

# Security Aspects of Utilizing Ethernet AVB as the Converged Vehicle Backbone

Robert Boatright  
 Harman International Industries Inc.

Joseph Tardo  
 Broadcom Corp

## ABSTRACT

With increasing demand for and sophistication of automotive applications such as infotainment and driver's assistance, the need for tighter integration between the many networks found in modern vehicles is likewise increasing. To enable this integrated vehicle architecture, there is a growing trend to use the Ethernet AVB as a converged backbone to enable cross-domain data exchange.

This paper examines requirements for security and integrity posed by these inter- and intra-ECU and inter-vehicle communications. Solutions are proposed - and gaps are identified - with emphasis given to mapping the broad spectrum of Ethernet security mechanisms to vehicle networking solutions. We begin by examining the security aspects of bridging Body, Chassis/Safety, Powertrain, and Infotainment data, alongside sensor and actuator data across an Ethernet AVB backbone. Specifically discussed is partitioning and application of various Ethernet security solutions including protocols, algorithms, and encryption mechanisms appropriate for vehicular requirements. This includes a discussion of the strengths and vulnerabilities afforded by Ethernet for authenticated ECU/LAN access, data/message integrity, and intrusion protection.

**CITATION:** Boatright, R. and Tardo, J., "Security Aspects of Utilizing Ethernet AVB as the Converged Vehicle Backbone," *SAE Int. J. Passeng. Cars - Electron. Electr. Syst.* 5(2):2012, doi:10.4271/2012-01-0735.

## INTRODUCTION

A key underlying technology enabling the sophisticated functionality of modern vehicles is the increasing number of intra- vehicle networks. Unfortunately, an inescapable consequence arising from automotive networking is increased vulnerability to malicious attack. The growing trend to include Ethernet - and Ethernet AVB - in vehicles for diagnostics, automotive control network bridging, and media streaming potentially increases this exposure but also brings with it a host of potential solutions.

Ethernet also provides functions that contribute to safety, such as a 32-bit cyclic redundancy check (CRC) on every packet to protect against corruption. The focus of this paper is security. For a discussion of safety and security aspects of Ethernet see [19].

This paper recaps the threats and vulnerabilities inherent to automotive networks and explores the broad spectrum of Ethernet security mechanisms available to automotive architects to counteract these vulnerabilities.

Economies of scale have helped propel Ethernet to become the world's most ubiquitous networking technology. A multiplicity of vendors holds promise that Ethernet will likewise find widespread acceptance in automotive networking due its cost-competitive nature. Ethernet does not just bring a lower cost, higher speed, more advanced interconnect technology, it also brings with it new architecture infrastructure (switched networks and layered Internet protocols), a body of security protection mechanisms (from rate limiting to firewalls), and its own history of "hackers" discovering and exploiting vulnerabilities.

Note that the hacker community has expanded its attention from just breaking into Internet nodes or disrupting networks to other, completely unrelated domains (e.g., lock picking seminars are routinely held at hacker conferences such as Black Hat [24], attacks have been documented on ATM machines [23] and road signs [22], among other things) - and have certainly not overlooked automobiles [21].

