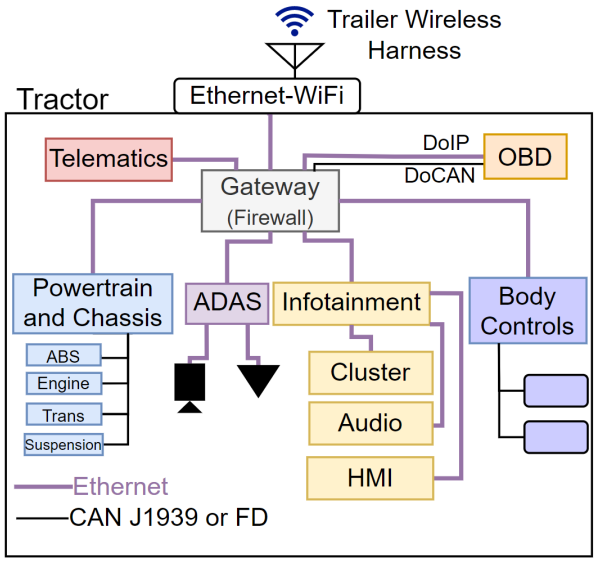


**Figure 3.3:** Future network architecture concept for trucks.

### 3.1.3 System Requirements

In order for the new trailer ABS to accommodate the autonomy needs, it needs to adhere to the requirements in Table 3.1:

**Table 3.1:** New Ethernet-based trailer ABS ECU system requirements

| ID | Requirement |
|---|---|
| **R1** | The trailer ABS ECU shall have additional inputs for different types of sensors such as the LiDAR, camera or ultrasonic to support autonomous driving in reverse. |
| **R2** | The sensors shall be mounted on the back of the trailer facing backwards to function as the reverse sensing system for the autonomous tractor. |

| ID | Requirement |
|---|---|
| **R3** | The trailer ECU shall be able to process sensors data and transmit it to the tractor. |
| **R4** | The trailer ECU shall comply with IEEE 802.3ch 2.5/5/10GB BASET1 to communicate with the tractor. |
| **R5** | The trailer ECU shall be able to wrap multiple communication protocols packets over Ethernet such as sensors data, AT CAN FD, CAN buses, tractor standard J1939 CAN, or diagnostics data simultaneously. |
| **R6** | A gateway shall be added on the AT side as an extension to the trailer ECU to route the incoming traffic to the appropriate buses at the AT. Similarly, the gateway shall wrap the traffic going from the AT to the trailer over Ethernet. |
| **R7** | The system shall integrate and be compatible with legacy truck communication protocols |
| **R8** | All the trailer features shall be included in the trailer ABS with no separate hardware modules. Features such as Telematics, GPS, temperature monitoring, trailer monitoring, lights control, Tire Pressure Monitoring System (TPMS), sensors data processing and communication over Ethernet. |
| **R9** | The system shall support data authenticity and confidentiality |

| ID | Requirement |
|---|---|
| **R10** | The system shall be able to meet the data timing requirements (e.g., 20 milliseconds for some CAN messages) |
| **R11** | The system shall be interoperable and compatible with tractors from different manufacturers |
| **R12** | The system shall operate with many tractors within the same fleet and support one-to-many relationships without conflicts or mixing information. |

In case of a wireless medium between the trailer and the tractor:

**Table 3.2:** New wireless harness-based trailer ABS ECU system requirements

| ID | Requirement |
|---|---|
| **RW1** | A multi-gig wireless medium shall be used for communication between the trailer and the AT |
| **RW2** | The trailer ECU shall be able to exchange different data types including sensors and CAN data over the wireless medium with the AT |

| ID | Requirement |
|---|---|
| **RW3** | The trailer and the AT shall be able to automatically pair upon power up and being physically connected. |
| **RW4** | Each of the trailer and the tractor shall be authenticated by a mutual root of trust before establishing a connection and being paired |
| **RW5** | After establishing a connection, the trailer and the tractor shall be able to exchange public keys for data packets encryption and authentication |
| **RW6** | The trailer wireless connection antenna (e.g., IEEE 802.11ad) shall be mounted on the front side of the trailer facing the back of the tractor where the tractor antenna is mounted. |
| **RW7** | All the data traffic exchanged between the ECUs shall be authenticated |

**Networking Protocol**

Using Ethernet or a wireless harness as the only communication link between the trailer and the autonomous tractor will require a proper networking protocol to allow the ECUs on the same network to exchange data and meet the timing and bandwidth

requirements. In this section, we will compare two different networking approaches, Named Data Networking (NDN) and Data Distribution Service (DDS).

**Comparison Between NDN and DDS**

Named Data Networking [82] is a content-based architecture that uses names for each data type, the data transfer is driven by the receiving device where it sends an interest packet containing the name of data and sender responds with a data packet that contains the name, the requested data and the signature as shown in Figure 3.4. NDN changes the architecture from an Internet Protocol (IP) address-based to a name-based, which makes it simpler to configure the network. Named Data Networking Forwarding Daemon (NFD) [83] is the network forwarder responsible for forwarding interest packets and data packets in each device. NFD forwards and communicates the packets over multiple network interfaces (Face), physical such as Ethernet, transport layers such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) or inter-process channel between the NFD and an application. A Face is also the interface connecting two devices on the network with an ID, local Uniform Resource Identifier (URI) and a remote URI for the remote device. NDN supports data security [84] by default and the signature is built-in the data packet structure.

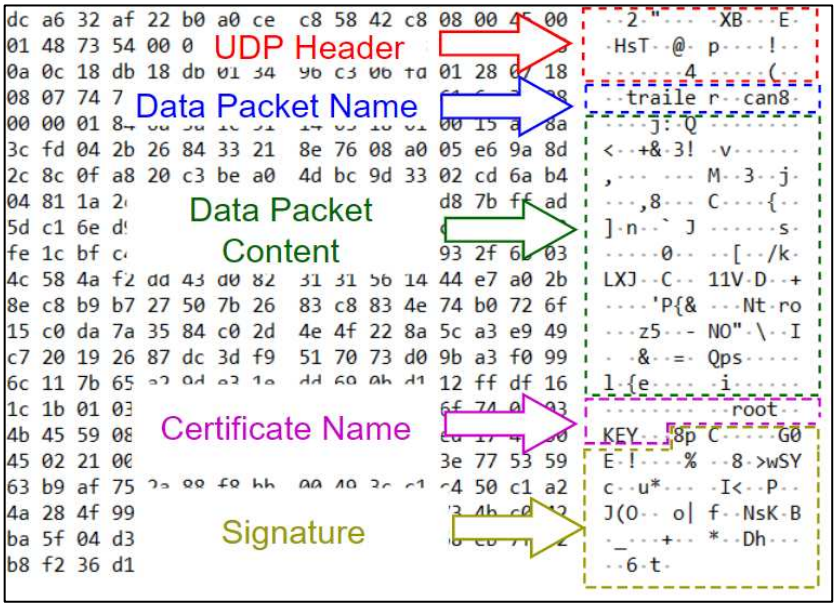


**Figure 3.4:** A demonstration of how a NDN data packet named /trailer/can looks over Ethernet.

DDS Real-Time Publish Subscribe (RTPS) is a known protocol that is used in high performance, low latency and real-time communication using the publisher-subscriber architecture.

## 3.2 Wireless Communication

Driverless and conventional trucks are becoming more capable with the addition of autonomy software and Advanced Driver Assistance Systems (ADAS) systems that bring different sensors to the truck. One of the challenging maneuvers for human and software drivers in semi-trucks is reverse driving due to the lack of rear facing sensors on the trailer to aid the driver while backing up. Legacy communication channels between the truck and the trailer have basic bitrate and cannot support sensors data transfer or meet the latency and bandwidth requirements for the new autonomy systems. There have

been proposals to use Ethernet between the trailer and the truck to support the new requirements, in addition to the automation of trailer hitching and unhitching process. Automation of the tractor-trailer physical hitching and unhitching will include plugging and unplugging data and control wires and connectors from the tractor to the trailer, which is a complex process to automate that requires the connectors to mate properly to fully plug in, which, for example, could be done using a robotic arm on the tractor or positioning the connectors in a precise location in each of the tractor and the trailer. It's expected that driverless trucks will not need a human during their mission including trailer pickup and drop off.

Wireless harness is one of the concepts that can meet the communication requirements, and bandwidth and at the same time greatly help the automation of the hitching and unhitching process since no wires or connectors will be needed and the pairing process between the truck Electronic Control Units (ECU) and the trailer ECU will be securely automated. Wireless harness has been proposed previously for vehicle in-cabin communication between different ECUs but has not been addressed for truck and trailer communication. Wireless harness leverages a variety of technologies and has been tested for in-cabin communication with promising results, technologies such as Impulse Radio Ultra-Wideband (IR-UWB) [8], Millimeter-Wave [85], ZigBee [10], IEEE 802.11ad [11] and IEEE 802.15.1 [12]. IEEE802.11ad appears to be the most appropriate technology to use since it can support the requirements of a gigabit or multi-gig networking between the truck and the trailer and at the same time, it’s a well-established technology with more development resources. IEEE802.11ad could be used between the trailer ECU and the truck ECU as shown in Figure 3.5 where an Ethernet-Wi-Fi bridge could be used on both

sides to enable communication between the trailer ECU and other ECUs on the truck side whether they are connected to an Ethernet Network using a switch, a Controller Area Network (CAN) bus which is managed by the truck gateway to enable two-way communication between the remote trailer ECU and local ECUs connected heterogeneous networks.

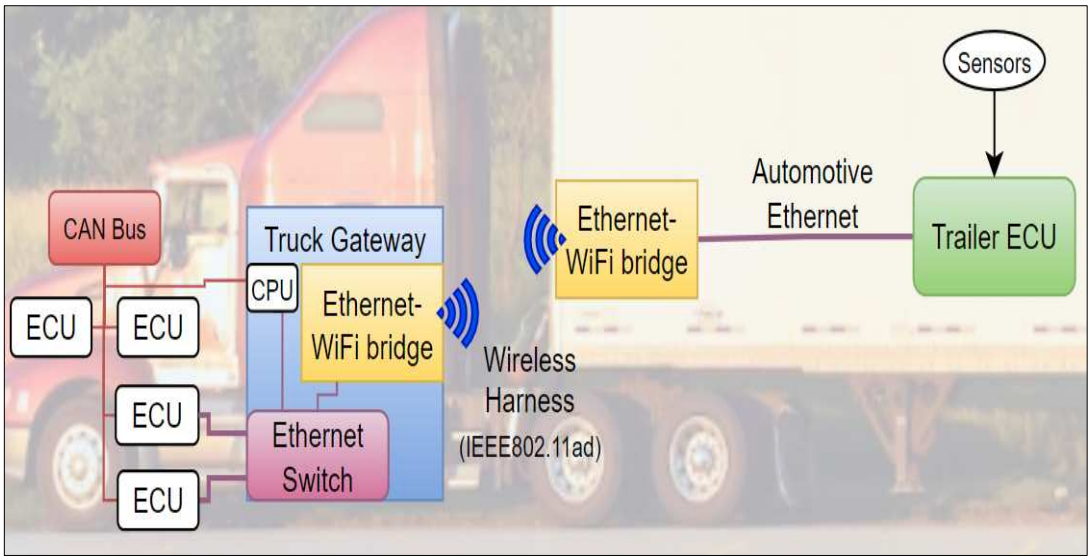


**Figure 3.5:** Concept of using IEEE802.11ad as a wireless harness for truck and trailer communication.

Using the wireless harness for communication between the truck and the trailer will eliminate the need for additional data wires or connectors since the heterogenous data could be digitized and wrapped in Wi-Fi frames including CAN, CAN Flexible Data (FD), sensors data or diagnostics data. In some cases, the truck is coupled with two trailers. Figure 3.6 shows the concept of two trailers using wireless harnesses and trailer 1 relaying the data from trailer 2 to the truck, in addition to its own data.

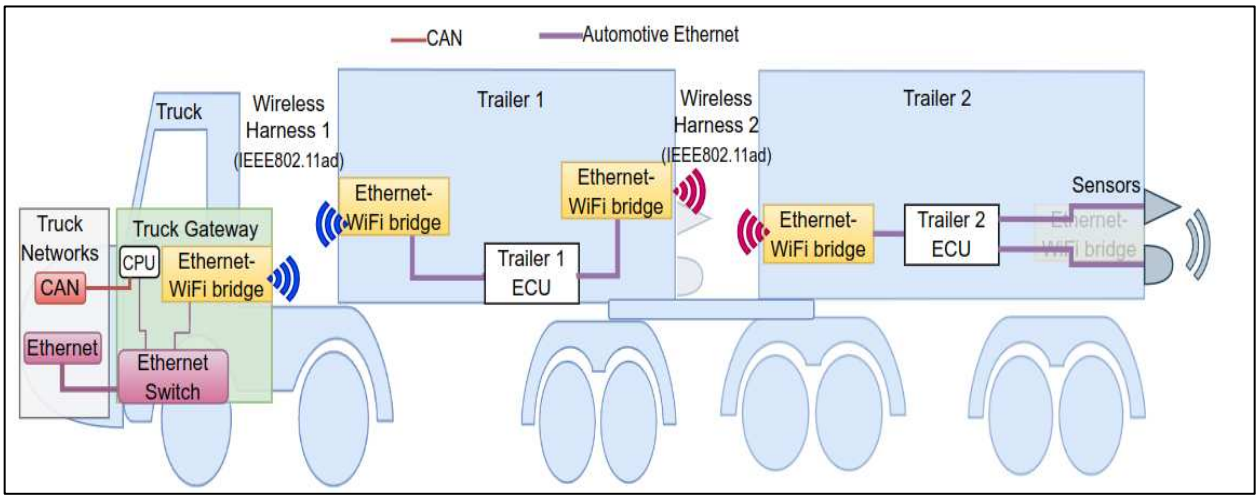


**Figure 3.6:** Concept of the wireless harness when two trailers are connected to the truck.

This newly introduced intra-communication will require a new networking approach to manage the different types of data exchanged including integration with existing native truck network and security such as data confidentiality, integrity, and authenticity since the attack surface will increase. One of the new networking protocols that has security by design and has been tested in the context of automotive communication with positive results is Named Data Networking (NDN) [38] [39] [40]. We previously included a literature review and discussed using Ethernet, NDN, and secure automated pairing in [86].

## 3.3 Security

In R1 from Table 3.1, adding additional inputs to the ABS ECU to take autonomy sensors data will increase the total number of sensors inputs since the main input from existing trailer sensors is the wheel speed sensors and other trailer monitoring sensors. Processing autonomy sensors requirement as in R3 will result in an increase in the

capabilities of the trailer ECU processing such as using a system-on-chip (SoC) instead of what being used currently in conventional trucks such as a Microcontroller (MCU) since the new ABS is expected to do additional processing.

Using Ethernet or the wireless harness as the only communication link between the trailer and the tractor will result in replacing legacy data communication wires (e.g., PLC, or ISO11992) with automotive Ethernet. The information the legacy communication protocols carry will be digitized and transmitted over Ethernet. To support native protocols and integrate with the tractor side, an Ethernet switch and a MCU is needed to be added on the tractor to function as a gateway for the trailer ECU where it routes the ethernet traffic coming from the new trailer ABS to different buses on the tractor such as PLC, CAN J1939, CAN FD and Ethernet. Additionally, all the features that are being used in the trailer need to be combined in one ECU to avoid the need for separate hardware modules on the trailer side.

### 3.3.1 Threats and Challenges

To achieve autonomous truck reverse driving, the trailer ECU will be the source of rear sensors data. The data will be transmitted to the sensor fusion ECU on the truck side to make driving and vehicle controls decisions. This will have a high impact on the trailer ECU security requirements, security implementation, and the lifecycle when compared to the PLC-based legacy ECU and its lifecycle. The new communication protocols and links will introduce new threats as shown in Figure 3.7. The architecture of ECU intra-communication needs to be security-centered since the communication is affecting the

self-driving software, for example, data confidentiality, integrity and authenticity will be needed.

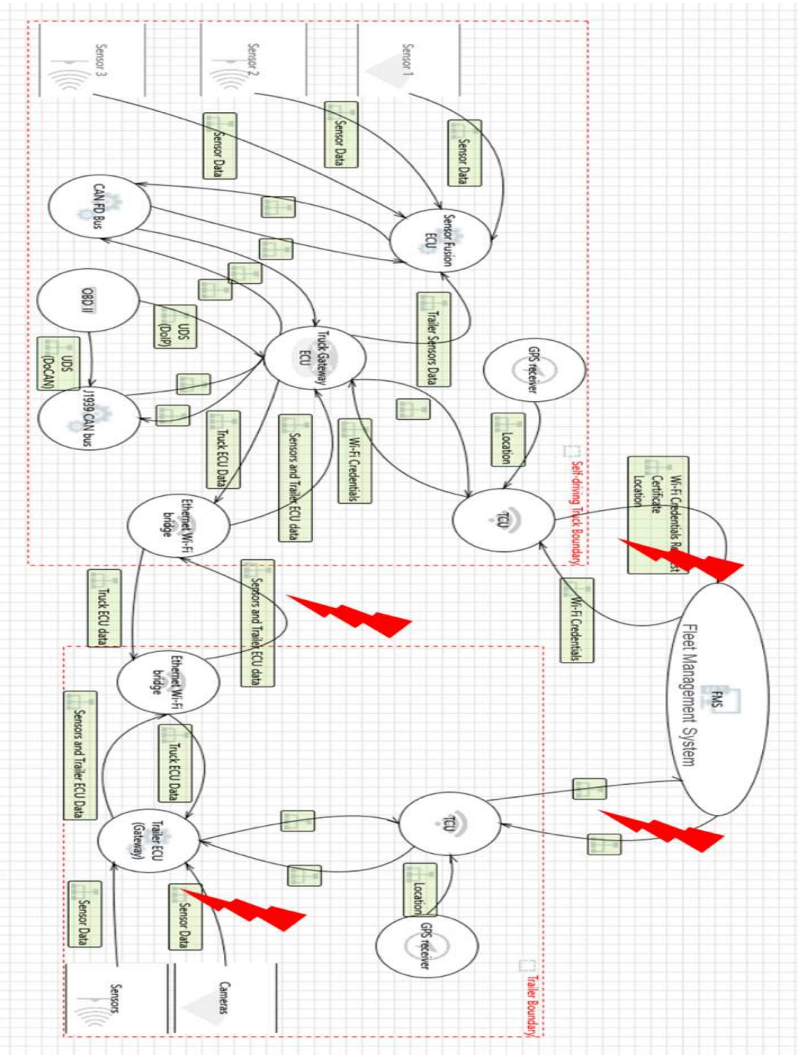


**Figure 3.7:** Data flow diagram of the interaction between different components in the truck, trailer, and the fleet management system in the case of using a wireless harness.

**Challenge one:** verifying the authenticity of the truck and the trailer before establishing data communication over Ethernet after being physically connected. Similarly, in the case of a wireless harness, both truck and the trailer will need to be authenticated before pairing over Wi-Fi and before establishing intra-communication to exchange data. The wireless harness will require a physical medium such as Wi-Fi which

will require access credentials to allow other devices to join the network. Assuming that the trailer will be the Wi-Fi access point and the truck will be the client, the client will need to have the wireless harness access credentials to access the network and start communication with the trailer.

**Challenge Two:** Using the same Wi-Fi credentials for all the trailers is less secure. The entire fleet would be compromised if one trailer is hacked, therefore, each trailer needs unique credentials. Each trailer is expected to have unique wireless harness network credentials. A truck cannot simply store the wireless harness access credentials of all the available trailers within the fleet due to the complexity and storage limitations in the truck ECU. For example, assume the number of possible trailers nationwide is 50,000 and a self-driving truck will get a random trailer assigned for a delivery trip. It's impractical and complex to have each truck in the fleet pre-store the wireless harness credentials or the public keys of all the trailers.

**Challenge Three:** The newly proposed architecture and communication links between the truck and trailer introduces new interfaces such as Ethernet or a wireless harness (i.e., Wi-Fi). Therefore, the attack surface will increase and will have an impact on the assets of the autonomous truck. Figure 2 shows the data flow diagram of the new architecture and the interactions between different components within the truck-trailer communication. In addition to ECU-to-ECU and ECU to cloud-based Fleet Management System (FMS) and the potential attacks after the integration of the new system. Telematics Control units (TCU) are commonly used in trucks and trailers for asset tracking since they could be from different manufacturers. TCU could be leveraged for

provisioning and additional FMS-based authentication before approving the truck-trailer pairing process over the wireless harness.

The newly added interface is Wi-Fi Ethernet bridge in case of using Wi-Fi as a wireless harness. It is used for data communication between the truck and the trailer, including the new rear sensors added to the trailer ECU. The wireless harness will be carrying different data types such as Controller Area Network (CAN) J1939, CAN Flexible Data (FD), and trailer rear sensors data. The trailer sensors data will be sent to the sensor fusion ECU on the truck side to make driving and vehicle controls decisions when necessary for vehicle maneuvers such as reverse driving. The Wi-Fi-based wireless harness is subject to several types of attacks such as Denial-of-Service (DOS), Man-in-the-Middle (MITM), rogue client, rogue access point, replay attack, and password cracking.

