A Survey of Remote Automotive Attack Surfaces

By Charlie Miller (Twitter: cmiller@openrce.org)

& Chris Valasek (IOActive: cvalasek@gmail.com)

Contents

Introduction

Modern automobiles consist of a number of different computer components, called Electronic Control Units (ECUs). Each automobile contains from 20-100 of these devices, with each ECU being responsible for one or more particular features of the vehicle. For example, there is an ECU for seatbelt tightening, one for monitoring the steering wheel angle, one to measure if a passenger is in the car, one to control the ABS system, and so on. These ECUs need to pass data to one another so they can make decisions on how to act. For example, an ECU may act differently depending on if the car is in drive or reverse or whether it is moving or stationary.

Some ECUs also communicate with the outside world as well as the internal vehicle network. These ECUs pose the biggest risk to the manufacturer, passenger, and vehicle. The options available to attackers will be influenced by the different remote endpoints offered, the topology of the vehicular network, as well as safety features programmed into the various ECUs under consideration. This paper attempts to analyze numerous automobiles varying in production year to show how remote attack surfaces have evolved with time and to try to quantify the difficulty of a remote attack for a variety of different automobiles. This analysis will include how large the remote attack surface is, how segmented the ECUs which have physical control of the automobile are from those accepting external input, and the features present in the automobile which allow computers to physically control it. Additionally, this paper recommends defensive strategies including an IDS-type system to detect and prevent these types of attacks.

Anatomy of a Remote Attack

Safety critical attacks against modern automobiles generally require three stages. The first stage consists of an attacker remotely gaining access to an internal automotive network. This will allow the attacker to inject messages into the cars networks, directly or indirectly controlling the desired ECU. You can imagine such an attack occurring by sending some kind of wireless signal and compromising a listening ECU, subsequently injecting code. Researchers from the University of Washington and the University California San Diego were able to get remote code execution on a telematics unit of a vehicle by exploiting a vulnerability in the Bluetooth stack of an ECU and separately compromising a cellular modem [3]. Depending on the desires of the attacker, this might be the end of the attack, for example the compromised ECU may control a microphone used to eavesdrop on the vehicle.

Cyber physical attacks (attacks that result in physical control of various aspects of the automobile), on the other hand, will require interaction with other ECUs. It is difficult to measure how susceptible a particular vehicle is to remote attacks since it depends on the presence (or absence) of vulnerabilities. What we can measure (and do measure in this paper) is the attack surface of each vehicle and use this information as a proxy to estimate susceptibility to the first stage of remote attack.

The compromised ECU mentioned in the first stage typically cannot directly control safety critical features of a vehicle. This ECUs job is typically only related to receiving and processing radio signals. Therefore, a cyber physical attack usually requires a second step which involves injecting messages onto the internal automotive network in an attempt to communicate with safety critical ECUs, such as those responsible for steering, braking, and acceleration.

In some vehicles, this may be trivial, but in many designs, the ECU which was compromised remotely will not be able to directly send messages to these safety critical ECUs. In this case, the attacker will have to somehow get messages bridged from the network of compromised ECU to the network where the target ECU lives.

This might require tricking the gateway ECU or compromising it outright. The academic researchers mentioned above demonstrated a way to compromise the bridge ECU in their vehicle to get from the less privileged CAN network to the one containing the ECU in charge of braking. In this paper we discuss the various architectures of different vehicles and examine the effect these topologies may have on a remote attack.

After the attacker has wirelessly compromised an ECU and acquired the ability to send messages to a desired target ECU, the attacker may communicate with safety critical ECUs. The final step is to make the target ECU behave in some way that compromises vehicle safety. This involves reverse engineering the messages on the network and figuring out the exact format to perform some physical action. Since each manufacturer (and perhaps each model and even each year) use different data in the messages on the bus, the message reverse engineering process requires a large amount of work and will be manufacturer specific. For example, the messages to lock the brakes on one manufacturer's vehicle likely won't work on a vehicle from a different manufacturer.

Additionally, some ECUs will only listen to certain messages and may have safety features built into them, such as not responding to certain messages while the vehicle is in motion. This third stage was the focus of our previous research efforts [9]. In general, it is tough to know without a detailed investigation whether it is possible to affect cyber physical features though message injection since it essentially relies on the implementation of the ECUs. In this document, we again take an approach similar to measuring remote attack surface.

For each vehicle, we list the computer-controlled features of the vehicle. For example, while it is possible to adversely affect ECUs sometimes using vulnerabilities (see how the braking on a Ford was manipulated in [9] or how the braking was manipulated in the Chevy in [3]), it is even easier when controlling braking is a *feature* of the automobile. In the Toyota Prius in [9], the collision prevention system was designed to stop the vehicle when certain CAN messages were received. This didn't require a vulnerability, but was a safety feature. So while all vehicles may (or may) not be vulnerable to safety critical actions through CAN message injection, we assume those with advanced computer controlled features are more susceptible since they are designed to take physical actions based on messages received on the internal network.

This paper

By looking at each car's remote attack surface, internal network architecture, and computer controlled features we are able to draw some conclusions about the suitability of the vehicle to remote attack. This doesn't mean that the most susceptible looking isn't in fact quite secure (i.e. coded very securely) or that the most secure looking isn't in fact trivially exploitable, but it does provide some objective measure of the security of a large number of vehicles that wouldn't be possible to examine in detail without a massive effort. It also provides an outline on how to design and construct secure vehicles, namely in making each of these three stages of exploitation as difficult as possible.

The authors also discuss different strategies to securing vehicles from remote attack in a layered, attack resilient fashion. In particular, it introduces a device that acts like a network intrusion detection and prevention device as well as discusses some early testing results.

Lastly, to the authors' knowledge, this is the first publicly available resource for automotive network architecture review. While network architecture review is commonplace in modern network/computer security, much of automobile topology has been shrouded in secrecy.

Remote Attacks not related to Automotive Networks

There are a number of remote attacks that have nothing to do with sending messages on automotive networks such as CAN, a large focus of this paper. These mostly fall into two categories. The first are attacks where the remotely attacked ECU is the final target of the attack. For example, a remote attack against the telematics unit may allow the attacker to listen and record conversations in the vehicle. If this is all the attacker wants, then the automotive network containing the telematics unit is likely to be irrelevant.

The second type of attack is one that doesn't actually get remote code execution, but still impacts the physical behavior of the vehicle. An example of this might include tricking the sensors of the vehicle. One could imagine sending radar signals that interfere with a car's collision detection system and cause it to think a collision is imminent, resulting in the brakes being engaged.

These types of attacks are interesting but are not a focus of this paper.

Author Notes

Automobile technical information sites, much like the vehicles they describe, vary from manufacturer to manufacturer. We did our best to normalize the data, such as ECU listings, attack surface, and network topology, while attempting to preserve the terminology used by individual automakers. This was not an easy task as just finding network topology information could take many hours (apparently the websites were not intuitive to us). Sometimes older models did not even appear to have publicly available information online, hence the variance in make, model, and year of vehicles detailed in this paper.

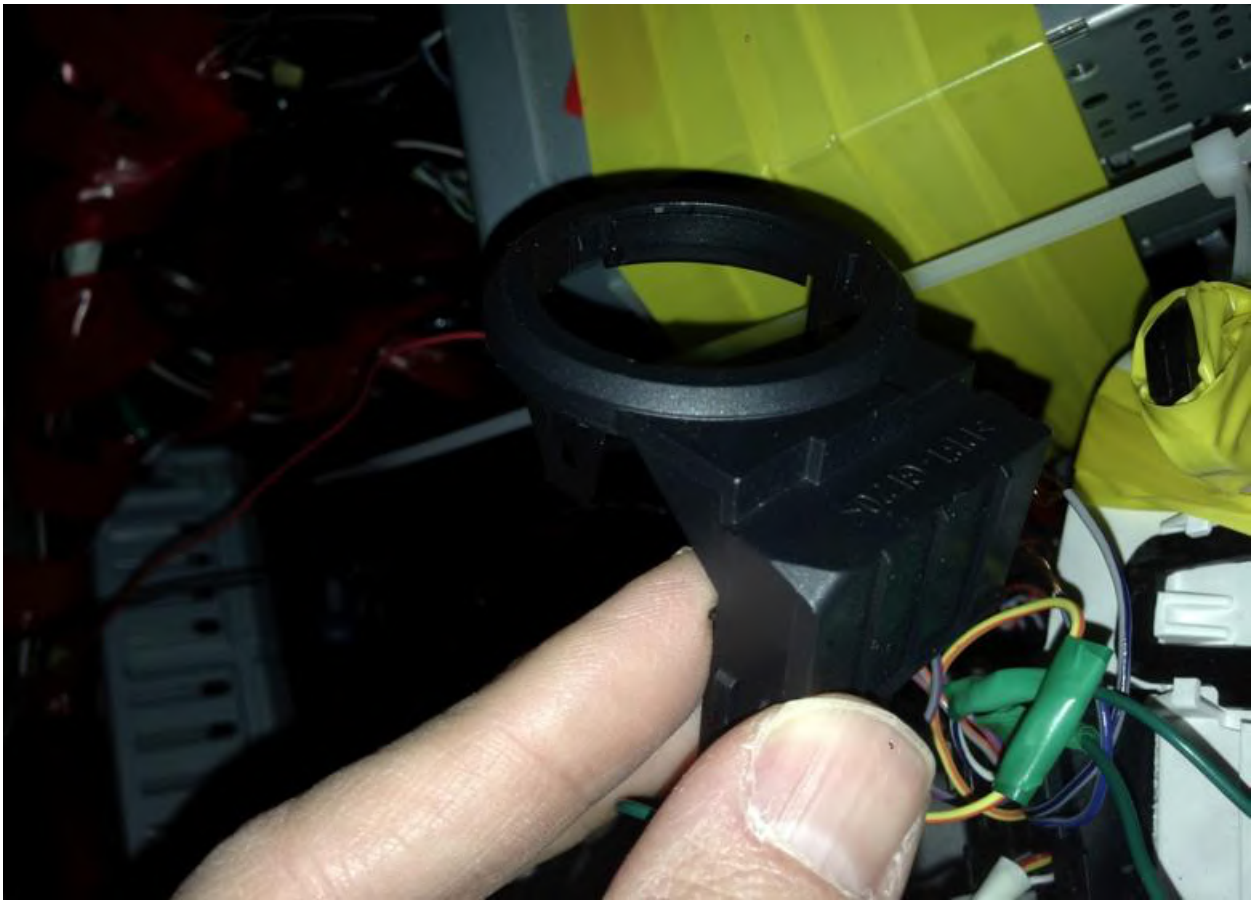
Remote Attack Surfaces of Automobiles

This section outlines some common remote attack vectors for modern automobiles in order to understand where, on the automotive network, an attacker may first arrive. While this discussion will be mostly general, for clarity we use examples from actual cars, usually a 2010 Ford Escape and 2010 Toyota Prius, since we are intimately familiar with these vehicles from previous research.

