Poster: An In-Vehicle Software Defined Network Architecture for Connected and Automated Vehicles

Peter Fussey
School of Engineering and Informatics
University of Sussex
Brighton, UK
P.M.Fussey@sussex.ac.uk

George Parisis
School of Engineering and Informatics
University of Sussex
Brighton, UK
G.Parisis@sussex.ac.uk

ABSTRACT

Vehicular network architectures are being reviewed and re-designed to meet requirements for increasing data rates and flexibility driven in part by the adoption of Connected and Automated Vehicles (CAV) strategies. A progressive move from traditional bus based networks, such as CAN, to Ethernet-based network architectures is being considered across the automotive industry. In this paper we advocate for an in-vehicle Software-Defined Network architecture and discuss benefits that such a shift in the architectural paradigm will bring by strengthening cyber-security defences and enabling a fail-operational capability through network programmability and provably correct networks.

KEYWORDS

Software-Defined Networking; In-Vehicle Networks; Cyber-security;

ACM Reference format:
Peter Fussey and George Parisis. 2017. Poster: An In-Vehicle Software Defined Network Architecture for Connected and Automated Vehicles. In *Proceedings of CarSys'17, Snowbird, UT, USA, October 20, 2017,* 2 pages.
DOI: 10.1145/3131944.3131954

1 INTRODUCTION

The evolution of in-vehicle, bus-based network architectures is being challenged by the requirements for increasing performance and flexibility of emerging in-vehicle functionality and vehicle-to-X connectivity to the outside world. The increase in bandwidth required for new Advanced Driver Assistance Systems (ADAS), Connected and Automated Vehicles (CAVs) and infotainment has motivated the study of Ethernet as an in-vehicle network protocol, [1], bringing advantages with respect to bandwidth availability, flexibility of a switched network and extensive industrial experience. Ethernet can be integrated within the vehicle network either as the backbone network that inter-connects existing bus networks or fully replacing existing networks and having all vehicle's Electronic Control Units (ECUs) communicating via Ethernet (Figure 1).

In-vehicle networks and systems are increasingly becoming more complex, transforming the vehicle itself into a small cloud, where data collection and processing is continuous. In-vehicle services, such as infotainment or real-time remote diagnostics, which would also require access to the Internet are becoming reality. Such services could be provided by different providers and require different access rights to systems and components of the vehicle. This would greatly benefit by the ability to slice the network to different providers efficiently and correctly. At the same time, the connection of vehicles to the outside world introduces them to cyber-security threats. Whilst the performance choices for the introduction of real-time Ethernet are being actively studied, there has been little discussion on the impact of an Ethernet-based network architecture on the cyber-resilience of the vehicle.

The requirements for an automotive network are continually evolving, however there are general principles that can be used to assess the advantages and disadvantages of a proposed network architecture.

(1) Functionality and requirement for real-time communication guarantees.
(2) Safety: automated vehicles increasingly need to be fail operational.
(3) Cyber-security: networks designed with cyber-security in mind from the outset.
(4) Robustness to electrically noisy environments in vehicle.
(5) Cost of the silicon within ECUs, shielded cabling, robust connectors, development effort.
(6) Future proof: vehicle product life is significantly longer than consumer electronics.

In this paper, we advocate for an in-vehicle Software-Defined Network (SDN) architecture as an enabling network technology for CAVs. Network programmability enables the introduction of advanced communication services into the vehicle but also communication with external entities. SDN also enables the verification of network properties and invariants [4], which in turn enables the provision of a cyber-secure network environment for services to communicate to each other and interoperate. In combination with real-time Ethernet, SDN could lead to a network infrastructure that is capable of supporting real-time network services together with bandwidth hungry applications in a secure and efficient fashion.

2 IN-VEHICLE SDN ARCHITECTURE

The introduction of automotive Ethernet provides an opportunity to review the overall vehicle network architectures. Replacing existing bus networks with Ethernet may address some bandwidth challenges and support new ADAS features, but this would miss an opportunity to take advantage of additional benefits a Software Defined Network could bring to an in-vehicle network that are described in this Section. The in-vehicle SDN would interface the external networks via a secure gateway, as illustrated in Figure 1.

CarSys'17, Snowbird, UT, USA

DOI: 10.1145/3131944.3131954

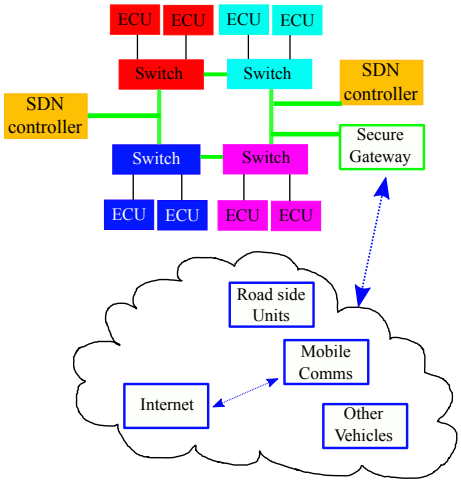

Figure 1: In-vehicle ethernet with SDN replacing traditional CAN/LIN/Flexray buses. A secure gateway provides V2X communication to the cloud.