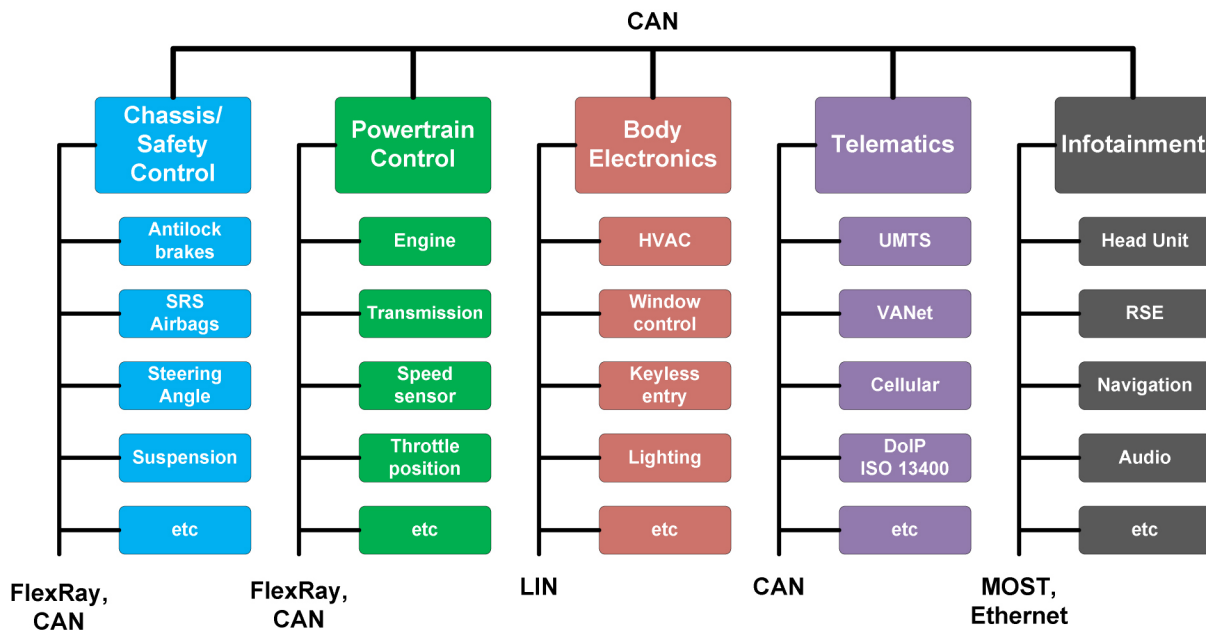


Figure 1. Representative Automotive "Federated Network"

## THE NEED FOR AUTOMOTIVE NETWORKING

A review of the electronics architecture of a typical modern vehicle reveals the root cause behind this increased vulnerability. In Figure 1, we see multiple interconnected electronics sub-systems. These systems are typically interconnected via CAN, FlexRay, MOST, and increasingly, Ethernet.

The sheer volume of ECUs (electronic control units) in modern cars<sup>1</sup> has resulted in an ever-increasing reliance on intra-vehicular networking [2]. Typically, there are multiple domains found in vehicles including Chassis/Safety, Powertrain, Body Electronics, and Infotainment. Within each of these domains, data is networked, most commonly using CAN, LIN, and FlexRay. Infotainment networks have historically been MOST-based but are increasingly moving towards Ethernet AVB.

To exchange data between the various domains, gateways have historically been implemented in the various domain controllers in what has oft times been referred to as a "Federated Architecture".

In light of the simultaneous needs to bound gateway complexity, limit cabling costs, and more tightly integrate the various automotive network domains, the impetus to adopt an "Integrated Architecture" approach to vehicle networking is accelerating. For purposes of this paper, we define this "Integrated Architecture" as a vehicular networking framework where Ethernet is used to transport streaming infotainment media alongside networked control data using a common networking framework.

Takeuchi et al [26] present a rigorous examination of the technical rationale and requirements of using Ethernet AVB as a converged backbone to bridge critical control alongside streaming multimedia. The discussions on the need for low latency, guaranteed deliver, and network management implications are of particular interest to this topic.

Kreifeldt et al [27] further examine automotive-specific applications of Ethernet AVB in "AVB for Automotive Use."

## Ethernet AVB Overview

Audio/Video Bridging - AVB - can be defined as a series of IEEE standards that allow low-latency, time-synchronized delivery of time-sensitive streams with guaranteed Quality of Service (QoS) through IEEE 802 bridged networks.

The IEEE standards defining AVB include:

- IEEE 802.1AS Timing and Synchronization [17]
- IEEE 802.1Qat Stream Reservation Protocol [18]
- IEEE 802.1Qav Forwarding and Queuing for Time-Sensitive Streams [11]

The AVnu Alliance [25] is an industry consortium dedicated to furthering the adoption of AVB in automotive, professional, and consumer markets. The AVnu Alliance is responsible for defining automotive profiles and related compliance and interoperability tests related to the use of Ethernet AVB in automotive environments.

## THREATS TO AUTOMOTIVE SECURITY

There have been a number of papers in the last few years that chronicled automotive security vulnerabilities and risks.

<sup>1</sup>"The number of ECUs varies from 40 in compact-class automobiles to 90 in luxury-class automobiles." [2]

Brooks et al [2] presented a model for analyzing automotive security based on the Computer Emergency Response Team (CERT) taxonomy. Koscher et al [3] demonstrated security issues by mounting and documenting a series of successful attacks against production vehicles. These required for the most part physical access to the vehicle. Subsequently, Checkoway et al demonstrated successful attacks using only wireless access [10].