Passive Anti-Theft System (PATS)

For many modern cars, there is a small chip in the ignition key that communicates with a sensor on the steering column. For the Escape, this sensor is wired directly into the Instrument Cluster (IC) ECU. When the key is turned, the on-board computer sends out an RF signal that is picked up by the transponder in the key. The transponder then returns a unique RF signal to the vehicle's computer, giving it confirmation to start and continue to run. This all happens in less than a second. If the on-board computer does not receive the correct identification code, certain components such as the fuel pump and, on some, the starter will remain disabled.

The instrument cluster (IC) for the 2010 Ford Escape



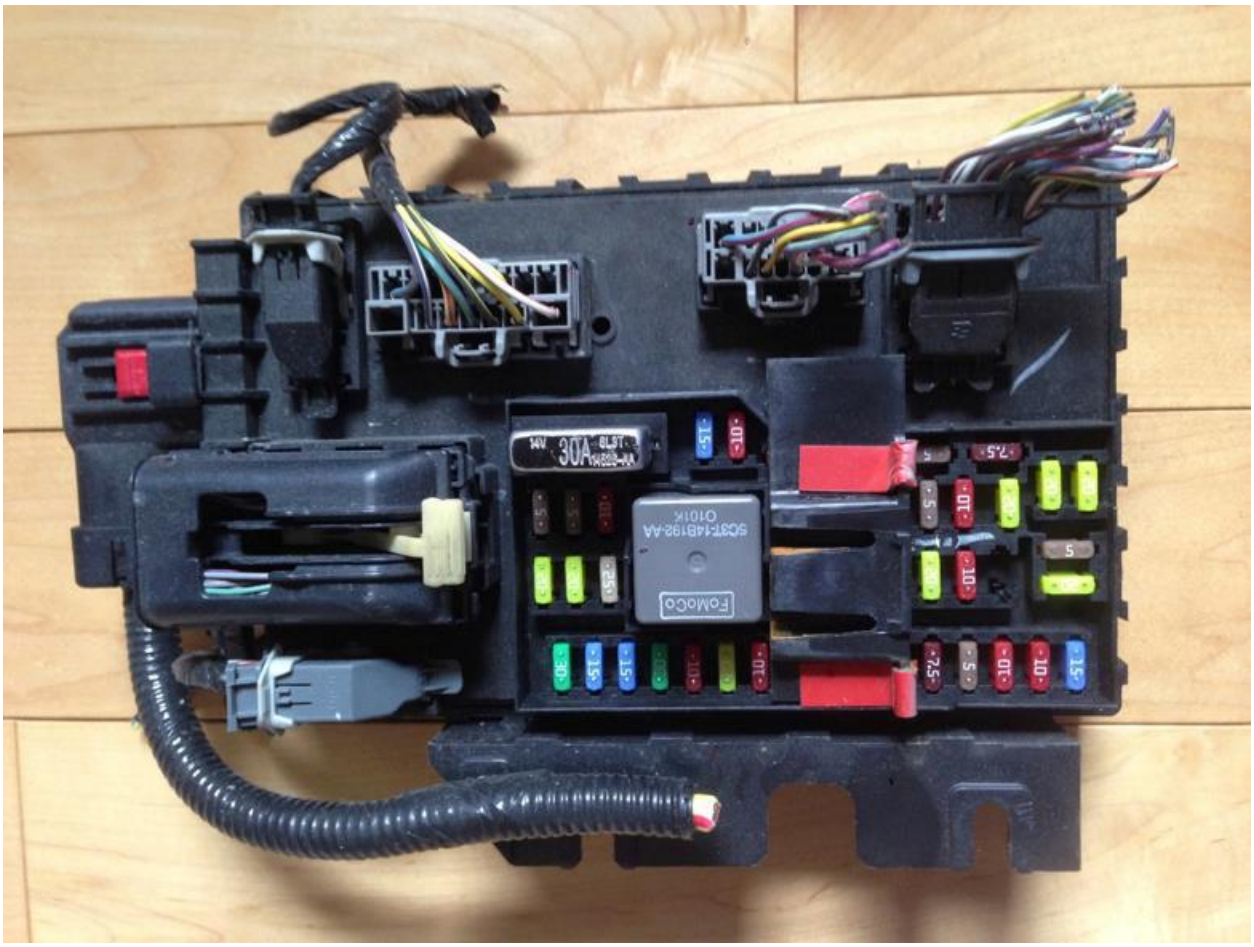
The PATS sensor for the 2010 Ford Escape

Range: ~10 centimeters.

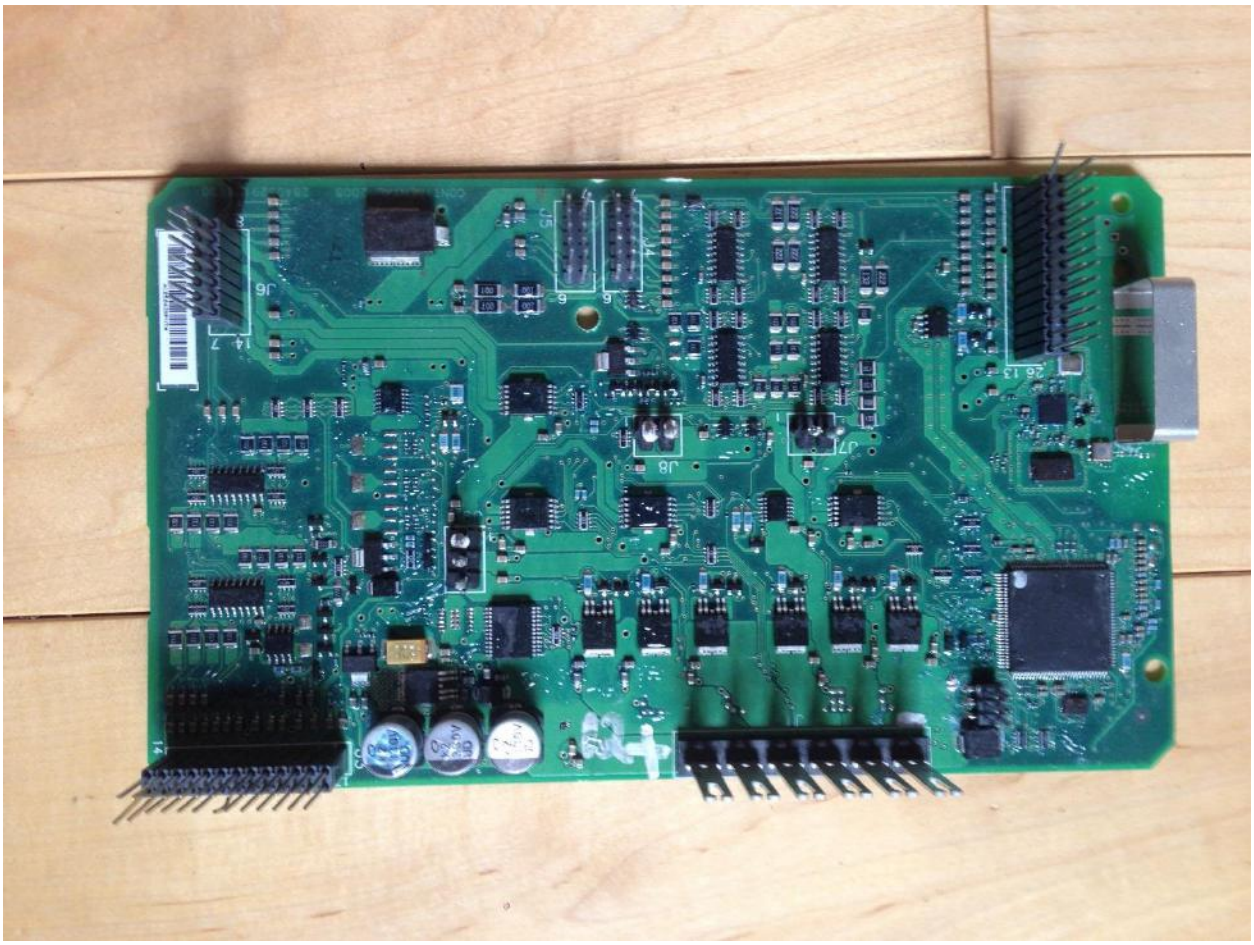
Analysis: It may be possible to create a denial of service attack that would cause the car not to start, even with the proper key inserted. As far as remote attacks are concerned, this attack surface is very small. The only data transferred (and processed by the software on the IC) is the identification code and the underlying RF signal. It is hard to imagine an exploitable vulnerability in this code, and even if there was, you would have to be very close to the sensor, as it is intentionally designed to only pick up nearby signals. The authors believe the main exploitation vector would be for vehicle theft, not remote code execution.

Tire Pressure Monitoring System (TPMS)

Each tire has a pressure sensor that is constantly measuring the tire pressure and transmitting real time data to an ECU. In the Escape, the receiving sensor is wired into the Smart Junction Box (SJB). This radio signal is proprietary, but some research has been done in understanding the TPMS system for some vehicles and investigating their underlying security [1] [2].