Table 3.3 shows the different types of attacks, the failure modes associated with each one, the risk level, and recommended countermeasures when a wireless harness is used.

**Table 3.3:** Truck-trailer wireless harness and the potential failure modes

| **Risk** | **Cause** | **Risk level** | **Failure Mode** | **Countermeasures** |
|---|---|---|---|---|
| Wi-Fi Crash | DoS | High | Lost communication between the | •Limited wireless harness physical range |

| Risk | Cause | Risk level | Failure Mode | Countermeasures |
|---|---|---|---|---|
| | | | truck and the trailer | •Backup wireless harness network<br>•Network segmentation<br>•Suspicious activity monitoring and reporting |
| | | | No rear sensors data | |
| | | | Inability to reverse drive | |
| Wi-Fi data sniffing | MITM | High | Confidential information disclosure such as access credentials | •Data encryption as necessary |
| | | Medium | Data logging such as sensors data and CAN data eases replay attack and reverse engineering. | |
| Rogue Wi-Fi access points | MITM | Medium | Trailer connects to attacker's Wi-Fi access point | •Multi-layer authentication mechanisms for each device before connecting to the wireless harness network and before enabling data communication |
| | | High | Truck connects to attacker's Wi-Fi access point | |
| | Rouge client | Medium | A rogue client impersonating a | |

| Risk | Cause | Risk level | Failure Mode | Countermeasures |
|---|---|---|---|---|
| Unauthorized client | | | trusted truck and connects to the wireless harness network to get unauthorized access to the trailer | •Limited wireless harness physical range |
| | | High | A rogue client impersonating a trusted trailer and connects to the wireless harness network to get unauthorized access to the truck | |
| Replaying modified or old data | Replay attack | High | Replaying modified or old trailer sensors data to the truck gateway, therefore, to the sensor fusion ECU | •Data packets signing and authentication<br>•Time-stamped data packets<br>•Using random nonces |
| | | | Replaying modified or old trailer CAN FD or J1939 data to the truck gateway | |

| Risk | Cause | Risk level | Failure Mode | Countermeasures |
|---|---|---|---|---|
| | | | Replaying modified or old truck CAN data to the trailer such as sending a fake trailer traction control command | |
| Wi-Fi credentials exposed | Password cracking | High | Wireless harness network access credentials compromised allowing attackers to gain unauthorized access | •Multi-layer authentication mechanisms for each device before connecting the wireless harness network<br>•Limited wireless harness physical range<br>•Unique access credentials per trailer<br>•Credentials expiration and updates after a period of time |
| Wi-Fi Interference / Jamming | Illegal electromagnetic wave generation | Low | Degraded wireless link or frequent link drops | •Use of directional antennas<br>•Operate in a different frequency when interference is detected |

**Challenge Four:** Due to using Ethernet or the wireless harness, the truck and trailer ECUs need to be authenticated before establishing a connection. In the case of the Ethernet, one certificate is needed for authenticating the connecting ECU. On the other hand, wireless harness will have additional credentials or certificate-based access to the wireless network. Digital certificate-based authentication is common but will have some challenges such as certificate storage, distribution, and management. This increases the need to have a cellular connection for the autonomous truck and the trailer. Cellular connections are available by default in self-driving trucks and becoming more common in trailers as well. Certificate authentication time is expected to increase since each ECU needs to query the status and verify the validity of the other ECU certificate by checking Certificate Revocation Lists (CRLs) or using the Online Certificate Status Protocol (OCSP). A self-driving truck or a trailer downloading CRL to check the certificate revocation status every time the pairing process happens is impractical. OCSP allows the truck and the trailer to send the certificate information including serial number to the OCSP responder to check the status of the certificate. One potential contributing factor in the authentication delay is using certificate serial numbers as unique identifiers (e.g., *cb:03:fa:f2:ed:e9:fe:84:7a:71:65:1c:co:ff:ee:7c*). This will require the server to look up the serial number of the certificate in its internal database to verify the status of the certificate. The server also may look up the associated identification information such as Vehicle Identification Number (VIN) to verify that the current truck and trailer combination is authorized.

### 3.3.2 The Impact on Security

Since the trailer will be a source of information and sensors data for the AT to drive, authentication or encryption of data packets exchanged between the trailer and the tractor will be required. Moreover, in the case of a wireless trailer ABS, an additional authentication step is required to assure that both of the trailer and tractor are authenticated and can connect securely over the wireless harness (e.g., 60 GHz Wi-Fi), especially if the pairing process and coupling the tractor and the trailer is expected to happen without human intervention.

Figure 3.8 shows trailer ABS keys provisioning using a cloud-based Fleet Management System (FMS) and a Certificate Authority (CA) over a Virtual Private Network (VPN). FMS will be responsible for managing provisioning, key generation requests, access control, and identities of the ECUs and other users. The trailer ABS is shown as an example and the tractor will follow the same process.

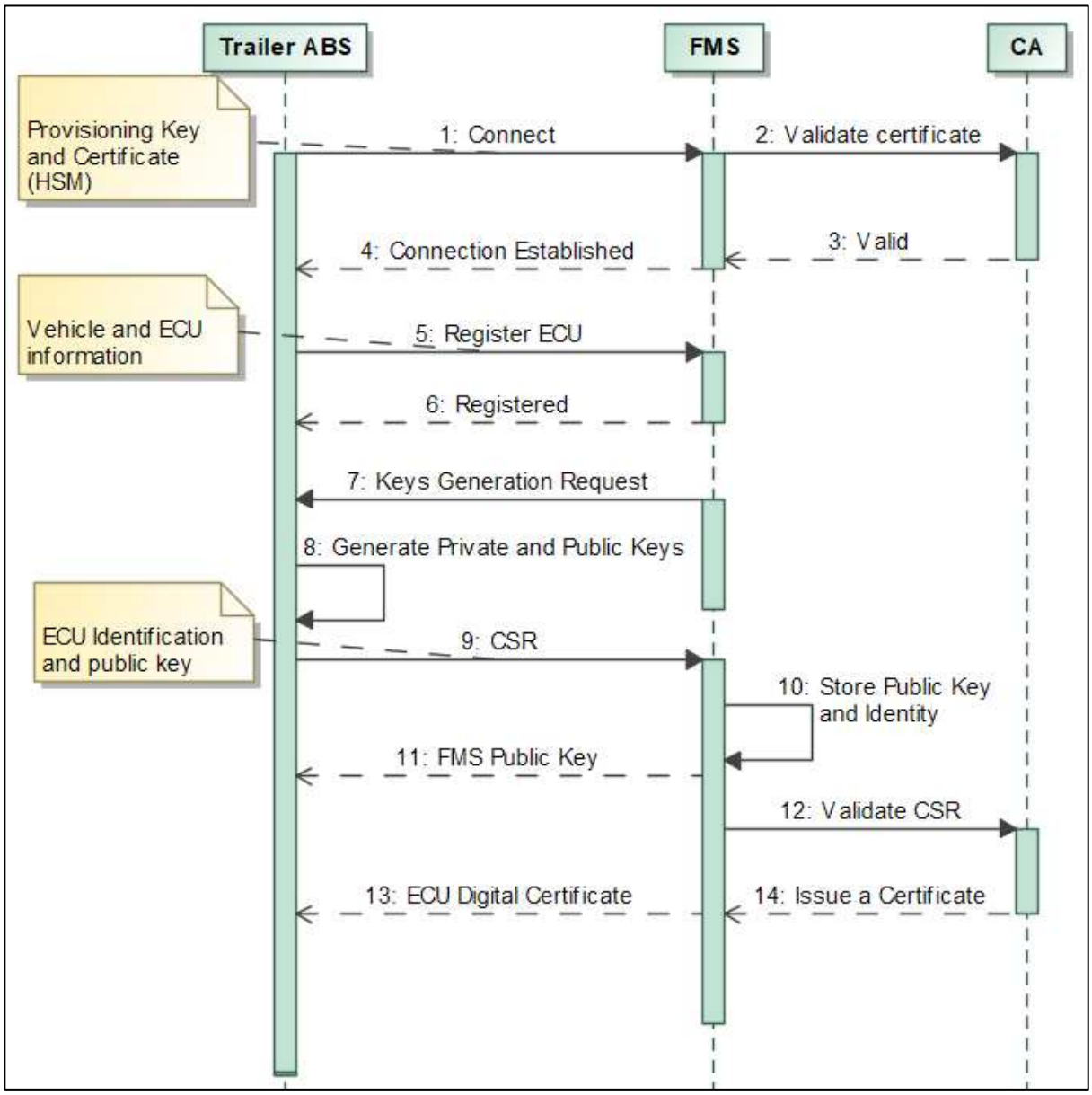


**Figure 3.8:** Trailer ECU provisioning using a cloud-based Fleet Management System (FMS).

A method to authenticate the trailer and the tractor using FMS before pairing with each other is shown in Figure 3.9. This is possible by leveraging the telematics unit available in the trailer and the tractor (i.e., cellular connection), in addition to using the GPS coordinates or One-Time Passcode (OTP) as an additional step to verify the integrity of the connection requests. The AT and the trailer will send the connection requests to

FMS and FMS will first authenticate each entity. After authentication, GPS coordinates or OPT will be compared and if they match, the requests can be approved and FMS then will generate Wi-Fi credentials with a defined access level and request the vehicle Wi-Fi server (e.g., AT) to locally update the Wi-Fi credentials and the access list with privileges defined such as the level of access and the types of data supported. After confirmation from the Wi-Fi server that it updated the Wi-Fi credentials and access list, FMS will send the pairing credentials to the Wi-Fi client (e.g., Trailer) to start pairing with the AT.

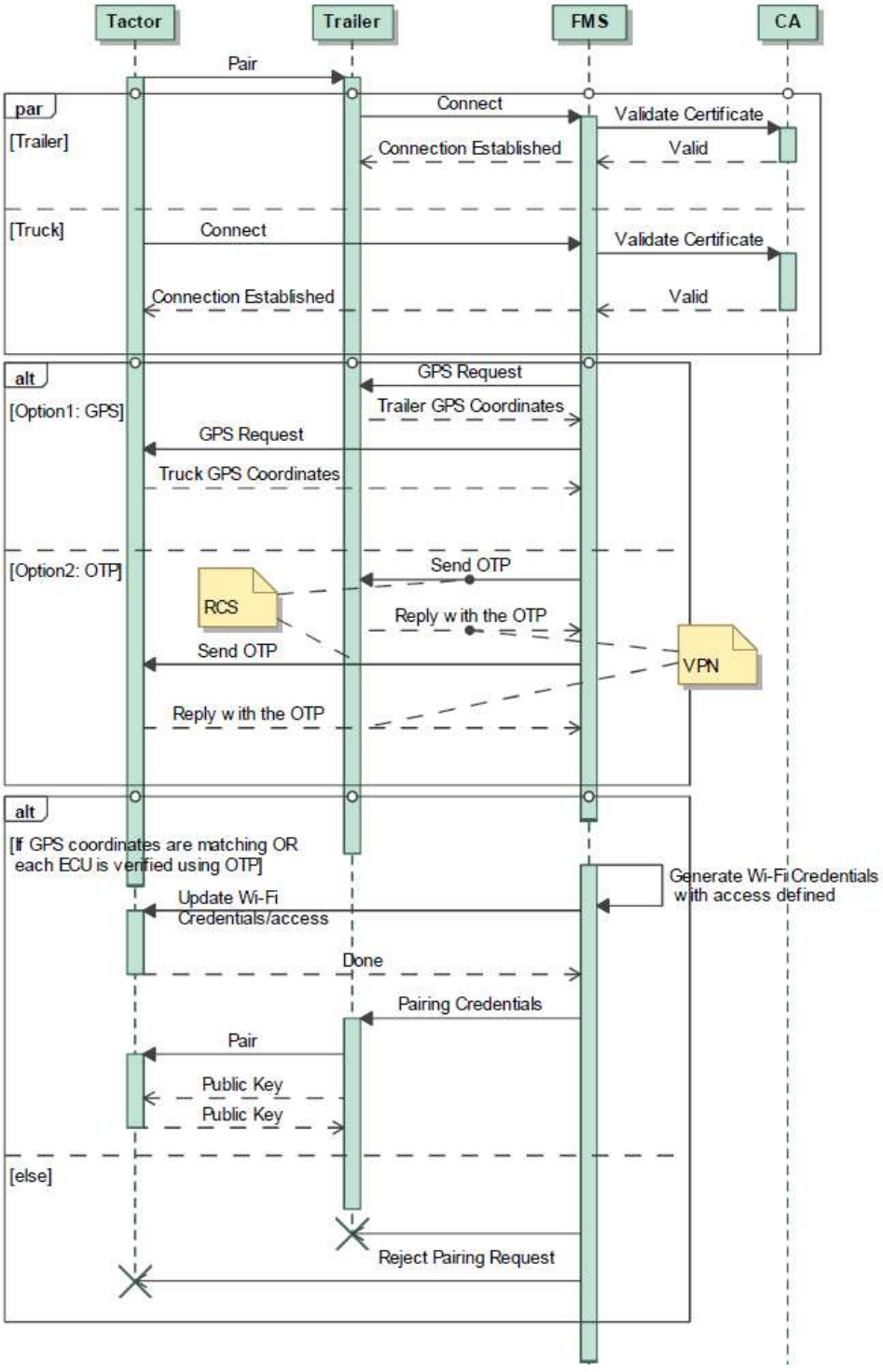


**Figure 3.9:** Authentication of the trailer and the tractor when connecting over the wireless harness using geo-location authentication or OTP.

### 3.3.3 GPS Spoofing

One of the concerns with using GPS coordinates as a geo-location authentication method during the tractor-trailer pairing process as shown in the previous method is GPS spoofing. The attackers use a transmitter that mimics the satellites to send fake GPS signals to the vehicle's GPS receiver causing the vehicle's GPS to report the attacker's desired coordinates. There are multiple approaches to detect and overcome GPS spoofing on the autonomous vehicle or autonomous tractor side such as dead-reckoning, prediction, sensor-fusion, or Visual Positioning System. The trailer could leverage the GPS from a coupled trusted AT as a source of truth and use it to detect spoofing. Assuming a trusted AT $T$ with an accurate GPS and connected to a trailer $R$ and the distance between the AT GPS and the trailer GPS is $d$ with a maximum GPS error of $e_T$ and $e_R$ respectively. The series of coordinates $x$ and $y$ for the AT and the trailer are described as follows:

$$[(x_{T1_{t1}}, y_{T1_{t1}}), (x_{T2_{t2}}, y_{T2_{t2}}), \dots, (x_{Ti_{ti}}, y_{Ti_{ti}})] \quad (1)$$

$$[(x_{R1_{t1}}, y_{R1_{t1}}), (x_{R2_{t2}}, y_{R2_{t2}}), \dots, (x_{Ri_{ti}}, y_{Ri_{ti}})] \quad (2)$$

From (1) and (2) series, any coordinates with series position $n$ and timestamp $tn$ will be evaluated using the following criteria:

$$|x_{Tn_{tn}} - (x_{Rn_{tn}} + d)| \leq e_T + e_R \quad (3)$$

$$|y_{Tn_{tn}} - (y_{Rn_{tn}} + d)| \leq e_T + e_R \quad (4)$$

If (3) or (4) is False, a GPS spoofing or malfunction is occurring on the trailer side. An alternative method in case geo-location authentication is not possible is sending a OTP in a message over Rich Communication Services (RCS) from the cloud to each ECU as shown in Figure 3.9. 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 receives 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.

### 3.3.4 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 [87], and SAE J3061 [88] 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 3.10 shows a multi-layer cybersecurity concept to protect against the new attacks on the ECU.

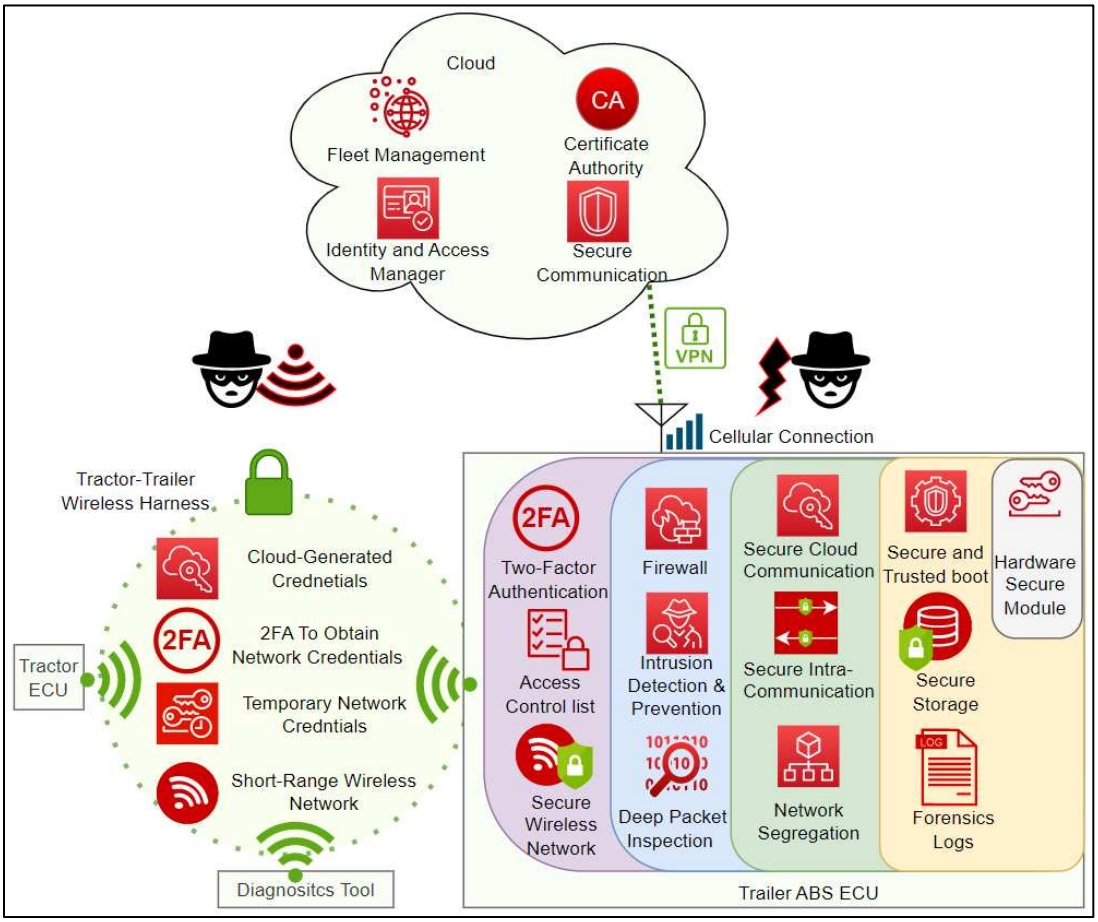


**Figure 3.10:** A multi-layer security concept for the new trailer ABS ECU and the tractor ECU.

Table 3.4 shows the impact on the lifecycle of the ECU and the new activities that need to be taken into consideration.

**Table 3.4:** Main impact of the new features and interfaces on the trailer ABS lifecycle phases and technical processes per the V-model and INCOSE [89]

| Technical Process | Phase Impact |
|---|---|
| **System Requirements Definition** | → ABS Hardware and software security and performance requirements<br>→ 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.<br>→ Wireless connections requirements such as the wireless harness and the cellular connection performance and bandwidth<br>→ Design and cybersecurity risk assessment of adding Wi-Fi and cellular to the ABS.<br>→ Distributed development in the case of the tractor and the trailer from two different OEMs.<br>→ 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. |

| Technical Process | Phase Impact |
|---|---|
| | → System analysis including cost, technical risks, and effectiveness analysis<br>→ Cybersecurity analysis to configure the proper cybersecurity level for the system.<br>→ Safety and cybersecurity by design |
| **Implementation and Integration** | → Secure hardware and software implementation<br>→ Integration, configuration, and testing of software and hardware components<br>→ Secure IT infrastructure<br>→ New procedures and training |
| **Verification, Validation and Testing** | → Scanning for vulnerabilities in the software and the hardware<br>→ Reverse Engineering, Fuzzing, and penetration testing<br>→ Conformance testing of the security functions and implementation<br>→ Testing of the wireless harness under different conditions including end-to-end data gatewaying<br>→ Features and cybersecurity integration testing<br>→ Software and hardware integration testing |

| Technical Process | Phase Impact |
|---|---|
| **Production, Operation, Maintenance and Updates** | → Refined security assessment<br>→ Personnel Training and cybersecurity culture<br>→ Diagnostics over the wireless harness and the impact on the tools and protocols used.<br>→ Software updates process such as Over-the-air or over-the-wireless-harness updates<br>→ Fleet monitoring for security incidents and incidents response<br>→ Pairing credentials handling and management |
| **Disposal** | → Disposal procedure and strategy<br>→ Secure disposal of the system and the data it contains |

### 3.3.5 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.

# Chapter 4 Tractor-Trailer Pairing Over a Wireless Harness[3]

When using a wireless harness between the truck and the trailer for intra-communication, a secure pairing mechanism is needed. Each device will be authenticated before gaining access to the wireless harness network and before the start of exchanging data. A truck is required to be able to pair and hitch to many trailers in the fleet, from different vendors and in various locations. Figure 4.1 shows the different cases of truck-trailer wireless pairing methods and security.