Threats to automotive network security emanate from multiple fronts including physical/direct access as well as wireless channels. These include subsystems such as powertrain, chassis/safety, body electronics, and infotainment. Specific channels open to direct physical attack include Onboard Diagnostics (OBD) ports, CD/DVD players, and consumer electronics on-ramps to the infotainment systems. Wireless channels include both short-range systems (Tire Pressure Monitoring System, or TPMS, Bluetooth, keyless entry, and RFID) as well as long-range (cellular, telematics, GPS, satellite radio, digital radio, DAB, Radio Data System (RDS) and Traffic Message Channel (TMC). In the future, threats may also arise from deployment of Vehicular Ad-Hoc Networks (VANets) for safety applications [3] such as vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications (i.e. IEEE P1609) using technologies such as 802.11.

For the same reason that access to computer data rooms is typically restricted, direct physical access to the vehicle remains a very real concern. An unscrupulous parking attendant could conceivably load compromised software to a vehicle via the OBD II diagnostics port. Repair shop employees could become unwitting participants to vehicle hacking if the software in their Diagnostics Code Readers were somehow compromised. ECU code corruption need not even be intentional to be of concern - a failed ECU software update could potentially be catastrophic if undetected.

One might be tempted to think that separate CAN buses are used to isolate critical systems (e.g., engine) from less critical ones (e.g., body). However much this appears, the justification is more due to reliability and bandwidth considerations. Isolation for security has typically not been a primary consideration when separate buses are bridged [10].

Early investigations in the vulnerability of automotive networks include an investigation to the very real possibility of remote spoofing of Tire Pressure Monitoring System (TPMS) messages [1]. While hardly a catastrophic attack, this was indicative of endemic weaknesses in automotive security.

In "Comprehensive Experimental Analyses of Automotive Attack Surfaces," [10], the authors convincingly detail a series of more serious vulnerabilities validated by a series of experiments. After reading of other threats and vulnerabilities as outlined in [2], [3], and [4], it is apparent that vehicular security is a subject that has not been an issue for automotive OEMs in the past but has now become a more prevalent concern.

The potential consequences of these vulnerabilities run the gamut from spoofed messages to stolen cars,

misappropriation of wireless parking/toll/gasoline charges, intentionally caused accidents. In one experiment [10], the authors describe their success at remote eavesdropping using in-cabin microphones to surreptitiously broadcast occupant's conversations after subverting onboard telematics services - no physical access to the car was required.

## ETHERNET IN CONVERGED AUTOMOTIVE NETWORKS

Ethernet employs a switched network architecture. In a switched architecture nodes are interconnected using point-to-point links to switches. Ethernet switches basically forward packets from one port towards their intended destination. This section describes basic features in IEEE 802.1Q [12] compliant Ethernet switches.

Bus architectures as used in CAN, FlexRay, or IDB1394 are physically broadcast media, i.e., a transmitted message is received by all stations on the same bus. This applies whether or not "repeaters", "hubs", or "active concentrators" are used to extend the bus. Earlier Ethernet CSMA/CD (Collision Sense Multiple Access/Collision Detection) networks also used a broadcast bus architecture, but this is not expected to be adopted for automotive networks since deterministic delivery of packets with bounded latency cannot be guaranteed in a CSMA/CD network.

The native bus characteristics provide certain physical access protection characteristics. For instance, a node on a shared bus that is not a talker can listen to all traffic on the bus undetected. In the case of a switched network, even if a node were allowed to connect to a switch port, the listener would only be forwarded frames intended for that port. As Ethernet evolved from shared CSMA/CD bus to a switched architecture over time, switches evolved with it. [Table 1](#) summarizes the differences between switched and bus architectures.

As switched Ethernet infrastructure became prevalent in wired Information Technology (IT), switch architecture evolved in response to emerging IT requirements, in particular, for security and access control. As a result, security and access control architectures were developed and incorporated into the Ethernet framework. Many of these capabilities could be directly adopted for in-vehicle networking and connectivity framework to help provide added security.

In bus systems, the access to and integrity of the bus must be protected. In a switched system, this would be analogous to protecting the access to the switched infrastructure.

The following highlight some basic Ethernet Switching functions that are both an intrinsic part of IEEE 802.1 and 802.3 standards and are relevant to security. These are broadly available in almost every switch offered in IT market, and are also applicable to in-vehicle applications. The assumptions for in-vehicle applications are that:

- a. most, if not all, end point devices are known, and networks are highly provisioned, unlike IT networks where