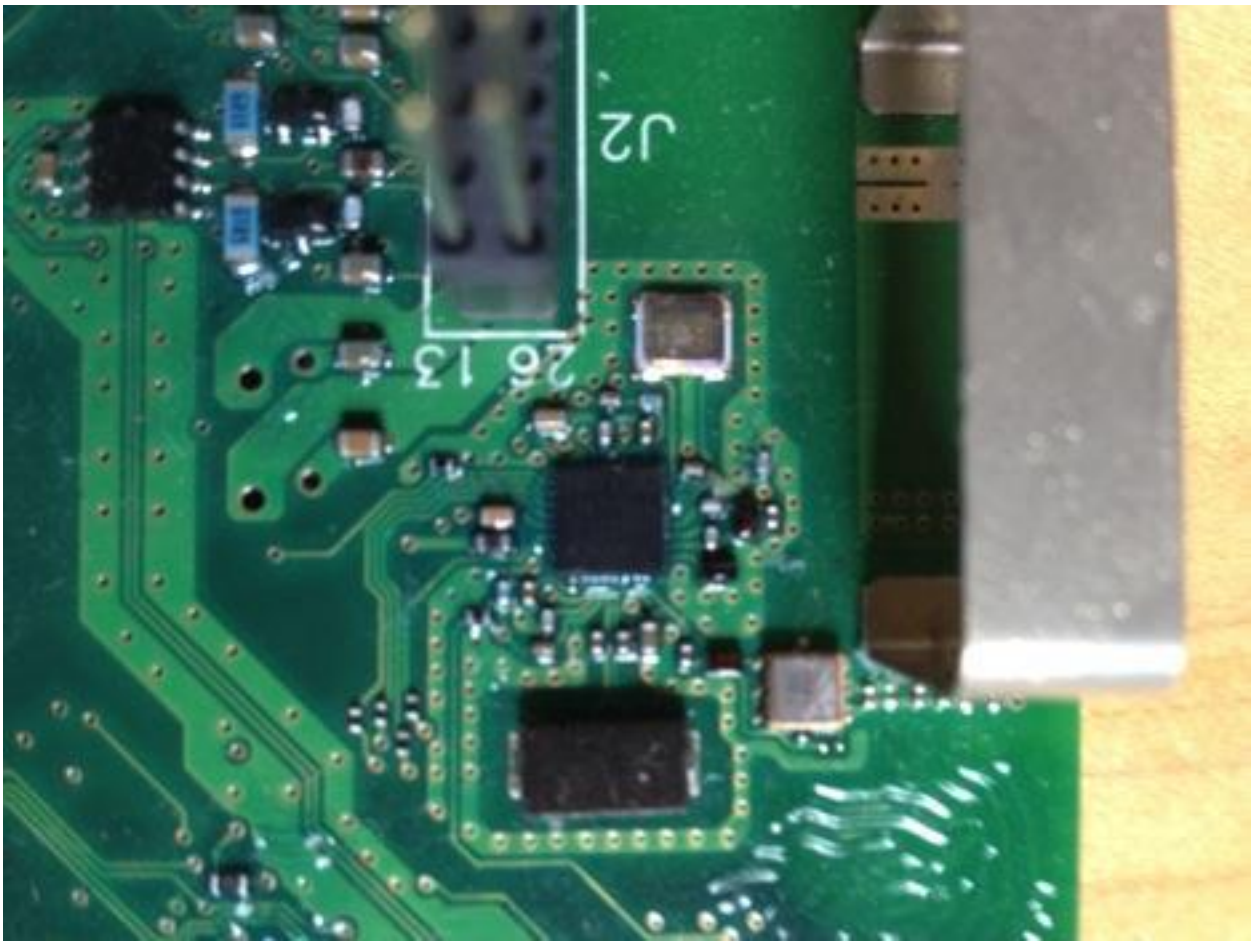


The SJB from the 2010 Ford Escape.



The circuit board from within the SJB of the 2010 Ford Escape.

The SJB contains a MAX1471A 315MHz/434MHz Low-Power, 3V/5V ASK/FSK Superheterodyne Receiver [5], see below, to receive the RF signals.



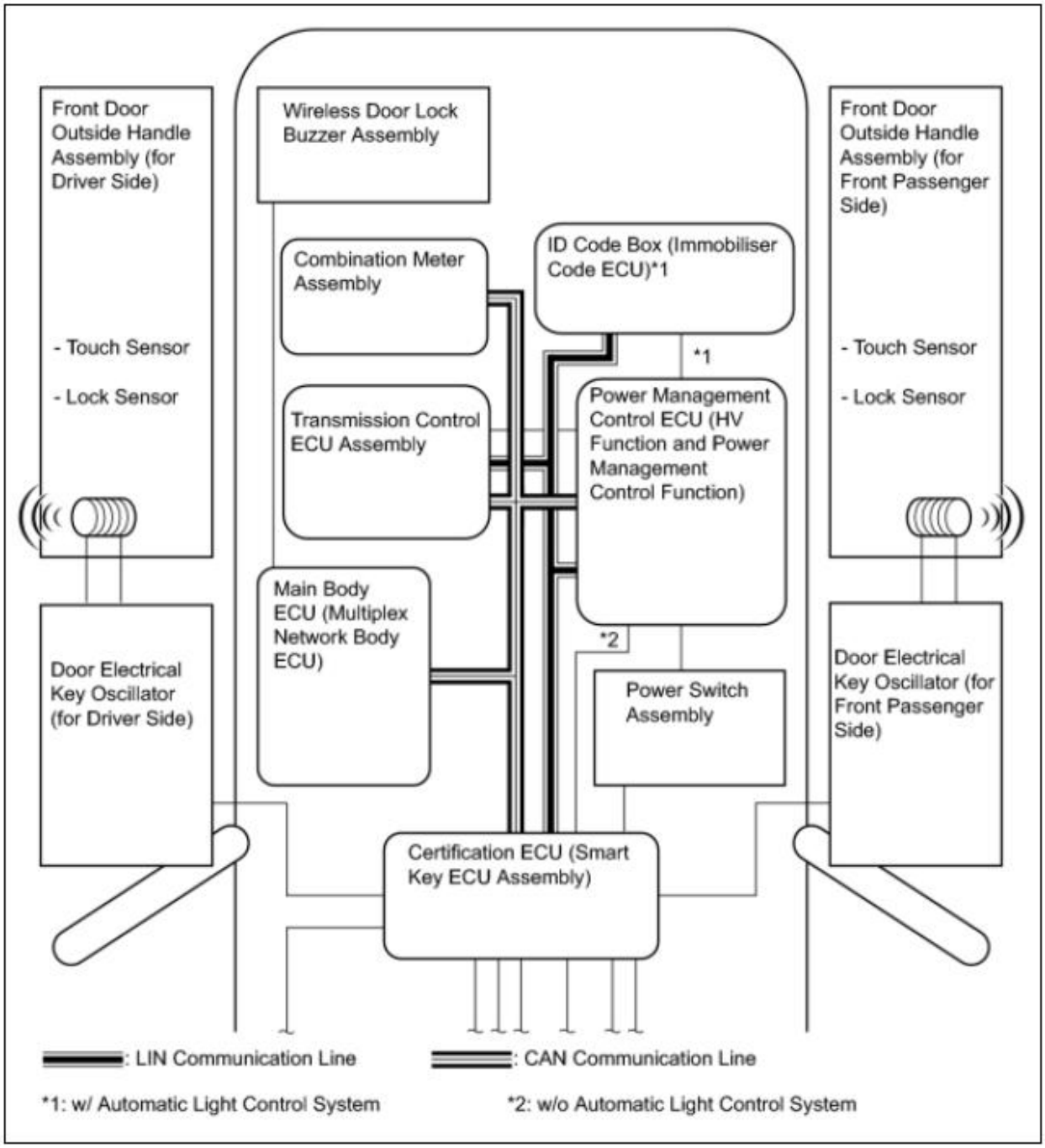
A close-up of the RF chip located on the SJB.

Range: ~1 meter.

Analysis: It is certainly possible to perform some actions against the TPMS, such as causing the vehicle to think it is having a tire problem, or problem with the TPMS system. Additionally, researchers have shown [2] that it is possible to actually crash and remotely brick the associated ECU in some cases. Regarding code execution possibilities, it seems the attack surface is rather small, but remote bricking indicates that data is being processed in an unsafe manner and so this might be possible. Additionally, many times the TPMS is not connected to the vehicle network, and is only responsible for illuminating a light on the instrument cluster.

Remote Keyless Entry / Start (RKE)

Key fobs contain a short-range radio transmitter that communicates with an ECU in the vehicle. The radio transmitter sends encrypted data containing identifying information from which the ECU can determine if the key is valid and subsequently lock, unlock, and start the vehicle. For example, in the Toyota Prius, the smart key sends a signal to a receiver, which in turn sends the information to the Smart Key ECU that is connected to the CAN and LIN buses.



Smart Key Diagram – 2010 Toyota Prius

Smart Key ECU – 2010 Toyota Prius

Range: ~5-20 meters

Analysis: Again, it may be possible to cause a denial of service that would not allow the car to be remotely locked/unlocked/started and in some cases it may be possible to unlock/start the car without the proper key fob. With regards to remote code execution, the attack surface is quite small. The Smart Key ECU must have some firmware to handle reading RF signals, encryption/decryption code, some logic to identify data from the key fob, and to be programmed for additional/replacement key fobs. While this is a possible avenue of remote code execution, the attack surface is quite small.

Bluetooth

Most vehicles have the ability to sync a device over Bluetooth with the vehicle. This represents a remote signal of some complexity processed by an ECU. In the Escape, the Bluetooth is received and processed by the Ford SYNC computer - also known as the Accessory Protocol Interface Module (APIM). This allows the car to access the address book of the phone and make phone calls. The car may also access and stream music and pictures from the phone.

The APIM for the 2010 Ford Escape

In order to pair a phone to the Escape, you have to press the phone button on the ACM, then add new phone. The ACM displays a random 6 digit PIN number that needs to be entered on the phone. The ACM even has a recorded voice instructing you what to do. There does not appear to be a way to covertly add a Bluetooth device without user interaction, although an unsolicited pairing vulnerability is not out of the realm of possibility.

Unlike the other signals up to now, the Bluetooth stack is quite large and represents a significant attack surface which has had vulnerabilities in the past [10]. There are generally two attack scenarios involving a Bluetooth stack. The first attack involves an un-paired phone. This attack is the most dangerous as any attacker can reach this code. The second method of exploitation occurs after pairing takes place, which is less of a threat as some user interaction is involved. Previously, researchers have shown remote compromise of a vehicle through the Bluetooth interface [3]. Researchers from Codenomicon have identified many crashes in common Bluetooth receivers found in automobiles [7].

Range: ~10 meters, possibly more depending on the protocol and antenna.

Analysis: Right now the authors of this paper consider Bluetooth to be one of the biggest and most viable attack surfaces on the modern automobile, due to the complexity of the protocol and underlying data. Additionally, Bluetooth has become ubiquitous within the automotive spectrum, giving attackers a very reliable entry point to test.

Radio Data System

The radio receives not only audio signals, but some other data as well. In the Escape, the Audio Control Module (ACM) has many such remote inputs, such as GPS, AM/FM Radio, and Satellite radio. These signals are mostly simply converted to audio output and don't represent significant parsing of data, which means they are likely to not contain exploitable vulnerabilities. One possible exception is likely to be the Radio Data System data that is used to send data along with FM analogue signals (or the equivalent on satellite radio). This is typically seen as radios will say the names of stations, the title of the song playing, etc. Here, the data must be parsed and displayed, making room for a security vulnerability.