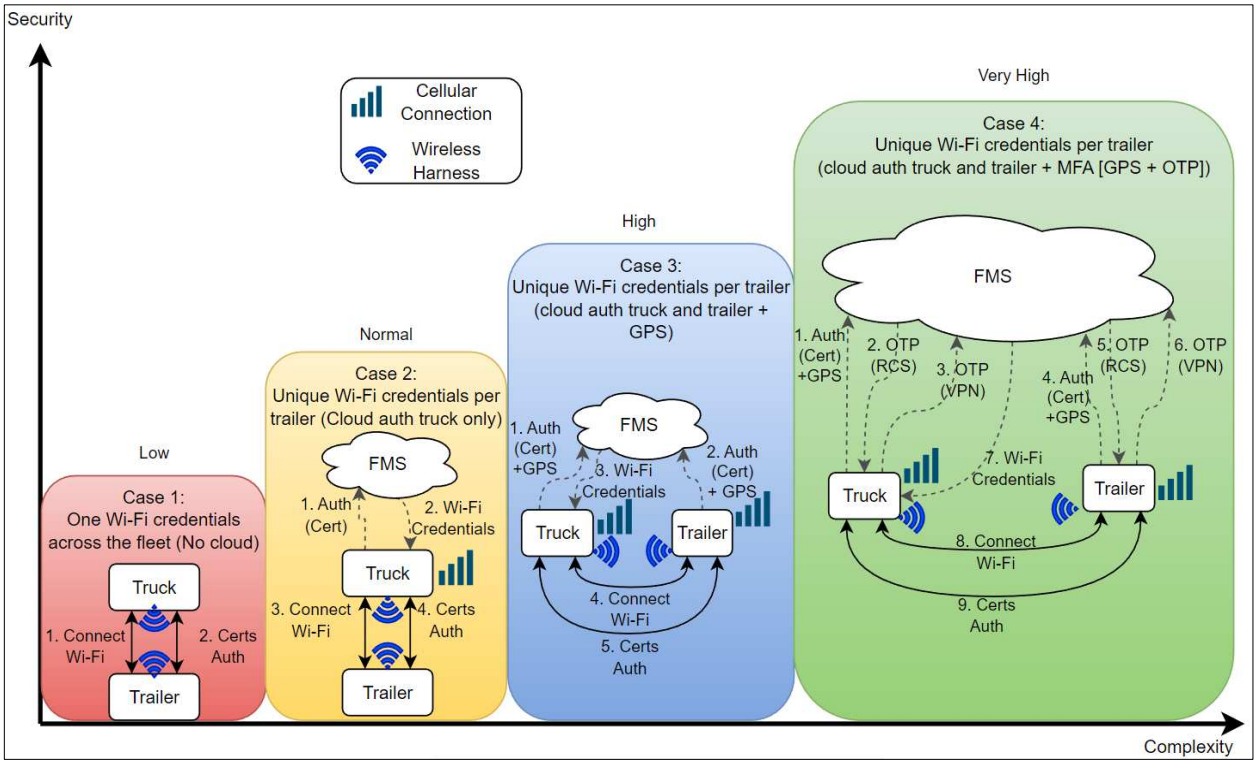


**Figure 4.1:** Different cases of authentication before pairing a truck with a trailer over a wireless medium.

[3] Contains content from [105]

It is assumed that the ECUs have been provisioned with certificates signed by a Certificate Authority (CA) private key and each ECU will use the CA's public key to authenticate the certificate during certificate exchange. It's also assumed that the truck is able to locate and identify the correct trailer using common methods such as QR code scanning to identify the trailer number. The trailer serves as wireless harness access point (i.e., Wi-Fi access point) and the truck will be the client which requires the trailer to be physically coupled with the truck and powered on. **Case 1** assumes there is always no FMS connection which uses the same wireless harness access credentials for all of the trailers due to the limited storage and complexity associated with unique credentials per trailer in the case of large fleets. A truck cannot store all of the unique credentials as discussed in challenge two. This makes case 1 less complex and less secure. If the Wi-Fi credentials for one trailer are exposed, the entire fleet would be compromised. Credentials update will require physical access to the truck and all of the trailers. Full communication between the truck and the trailer in case 1 requires the Wi-Fi credentials and certificate-based authentication between the two ECUs. Unlike case 1, **case 2** will have unique Wi-Fi access credentials per trailer and it assumes the availability of the TCU in the truck side only to connect to FMS. Initially, the truck will connect to FMS to get authenticated by presenting its certificate, and after being approved, FMS will send the wireless harness network access credentials and the truck will be able to join the same network as the trailer. The truck and the trailer can then exchange certificates to authenticate each other. **Case 3**, both of the truck and the trailer have a TCU which will allow them to connect to FMS as part of the authentication process before pairing. Each of the truck and the trailer connect to FMS and present their certificate and GPS location, and if both are approved with GPS coordinates matching, the truck will get the Wi-Fi credentials to connect to the

wireless harness network. **Case 4** is similar to case 3 with an additional layer of authentication. A one-time-passcode (OTP) being sent to each TCU over a different communication channel such as Rich Communication Services (RCS) which offers data encryption. After the TCU receives the OTP, it can respond to FMS over the cellular connection (e.g., VPN). This method could provide more security but at the same time it is more complex and has high dependency on the cloud connection. The pairing process is expected to occur in a controlled environment such as trailer pickup or delivery yards, so the cellular connection will not be needed all the time and expected to be available. Another step could be added to case 4 to change or update the trailer's Wi-Fi access credentials upon pairing request and FMS will share the updated credentials with the truck.

## 4.1 The Impact on The System Lifecycle When a Wireless Interface Is Used

The current trailer ABS ECU uses wired communication only and does not have the telematics functionality nor the integrated wireless harness. Adding the wireless harness and telematics to the trailer ABS will bring a new design and would require new design considerations, cybersecurity measures, and development process. Additionally, it will have an impact on the different phases in the life cycle compared to the PLC-based legacy ECU. In this section, we will discuss the impact of the new design on the different system life-cycle technical processes as defined in ISO/IEC/IEEE 15288:2015, INCOSE [90], SAE J3061® [91] and the Vee Model.

## 4.2 Concept of Operation and Requirements

The mission requires enabling the autonomous tractor to drive in reverse with a coupled trailer with the goal of achieving full automation of the end-to-end autonomous tractors' operation and reduction or elimination of human intervention. This includes coupling, uncoupling, pairing, and unpairing the trailer while also considering cybersecurity. Stakeholders in the case of L4 and L5 trucks include but are not limited to tractor Original Equipment Manufacturer (OEM), autonomy software and hardware OEM, trailer OEM, the autonomous tractor customer or end user, and IT. To ensure proper operation, integration, and security of the new concept and design, the needs and requirements of these stakeholders must be considered. An example would be the compatibility of the tractor with distinct types of trailers regardless of their OEMs. To ensure secure pairing, the tractor and trailer must have a mutual root of trust, which can be established by aligning and agreeing to use and share a cloud-based Fleet Management System (FMS), for instance.

To meet the new needs while ensuring cybersecurity, additional requirements must be defined. Due to the integration of the wireless harness and the telematics to the trailer's ABS, a modern design and cybersecurity risk assessment are necessary. This involves identifying and analyzing the new threats and vulnerabilities that will face the truck-trailer system through the cellular connection or the wireless harness interfaces. The new truck-trailer cybersecurity requirements include secure hardware, software, and IT infrastructure, management of access and identities of trucks and trailers within the fleet including keys management. Moreover, security requirements must be established

for ECU-cloud and intra-communication, security of the wireless network, and identification of the new threats and vulnerabilities that the new system adds. There are also the requirements of distributed development to consider since multiple vendors and OEMs will be involved such as tractor OEM, trailer OEM, IT, and autonomy ECUs OEMs. Finally, automated pairing and authentication requirements must be met before establishing a communication channel.

Cybersecurity implementation needs to take the overall system requirements into account such as Key Performance Indicators (KPIs) such as reliability, bandwidth, and latency for the wireless harness and the cellular connection. There is also vehicle integration to support tractor platform communication channels (e.g., J1939, PLC, CAN FD, or Ethernet) while only using the wireless harness to communicate with the tractor. Interoperability of the trailer with different types of tractors, regardless of their OEMs, is critical due to the use of a wireless medium between the tractor and the trailer. The use of a wireless harness will bring new regulatory requirements and the ECU certification process. Finally, trade-off and cost-benefit analysis must be conducted to select the optimal solution.

## 4.3 System Architecture, Implementation, and Integration

The architecture of the new system must be cybersecurity-centered and have multi-layer protection such as the ECU itself, intra-communication (ECU-to-ECU), and cloud communication. This requires new architecture for the software, hardware, and IT infrastructure of the commercial vehicles including secure hardware implementation,

software coding, and cloud infrastructure. The new system introduces significant changes (i.e., the truck-trailer-cloud communications), complete system specification, and training are required for users at various levels to enable them to implement, operate, and maintain the system. Due to the lack of security standardization for commercial vehicles, implementation and integration need to be compatible with trucks and tractors from different OEMs which is a challenge.

Secure implementation within the autonomous truck and trailer ECUs needs to cover different levels of security as shown in Fig. 4. From an ECU perspective, security features include secure boot, Hardware Secure Module (HSM), ECU firewalling, Deep Packet Inspection (DPI), Two Factor Authentication (2FA, e.g., GPS and OTP), FMS-based Access Control List updates, intrusion detection, prevention and reporting, secure in-vehicle and cloud communications, network segregation and forensic logs. Secure implementation of the wireless harness involves several measures to enhance safety and prevent unauthorized access. These measures include limiting the wireless network range to restrict physical access beyond the truck and trailer wireless transceivers, providing temporary network credentials that expire after a defined period, employing cloud-based authentication of network clients, and using two-factor authentication (2FA). Additionally, implementing the latest security technology for the wireless harness interface, such as Wi-Fi Protected Access 3 (WPA3), and following best practices for securing a wireless network further strengthens the overall security.

## 4.4 Testing

Due to the new features and wireless interfaces introduced in the ABS, new test procedures will be added with an emphasis on cybersecurity testing. Design Verification Plan (DVP) is needed to include the wireless harness, telematics, and the new cybersecurity features. The new DVP includes activities such as scanning for software and hardware vulnerabilities, reverse engineering, fuzzing, and penetration testing. Additionally, Testing of the system and features implementation and conformance to the cybersecurity standards. With the cybersecurity implementation enabled, the system needs to be tested at different levels starting with bench testing to in-vehicle testing for full integration. A new DVP is needed to include test plans for the wireless harness when integrated and used in the field under different conditions, environments, and vehicle maneuvers to ensure robustness and reliability. Additionally, testing failure modes are defined in the technical risk assessment, such as testing under interference and other noise factors that would impact the tractor-trailer wireless communication. To ensure conformance with safety and regulatory standards when a wireless harness and cellular antennas are used, compliance and certification will need to be conducted for the truck and the trailer ECUs.

## 4.5 Production, Operation, Maintenance, and Updates

Since the truck is communicating with the trailer over a wireless medium and the pairing is being automated, it becomes critical to clearly define how the pairing

credentials, keys, certificates, and pairing authentication process is being handled including storage, adding, revocation, and renewal of keys and certificates. During mass production, for example, truck and trailer ECUs will need to be provisioned during the end-of-line (EOL) with a certificate signed by the CA private key to be used as part of the pairing authentication process. Additionally, the Wi-Fi access point will be provisioned with the network access credentials.

Due to the new methods and the unusual functionalities added to the trailer ECU compared to the legacy wired ECU, deploying the new trailer ECU will require personnel training and fostering a cybersecurity culture. Fleet monitoring for cybersecurity incidents, response methods, and teams needs to be defined on several levels such as ECU reporting and response, cloud response, and actions. In addition to the designated response individuals. Using the intrusion detection algorithms and the TCU within the truck or the trailer will expedite the process of incident reporting and reduce the time taken to respond to the attack. For example, a denial-of-service attack on the wireless harness means there is a person present near the truck performing this attack due to the short range of the wireless harness.

Autonomous truck and trailer updates and diagnostics will be impacted due to replacing truck-trailer wired communication with a wireless medium which will change the physical access, tools, and protocols used for diagnostics for the trailer. Maintenance or software updates could be done through the wireless harness. For example, if IEEE802.11ad is used, Diagnostics over IP (DoIP) could be used instead of a physical connection which will require new tools to be used and new procedures to be followed.

Additionally, the telematics unit with the trailer ECU could be leveraged for over-the-air updates.

## 4.6 Disposal

At the end of the ECU lifecycle, it will contain the wireless harness credentials, keys, cloud access certificate, and confidential information stored. A new disposal process and strategy to securely dispose of the system and the data it contains is needed.

# Chapter 5 Named Data Networking[4]

Named data networking is a data-centric networking protocol that uses data packets and interest packets for communication where each data type has a name that is being used for communication instead of an Internet Protocol address (IP). The data packet contains the name of the data, the content, meta data such as freshness period, and the signature. Similarly, the interest packet contains the name of the data, metadata such as interest lifetime, and an optional signature. NDN Forwarding Daemon (NFD) [92] handles the routing and forwarding of the interests packets and data packets using the forwarding plane [93] based on the predefined network interfaces. As shown in Figure 5.1, let's say ECU1 is on the truck with NFD1 and ECU2 is on the trailer with NFD2. The application in ECU1 needs sensor data from the trailer that is named `/trailer/sensor1` so it generates an interest packet using that name. NFD1 checks the Content Store (CS) of ECU1 where the received data is cached, if no match, it checks for a similar interest packet in Pending Interest Table (PIT), if there is a match it adds the new interface to the table, if not, NFD1 checks in Forwarding Information Base (FIB) to identify the forwarding route for the interest packet based on the prefix of the name and then it will determine the next hop. The interest packet is delivered now to NFD2 in ECU2 where it checks CS2 for the data that matches the new interest packet, if no match, it will check PIT2, and if no match it will add a pending interest packet to the table. NFD2 will check FIB2 for the route to determine the next hop, and the interest packet will be

[4] Contains content from [104] [105] [106]

forwarded to ECU2 application to get the data packet as shown in0, otherwise, it will forward it to the next node as defined in FIB2. The app can validate the interest packet using the validation key and check other parameters such as the freshness period of the interest.

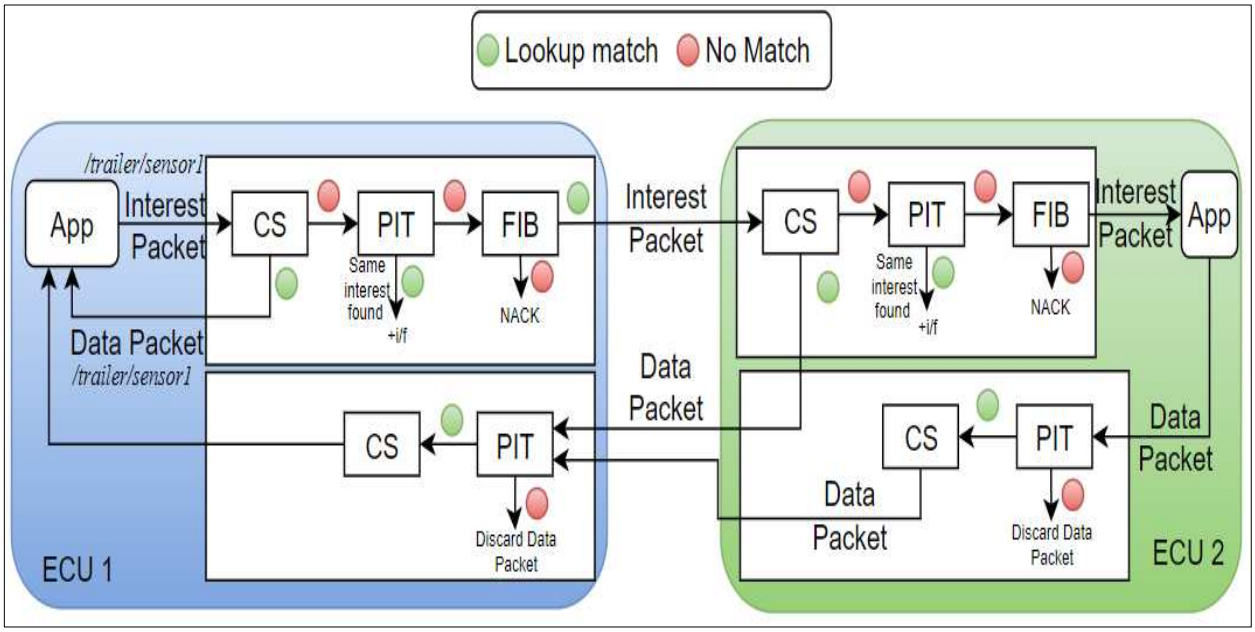


**Figure 5.1:** Interest packet and data packet example communication when ECU1 is requesting data from ECU2 over NDN.

The Application within ECU2 will respond with the data packet so NFD2 will check if the interest is still valid within PIT2, if so, it can cache the data within CS2 before forwarding the data packet to ECU1. Once the data packet is forwarded to NFD1, it will check PIT1, if there is a match, it will cache the data in CS1 and route the data to the application or as defined in FIB1. The data packet will be signed using ECU2, the producer, private key, and ECU1, the consumer, can validate the data packet using the validation or the public key. Similarly, interest packets could be signed and validated the same way assuming ECU1 and ECU2 did the key exchange for authentication.

The usage of a wireless harness will increase the need for additional cybersecurity measures and security by design which makes NDN a strong candidate for this type of architecture when wireless interfaces are used within an ECU since it supports interest and data packets security by default such as packet signing or encryption.

In-vehicle networks comprise many ECUs that are connected to a gateway directly or through another ECU. Using unoptimized NDN scheme in an automotive network, for example as shown Figure 5.2, may introduce delays in receiving data packets. This is due to the number of lookups in CS, PIT, and FIB within each node between the origin of the interest packet and the retrieval location of the data packets. While caching helps reduce the need to travel the full path to the original data generator, NDN needs to be optimized for automotive applications to reduce latency and the load on the gateway.