2.1 Dynamic reconfigurability

A software-defined in-vehicle network would be dynamically reconfigurable providing opportunities to; 1) locally reconfigure the network in response to the diagnosis of a faulty component and 2) to reconfigure the network in response to a centralised analysis based in the OEMs cloud, e.g. to improve network performance or deal with a recently identified defect. Dynamic reconfigurability is a central element of a fail operational approach that will be required as CAVs move to SAE levels 3 and 4 [5].

2.2 Firewalling

An SDN architecture provides a robust and flexible mechanism that protects the vehicle's systems from external threats, allowing for fine-grained control over which network flows and external users can access specific parts of the network. Such a facility, along with being able to slice the network, provides a very strong mechanism for protecting crucial systems in the vehicle. This is increasingly significant as ECU's move to over the air updates.

2.3 Network Slicing and Flow Isolation

The future of in-vehicle networks is one where multiple applications with different bandwidth, latency and jitter requirements run in parallel (in and out of the vehicle) and access different in-vehicle systems. The network should be able to support QoS differentiation which, in turn, would require network flows to be isolated from each other. Moreover, different applications will be trusted differently by the in-vehicle network, and therefore there would have to be a way to slice the network at the physical level or otherwise provide explicit QoS guarantees to specific network flows. These functionalities can be supported by a SDN.

2.4 Programmable QoS and Real-Time Ethernet

Following on from the network slicing and flow isolation capabilities offered by an in-vehicle SDN deployment, we emphasise the capabilities of SDN for supporting different QoS classes, [6]. An approach like the one followed in recent work on Software-Defined Radio for slicing [2] 5G networks, could enable the network operator (potentially the vehicle manufacturer and vehicle owner) and applications (through the Northbound API) to efficiently allocate network resources to different applications.

2.5 SDN Verification

SDN assumes a logically centralised piece of software that configures and operates the network. This centralisation opens up an excellent opportunity for controlling the correctness of the operated software and, consequently, the correctness of the network being operated by it. During the past years, a plethora of techniques and systems inspired by the software verification worlds have been proposed [3][4]. Network verification could be an extremely strong driver of SDN in in-vehicle networks.

2.6 Impact of SDN on fail operational strategies

The ability to fail operational is important for CAVs since they do not have the option of defaulting to a 'safe' state. Current electrical and electronic architectures are built from ECUs that are configured to specific tasks and may be located on fixed network structures. Many safety critical systems include network communications that require redundancy. This can be extended with a SDN where the controller can provide fail operational opportunities by being designed to detect faults and re-configure the network to work around the faults. In addition to responding to known faults, the SDN could also be updated during the life of the vehicle to respond to new faults that emerge and are logged in other similar vehicles.

3 FUTURE DIRECTIONS AND CHALLENGES

Automotive Ethernet is being progressively adopted in ADAS and CAV development. The degree to which it replaces existing networks depends on confirmation of network performance and QoS and quantified benefits from its deployment. The benefits may be in terms of performance and bandwidth but can be significantly increased by combining with a SDN. This brings additional benefits of being able to reconfigure the network dynamically, verification of the network flows, options for fail-operational behaviour and new commercial models with slicing and partitioning that may allow Tier 1 suppliers to operate in separate slices.

REFERENCES

[1] Lucia Lo Bello. 2011. The Case for Ethernet in Automotive Communications. *SIGBED Rev.* 8, 4 (Dec. 2011), 7–15.
[2] X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina. 2017. Network Slicing in 5G: Survey and Challenges. *IEEE Communications Magazine* 55, 5 (2017), 94–100.
[3] Peyman Kazemian, George Varghese, and Nick McKeown. 2012. Header Space Analysis: Static Checking for Networks. In *Proc. of NSDI 2012.*
[4] Ahmed Khurshid, Xuan Zou, Wenxuan Zhou, Matthew Caesar, and P. Brighten Godfrey. 2013. VeriFlow: Verifying Network-Wide Invariants in Real Time. In *Proc. of NSDI 2013.*
[5] SAE. 2014. J3016: Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems. (2014).
[6] S. Sharma, D. Staessens, D. Colle, D. Palma, J. Gonalves, R. Figueiredo, D. Morris, M. Pickavet, and P. Demeester. 2014. Implementing Quality of Service for the Software Defined Networking Enabled Future Internet. In *Proc. of EWSDN 2014.*