The ACM for the 2010 Ford Escape

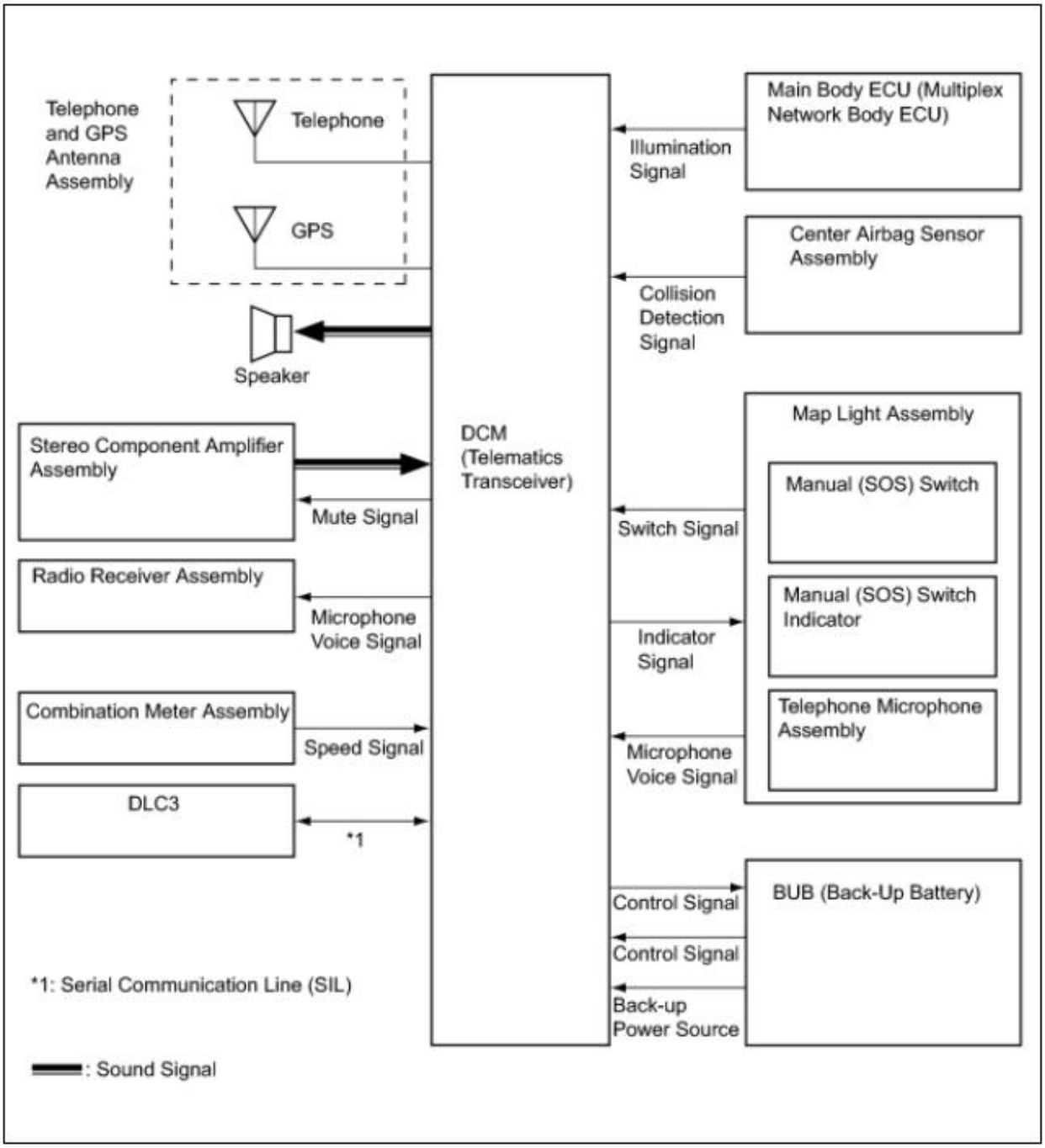
Range: Theoretically miles, but more realistically around 100 meters

Analysis: Although the end result is the same as Bluetooth, the likelihood of this attack occurring and being successful is much lower. Therefore while you could have control of the ACM, we don't perceive the threat to be as great.

Telematics / Cellular / Wi-Fi

Many modern automobiles contain a cellular radio, which is used to connect to the vehicle to a cellular network, for example GM's OnStar. It can also be used to retrieve data, such as traffic or weather information. In some newer vehicles, it even serves as a remote Wi-Fi hotspot.

The Toyota Prius came with the 'Safety Connect' feature, more generically known as a telematics system. The Safety Connect systems permit for emergency calling, stolen vehicle tracking, and roadside assistance via audio and data communications between the call center and the vehicle.



The telematics receiver in the Prius used a Qualcomm chip and communicates over a 3G/CDMA connection, as shown below.

Telematics ECU – 2010 Toyota Prius

Range: Board / Varying

Analysis: This is the holy grail of automotive attacks since the range is quite broad (i.e. as long as the car can have cellular communications). Even though a telematics unit may not reside directly on the CAN bus, it does have the ability to remotely transfer data/voice, via the microphone, to another location. Researchers previously remotely exploited a telematics unit of an automobile without user interaction [3].

Internet / Apps

As cars move into the future, they are being more connected with features normally found in desktop computers like apps and even web browsers. The 2014 Jeep Cherokee even has a Wi-Fi hotspot with open ports (when not using encryption).

```
Starting Nmap 6.01 ( http://nmap.org ) at 2014-07-27 21:57 CDT
Nmap scan report for 192.168.5.1
Host is up (0.0022s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE   VERSION
2021/tcp open  servexec?
6667/tcp open  irc?

$ nc 192.168.5.1 2021
<GCF  000059 TS_10_0000517828>CALL NADPhone:4564 NetAccess_Read handle=1
codec=CODEC_HEX;
<GCF  000084 TS_10_0000517829>CALL NADPhone:4565 NetAccess_Write handle=1
codec=CODEC_HEX data='41542B434545520D';
<GCF  000058 TS_10_0000517830>RESP NADPhone:4565 NetAccess_Write
error=WRITE_ERROR_NONE;
<GCF  000158 TS_10_0000517983>RESP NADPhone:4564 NetAccess_Read
data='0D0A2B434545523A204E6F20636175736520696E666F726D6174696F6E20617661696C61626C650D
0A0D0A4F4B0D0A' error=READ_ERROR_NONE;
```

BMW running a web browser -- http://www.techradar.com/news/car-tech/bmw-upgrades-connecteddrive-with-touch-3g-internet-apps-and-more-1159983/2

Range: N/A

Analysis: We believe this new technology opens up many attack vectors that did not exist before, such as web browser exploits, malicious apps, and internet service exploitation. Not only is the added attack surface being added in droves, but the underlying research and exploitation methodologies are widely understood by attackers. Complex code is being added to vehicles and there is no reason to believe corresponding anti-exploitation technologies are being added with them.

Cyber-physical features

In the final stage of a cyber-physical attack, the attacker wishes to send messages to a safety-critical ECU and make it take some unsafe action, such as locking up the brakes or turning the steering wheel. While this may be possible even without cyber-physical features, having the presence of computers that control physical actions make the likelihood of cyber physical attacks much higher. These advanced technology features ensure that these ECUs are listening to the messages on the network and making physical changes to the vehicle based on messages seen. We have seen safety mechanisms built into ECUs that can limit what an attacker can do. For example, the messages which indicate the steering ECU to turn the wheel for parking assist may only work if the vehicle is moving very slowly or the messages which tell the steering ECU to turn the wheel for lane keep assist may only allow very small movements of the wheel. In other words, the presence of these features is not necessarily for attack and can have protections built in, but attacks are likely easier in their presence than in their absence. Below we briefly introduce some of these cyber-physical features present on some modern automobiles.

Park assist

Park assist, also referred by some manufacturers as intelligent park assist, active park assist, parking maneuver assistant, or automatic self-parking helps the driver park in tight spots. There is usually a dedicated ECU that takes in data from sensors and calculates how the steering wheel should be turned to park in a spot. It communicates the desired steering wheel position with the steering wheel ECU that then turns the wheel. This features means that under some conditions, the steering can be turned by sending messages over the automotive network. This feature is only needed when the vehicle is moving very slowly, and in practice there are typically safety mechanisms that try to prevent the wheel from turning due to this feature when the vehicle is at anything but slow speed.

Adaptive cruise control

Adaptive cruise control is a feature that tries to maintain the desired speed of the vehicle even in the presence of other vehicles. As the vehicle approaches a slower car, it will apply the brakes to slow down, sometimes all the way to a stop if necessary. As the slower car speeds up or gets out of the way, the automobile will speed up again to the desired speed. This means that a computer is controlling the braking and acceleration of the vehicle based on sensor readings. Portions of the vehicle control are performed over the internal vehicle network and are designed to work at speed.

Collision prevention

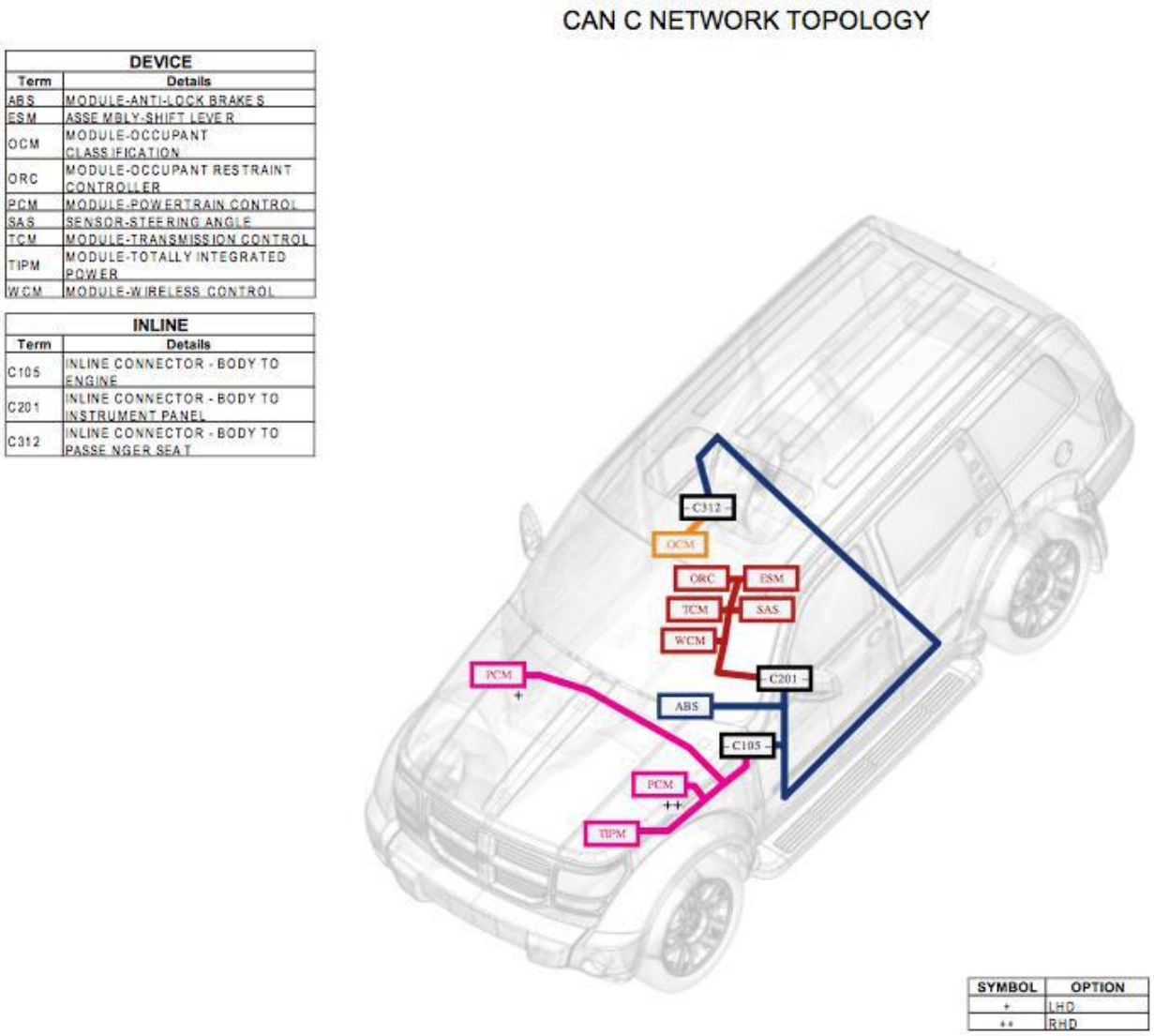
Collision prevention systems, sometimes called crash mitigation, automatic braking, city braking, or pre-collision systems are designed to prevent or lessen crashes by applying the brakes when a crash is eminent. The sensors and collision calculations are typically performed by one ECU and messages are sent to the brakes to tell them to engage. This system is designed to work at speed.