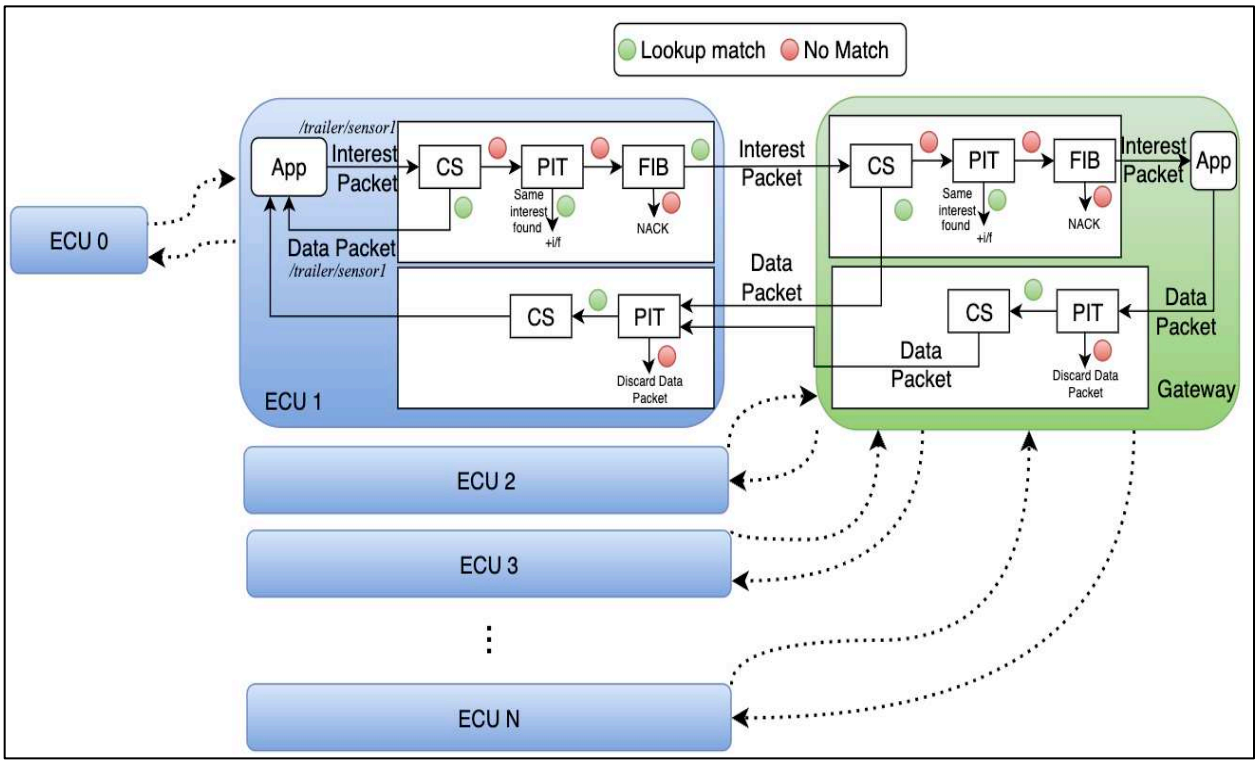


**Figure 5.2:** Example of multiple ECUs connections to the gateway directly or through another ECU

## 5.1 System Requirements

The overall requirements of the communication system between the truck and the trailer are shown in Table 5.1

**Table 5.1:** System requirements of the communication between the truck and the trailer

| ID | Requirement |
|---|---|
| **R1** | The system shall support automotive communication requirements |
| **R2** | The system shall be integrated with the existing platforms hardware |
| **R3** | The system shall be able to communicate with heterogeneous automotive networks simultaneously |
| **R4** | The system shall support data integrity, authenticity, and confidentiality |
| **R5** | The system shall support communication timing requirements such as CAN signals timing of 20 milliseconds |
| **R6** | The system shall support at least 1 gigabit bandwidth |
| **R7** | The wireless harness shall support automated pairing between trailer ECU and the tractor ECU or other authorized devices |
| **R8** | The wireless harness shall support diagnostics and software updates access |
| **R9** | The wireless harness shall have high reliability and stability like the physical connections |
| **R10** | The wireless harness shall be stable at normal driving conditions and maneuvers |

## 5.2 Data Management

Within NDN, different data is given different name such as `/trailer/sensor1`, `/trailer/sensor2`, `/trailer/J1939`, and `/trailer/CANFD`. NDN Data packets are 8800 bytes in size which allows for a bigger payload. The payload of the data packets could be managed further to transmit different data simultaneously such as multiple CAN frames or sensors data with CAN frames attached to it as an annotation. The trailer ECU will collect the data from different sources, format them based on their standard specification and the intended destination at the tractor side, construct them using a software multiplexer in one construct $P$ as follows:

$$P = (c,\ s,\ A,\ a) \tag{5}$$

$P$ is the hybrid construct that contains $m$ frames of heterogenous vehicle network protocols or sensor bytes, $c$ is the total size of $P$, $s$ = timestamp for the construct $P$, $A$ is the hybrid payload that contains automotive protocol frames, sensor bytes, or any type of data that will be transmitted to truck communication buses such as J1939, CAN FD, radar CAN and Ethernet, or LiDAR data bytes and $a$ is an authentication tag, if not included by default (i.e., other protocols), that results from the encryption of $c,\ s$ and $A$.

$$A = [r_i \quad t_i \quad p_i \quad l_i \quad f_i] \tag{6}$$

$r$ is the transmission priority number assigned to each protocol or data frame, $t$ is timestamp for each data type, $p$ is the protocol definition (e.g., $p_0$ = Sensor data bytes, $p_1$ = J1939 frame, $p_1$ = CAN FD frame, $p_2$ = CAN FD frame and $p_m$ is any other automotive data or protocol that could be packed as a part of $A$), $l$ = total length of each data type

(e.g., number of bytes of the sensor data or the CAN frame), $f$ is the actual CAN or sensors bytes that will be transmitted to the AT communication bus or to the AT ECUs and $i$ is the index for each unique data frame, $i = [0,1,\cdots,m]$, where $m$ is the maximum number of frames within $A$.

$$A = \begin{bmatrix} r_0 & t_0 & p_0 & l_0 & f_0 \\ r_1 & t_1 & p_1 & l_1 & f_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ r_m & t_m & p_m & l_m & f_m \end{bmatrix} \tag{7}$$

$A$ could contain multiple data types such as sensor data ($i = 0$), LiDAR data packet ($i = 1$) along with CAN FD frame 1 ($i = 2$), CAN FD frame 2 ($i = 3$), J1939 CAN frame ($i = 4 = m$) frames or any other data type. The size of $A$ will vary depending on the used networking protocol and the maximum allowed payload, in the case of NDN, the maximum size for the data packet is 8800 bytes.

A different $P$ construct could be used for each data type. For example, $P_v$ for one video frame ($i = m = 0$ in $A$), $P_l$ for a LiDAR data packet ($i = m = 0$ in $A$) and $P_s$ for AT serial bus data which will contain multiple frames, first CAN FD frame is for AT CAN FD channel 1 ($i = 0$), second CAN FD frame is for AT CAN FD channel 2 ($i = 1$) and third CAN frame is for the AT J1939 bus ($i = m = 3$).

## 5.3 Test And Evaluation

In this section, NDN is compared with DDS when used over a wireless medium and automotive-like data is being transmitted.

### 5.3.1 Testbed

The test setup includes a PC that functions as the data producer (e.g., trailer ECU) communicating over a Wi-Fi connection with three receivers via a router. The receivers are wired to the router with Ethernet cable. The receivers (e.g., truck ECUs) are Raspberry Pis (RPi) running Ubuntu Server 21.10 OS. The Wi-Fi network is 802.11ac, 5.745GHz, transmission power of 22 dBm and signal level of -30 dBm. Using the 60GHz Wi-Fi on a trailer is part of the future work. 802.11ac was used for networking evaluation and Wi-Fi link stability when used in this setup and data types.

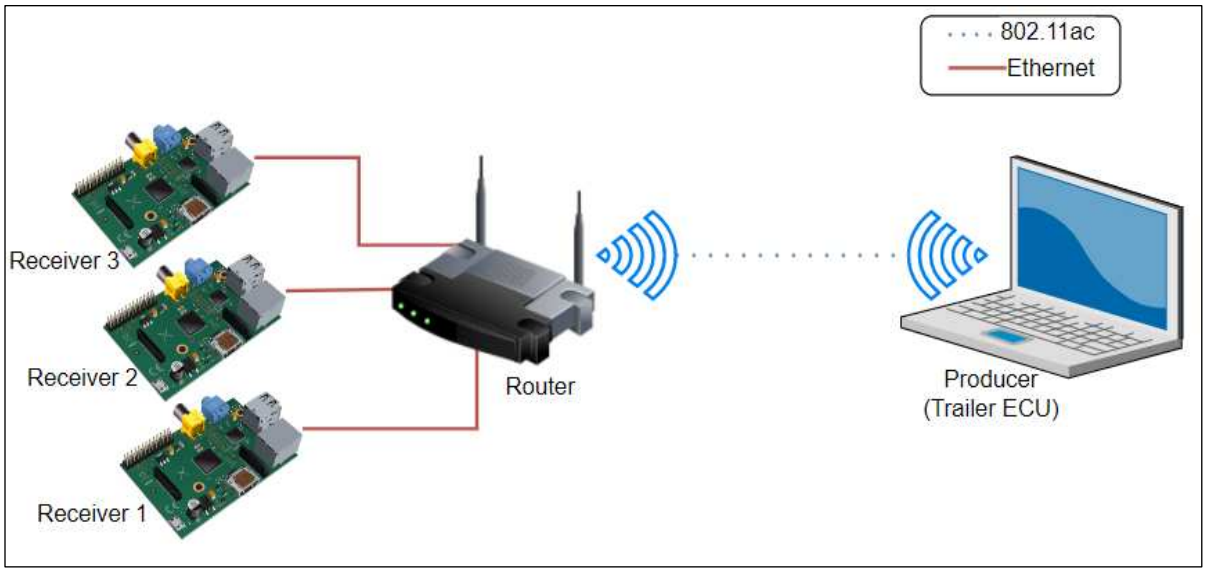


**Figure 5.3:** Testbed used for evaluating the networking protocols.

### 5.3.2 Test Configuration and Method

The PC is hosting three producers' scripts, one for each data type. Assuming we have three different types of data as follows: lidar data, cam data and CAN data. The lidar data is 1600 bytes transmitted every 5 milliseconds (*ms*), the CAN data is 160 bytes transmitted every 8 *ms* and the cam data is 4000 bytes transmitted every 20 *ms*. Each

RPi is receiving only one data type hosting one receiving script. In DDS, three topics were created and within each there is string data type, and each receiver can subscribe to one data type.

### NDN configuration

Each data type is given a name as follows: `/trailer/cam, /trailer/lidar, /trailer/can`. The test requires defining interfaces (faces) between the producer and the consumers as shown in Table 5.2

**Table 5.2:** faces definition used in the test

| Node | Face Address | Route |
|---|---|---|
| **PC** | Face1 to RPi1: udp://192.168.10.11 | */trailer/lidar* via face1 |
| | Face2 to RPi2: udp://192.168.10.12 | */trailer/can* via face2 |
| | Face3 to RPi3: udp://192.168.10.13 | */trailer/cam* via face3 |
| **RPi1** | Face1 to PC: udp://192.168.10.33 | */trailer/lidar* via face1 |
| **RPi2** | Face1 to PC: udp://192.168.10.33 | */trailer/can* via face1 |
| **RPi3** | Face1 to PC: udp://192.168.10.33 | */trailer/cam* via face1 |

### 5.3.3 Test Method

DDS Real-Time Publisher-Subscriber (RTPS), NDN over Transmission Control Protocol (TCP) and NDN over User Datagram Protocol (UDP) were tested separately using the testbed. DDS was limited to a string variable only as the payload where NDN was tested with serializing bytes, referred to as (B) as well as a string variable, referred to as (S). In the case of the string variable, a string variable is generated at the beginning of the test and then randomized for each data packet transmission and the random bytes were generated with each data packet transmission. In the case of NDN, each receiver will be simultaneously sending an interest packet with a different data name to the producer to get a new data packet. Similarly, DDS subscribers get the data published simultaneously.

## 5.4 Test Results and Discussion

The two performance parameters captured were latency and core CPU consumption. Latency was calculated as the time difference between each received packet at each receiver. CPU utilization percentage was captured at the data producer and each of the consumers as well. The dashed red line in the latency results is periodic transmission time or the hardcoded delay. Wi-Fi Encryption and data packets signing are not in the scope of this test.

### 5.4.1 Latency

Latency of received CAN packets looked overall similar between all the approaches as shown in Figure 5.4 with DDS RTPS slightly better performance.

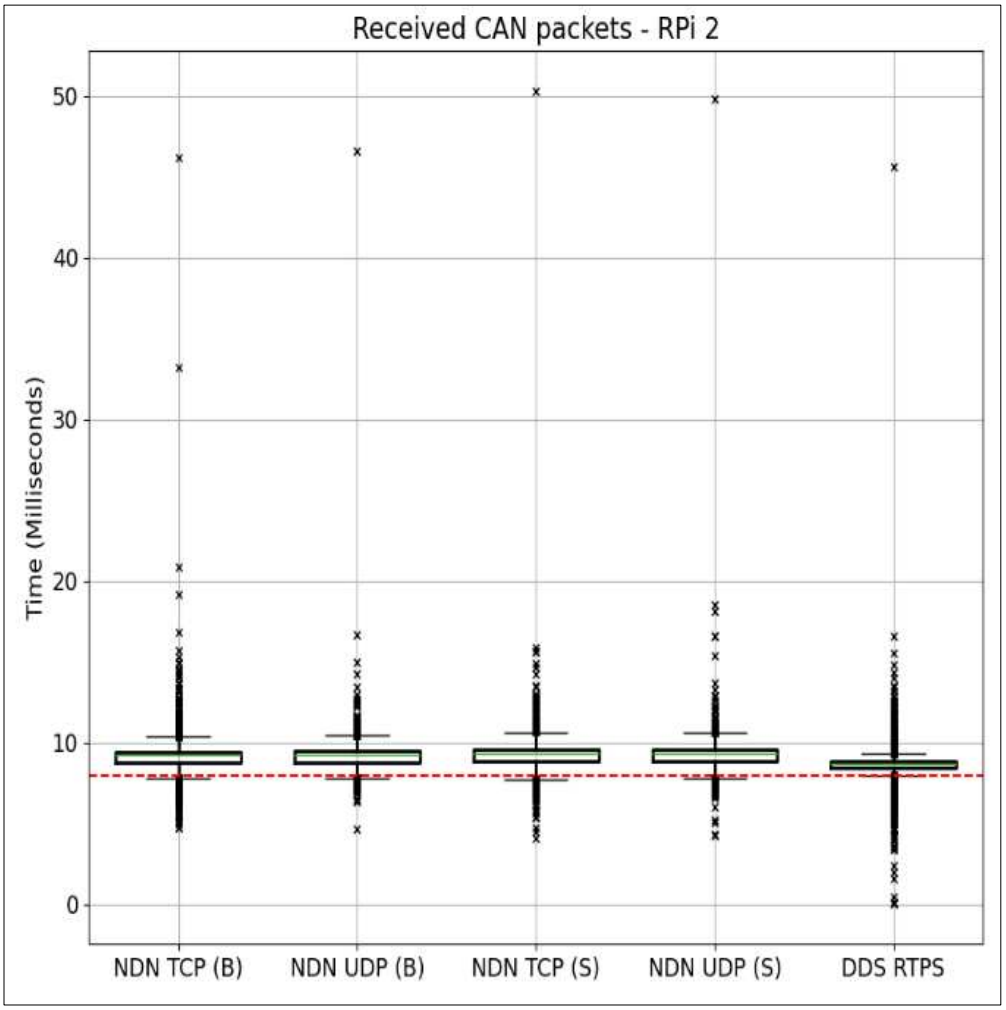


**Figure 5.4:** Latency comparison for */trailer/can* data at the receiver

For the latency when lidar packets were transmitted, it's an increased load of 1600 bytes so the difference in performance started to appear especially when serializing bytes compared to serializing strings as shown in Figure 5.5. NDN (B) is performing better due to the less encoding that needs to be done on the payload. NDN (S) and DDS used strings and they had similar performance due to the additional encoding done at the producer and the consumer in both cases. However, DDS used JSON encoding where NDN used Type-Length-Value (TLV). JSON is more efficient for strings when compared with TLV with strings since TLV encodes the data in binary format, therefore, more bytes will be

required when encoding strings in the case of NDN and it will cause the latency performance of the application to degrade when serializing strings.

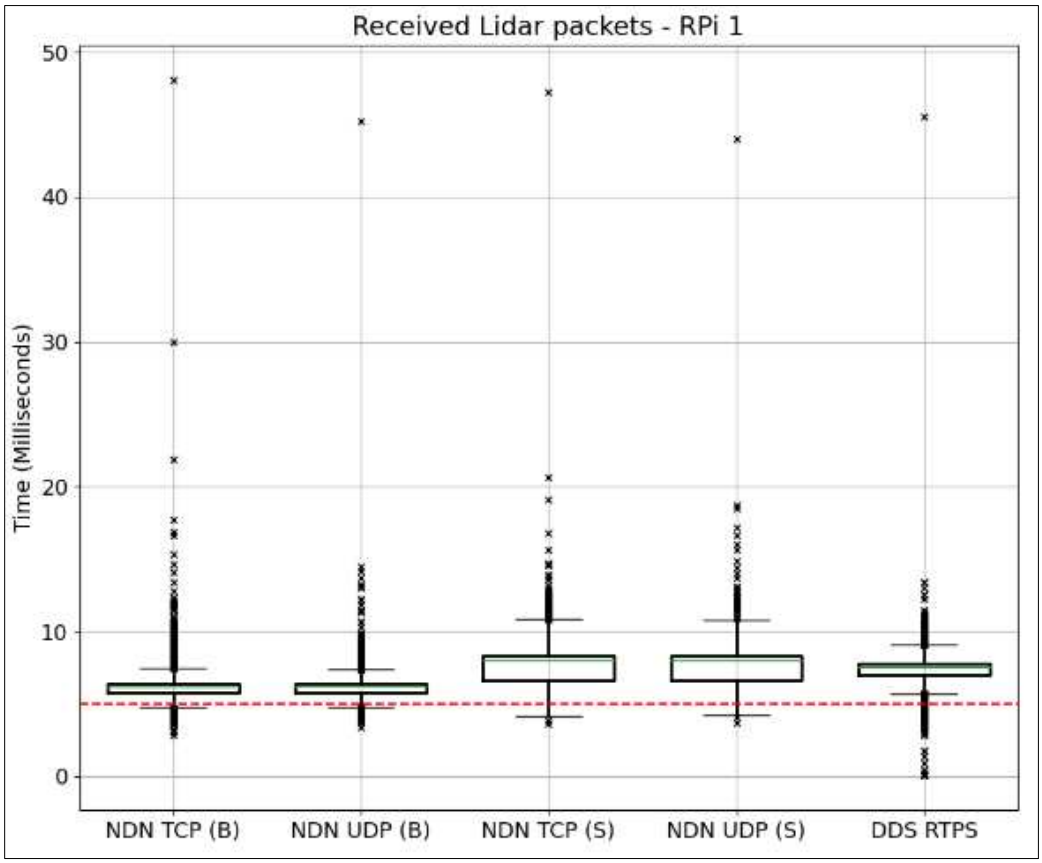


**Figure 5.5:** Latency comparison for */trailer/lidar* data at the receiver

Similarly, for `/trailer/cam`, NDN and DDS serializing strings show similar performance showing similar mean latency with DDS performing slightly better. NDN serializing bytes is shown to be the most efficient with bigger payload.

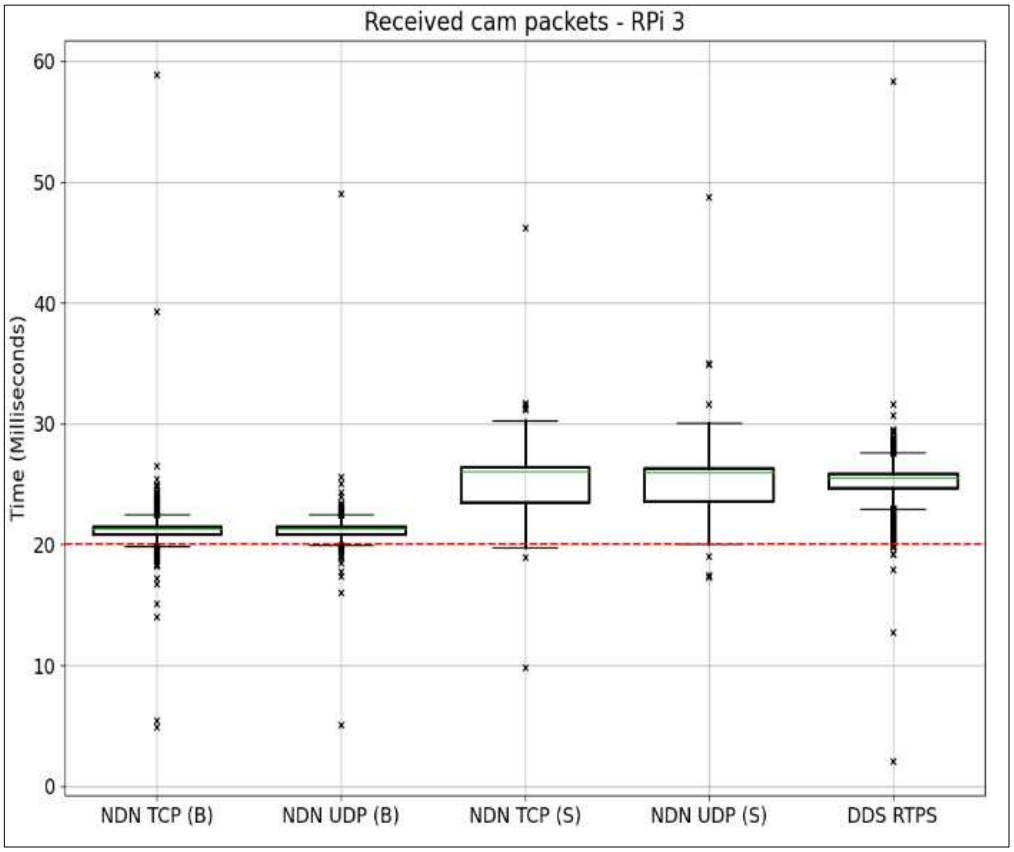


**Figure 5.6:** Latency comparison for */trailer/cam* data at the receiver

## 5.4.2 Core CPU Utilization

Core CPU utilization percentage was recorded at the producer for each producing script and on each receiver. NFD was also added for NDN at each of the producer and the receiver.

### CPU Utilization at The Transmitter

There was no high difference between the CPU utilization percentage when comparing the scripts of each data type as shown in Figure 5.7, for example, lidar over NDN TCP is 2-3% higher than Lidar over DDS. Overall, they have similar utilization and tolerable differences. It was also shown that NFD had a low CPU utilization in both cases.