Lane keep assist

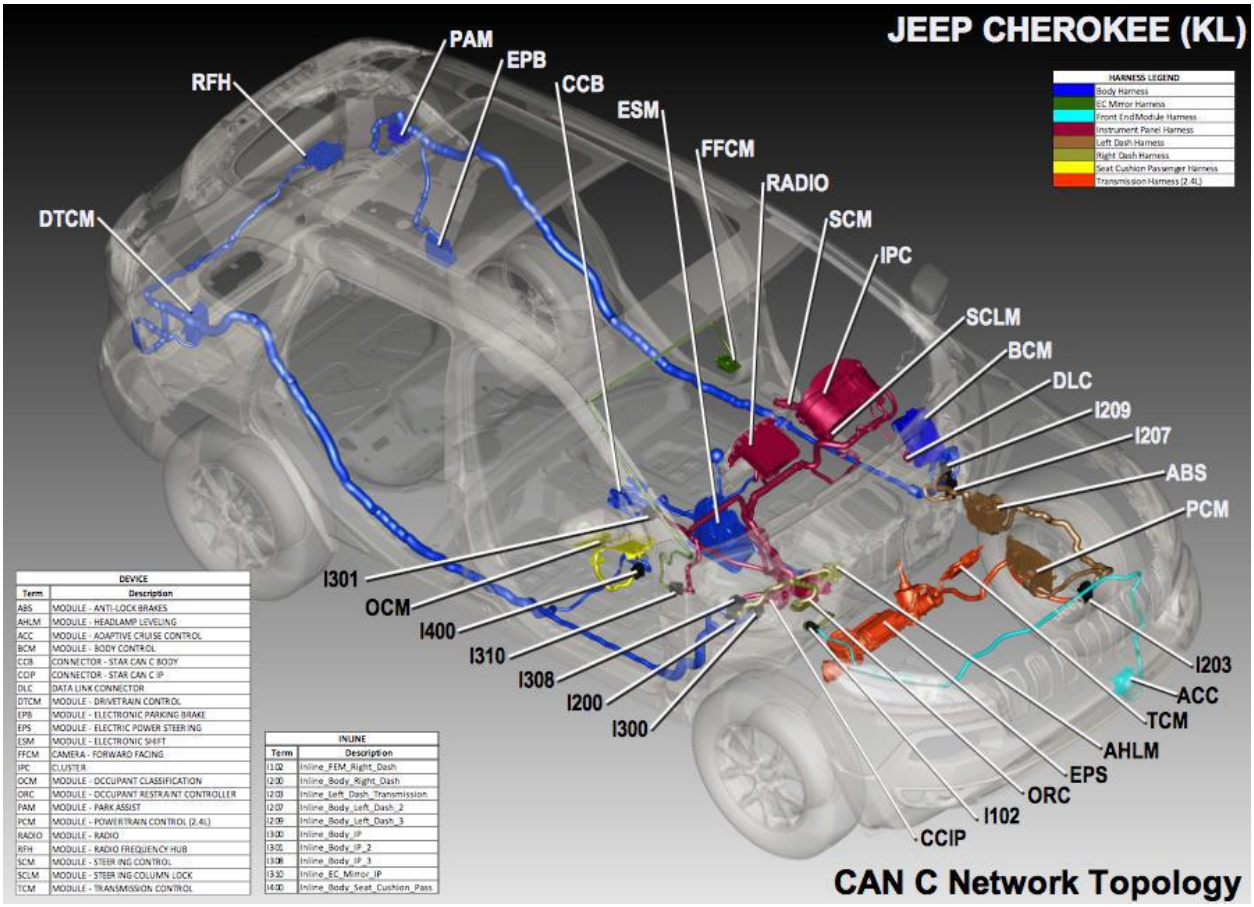
Lane keep assist, sometimes called active lane assist, LaneSense, or lane keeping assist is designed to prevent cars from leaving their lane on accident. A camera detects the lines of the lane and an ECU computes if the car is about to leave the lane. By either sending messages to the steering or brakes, the car is able to adjust the location of the car within the lane. This is another system designed to work at speed.

Evolution of Automotive Networks

As vehicles have gotten more complex, the remote attack surface has expanded. Additionally, the number of ECUs in a vehicle has gone up with the complexity of the automotive network increasing. For example, consider the Jeep Cherokee from 2010 vs 2014. In just 4 years, the number of ECUs has more than doubled. Below are illustrations of the CAN C network for this vehicle from 2010 and 2014.



CAN-C Network – 2010 Jeep Cherokee



CAN-C Network – 2014 Jeep Cherokee

As you can see, the 2014 Jeep has almost twice as many ECUs, resulting in added complexity and also denotes a manufacturer's necessity to multiplex more of the automobile. New features are more easily added into existing automobile infrastructure, instead of running new wires or adding additional networks.

Remote Survey

The cars examined in this paper have had their features, standards, and network architecture examined to determine the functionality and subsequent remote attack surface documented. For each vehicle we document

- The remote attack surface (i.e. Bluetooth, telematics, etc)
- The cyber physical computer controlled features. The term cyber physical is used to denote automotive features that perform physical actions through the input of message on the automotive network, such as adaptive cruise control, collision prevention, and many others
- Layout of the internal automotive network, including the ECUs with remote attack surface and the ECUs with safety critical components

By looking at the layout of the internal automotive networks, the locations of the various ECUs, and considering the safety critical computer controlled features, one can begin to get a grasp on the difficulty (or simplicity) of remote attacks against that particular vehicle.

Obviously we were not able to acquire each vehicle for detailed testing, but the first step in any automotive assessment would be a features and architecture review. ECUs that are bolded have significance with regards to wireless exploitation, communications bridging, or having cyber physical functionality.

We were aware that certain manufacturers are not present in this paper. Many times it was due to overlap in parent company's vehicles and other times we found their online experience too painful to navigate.

Legend

2014 Audi A8

http://image.motortrend.com/f/roadtests/sedans/1307_2014_audi_a8_l_tdi_first_test/52692898/2013-audi-a8-l-3-0t-side-in-motion.jpg

Standards: CAN, LIN, MOST, FlexRay

Wireless Communications: Remote Keyless Entry / Start, Bluetooth, Cellular, Wi-Fi, AM/FM/XM Radio, Proprietary Radio, Audi Connect

Cyber Physical: Adaptive Cruise Control, Active Lane Assist, Audi Pre-Sense

Drivetrain CAN
1. ECM (J623) 2. ABS (J104) 3. Airbag Control (J234) 4. Transmission Control Module (J217) 5. Electrical Drive Main Relay (J437) 6. Electro-Mechanical Parking Brake Control Module (J540) 7. Level Control System Control Module (J197) 8. Steering Angle Sensor (G85) **9. Data Bus on Board Diagnostic Interface (J533)**

Convenience CAN

1. Driver's Door Control Module (J386)
2. Front Passengers Door Control Module (J387)
3. Left Rear Door Control Module (J388)
4. Right Rear Door Control Module (J389)
5. Memory Seat / Steering Column Adjustment Control Module (J136)
6. Passenger Memory Seat Control Module (J521)
7. Towing Recognition Control Module (J345)
8. Steering Column Electronics System Control Module (J527)
9. **Tire Pressure Monitoring Control Module** (J502)
    a. Connected via LIN to TPMS Transmitters
10. Climatronic Control Module (J255)
    a. Connected via LIN to A/C
11. Comfort System Central Control Module (J393)
12. Vehicle Electronic System Control Module (J519)
13. **Access/Start Control Module (J518)**
    a. Connected via LIN to Access/Start Authorization Switch (E415) & Keyless Access Authorization Antenna Reader (J723)
14. Vehicle Electrical System Control Module (J520)
15. Parking Aid Control Module (J446)
16. Auxiliary Heater Control Module (J364)
17. Energy Management Control Module (J644)
18. **Data Bus on Board Diagnostic Interface (J533)**

Instrument Cluster / Gateway CAN

1. Instrument Cluster Control Module (J285)
2. **Data Bus on Board Diagnostic Interface (J533)**

Distance Control CAN

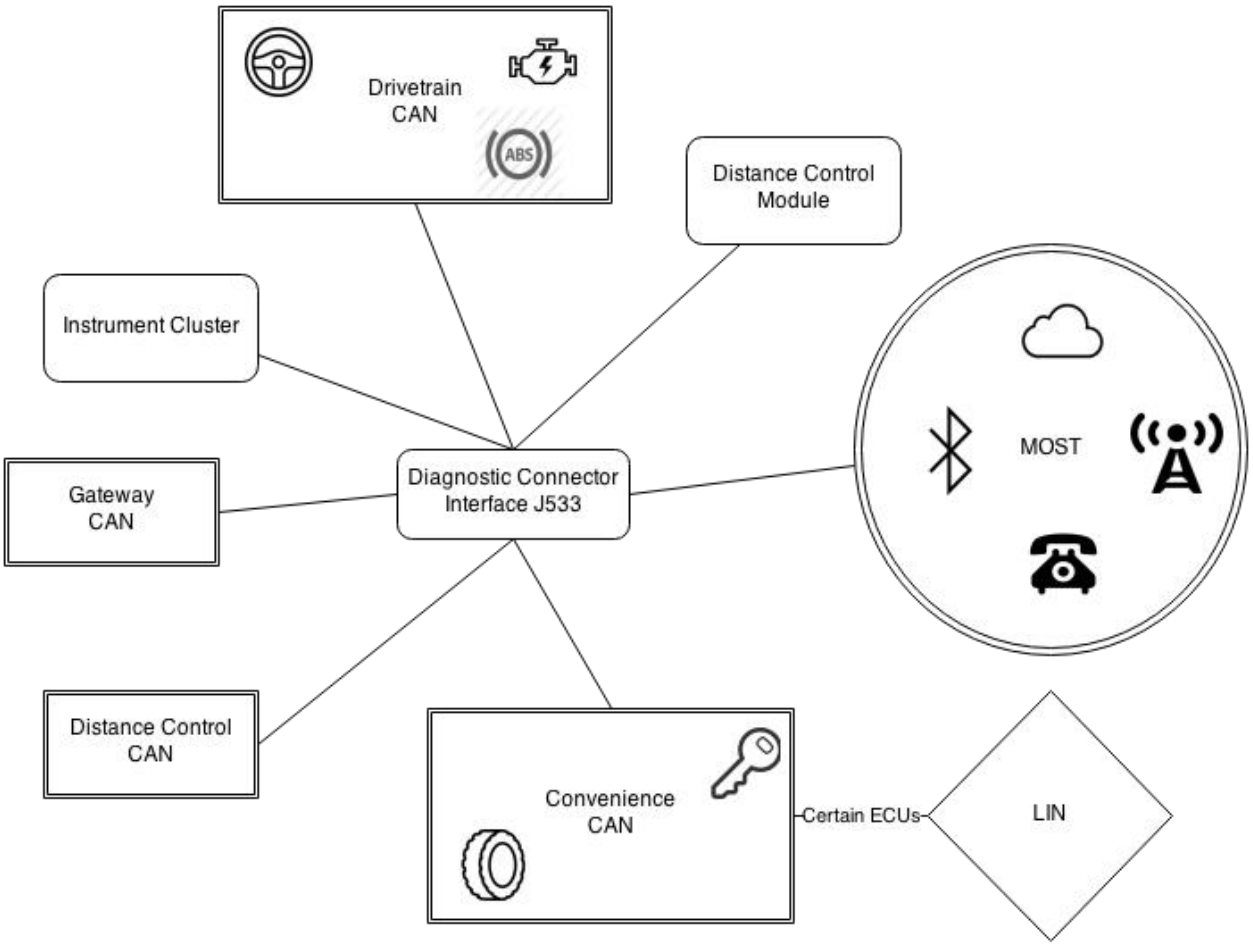
1. Distance Regulation Control Module (J428)
2. **Data Bus on Board Diagnostic Interface (J533)**

MOST Ring

1. CD Changer (R41)
2. Digital Sound System Control Module (J525)
3. Radio & Speech Input Control Module (J507)
4. TV Tuner (R78)
5. Navigation system w/ CD Drive Control Module (J401)
6. **Telephone/Telematics Control Module (J526)**
    a. Bluetooth
    b. Telephone Handset (R37)
7. **Telephone Transceiver (R36)**
8. Front Information Control Head Control Module (J523)
9. **Data Bus on Board Diagnostic Interface (J533)**

Entry Point	ECU	Bus
RKE	Access Control Module	Convenience CAN
TPMS	Tire Pressure Control Module	Convenience CAN
Bluetooth	Telematics Control Unit	MOST Ring
FM/AM/XM	Radio Control Module	MOST Ring
Cellular	Telematics Control Module	MOST Ring
Internet / Apps	Audi Connect System	MOST Ring

Diagram



2014 Honda Accord LX (Sedan)

http://images.newcars.com/images/car-pictures/original/2014-Honda-Accord-Sedan-LX-4dr-Sedan-Photo.png

Standards: CAN, K-Line, S-NET

Wireless Communications: Remote Keyless Entry, Bluetooth, AM/FM/XM Radio, Proprietary Radio, HondaLink

Cyber Physical: Adaptive Cruise Control, Forward Collision Warning, Lane Watch

B-CAN
1. Under-Dash Fuse/Relay Box **2. Audio Unit / Navigation Unit** 3. HVAC Control / Climate Control Unit 4. Power Window Master Switch **5. Center Junction Box** **6. Driver's Junction Box** 7. Sunlight Sensor 8. Gauge Control Module **9. Keyless Access Control Unit** **10.** Power Seat Control Unit

F-CAN

1. Powertrain Control Module (PCM)
2. VSA Modulator-Control Unit
3. EPS Control Unit
4. Engine Mount Control Unit
5. SRS Unit
6. ANC / Active Sound Control Unit
7. DLC
8. **Center Junction Box**
9. Steering Angle Sensor
10. Gauge Control Module
11. ACC Unit
12. **Audio Unit / Navigation Unit**
13. **Driver's Junction Box**
14. FCW/LDW Camera Unit

K-Line

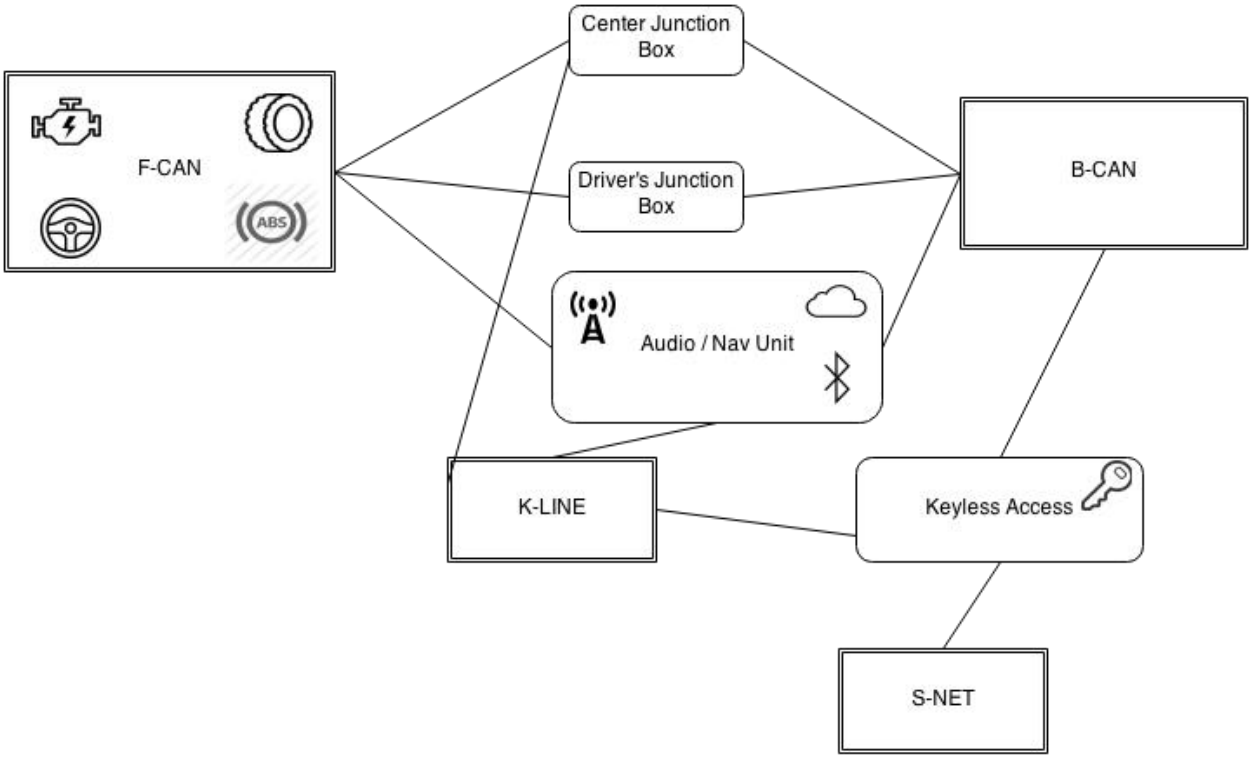
1. Front Passenger's Weight Sensor
2. VSA Modulator-Control Unit
3. EPS Control Unit
4. Under-Dash Fuse / Relay Box
5. ANC/Active Sound Control Unit
6. **Audio Unit / Navigation Unit**
7. **Keyless Access Control Unit**
8. **DLC**
9. **Center Junction Box**

S-NET

1. Under-Dash Fuse / Relay Box
2. **Keyless Access Control Unit**
3. PCM

Entry Point	ECU	Bus
RKE	Keyless Access Control Unit	B-CAN / K-Line / S-NET
TPMS	VSA Modulator-Control Unit	F-CAN
Bluetooth	Audio Unit / Navigation Unit	F-CAN / B-CAN / K-Line
FM/AM/XM	Audio Unit / Navigation Unit	F-CAN / B-CAN / K-Line
Cellular	N/A	N/A
Internet / Apps	HondaLink	F-CAN / B-CAN / K-Line

Diagram


Center Junction Box
F-CAN
Driver's Junction Box
B-CAN
Audio / Nav Unit
K-LINE
Keyless Access
S-NET

2014 Infiniti Q50

http://images.dealer.com/autodata/us/640/color/2014/USC40INC251A0/GAC.jpg

Standards: CAN

Wireless Communications: Remote Keyless Entry, Bluetooth, Cellular, AM/FM/XM Radio, Proprietary Radio, Infiniti Connect

Cyber Physical: Adaptive Cruise Control, Direct Adaptive Steering, Steer-by-wire, Driver Assistance System

Intelligent Transportation Systems (ITS) Communications Circuit
1. Side Radar LH **2. Around view Mirror Control Unit** 3. Driver Assistance Buzzer Control Unit 4. Side Radar RH 5. Acceleration Pedal Actuator 6. Sonar Control Unit **7. ICC Sensor** **8. ADAS Control Unit (GATEWAY)**