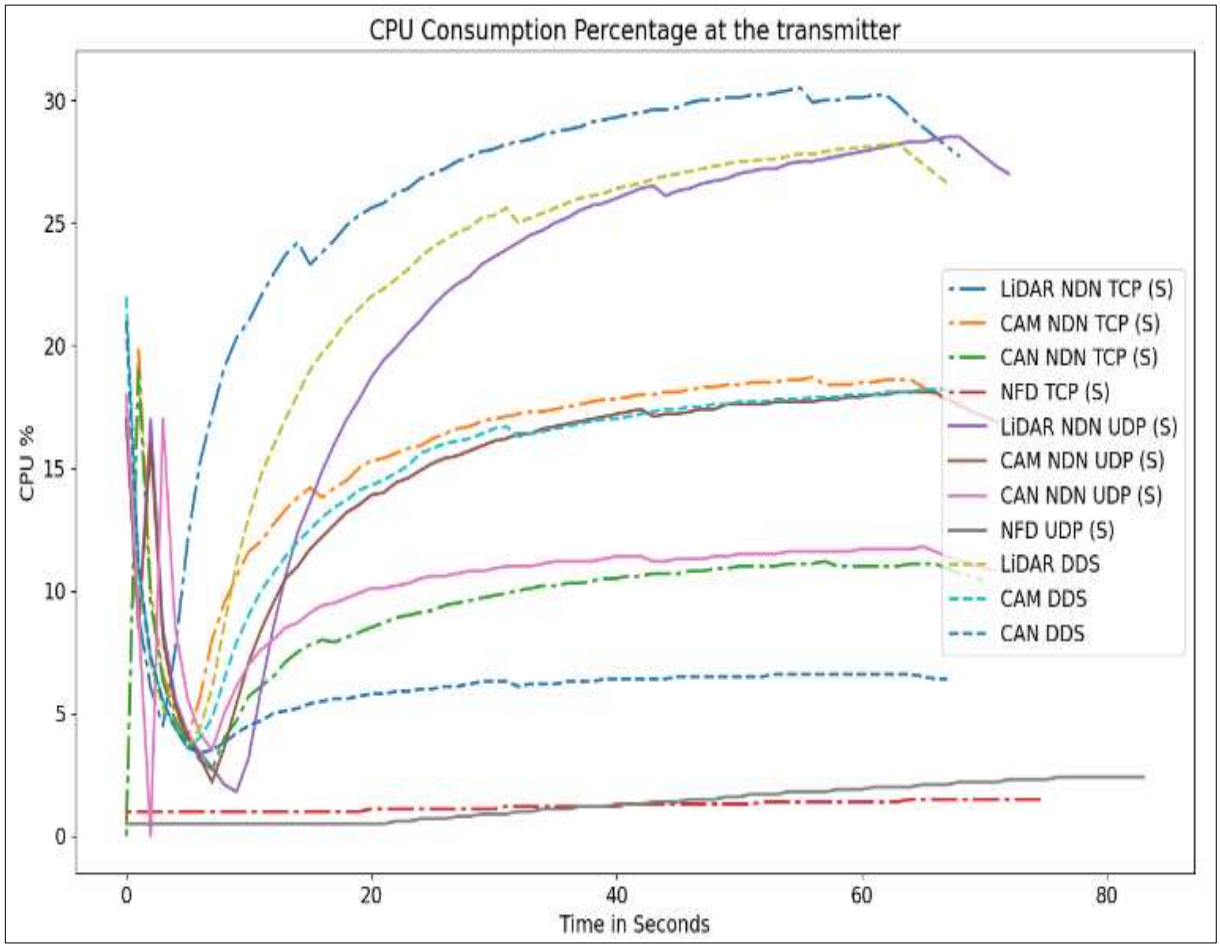


**Figure 5.7:** CPU Utilization percentage at the producer for each script

### CPU Utilization at The Receiver

Figure 5.8 shows the CPU utilization percentage for each script at each receiver. Overall, the three networking approaches had no high difference in CPU utilization, however, NDN TCP had a slightly higher utilization due to the continuous transmission of interest packets to the producer. In the case of the NDN over TCP, its response with an ACK in addition to the interest packet.

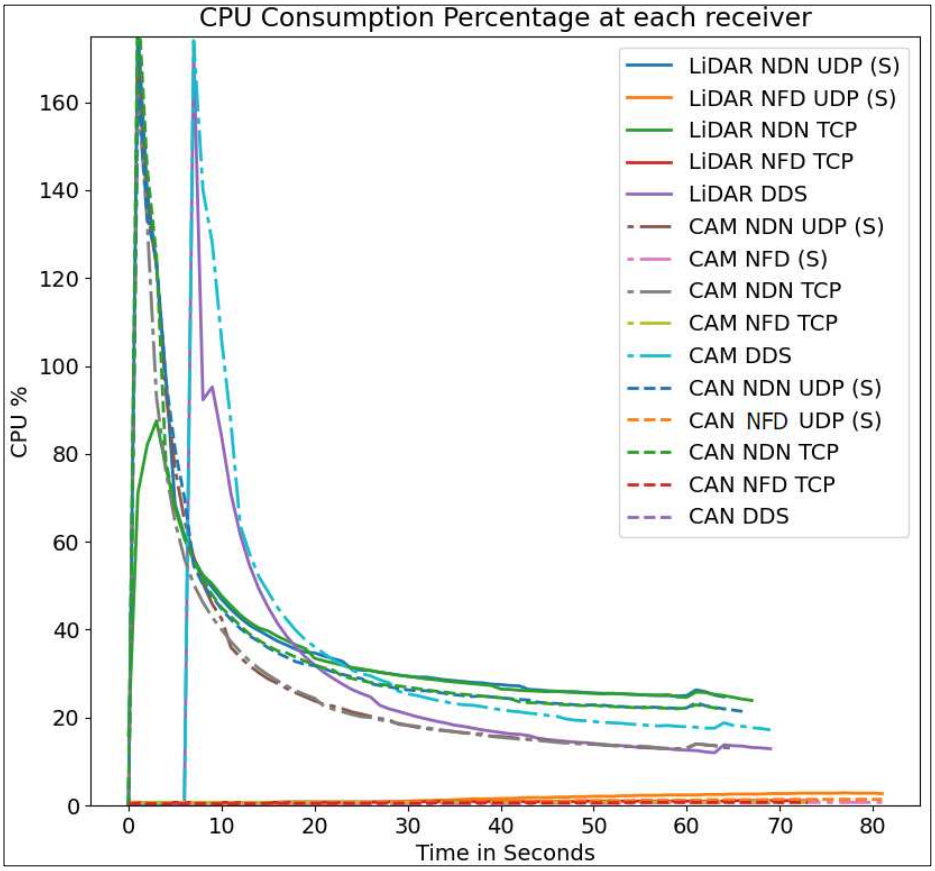


**Figure 5.8:** CPU Utilization percentage for each script at each receiver (RPi)

Within this setup, NDN had a similar performance or slightly less when compared to a well-established protocol such as DDS when serializing strings over Wi-Fi. Additionally, the test did not show abnormal number of latency spikes or Wi-Fi lagging when sending data packets at that fast rate and the number of latency outliers is limited. NDN also is shown to be efficient when used to serialize bytes over Wi-Fi and Ethernet especially for bigger packets such as the case above of 1600 bytes and 4000 bytes.

## 5.5 Secure Communication Using Named Data Networking

The security challenges discussed here require communication architecture that is secure by design. This will mitigate attacks on the communication links (i.e., Ethernet or a wireless harness) between the truck and the trailer or between the TCU to the cloud. Traditional automotive networking approaches are based on IP and are not secure by design. They require additional security layers and plugins which leads to a higher complexity and cost in the design and the implementation [94]. This is due to the different solutions needed for different communication types such as vehicle intra-communication or vehicle to cloud. Additionally, the various operating systems and physical communication protocols are utilized within one self-driving vehicle. For example, Message Queuing Telemetry Transport (MQTT) is used for TCU-to-cloud communication but it's not secure by itself and it requires Transport Layer Security (TLS). TCU-to-cloud communication for provisioning or certificate-based authentication could be done over Hypertext Transfer Protocol (HTTP) and TLS. Data Distribution Service (DDS) could be used to transmit sensors data, and since it is not secure by default, it requires an additional security plugin. Finally, SOME/IP could be used for CAN over IP which requires an additional security layer such as Secure Onboard Communication (SecOC). Table 5.3 shows the common automotive security protocols and their associated features [95] [96].

**Table 5.3:** Common security protocols used in the automotive industry and supported features.

| Protocol | Standard | Layer | Authentication | Encryption | Multicast | Note |
|---|---|---|---|---|---|---|
| TLS | IETF RFC 5246 | 4 | Yes | Yes | No | Mainly for TCP but also supports UDP |
| MACsec | IEEE 802.1AE | 2 | Yes | Yes | Yes | Keys are required at each receiving/forwarding ECU. Does not secure L3. |
| SecOC | AUTOSAR | 2 | Yes | No, but capable | Yes | CAN/Ethernet<br><br>(AUTOSAR-to-AUTOSAR) |
| IPSec ESP | IETF RFC 4303 | 3 | Yes | Yes | No, based on AUTOSAR implementation | Encapsulating Security Payload. Impractical for vehicle networks.<br><br>(VPN, Security Association) |

Multicast is a key feature in automotive networking and communication to allow multiple ECUs to receive the data from a gateway or the transmitting ECU simultaneously. It will be a key point in making the decision while selecting the security protocol. For example, TLS and Internet Protocol Security Encapsulating Security Payload (IPSec ESP) do not support multicast based on automotive implementation

therefore cannot be used when multicast is required to transfer sensors data. SecOC supports multicast, but it requires AUTomotive Open System Architecture (AUTOSAR) on both of the receiver and the transmitter which makes it incompatible with other operating systems by default. IPSec is impractical when using multicast due to the security association overhead with an increased number of ECUs on the IPSec-protected network where it requires a unique communication link with unique keys and security between each transmitter and receiver. The current solutions are focused on the security of a specific layer in the Open Systems Interconnection (OSI) model. For example, Media Access Control Security (MACsec) secures the second layer of the OSI model but does not secure level 3 and will require additional security solution to protect the data in layer 3.

Named Data Networking (NDN) is a promising networking protocol that is content-centric and supports security by design such as data signing and encryption [97]. In addition, it supports key automotive networking features such as multicast. It uses names for data communication instead of an IP address. In the context of automotive communications, NDN uses interest packets which are sent by the consumer ECU to request data. Data packets are sent by the producer ECU with the necessary content as a response to the interest packet that carries the same name. Names for data types such as CAN and sensors data to a consumer ECU or telemetry data to a consumer application in the cloud-based FMS. The default structure of data packets comprises the name of the data, the content or the payload, metadata such as freshness period and a required packet signature. Similarly, interest packet structure comprises a data name, metadata such as the interest lifetime, and an optional signature. The data packet and the interest packet follow specific paths in the network based on the interface defined and the names

associated with it. The consumer ECU will only accept data that matches the metadata of the interest packet is sent such as the freshness period, which makes replay attacks more difficult.

Data names could be /trailer/ECU/canfd/, /trailer/ECU/j1939/, /trailer/ECU/cameraframes/, /trailer/ECU/sensors/, /truck/ECU/sensorfusion/, /truck/gateway/canfdbus/, /truck/gateway/telemetry, or /fms/authorization/. NDN is also capable of generating and managing keys and assigning a different key to each data name if necessary. Each data name could have its own signing key so a signed data packet could look like /trailer/ECU/sensors/lidardata/timestamp/key/key-id. This allows the consumer ECU to use the corresponding validation key to authenticate and check the integrity of the data packet [98]. NDN focuses directly on the security and integrity of the data packet itself rather than the security of the communication link between devices. NDN also uses names for keys and certificates using a hierarchical naming scheme that reflects their properties and attributes. The name will be unique to easily identify the key or certificate, which could be used as part of the ECU provisioning during the end of line process. As part of the EOL process, an ECU could be provisioned with a temporary certificate to allow it to connect with the cloud, in addition to generating a private and a public key following NDN naming scheme. It will allow the ECU to get a CA-signed certificate for authentication with other ECUs on the vehicle during operation. Each NDN node (e.g., ECU) should have a corresponding identity (i.e., namespace) on the vehicle platform and the corresponding certificate.

NDNCERT is a Certificate Management Protocol that enables secure certificate management in Named Data Networking (NDN) networks such as NDN-based ECU-to-ECU or TCU-to-cloud communication. It provides a robust and flexible framework for managing digital certificates. NDNCERT is an intermediary between the vehicle ECUs and the CA to get the corresponding certificates based on the ECU namespaces that each ECU will use to get authenticated by other ECUs on the network. NDNCERT Enables secure certificate management in Named Data Networking (NDN) networks such as NDN-based ECU-to-ECU or TCU-to-cloud communication. It enables automatic certificate management in NDN. Figure 5.9 shows an example of using NDNCERT in conjunction with securing NDN communication onboard and offboard links. NDNCERT could be used in the provisioning, pairing, authentication, revocation, and certificates management.

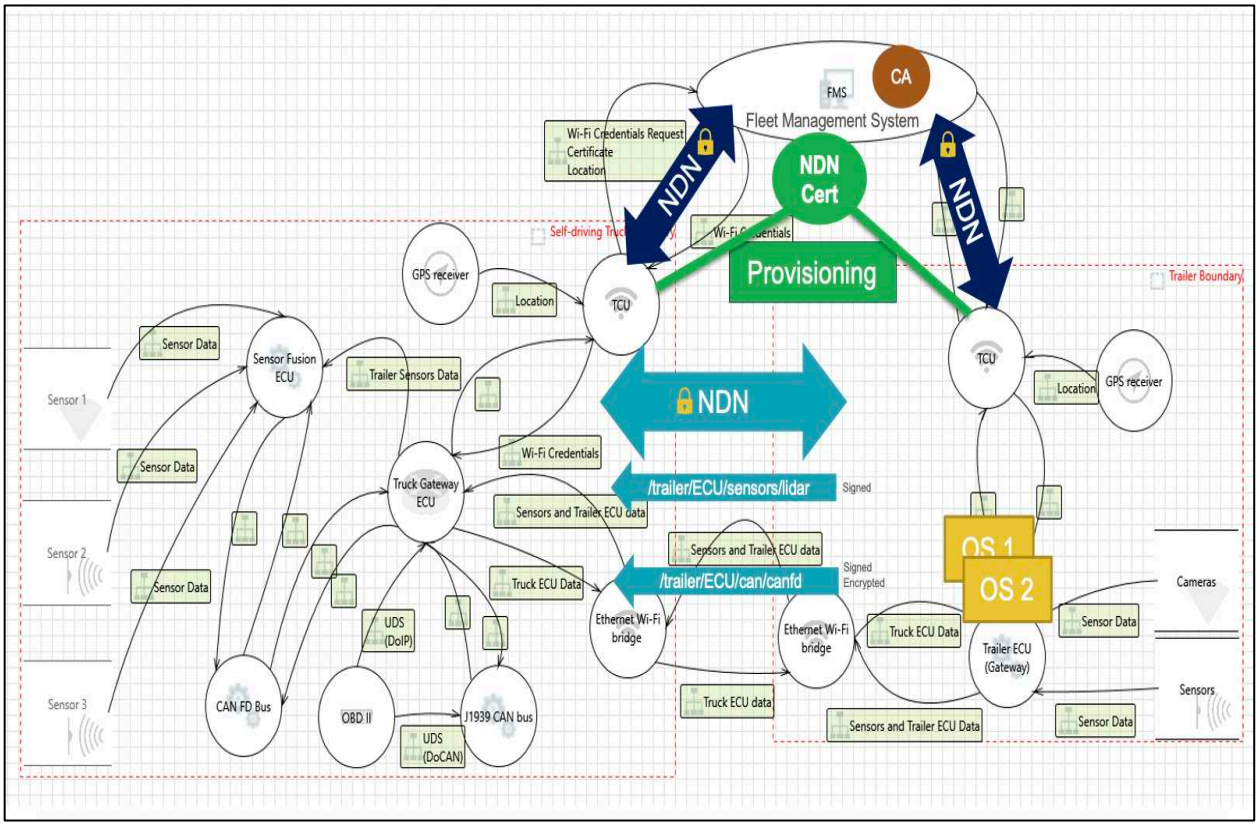


**Figure 5.9:** Example of how NDN is used to secure onboard and off-board communication and NDNCERT

NDN uses a name for the certificate instead of a serial number which reduces the complexities mentioned in challenge four. A certificate name could contain different identifiers such as OEM, and Vehicle Identification Numbers (VINs) to ease locating the certificate and checking its validity instead of looking up the database that contains all the possible certificates. For example, a certificate name for the truck is `/OEMX/truck/VIN/gatewayECU/KEY/Key-id1/v1`. As for the trailer, a certificate used for ECU-to-ECU authentication is `/OEMY/trailer/VIN/ABS/KEY/key-id1/v3`. Another certificate for wireless harness access is: `/OEMY/trailer/VIN/ABS/wifi/KEY/key-id2/v1`. In the case of using a certificate serial number, OCSP will be used to verify the revocation status. The CA will look up its internal databases, which contain all fleet certificates, to verify the status of the requested

certificate using the serial number. A certificate name could be used to save lookup time. A certificate name includes the identity of the vehicle (i.e., VIN) and the device (e.g., ECU name) to be authenticated, so the cloud can look up that particular device only and not the entire fleet database, CRL, or CTL.

NDN Trust schema [99] is a set of rules to establish trust between different entities on the NDN network. The trust is established using cryptographic keys and certificates which are used for packet signing and authentication. It provides the data producers and consumers with an automatic way to select the corresponding validation or signing key by identifying the common prefix between the data name and the key name. In addition to providing mechanisms for key revocation or update. Additional security that the trust schema provides is the capability of a vehicle ECU trust anchor to sign other keys. For example, assuming we have three sensor types, and each has its own key, `/trailer/ECU/key/key-id_1` is the trust anchor that signs `/trailer/ECU/sensors/key/key-id_2` that covers the sensors domain in general, and the related communication and the second key signs `/trailer/ECU/sensors/lidar/key/key-id_3` which is limited to the lidar data packets only. This approach enhances security by assuring the integrity of keys used and limiting the impact in case one key gets leaked. This provides more granular control over access and use of various parts and data of the system.

## 5.6 Constituent Systems Communication

AV deployments are planned to be at scale nationwide or globally. The communication between the constituent systems becomes critical in terms of efficiency

and security. Inefficiencies in the communication may lead to undesired delays or vulnerabilities. In this section, we discuss constituent systems communication, a queuing model for cloud requests, and using named vehicle signals in communication. Named Data Networking (NDN) is presented as a communication protocol as a networking candidate with strong potential that could improve the on-board and off-board communication at scale. NDN is also compared to Scalable service-Oriented MiddlewarE over IP (SOME/IP). We previously presented the literature review for vehicle networking and security. NDN uses names for data packets and is secure by default, unlike common automotive protocols where additional layers of security or plug-ins are required. Security by design is one of the biggest advantages NDN brings to the communication between systems.

## 5.7 NDN vs. SOME/IP

SOME/IP is a common automotive onboard communication protocol between ECUs. NDN is compared to SOME/IP when used in the same setup while the data producer is multicasting the data to multiple receivers.

### 5.7.1 Test Setup

A laptop acting as a multicast data producer that is connected to three receivers over an Ethernet switch as shown in Figure 5.10 Receivers 1 and 2 send requests to get new 8KB data from the producer every 20 milliseconds. Receiver 3 requests for new 8KB data every 10 milliseconds. In the case of NDN, it sends an interest packet and receives a data packet as a response. Security and caching are not in the scope of this test. SOME/IP

was tested using User Datagram Protocol (UDP) and NDN was tested using UDP and Transmission Control Protocol (TCP). The performance was evaluated based on the time difference between each received data packet at each of the receivers.

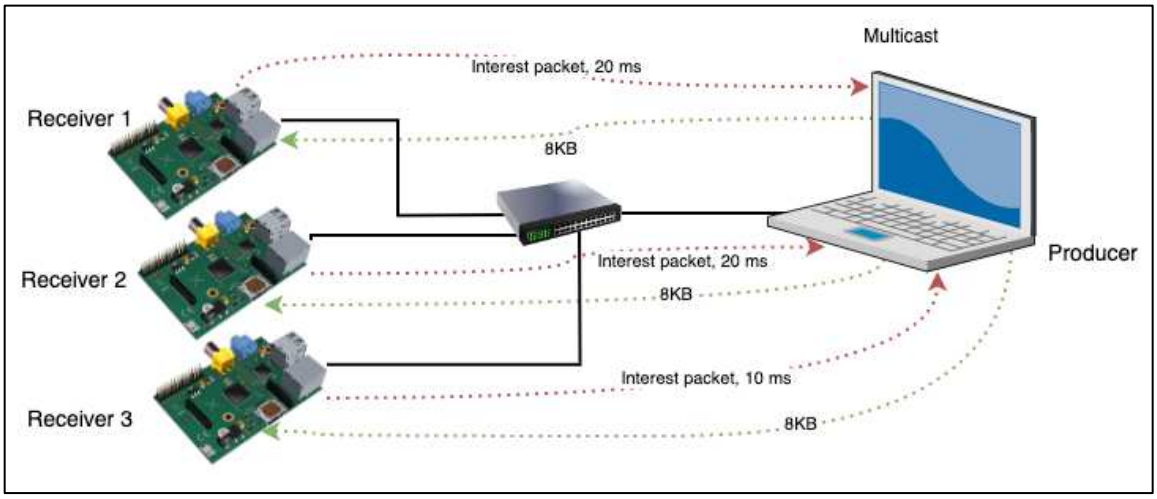


**Figure 5.10:** Test setup to evaluate NDN compared to SOME/IP.

## 5.7.2 Test Results

The boxplots in Figure 5.11 show the performance comparison between NDN over TCP and UDP and SOME/IP when used in the same setup and timing. The time is calculated at each receiver which is the difference between each received data packet. The red line represents the reference line, the frequency of requesting new data for 10 and 20 milliseconds. The results show that NDN has a similar performance to SOME/IP with a 3 to 4 milliseconds delay in the NDN cases. Receivers 1 and 2 are observed to be balanced and receive the data packet at similar times. This is different from SOME/IP where receivers 1 and 2 had some variation in data packet receiving time. NDN is still under development and has a strong potential if used within the automotive industry or autonomous vehicles.