Chassis Communications Circuit

1. Steering Angle Main Control Module
2. Lane Camera Unit
3. **Chassis Control Module (Gateway)**

CAN Communications Circuit 2

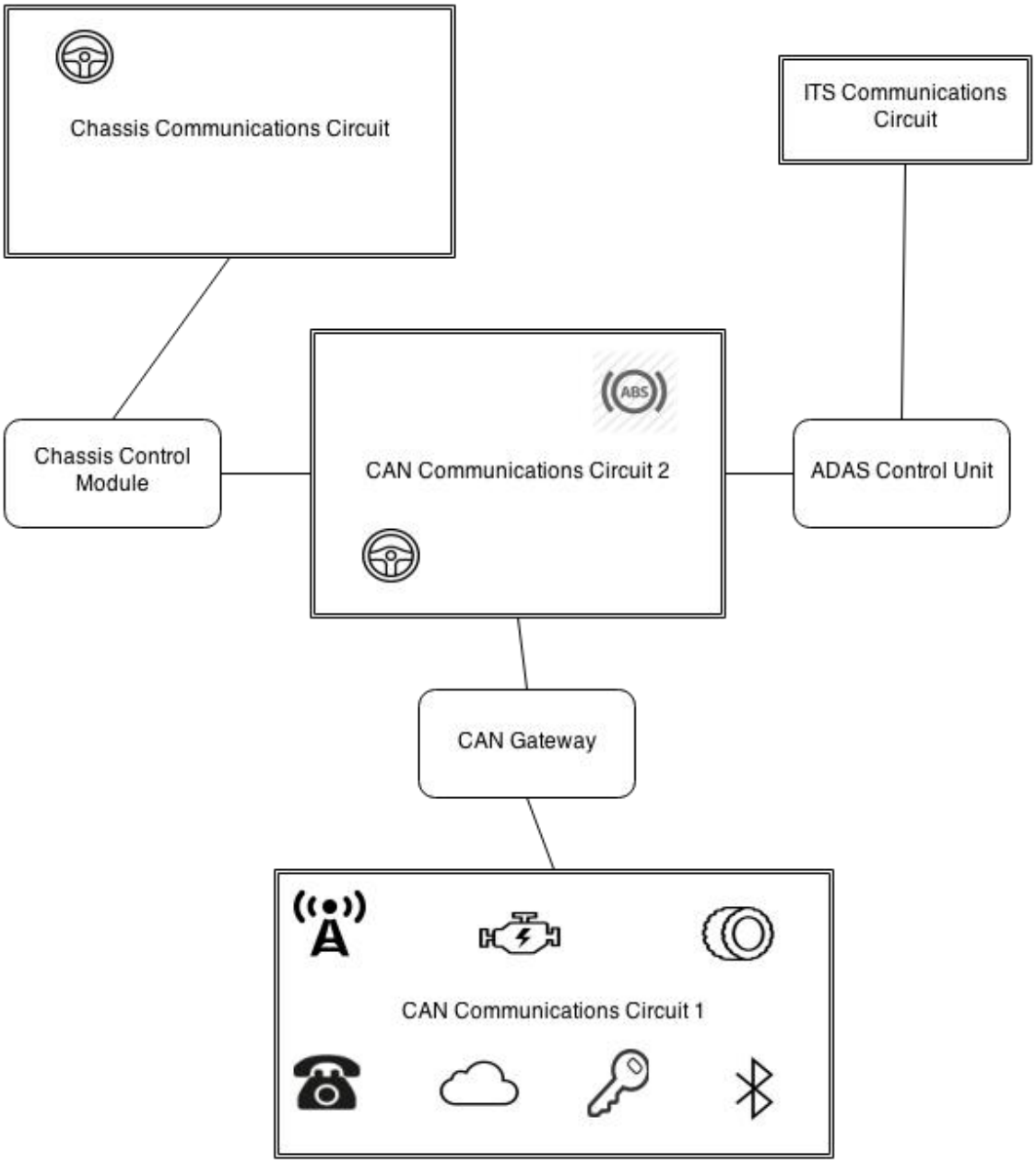
1. **Chassis Control Module (Gateway)**
2. **ADAS Control Unit (Gateway)**
3. ABS Control Unit
4. Pre-Crash Seat Belt Control
5. AWD Control Unit
6. Driver Seat Control Unit
7. **Steering Force Control Module**
8. Steering Angle Sensor
9. DLC (ODB-II)
10. **CAN Gateway (Gateway)**

CAN Communications Circuit 1

1. IPDM E/R (Intelligent Power Distribution Module Engine Room)
2. Combination Meter
3. AFS Control Unit (Adaptive Front lighting System)
4. High Beam Assist Control Module
5. ECM (Engine Control Module)
6. TCM (Transmission Control Module)
7. A/C Auto Amp
8. Airbag Diagnosis Sensor Unit
9. Display Control Unit
10. **TCU (Telematics Control Unit)**
11. **BCM (Body Control Module)**
12. DLC (ODB-II)
13. **CAN Gateway (Gateway)**

Entry Point	ECU	Bus
RKE	BCM	CAN Communications Circuit 1
TPMS	BCM	CAN Communications Circuit 1
Bluetooth	TCU	CAN Communications Circuit 1
FM/AM/XM	TCU	CAN Communications Circuit 1
Cellular	TCU	CAN Communications Circuit 1
Internet / Apps	TCU	CAN Communications Circuit 1

Diagram


Chassis Communications Circuit
ITS Communications Circuit
Chassis Control Module
CAN Communications Circuit 2
ADAS Control Unit
CAN Gateway
CAN Communications Circuit 1

2010 Infiniti G37 (Sedan)

http://images.thecarconnection.com/lrg/2010-infiniti-g37-sedan_100234015_l.jpg

Standards: CAN

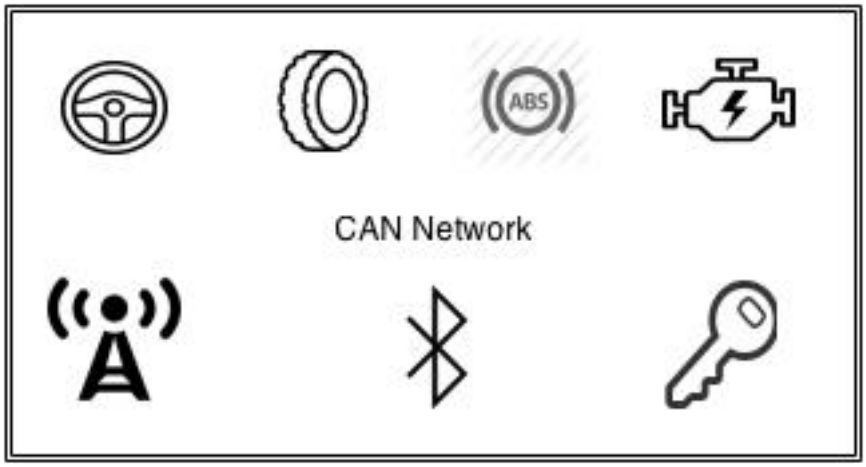
Wireless Communications: Remote Keyless Entry, Bluetooth, AM/FM/XM Radio, Proprietary Radio

Cyber Physical: Adaptive Cruise Control, Pre-Crash System

CAN Network
1. Steering Angle Sensor 2. Unified Meter and A/C Amp 3. TCM (Transmission Control Module) 4. Pre-Crash Seat Belt Control Unit 5. ECM (Engine Control Module) 6. AWD Control Unit **7. A/V Control Unit** 8. Airbag Diagnosis Sensor Unit **9. BCM (Body Control Module)** 10. ICC Integrated Circuit (Intelligent Cruise Control) 11. IPDM E/R (Intelligent Power Distribution Module Engine Room) 12. ABS Actuator and ECU 13. 4WAS Main Control Unit 14. Driver Seat Control Unit **15. DLC**

Entry Point	ECU	Bus
RKE	BCM	CAN
TPMS	BCM	CAN
Bluetooth	A/V Control Unit	CAN
FM/AM/XM	A/V Control Unit	CAN
Cellular	N/A	N/A
Internet / Apps	N/A	N/A

Diagram



2006 Infiniti G35 (Sedan)

http://upload.wikimedia.org/wikipedia/commons/f/f2/2006-Infiniti-G35-sedan.jpg

Standards: CAN

Wireless Communications: Remote Keyless Entry, Bluetooth, AM/FM/XM Radio, Proprietary Radio

Cyber Physical: Adaptive Cruise Control, Pre-Crash System

CAN Communications
1. ABS/TCS/VDS 2. Intelligent Key Unit 3. IPDM E/R 4. ECM 5. AWD ECU 6. Combination Meter **7. BCM** 8. Steering Angle Sensor 9. Driver Seat Control Unit 10. Transmission Control Module (A/T Assembly) 11. DLC

Entry Point	ECU	Bus
RKE	BCM	CAN
TPMS	BCM	CAN
Bluetooth	A/V Control Unit	None
FM/AM/XM	A/V Control Unit	None
Cellular	N/A	N/A
Internet / Apps	N/A	N/A

Diagram

2014 Jeep Cherokee

http://www.digitaltrends.com/wp-content/uploads/2013/02/2014-jeep-cherokee-1.jpg

Standards: CAN, LIN

Wireless Communications: Remote Keyless Entry, Bluetooth, AM/FM/XM Radio, Cellular, Wi-Fi, Proprietary Radio, Uconnect

Cyber Physical: Adaptive Cruise Control with Stop and go, Parallel and Perpendicular Parking Assist, Forward Collision Warning with Crash Mitigation, LaneSense Lane Departure Warning

CAN C Bus

1. ABS MODULE - ANTI-LOCK BRAKES
2. AHLM MODULE - HEADLAMP LEVELING
3. ACC MODULE - ADAPTIVE CRUISE CONTROL
4. **BCM MODULE - BODY CONTROL**
5. CCB CONNECTOR - STAR CAN C BODY
6. CCIP CONNECTOR - STAR CAN C IP
7. **DLC DATA LINK CONNECTOR**
8. DTCM MODULE - DRIVETRAIN CONTROL
9. EPB MODULE - ELECTRONIC PARKING BRAKE
10. EPS MODULE - ELECTRIC POWER STEERING
11. ESM MODULE - ELECTRONIC SHIFT
12. FFCM CAMERA - FORWARD FACING
13. IPC CLUSTER
14. OCM MODULE - OCCUPANT CLASSIFICATION
15. ORC MODULE - OCCUPANT RESTRAINT CONTROLLER
16. PAM MODULE - PARK ASSIST
17. PCM MODULE - POWERTRAIN CONTROL (2.4L)
18. **RADIO MODULE - RADIO**
19. RFH MODULE - RADIO FREQUENCY HUB
20. SCM MODULE - STEERING CONTROL
21. SCLM MODULE - STEERING COLUMN LOCK
22. TCM MODULE - TRANSMISSION CONTROL