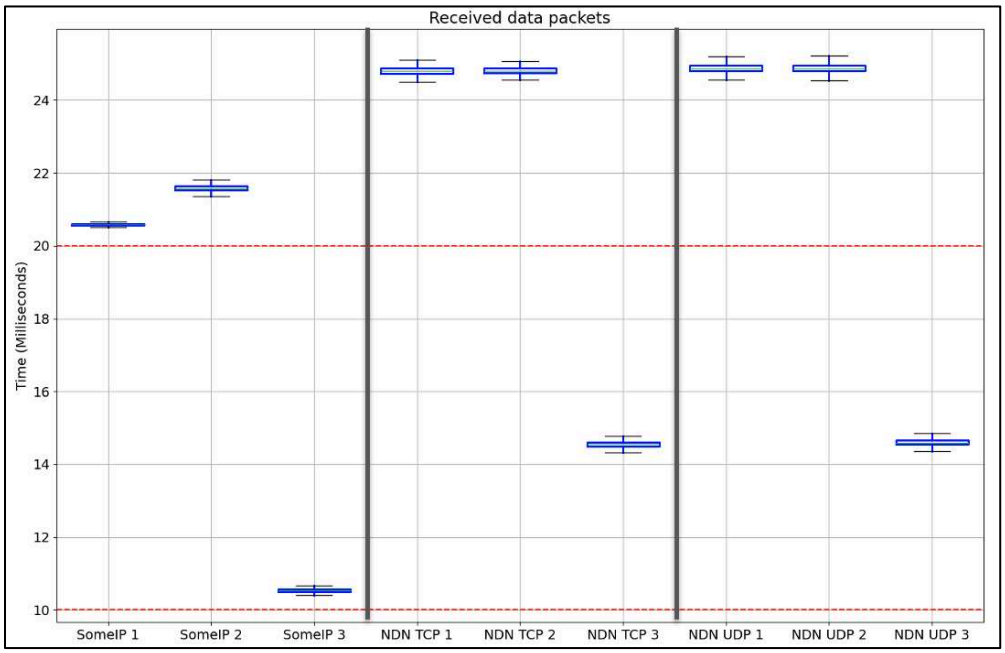


**Figure 5.11:** Test results of NDN performance when used over TCP and UDP compared to SOME/IP.

## 5.8 Queuing Model

Cloud communication plays a key role in a scalable driverless vehicle. Vehicle operation or trip start could be dependent on request or certificate verification by the cloud. With the increased number of vehicles, the cloud load for a particular service may increase and introduce delays because of the queued requests from many vehicles. For instance, Public Key Infrastructure (PKI) could be used for on-board and off-board communication, so that may result in multiple certificates per ECU and many certificates per vehicle. As part of the authentication process (e.g., security handshake for communication, or software updates) is checking the certificate status (e.g., revocation). This could be possible by looking up the certificate serial number in the cloud certificate databases following the traditional methods. The number of certificates serial numbers for the SoS within the cloud could be significant due to the total number of ECUs with the

SoS. A certificate serial number is an identifier used for the look-up, for example, `0c:8o:4l:do:0r:1a:bd:4o:5s:1t:3a:0t:1e:2u:2n:8i:6v:4e:6r:ds` is a certificate serial number. It is not in a human-readable format and is not structured to easily allow categorization or hierarchy. When the autonomous fleet scales, many trucks to many trailers' connections are expected as shown in Figure 5.12, so using the same credentials for the entire fleet to reduce complexity is insecure. An autonomous truck within the fleet could be assigned any random trailer nationwide. Additionally, assuming unique credentials per vehicle (truck or trailer) is used, storing the credentials of the entire fleet on each vehicle is insecure and impractical.

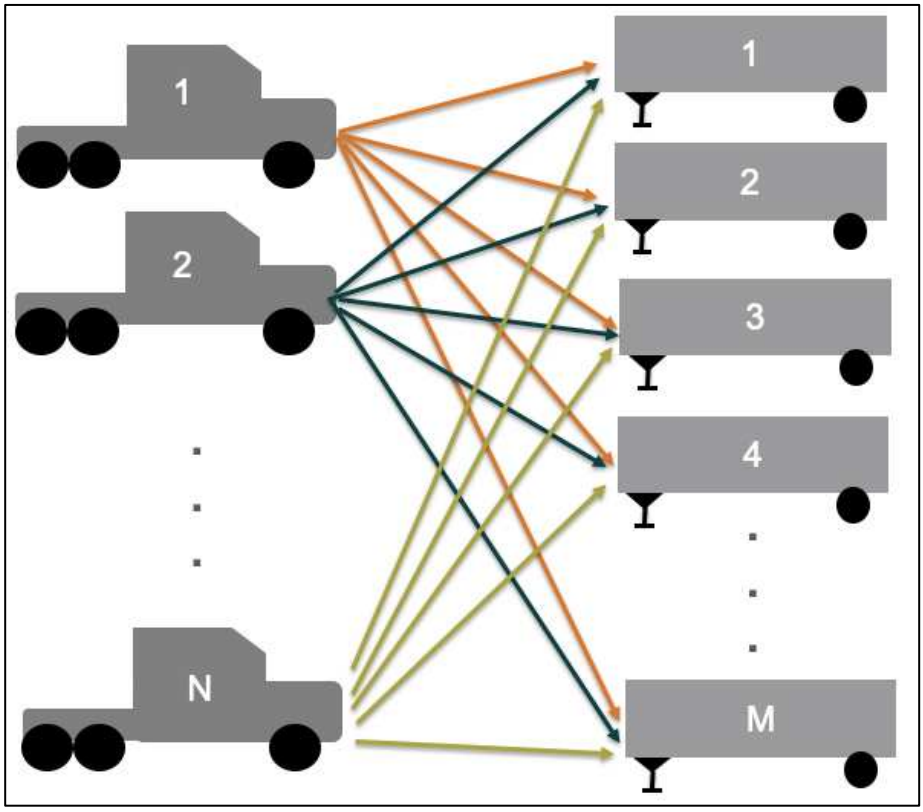


**Figure 5.12:** Many trucks to many trailers relationships

NDN provides a named certificate approach that could reduce the lookup time due to the hierarchy format of the name. The certificate name for a particular function with an ECU is `/OEM1/truck/VIN/ECU/KEY1/version`. When the named certificate lookup request has reached to cloud, it's immediately known where to look based on the hierarchy in the name. For instance, based on the previous example, the focus of the certificate lookup will be on `/OEM1/truck/` domain only. If there are other types of vehicles or devices (e.g., company devices, passenger car AVs, or trailers), they will be skipped.

A multi-server queuing model M/M/s was used to evaluate the performance of using NDN named certificates. The model simulates the requests queue going to the cloud for certificate lookup in the case of NDN using names and the traditional approach using serial numbers. The model calculates average waiting times based on the number of requests received and the number of available servers. The model focuses on the requests waiting time when it arrives at the server. Additional delays before reaching the queue in the server such as cellular latency or other cloud-impacting factors are not considered. These additional conditions are expected to be the same in both cases.

$\lambda$, the arrival rate of $n$ requests, is ranging between 1000 to 10,000 in this model. In some cases, there could be a spike of requests and the majority of the fleet is making requests. For example, when the fleet is grounded or recalled for a software update there will be software updates requests and then released for service, there will be ECU-to-ECU authentication requests. $\mu$ is the service rate, the NDN service rate $\mu_N$ = 150 due to the use of named certificates and the caching feature. The traditional service rate $\mu_T$ = 100 due to

the longer time taken for the lookup using the serial number in the databases. The model Pseudo code is shown in Figure 5.13. Where:

- $T_i$: Interarrival time between request $i$ and $i-1$
- $S_i$: Service time for request $i$
- $A_i$: Sum of $T_i$ (arrival times)
- $F_i$: Time when server $j$ is free for the next request.
- $D_i$: Departure time for request $i$
- $W_i$: Waiting time for request $i$

**Algorithm 1** Requests Queue Simulation

```
1:  procedure SimulateQueue(λ, μ, s, n)
2:      T_i ← ExponentialDistribution(1/λ, n)
3:      S_i ← ExponentialDistribution(1/μ, n)
4:      A_i ← CumulativeSum(T_i)
5:      F_j ← InitializeArray(s, 0)
6:      D_i ← InitializeArray(n, 0)
7:      for i ← 1 to n do
8:          j ← MinValueIndex(F)
9:          start ← Max(A_i, F_j)
10:         D_i ← start + S_i
11:         F_j ← D_i
12:     end for
13:     W_i ← SubtractArrays(D_i, A_i)
14:     return W_i
15: end procedure
16: procedure CDF(W)
17:     sortedW ← Sort(W)        ▷ Sort waiting times in ascending order
18:     n ← Length(W)                          ▷ Number of waiting times
19:     CDF ← InitializeArray(n, 0)        ▷ Array to store CDF values
20:     for i ← 1 to n do
21:         CDF_i ← i/n ▷ Empirical CDF value at ith sorted waiting time
22:     end for
23:     return CDF
24: end procedure
```

**Figure 5.13:** Pseudo code for the M/M/s queuing model used.

The average waiting time based on the number of requests and the number of servers available is shown in Figure 5.14. Cumulative Distribution Function (CDF) is also shown in Figure 5.15. The results indicate that as the system becomes scalable, the average wait time could significantly increase exponentially if not optimized.

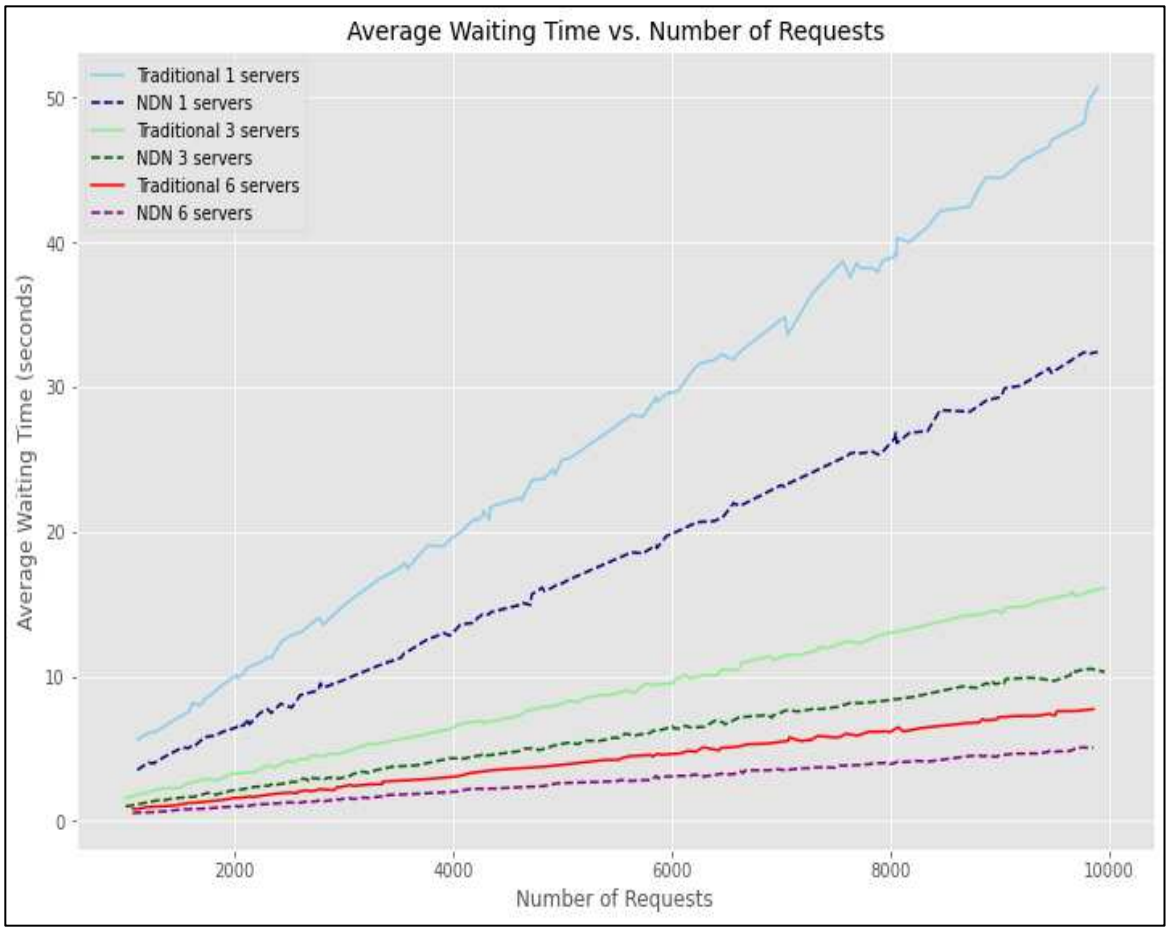


**Figure 5.14:** The average waiting time based on the number of requests and the available number of servers.

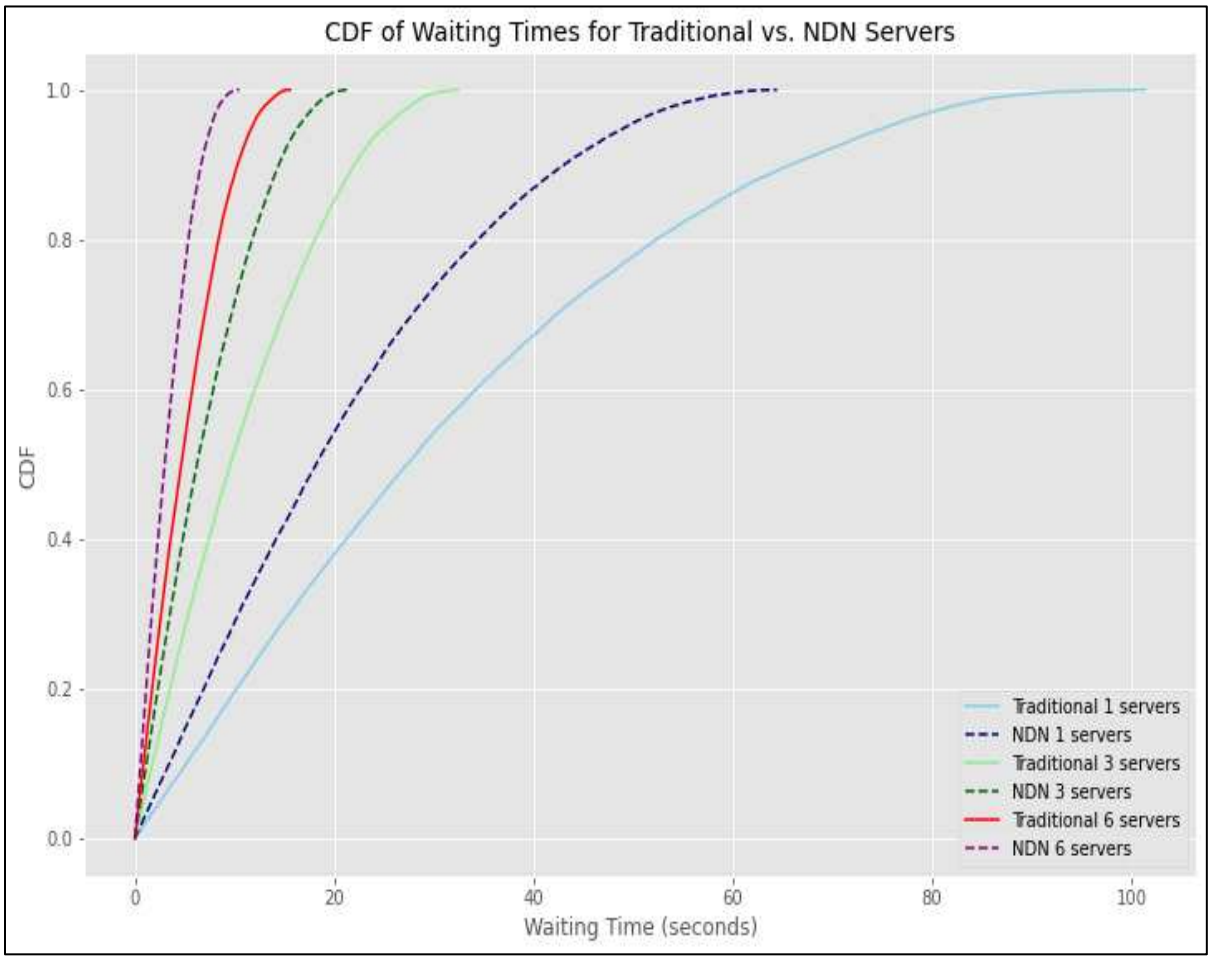


**Figure 5.15:** Cumulative Distribution Function (CDF) of the waiting times based on the number of requests and the available servers

Based on the results, the case of a single server in the traditional case using serial numbers could result in higher wait times as the system scales. More resources would be required to reduce the waiting time to process requests. Through named certificates or requests in general and caching, NDN offers an opportunity to optimize the communication between the cloud and autonomous vehicles. It reduces the lookup effort and time needed in the traditional methods.

## 5.9 Named J1939 Vehicle Signals using NDN and VSS

In the case of autonomous trucks, the truck platform communication between native onboard ECUs is over CAN J1939 [100] which contains vehicle data of interest for other off-board constituent systems. Additional autonomy ECUs needs to either connect to the J1939 CAN bus directly or get the data through another ECU. Additionally, the vehicle data could be sent to off-board systems such as the cloud or V2X. Sharing this data becomes an apparent issue when multiple constituent systems (onboard or off-board) request the same information using different methods or formats. Standardized J1939 uses pre-defined Parameter Group Number (PGN) and each PGN defines Suspect Parameter Numbers (SPNs) in a CAN signal. The PGN is identified based on the signal ID and SPN is identified based on the location in the signal. For example, to identify vehicle speed from the vehicle network, the J1939 pre-defined PGN and SPN are needed. In this case, Cruise Control/Vehicle Speed is PGN 65265 and Wheel-Based Vehicle Speed SPN 84. The PGN and SPN equivalate to `0xFEF1` CAN signal ID and the first two bytes of the signal for value of the vehicle speed respectively.

Constituent systems not directly connected to the CAN bus obtain vehicle information by either decoding the raw CAN frames or receiving the decoded values sent by another ECU. For instance, if the vehicle speed needs to be displayed on a tablet in the operation center, the request travels from the tablet to the cloud, then to vehicle telematics ECU and vehicle gateway. Each network transition may involve different implementation and structure since transmission of J1939 signals outside of the CAN bus has not been standardized. This adds complexity and efforts for integration and

communication between the constituent systems. Figure 5.16 shows an example of the hierarchy of the naming J1939 CAN signals for real-time communication and diagnostics. There are two approaches to naming the signals, NDN and Vehicle Signal Specification (VSS) [101]. NDN is a networking protocol that offers naming, caching, and security for the data packets whereas VSS is an automotive specification for naming the signals. Vehicle ID is added in the case of off-board communication such as cloud or V2X communication.

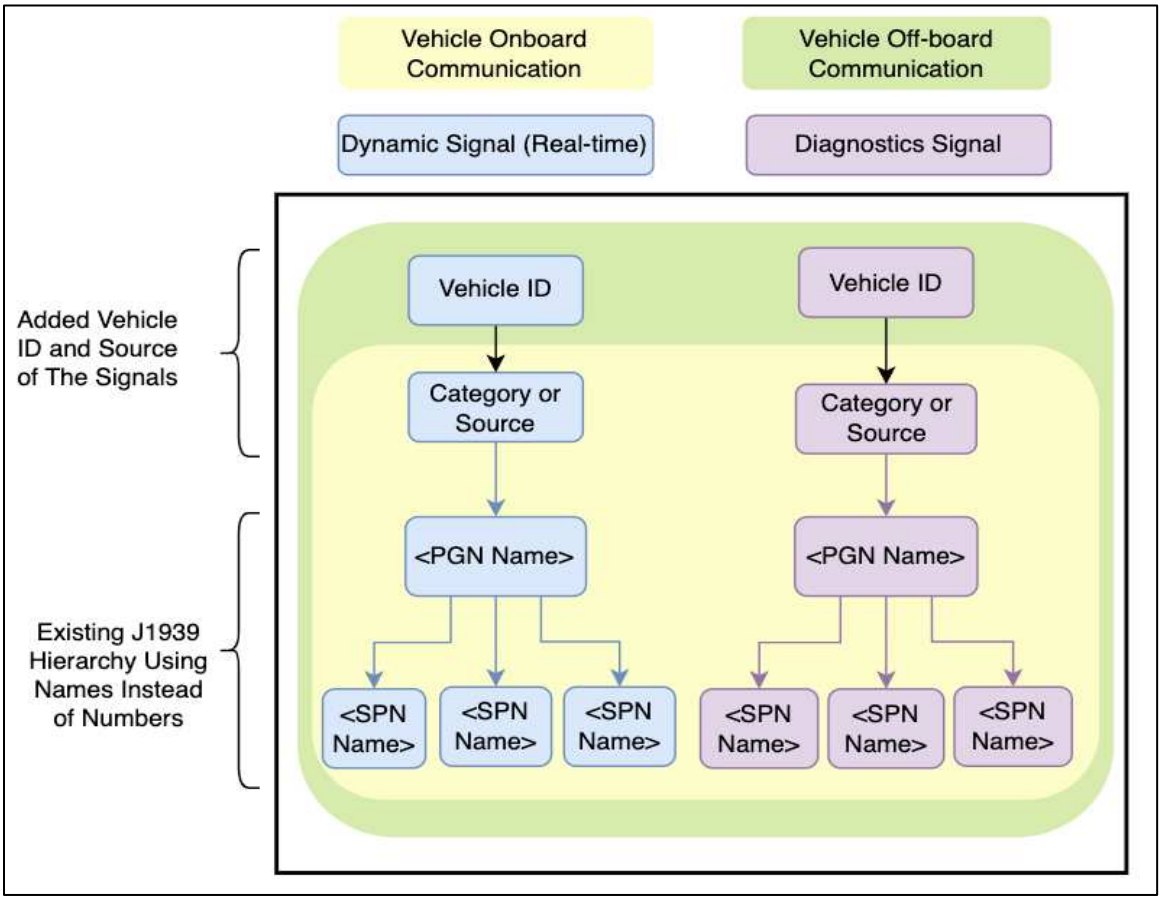


**Figure 5.16:** Named J1939 vehicle signals using a category or the source of information and the existing J1939 hierarchy using names instead of numbers.

### 5.9.1 Using NDN

NDN provides the ability to name, structure, secure, and cache the data by design. The name of each vehicle signal will be mapped to the J1939 signals standard. Named Vehicle Signals could be standardized outside of the CAN bus and named based on the J1939 definitions for on-board or off-board communication. For instance, the signal name could be structured using the category, source ECU, or vehicle identification number (VIN) as follows: `/VIN/PGN/Timestamp` to get the entire PGN (including all SPNs) or specify a SPN such as `/VIN/PGN/SPN/Timestamp`. The vehicle speed named signal based on the previous example becomes `/VIN/Powertrain/CruiseControl-VehicleSpeed/Wheel-Based-VehicleSpeed/16340700`. Another example from J1939 is High Voltage Energy Storage System History (HVESS, PGN 64606) and the battery state of health (SPN 8121) [102] `/VIN/Powertrain/HVESS/StateofHealth/` This approach results in a human-readable signal and would ease implementation across different constituent systems.

Another feature NDN brings to improve communication between the constituent systems when the AVs are scaled is caching and built-in security. Some types of data do not require real-time updates and could be updated every few minutes. This caching mechanism is available by default in each NDN node regardless of its location or function such as a cellular network node or a cloud. This expands the caching capabilities and not necessarily centralizing the data caching to one node such as the cloud, edge computer or a cellular network node.

### 5.9.2 Using VSS

Similarly, the same approach could be used to name J1939 vehicle signals using VSS instead of NDN. This could be done without creating completely new categories or mapping but leveraging the existing J1939 hierarchy. For instance, the vehicle speed signal will be as follows `Signal.Powertrain.CruiseControl-VehicleSpeed.Wheel-Based-VehicleSpeed` where "signal" and "Powertrain" are added to indicate that it's dynamic information and the source is powertrain as there are multiple sources for the same information. The second example of the HVESS state of health is `Signal.Powertrain.HVESS.StateofHealth`.

# Chapter 6 Autonomous Vehicles Development as a System of Systems[5]

In this section, autonomous vehicles development as a directed system of systems is discussed. Additionally, AV SoS vee-model is presented and the interaction between the SoS level and the constituent systems level.

## 6.1 AV as a Directed SoS

There are multiple types of SoS, and AVs are considered a Directed SoS [103] since the developer or owner (O1) of the end product (i.e., autonomous vehicle) directs the development of several constituent systems (S) as shown in 0. Each constituent system could have a different owner or developer, therefore, directed development and operation is required and is provided by O1. The owner (O1) of the autonomous vehicle SoS defines the design for other systems through the owners of the constituent systems. In some cases, such as Vehicle-to-Everything (V2X) infrastructure, O3 will be defining the design since it's related to a standardized communication protocol and the existing infrastructure.

In this example, as shown in Figure 6.1, S1, the autonomous vehicle, is a SoS that includes several constituent systems. These systems include the vehicle platform, autonomy hardware, autonomy software, and the trailer, in the case of autonomous

[5] Contains content from [106]

trucks. Some of these systems within S1 could have a different owner, for example O4 owns S1.4, therefore, it's the responsibility of O1 to define and direct the design of S1.4. Other constituent systems within S1 could be considered a SoS such as S1.1, the vehicle platform as they become complex and contain multiple systems. For instance, the modern base truck platform could contain several driver-assist systems or energy systems for high-voltage battery in the case of hybrid or electric trucks. Additionally for autonomous trucks, the trailer (S1.2) is another constituent system within S1 that needs to be taken into consideration during development.

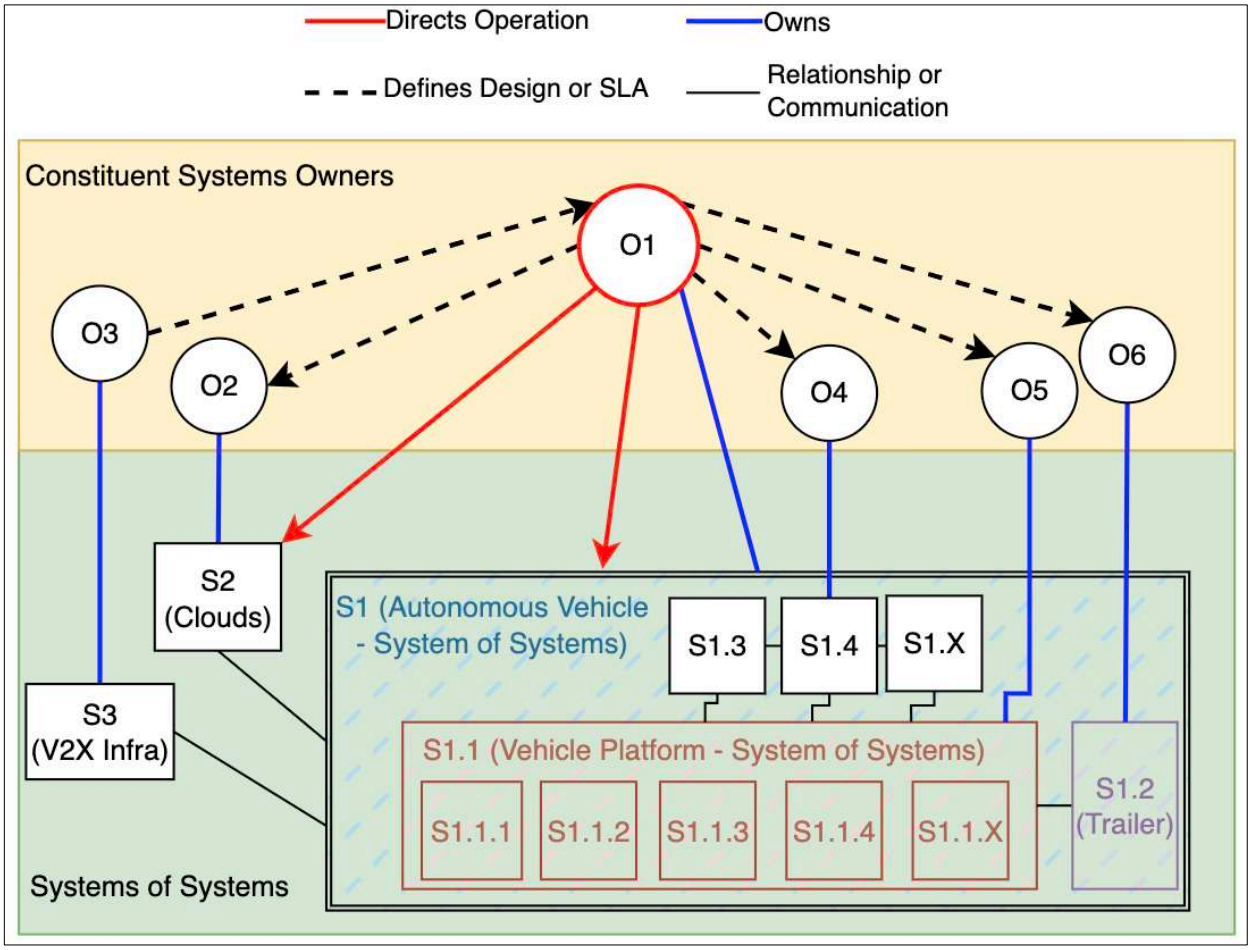


**Figure 6.1:** Relationships between systems owners and the constituent systems.

## 6.2 AV SoS Vee Model

There are many systems and owners involved in the development process of an autonomous vehicle. It's often a distributed development with global OEMs or suppliers. The development often involves many coordinators between development entities with no defined framework at the SoS level. Figure 6.3 shows the interactions between the responsible individuals and the different development parties such as vehicle OEMs, software, hardware, and cloud. Each entity is expected to follow its own internal process and development model.

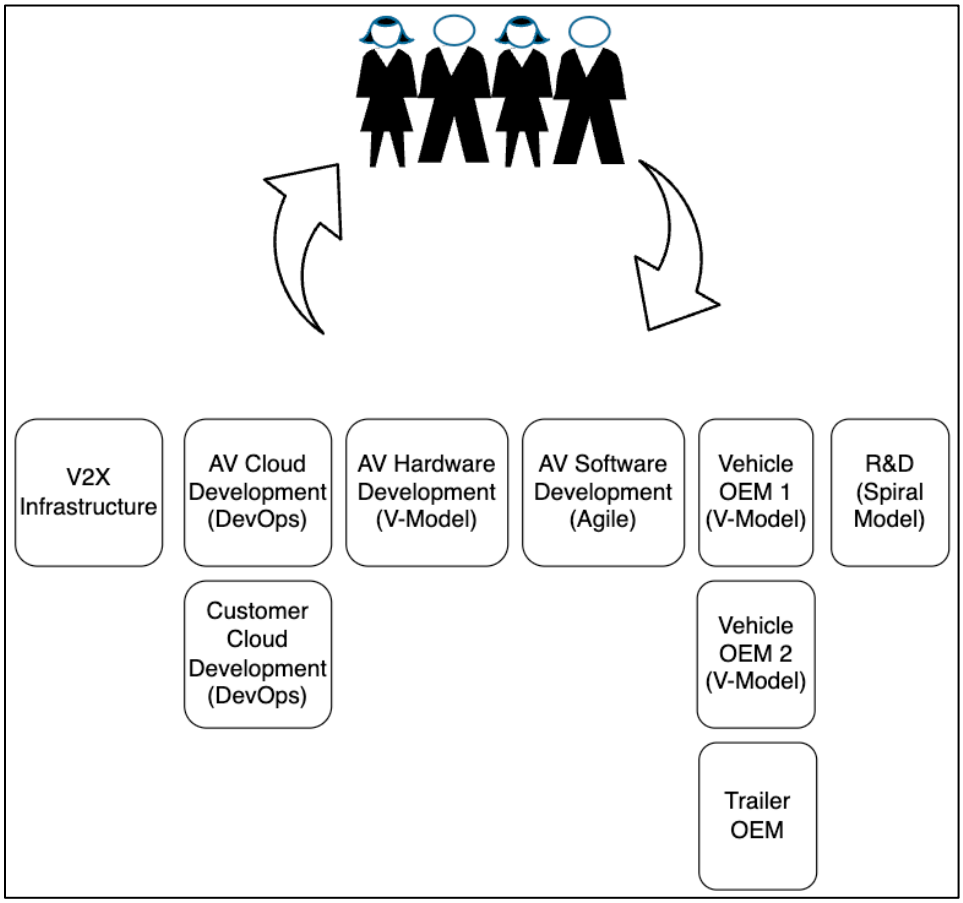


**Figure 6.2:** Example of human interaction with different development entities.

Synchronization, feedback, and conflicts between the different development streams and parties are not driven by a specific framework but are dependent on human efforts which are subject to errors. There is a need for a formal SoS development framework to direct and govern the development of the constituent systems in autonomous vehicles SoS. A SoS Vee model in Figure 6.3 is tailored to autonomous vehicles that act as the governing and guiding framework for the constituent systems during development. Additionally, security and safety are integrated at the SoS level to guide the safety and security processes of the constituent systems. The AV SoS Vee model will also continuously coordinate and synchronize the constituent systems based on the feedback received from the systems. The model also suggests developing functional, security, and safety goals and requirements at the SoS level not just the vehicle level, and then decomposing the SoS requirements to each constituent system.

Moreover, it's necessary for the model to be flexible to accommodate the various development approaches. For instance, software systems might adopt Agile methodology, hardware systems choose the Vee model, and research, and development (R&D) could follow the spiral model. The SoS framework is tailored here to align with diverse models. Each phase in the Vee model decomposes and guides the corresponding phase in the constituent systems models, including defining the level of requirements and the deliverables of each phase.

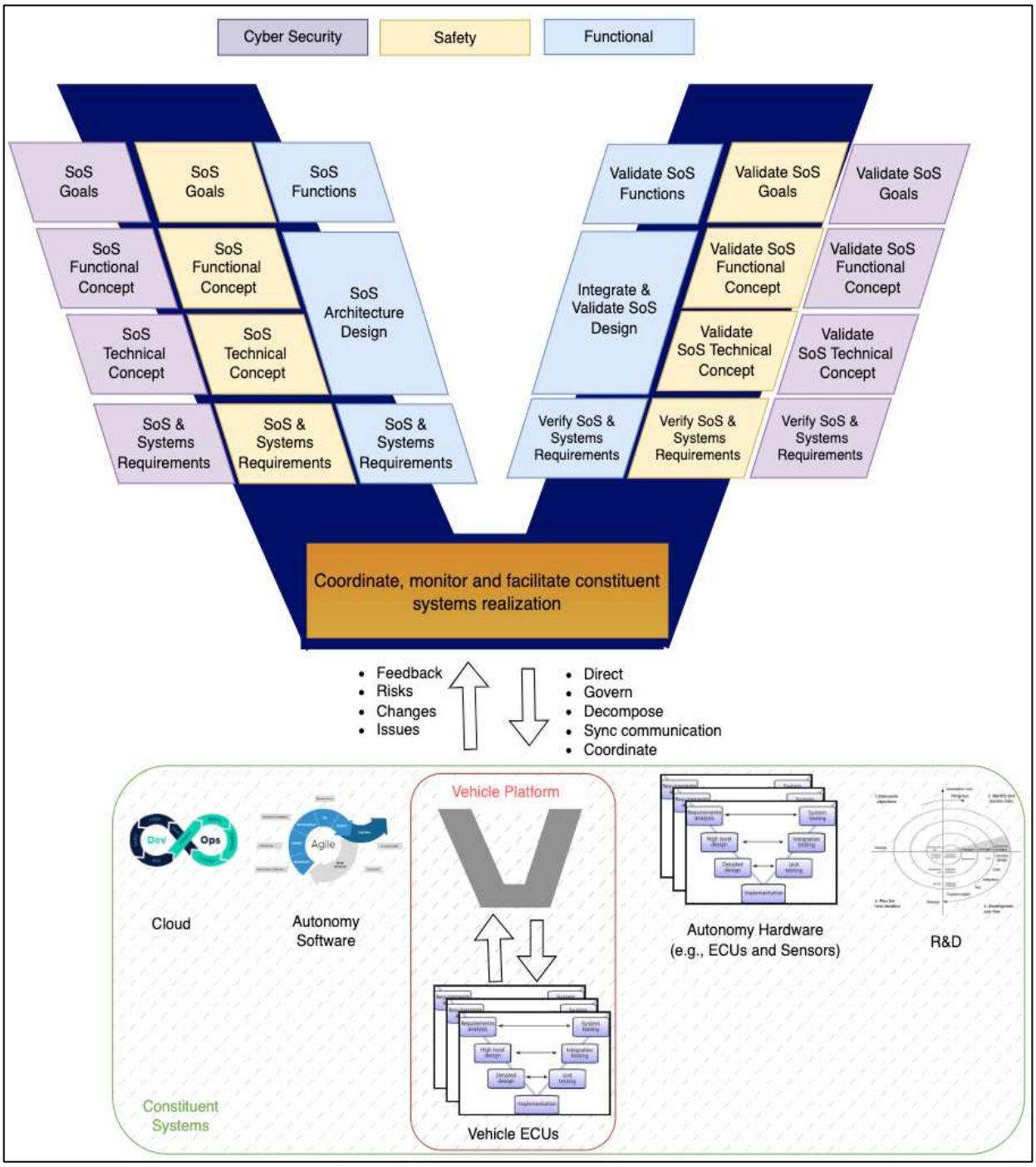


**Figure 6.3:** SoS Model and the interaction with the models of constituent systems.

It also takes the feedback from a constituent system and directs it as appropriate. Furthermore, it establishes a formal communication framework to address requirements

conflicts and promotes awareness of changes in one constituent system that could have an impact on another system. Finally, the framework assures robust communication between the different systems owners, especially in the case of distributed development, which is often global. This becomes essential where there are changes in the requirements of one system that impact other systems on-board or off-board the vehicle.

At the constituent systems levels, there could be another system of systems such as the vehicle platform. The vehicle platform is used for autonomy hardware and software integration. The platform development becomes complex as well due to the number of systems included and the new development in the context of autonomy. This includes modern systems such as native driver assist features and electric powertrain (i.e., Electric or hybrid). This requires close collaboration and continuous two-way feedback with the platform OEMs and their sub-systems developers.

# Chapter 7 Conclusion

Autonomous vehicles are becoming complex in their development because of the numerous systems and developers involved. This introduces challenges during development which requires a robust development framework. This study has presented the effectiveness of a tailored SoS Vee model in governing constituent systems. A second challenge the study addresses is the communication between the constituent systems as the fleet of autonomous vehicles is scaled. Through comparative analysis, we have shown that NDN has a strong potential when compared with SOME/IP providing a similar performance with a slight delay. Furthermore, a queuing model is explored to demonstrate the advantages of employing named certificates compared to the traditional approach using serial numbers when looking a certificate up. We also introduced the concept of named J1939 vehicle signals for dynamic and diagnostics signals, which could significantly improve the integration between several systems, especially off-board systems.

Using Ethernet or a wireless harness between an autonomous truck and the trailer brings new cybersecurity challenges to heavy-duty vehicles due to the new interfaces introduced in the trailer and truck ECUs. For example, if Ethernet is used, an external Ethernet port will be accessible and subject to attackers physically plugging their cables in. Similarly in the case of the wireless harness, attackers will try to gain unauthorized access to the wireless harness network. We discussed truck and trailer pairing and authentication, threats for this architecture, the impact of the new architecture on the

different phases of the system lifecycle and using Named Data Networking to secure cloud and intra-communication including provisioning.

For SAE level 4 and 5 autonomous tractors to drive in reverse, they need additional autonomy sensors on the back of the trailer, and the 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 contains 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.

We proposed using the 60 GHz Wi-Fi wireless harness for communication between the truck and the trailer to combat bandwidth and timing limitations in the existing truck-

trailer communication and at the same time support the automation process of coupling and uncoupling a truck with a trailer by enabling the automated pairing between truck ECU and trailer ECU and eliminate the need for data wires. Using NDN for truck-trailer communication was also discussed in this context and how interest and data packets will be handled between the two ECUs. A testbed is used to evaluate NDN and DDS over an 802.11ac link and the test indicated that NDN and DDS in the case of serializing strings had similar performance and CPU utilization with DDS being slightly better due to the differences in encoding used. Additionally, serializing bytes over NDN is shown to be the most efficient approach when comparing NDN and DDS serializing strings.

We discussed using a wireless harness as the communication link between the autonomous trucks and trailer, the additional security measures, and architecture that is secure by design. A secure pairing solution is discussed at different levels to automate truck-trailer pairing over Wi-Fi without the need for human intervention. Using Wi-Fi as a wireless link has a significant impact on the lifecycle of the ECU which requires new development processes and new considerations in different phases of the ECU lifecycle. Named Data Networking is one of the promising networking protocols that provide security by design. It is still under development, and it has not been standardized for automotive applications, but it can reduce the complexity of the security of the in-vehicle communication networks where it provides a networking solution with security by design. The solution could also be applied to ECU-to-ECU communication or TCU-to-cloud communication. It is capable of facilitating certificates management and issuance.

# Bibliography


[1] SAE International, "Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles," no. J3016_202104.

[2] P. Nyberg, "Stabilization, Sensor Fusion and Path Following for Autonomous Reversing of a Full-scale Truck and Trailer System," *Linköping University,* 2016.

[3] V. Josef, "Trailer parking assistant," in *Proceedings of the 16th International Conference on Mechatronics - Mechatronika 2014*, 2014.

[4] D. Parthasarathy, R. Whiton, J. Hagerskans and T. Gustafsson, "An in-vehicle wireless sensor network for heavy vehicles," *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA),* pp. 1-8, 2016.

[5] J.-R. Lin, T. Talty and O. K. Tonguz, "An empirical performance study of Intra-vehicular Wireless Sensor Networks under WiFi and Bluetooth interference," *2013 IEEE Global Communications Conference (GLOBECOM),* pp. 581-586, 2013.

[6] M. Potdar and S. Wani, "Wireless Sensor Network in Vehicles," *SAE Technical Paper 2015-01-0241,* 2015.

[7] B. Shaer, D. L. Marcum, C. Becker, G. Gressett and M. Schmieder, "Wireless Blind Spot Detection and Embedded Microcontroller," *Advances in Security, Networks, and Internet of Things ,* pp. 717-730, 2021.

[8] I. T. a. A. Kajiwara, "Intra-vehicle wireless harness with mesh-networking," *2016 IEEE-APS Topical Conference on Antennas and Propagation in Wireless Communications (APWC),* pp. 146-149, 2016.

[9] R. Yamada and A. Kajiwara, "Automotive millimeter-wave," *IEICE Communications Express,* vol. 1, pp. 1-6, 2021.

[10] A. D. G. Reddy, "Simulation studies on ZigBee network for in-vehicle wireless communications," *2014 International Conference on Computer Communication and Informatics,* pp. 1-6, 2014.

[11] R. NINO, T. NISHIO and T. MURASE, "IEEE 802.11ad Communication Quality Measurement in In-vehicle Wireless Communication with Real Machines," *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON),* pp. 0700-0706, 2020.

[12] K. Akingbehin, "Hybrid Wireless Harness for Low Mass Vehicular Applications," *2012 21st International Conference on Computer Communications and Networks (ICCCN),* pp. 1-5, 2012.

[13] A. Reddy, G. Dhadyalla and N. Kumari, "Experimental validation of CAN to Bluetooth gateway for in-vehicle wireless networks," *2013 International Conference on Emerging Trends in Communication, Control, Signal Processing and Computing Applications (C2SPCA),* pp. 1-5, 2013.

[14] W. L. Ng, C. K. Ng, N. K. Noordin and B. M. Ali, "Performance Analysis of Wireless Control Area Network (WCAN) Using Token Frame Scheme," *2012 Third International Conference on Intelligent Systems Modelling and Simulation,* pp. 695-699, 2012.

[15] Z. Zuo, S. Yang, B. Ma, B. Zou, Y. Cao, Q. Li, S. Zhou and J. Li, "Design of a CANFD to SOME/IP Gateway Considering Security for In-Vehicle Networks," *Sensors,* p. 23, 2021.

[16] T.-C. Nichiţelea and M.-G. Unguritu, "Automotive Ethernet Applications Using Scalable Service-Oriented Middleware over IP: Service Discovery," *2019 24th International Conference on Methods and Models in Automation and Robotics (MMAR),* pp. 576-581, 2019.

[17] S. Kugele, D. Hettler and J. Peter, "Data-Centric Communication and Containerization for Future Automotive Software Architectures," *2018 IEEE International Conference on Software Architecture (ICSA),* pp. 65-6509, 2018.

[18] M. Postolache, G. Neamtu and S. D. Trofin, "CAN - Ethernet gateway for automotive applications," *2013 17th International Conference on System Theory, Control and Computing (ICSTCC),* pp. 422-427, 2013.

[19] T.-Y. Lee, I.-A. Lin and R.-H. Liao, "Design of a FlexRay/Ethernet Gateway and Security Mechanism for In-Vehicle Networks," *Sensors,* p. 641, 2020.

[20] J. H. Kim, S.-H. Seo, N.-T. Hai, B. M. Cheon, Y. S. Lee and J. W. Jeon, "Gateway Framework for In-Vehicle Networks Based on CAN, FlexRay, and Ethernet," *IEEE Transactions on Vehicular Technology,* vol. 64, no. 10, pp. 4472-4486, 2015.

[21] M. Ashjaei, L. Lo Bello, M. Daneshtalab, G. Patti, S. Saponara and S. Mubeen, "Time-Sensitive Networking in automotive embedded systems: State of the art and research opportunities," *Journal of Systems Architecture,* vol. 117, 2021.

[22] G. Xie, Y. Li, Y. Han, Y. Xie, G. Zeng and R. Li, "Recent Advances and Future Trends for Automotive Functional Safety Design Methodologies," *IEEE Transactions on Industrial Informatics,* vol. 16, pp. 5629-5642, 2020.

[23] H. Zinner, J. Brand, D. Hopf and ContinentalAG, "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] O. Alparslan, S. Arakawa and M. Murata, "Next Generation Intra-Vehicle Backbone Network Architectures," *2021 IEEE 22nd International Conference on High Performance Switching and Routing (HPSR),* pp. 1-7, 2021.

[25] R. Mihalache, "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] D. Olsen, "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] B. Carlson, "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] D. Kraus, E. Leitgeb, T. Plank and M. Löschnigg, "Replacement of the Controller Area Network (CAN) protocol for future automotive bus system solutions by substitution via optical networks," *2016 18th International Conference on Transparent Optical Networks (ICTON),* pp. 1-8, 2016.

[30] T.-C. Nichiţelea and M.-G. Unguritu, "Automotive Ethernet Applications Using Scalable Service-Oriented Middleware over IP: Service Discovery," *2019 24th International Conference on Methods and Models in Automation and Robotics (MMAR),* pp. 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] D. B. Rawat, R. Doku, A. Adebayo, C. Bajracharya and C. Kamhoua, "Blockchain Enabled Named Data Networking for Secure Vehicle-to-Everything Communications," *IEEE Network,* vol. 34, no. 5, pp. 185-189, 2020.

[33] R. Hou, S. Zhou, M. Cui, L. Zhou, D. Zeng, J. Luo and M. Ma, "Data Forwarding Scheme for Vehicle Tracking in Named Data Networking," *IEEE Transactions on Vehicular Technology,* vol. 70, no. 7, pp. 6684-6695, 2021.

[34] D. Saxena, V. Raychoudhury, N. Suri, C. Becker and J. Cao, "Named Data Networking: A survey," *Computer Science Review,* pp. 15-55, 2016.

[35] C. A. Kerrche, F. Ahmad, M. Elhoseny, A. Adnane, Z. Ahmad and B. Nour, "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] M. Chen, D. O. Mau, Y. Zhang, T. Taleb and V. C. Leung, "VENDNET: VEhicular Named Data NETwork," *Vehicular Communications,* vol. 1, no. 4, pp. 208-213, 2014.

[37] A. Wang, T. Chen, H. Chen, X. Ji, W. Wei, X. Han and F. Chen, "NDNVIC: Named Data Networking for Vehicle Infrastructure Cooperation," *IEEE Access,* vol. 7, pp. 62231-62239, 2019.

[38] C. Papadopoulos, S. Shannigrahi and A. Afanaseyv, "In-vehicle Networking with NDN," *Proceedings of the 8th ACM Conference on Information-Centric Networking,* p. 127–129, 2021.

[39] C. Papadopoulos, A. Afanasyev and S. Shannigrahi, "A Name-Based Secure Communications Architecture for Vehicular Networks," *2021 IEEE Vehicular Networking Conference (VNC),* pp. 178-181, 2021.

[40] Z. Threet, C. Papadopoulos, P. Poddar, A. Afanasyev, H. B. William Lambert (Tennessee Tech), S. Ghafoor and S. Shannigrahi, "Demo: In-Vehicle Communication Using Named," *Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2022,* 2022.

[41] N. R. Syambas, H. Tatimma, A. Mustafa and F. Pratama, "Performance Comparison of Named Data and IP-based Network—Case Study on the Indonesia Higher Education Network," *Journal of Communications,* vol. 13, no. 10, 2018.

[42] P. Nyberg, "Stabilization, Sensor Fusion and Path Following for Autonomous Reversing of a Full-scale Truck and Trailer System," 2016.

[43] V. Josef, "Trailer parking assistant," *Proceedings of the 16th International Conference on Mechatronics - Mechatronika 2014,* pp. 677-682, 2014.

[44] U. Koppe, "Combining CANopen and SAE J1939 networks," *1st international Mobile Machine Control (MMC),* pp. 7-11, 2013.

[45] J. S. Daily and P. Kulkarni, "SECURE HEAVY VEHICLE DIAGNOSTICS," *2020 NDIA GROUND VEHICLE SYSTEMS ENGINEERING AND TECHNOLOGY,* 2020.

[46] J. Daily, D. Nnaji and B. Ettlinger, "Securing CAN Traffic on J1939 Networks," *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] B. Gardiner, "NMFTA Letter - Disclosure of Confirmed Remote Write," 03 March 2022. [Online]. Available: http://www.nmfta.org/documents/ctsrp/Disclosure_of_Confirmed_Remote_Write_v4_DIST.pdf?v=1.

[49] B. Gardiner, "PowerLine Truck Hacking 2TOOLS4PLC4TRUCKS," DEF CON Safe Mode ICS Village , 2020.

[50] M. Wolf and R. Lambert, "Hacking Trucks - Cybersecurity Risks and Effective Cybersecurity Protection for Heavy Duty Vehicles," *Dencker, P., Klenk, H., Keller, H. B. & Plödererder, E. (Hrsg.), Automotive - Safety & Security 2017 - Sicherheit und Zuverlässigkeit für automobile Informationstechnik,* pp. 45-60, 2017.

[51] S. Stachowski, R. Bielawski and A. Weimerskirch, "Cybersecurity Research Considerations for Heavy Vehicles," *National Highway Traffic Safety Administration,* no. (Report No. DOT HS 812 636), 2018.

[52] C. Gao, G. Wang, W. Shi, Z. Wang and Y. Chen, "Autonomous Driving Security: State of the Art and Challenges," *IEEE INTERNET OF THINGS JOURNAL,* vol. 9, no. 10, 2022.

[53] S. R. Dadam, D. Zhu, V. K. a. V. Ravi and V. S. S. Palukuru, "Onboard Cybersecurity Diagnostic System for Connected Vehicles," *SAE International,* 2021.

[54] A. Goers and S. Kühne, "CAN over Automotive Ethernet for Trailer Interface," *In: Bertram, T. (eds) Fahrerassistenzsysteme 2018. Proceedings. ,* 2019.

[55] Force, Future Chassis & Brake Systems Task, "Recommendations Regarding Future TractorTrailer Coupling Technology," *Technology & Maintenance Council's (TMC),* 2021.

[56] SAE International, "Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles," no. J3016, 2021.

[57] International Organization for Standardization, "ISO/IEC/IEEE 15288:2015, Systems and software engineering — System life cycle processes," 2015.

[58] M. A. Assaad, R. Talj and A. Charara, "A system of systems framework: Cooperative Maneuvers Manager for Autonomous Vehicles," *2018 13th Annual Conference on System of Systems Engineering (SoSE),* 2018.

[59] M. A. Assaad, R. Talj and A. Charara, "Autonomous Driving as System of Systems: roadmap for accelerating development," *2019 14th Annual Conference System of Systems Engineering (SoSE),* 2019.

[60] P. Pelliccione, E. Knauss, S. M. Ågren, R. Heldal, C. Bergenhem, A. Vinel and O. Brunnegård, "Beyond connected cars: A systems of systems perspective," *Science of Computer Programming,* 2018.

[61] A. M. Madni, "Chapter 10: Autonomous System-of-Systems," in *Transdisciplinary Systems Engineering: Exploiting Convergence in a Hyper-Connected World.*, Springer, 2018.

[62] O. M. Hoehne and G. Rushton, "A System of Systems Approach to Automotive Challenges," *SAE International,* 2018.

[63] Y. Feng, Y. Chen, J. Zhang, C. Tian, R. Ren, T. Han and R. W. Proctor, "Human-centred design of next generation transportation infrastructure with connected and automated vehicles: a system-of-systems perspective," *Theoretical Issues in Ergonomics Science,* 2023.

[64] M. A. Assaad, "An overview on systems of systems control: general discussions and application to multiple autonomous vehicles," *Université de Technologie de Compiègne,* 2019.

[65] CIMdata, "Siemens Broadens MBSE to Engineer Beyond Individual Autonomous Vehicles," CIMdata, Inc., 2021.

[66] A. M. Madni, M. W. Sievers, J. Humann, E. Ordoukhanian, J. D'Ambrosio and P. Sundaram, "Model-Based Approach for Engineering Resilient System-of-Systems: Application to Autonomous Vehicle Networks," in *Disciplinary Convergence in Systems Engineering Research*, Springer, Cham, 2018.

[67] S. Baumgart and S. Punnekkat, "A Model-Based Approach to Document a System-of-Systems," in *2021 IEEE International Systems Conference (SysCon)*, Vancouver, BC, Canada, 2021.

[68] T. Ertener, C. Raulf and D. N. Schmidt, "System of Systems Based Approach for the Development of Autonomous Ride-Pooling Vehicles," in *Internationales Stuttgarter Symposium. ISSYM 2023. Proceedings. Springer.*, 2023.

[69] J. Straub, J. McMillan, B. Yaniero, M. Schumacher, A. Almosalami, K. Boatey and J. Hartman, "CyberSecurity considerations for an interconnected self-driving car system of systems," *2017 12th System of Systems Engineering Conference (SoSE),* 20174.

[70] G. Matta, S. Chlup, A. Shaaban, C. Schmittner, A. Pinzenöhler, E. Szalai and M. Tauber, "Risk Management and Standard Compliance for Cyber-Physical Systems of Systems," *Infocommunications Journal ,* 2021.

[71] C. W. Axelrod, "Cybersecurity challenges of systems-of-systems for fully-autonomous road vehicles," *2017 13th International Conference and Expo on Emerging Technologies for a Smarter World (CEWIT),* 2017.

[72] C. W. Axelrod, "Cybersecurity in the age of autonomous vehicles, intelligent traffic controls and pervasive transportation networks," *2017 IEEE Long Island Systems, Applications and Technology Conference (LISAT),* 2017.

[73] J. Dahmann, G. Rebovich, M. McEvilley and G. Turner, "Security engineering in a system of systems environment," in *2013 IEEE International Systems Conference (SysCon)*, Orlando, FL, USA, 2013.

[74] A. K. Saberi, E. Barbier, F. Benders and M. v. d. Brand, "On functional safety methods: A system of systems approach," *2018 Annual IEEE International Systems Conference (SysCon),* 2018.

[75] M. Skoglund, F. Warg and B. Sangchoolie, "In Search of Synergies in a Multi-concern Development Lifecycle: Safety and Cybersecurity," *Springer International Publishing,* 2018.

[76] Y. G. Dantas and V. Nigam, "Automating Safety and Security Co-design through Semantically Rich Architecture Patterns," *ACM Transactions on Cyber-Physical Systems,* 2023.

[77] A. H. El-Kad, S. Halim, M. M. El-Halwagi and F. Khan, "Analysis of safety and security challenges and opportunities related to cyber-physical systems," *Process Safety and Environmental Protection,* vol. 173, 2023.

[78] S. Baumgart, J. Fröberg and S. Punnekkat, "A Structured Safety Analysis Process for Systems-of-Systems (SafeSoS)," *Elsevier,* 2021.

[79] Office of the Deputy Under Secretary of Defense for Acquisition and Technology, Systems and Software Engineering, "Systems Engineering Guide for Systems of Systems," 2008.

[80] O. Hoehne, "The SoS-VEE Model: Mastering the Socio-Technical Aspects and Complexity of Systems of Systems Engineering (SoSE)," *INCOSE International Symposium, 26,* pp. 1494-1508, 2016.

[81] P. Uday and K. Marais, "Designing Resilient Systems-of-Systems: A Survey of Metrics, Methods, and Challenges," *INCOSE - International Council on Systems Engineering ,* 2015.

[82] L. Zhang, k. claffy, P. Crowley, C. Papadopoulos, L. Wang and B. Zhang, "Named Data Networking," *ACM SIGCOMM Computer Communication Review,* vol. 44, no. 3, 2014.

[83] 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.

[84] Z. Zhang, Y. Yu, H. Zhang, E. Newberry, S. Mastorakis, Y. Li, A. Afanasyev and L. Zhang, "An Overview of Security Support in Named Data Networking," *IEEE Communications Magazine,* 2018.

[85] R. Yamada and A. Kajiwara, "Automotive millimeter-wave," *IEICE Communications Express,* vol. 1, pp. 1-6, 2021.

[86] A. Elhadeedy and J. Daily, "Using Ethernet or A Wireless Harness and Named Data Networking in Autonomous Tractor-Trailer Communication," in *SAE World Congress Experience*, Detroit, 2023.

[87] SAE International, "Hardware Protected Security for Ground Vehicles," no. J3101, FEB2020.

[88] SAE International, "J3061® Cybersecurity Guidebook for Cyber-Physical Vehicle Systems," JAN2016.

[89] D. D. Walden, G. J. Roedler, K. J. Forsberg, R. D. Hamelin and T. M. Shortell, INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities, 4th Edition, 2015.

[90] D. D. Walden, G. J. Roedler, K. J. Forsberg, R. D. Hamelin and T. M. Shortell, INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities, 4th Edition, 2015.

[91] SAE International, "J3061® Cybersecurity Guidebook for Cyber-Physical Vehicle Systems," 2016.

[92] NFD Team, "NFD Developer's Guide," August 2021.

[93] C. Yi, A. Afanasyev, I. Moiseenko, L. Wang, B. Zhang and L. Zhang, "A case for stateful forwarding plane," *Computer Communications,* vol. 36, no. 7, pp. 779-791, 2013.

[94] C. Papadopoulos, A. Afanasyev and S. Shannigrahi, "A Name-Based Secure Communications Architecture for Vehicular Networks," in *2021 IEEE Vehicular Networking Conference (VNC)*, Ulm, Germany, 2021.

[95] R. Pallierer and M. Ziehensack, "Secure Ethernet Communication for Autonomous Driving," in *Automotive Ethernet Congress*, 2016.

[96] C. Papadopoulos, A. Afanasyev and S. Shannigrahi, "A Name-Based Secure Communications Architecture for Vehicular Networks," in *2021 IEEE Vehicular Networking Conference (VNC)*, Ulm, Germany.

[97] Z. Zhang, Y. Yu, H. Zhang, E. Newberry, S. Mastorakis, Y. Li, A. Afanasyev and L. Zhang, "An Overview of Security Support in Named Data Networking," *EEE Communications Magazine,* pp. 62-68, 2018.

[98] M. Chowdhury, A. Gawande and L. Wang, "Secure Information Sharing among Autonomous Vehicles in NDN," *2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI),* pp. 15-26, 2017.

[99] Y. Yu, A. Afanasyev, D. Clark, k. claffy, V. Jacobson and L. Zhang, "Schematizing Trust in Named Data Networking," in *2nd ACM Conference on Information-Centric Networking (ACM-ICN '15)*, New York, 2015.

[100] SAE International, *J1939_201206: Serial Control and Communications Heavy Duty Vehicle Network - Top Level Document,* 2012.

[101] K. Benjamin, T. Raphaël, W. Daniel and B. Christian, "VSSo: a Vehicle Signal and Attribute Ontology for the Web of Things," *9 th International Semantic Sensor Networks Workshop – SSN 2018,* 2018.

[102] Truck Bus Control and Communications Network Committee, "OBD Traceability Matrix - Commerical Vehicle," *SAE International* .

[103] J. S. Dahmann, "Systems of Systems Characterization and Types," *Systems of Systems Engineering for NATO Defense Applications ,* 2015.

[104] A. Elhadeedy and J. Daily, "60 GHz Wi-Fi as a Tractor-Trailer Wireless Harness," in *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, 2023.

[105] A. Elhadeedy and J. Daily, "Securing New Autonomous Truck-Trailer Communication Protocols," in *2023 IEEE World AI IoT Congress (AIIoT)*, Seattle, WA, USA, 2023.

[106] A. Elhadeedy and J. Daily, "Autonomous Vehicle Development as a System of Systems and Constituent Systems Networking," in *The 18th Annual International Systems Conference (SysCon)*, Montreal, QC, Canada, 2024.

# LIST OF ABBREVIATIONS

| | |
|---|---|
| AT | Autonomous Tractor or Truck |
| AV | Autonomous Vehicle |
| ECU | Electronic Control Unit |
| NDN | Named Data Networking |
| NFD | Named Data Networking Forwarding Daemon |
| NDNCERT | NDN certificate management protocol |
| CAN | Controller Area Network |
| ABS | Anti-Lock Braking System |
| PLC | Power Line Carrier |
| SOME/IP | Scalable service-Oriented MiddlewarE over IP |
| DDS | Data Distribution Service |
| SoS | System of Systems |
| SPN | Suspect Parameter Number |
| PGN | Parameter Group Number |
| OEM | Original Equipment Manufacturer |