CAN IHS Bus

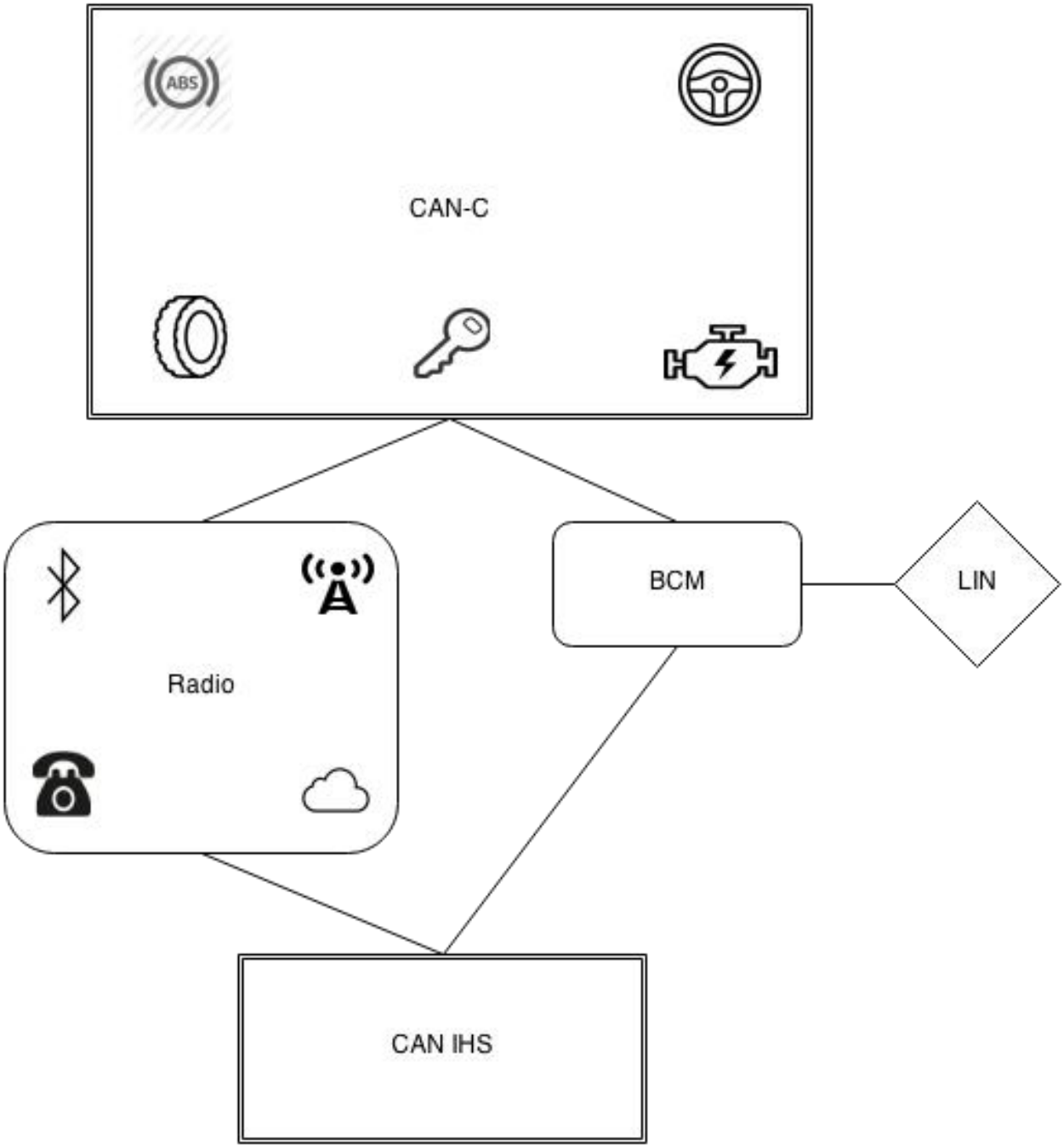
1. AMP AMPLIFIER - RADIO
2. **BCM MODULE - BODY CONTROL**
3. CCB CONNECTOR - STAR CAN IHS BODY
4. CCIP CONNECTOR - STAR CAN IHS IP
5. DDM MODULE - DOOR DRIVER
6. DLC DATA LINK CONNECTOR
7. EDM MODULE - EXTERNAL DISC
8. HSM MODULE - HEATED SEATS
9. HVAC MODULE - A/C HEATER
10. ICS MODULE - INTEGRATED CENTER STACK SWITCH
11. IPC MODULE - CLUSTER
12. LBSS SENSOR - BLIND SPOT LEFT REAR
13. MSM MODULE - MEMORY SEAT DRIVER
14. PDM MODULE - DOOR PASSENGER
15. PLGM MODULE - POWER LIFTGATE
16. **RADIO MODULE - RADIO (Not a Bridge)**
17. RBSS SENSOR - BLIND SPOT RIGHT REAR

LIN Bus

1. AGS ACTUATOR-GRILL SHUTTER
2. AHLM MODULE-HEADLAMP LEVELING
3. ASBM SWITCH-BANK
4. ASU SIREN
5. **BCM MODULE-BODY CONTROL**
6. CRVMM ASSEMBLY-REAR VIEW MIRROR
7. DDM MODULE-DOOR-DRIVER
8. DSBM SWITCH-WINDOW / DOOR LOCK-DRIVER
9. FLLA ASSEMBLY-LAMP-LEFT FRONT
10. FRLA ASSEMBLY-LAMP-RIGHT FRONT
11. GEN GENERATOR
12. HUM SENSOR-HUMIDITY
13. IBS SENSOR-BATTERY CURRENT
14. IPC MODULE-CLUSTER
15. ITM MODULE-INTRUSION
16. LRSM MODULE-LIGHT RAIN SENSOR
17. PADL LAMP-AIRBAG DISABLE
18. PCM MODULE-POWERTRAIN CONTROL
19. PCM Diesel MODULE-POWERTRAIN CONTROL
20. RVCM ASSEMBLY-VIDEO CAMERA
21. SCCM MODULE-STEERING CONTROL
22. TSBM MODULE-TERRAIN SWITCH BANK
23. VSM MODULE-VOLTAGE STABILITY
24. WCPM MODULE-CHARGER WIRELESS

Entry Point	ECU	Bus
RKE	RFHM	CAN C
TPMS	RFHM	CAN C
Bluetooth	Radio	CAN C, CAN IHS
FM/AM/XM	Radio	CAN C, CAN IHS
Cellular	Radio	CAN C, CAN IHS
Internet / Apps	Radio	CAN C, CAN IHS

Diagram



2014 Dodge Ram 3500

http://images6.alphacoders.com/417/417590.jpg

Standards: CAN, LIN

Wireless Communications: Remote Keyless Entry, Bluetooth, AM/FM/XM Radio, Cellular, Wi-Fi, Proprietary Radio, Uconnect

Cyber Physical: It's big. It burns lots of gas.

CAN C Bus
1. ABS 2. ASCM 3. BCM 4. DTCM 5. ITBM 6. PAM 7. PCM 8. ORC 9. RADIO 10. RFH 11. SCCM 12. TCM **13.** VSIM

CAN IHS Bus

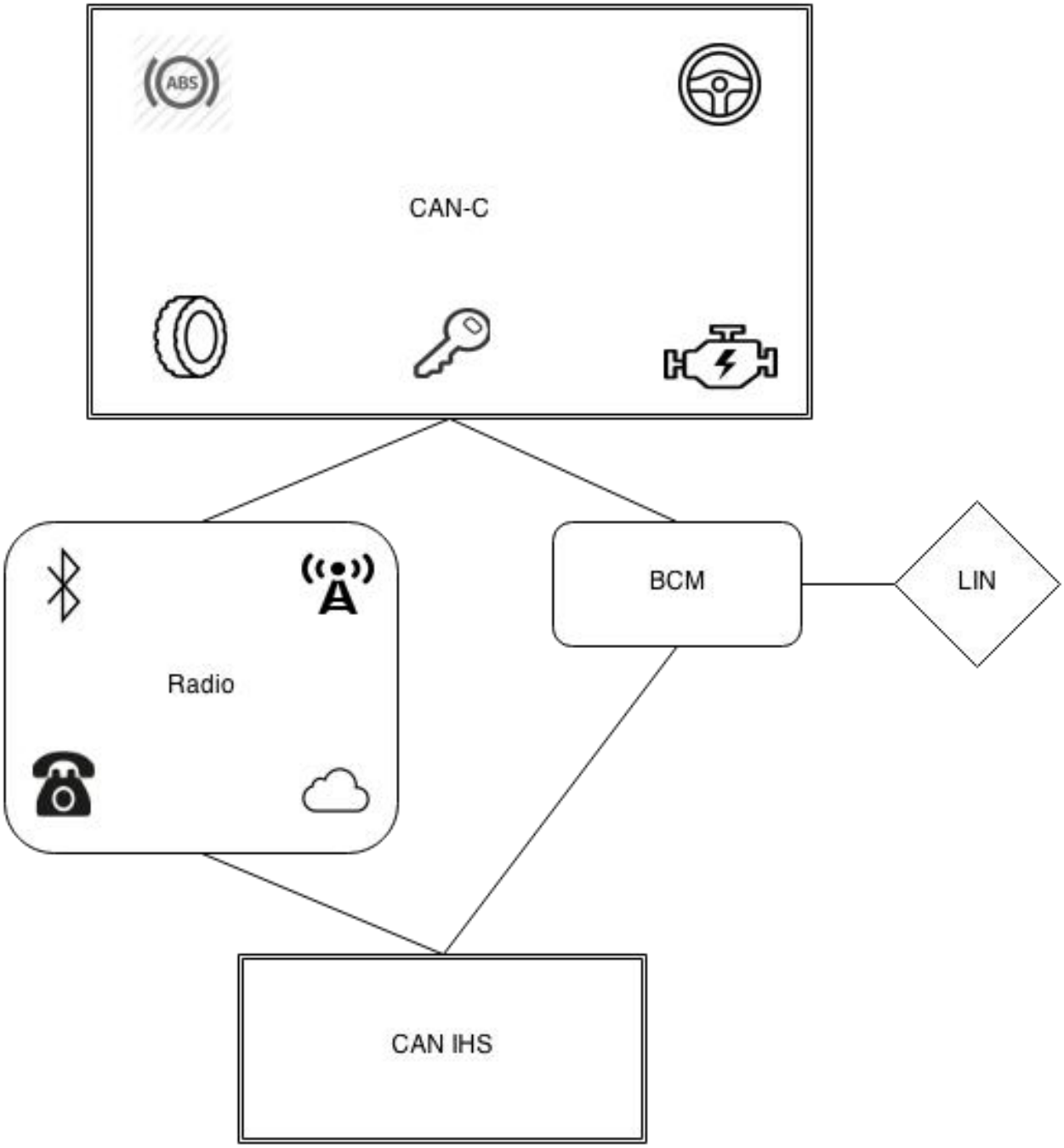
1. AMP
2. BCM
3. DDM
4. EDM
5. HSM
6. HVAC
7. ICS
8. MSM
9. PDM
10. RADIO

LIN Bus

1. BCM
2. COM
3. DDM
4. LRSM
5. SCCM

Entry Point	ECU	Bus
RKE	RFH	CAN C
TPMS	RFH	CAN C
Bluetooth	Radio	CAN C, CAN IHS
FM/AM/XM	Radio	CAN C, CAN IHS
Cellular	Radio	CAN C, CAN IHS
Internet / Apps	Radio	CAN C, CAN IHS

Diagram



2014 Chrysler 300

http://www.chrysler.com/assets/images/Vehicles/2014/300/PhotosVideos/Exterior/large/300_ext_expand_0000_15.jpg

Standards: CAN, LIN

Wireless Communications: Remote Keyless Entry, Bluetooth, AM/FM/XM Radio, Wi-Fi, Cellular, Proprietary Radio, Uconnect

Cyber Physical: Adaptive Cruise Control, Park Assist

CAN C Bus
1. ABS 2. AFLS 3. **BCM** 4. IPC 5. ORC 6. PAM 7. PCM 8. RFH 9. SCCM 10. TCP 11. TPM

CAN IHS Bus

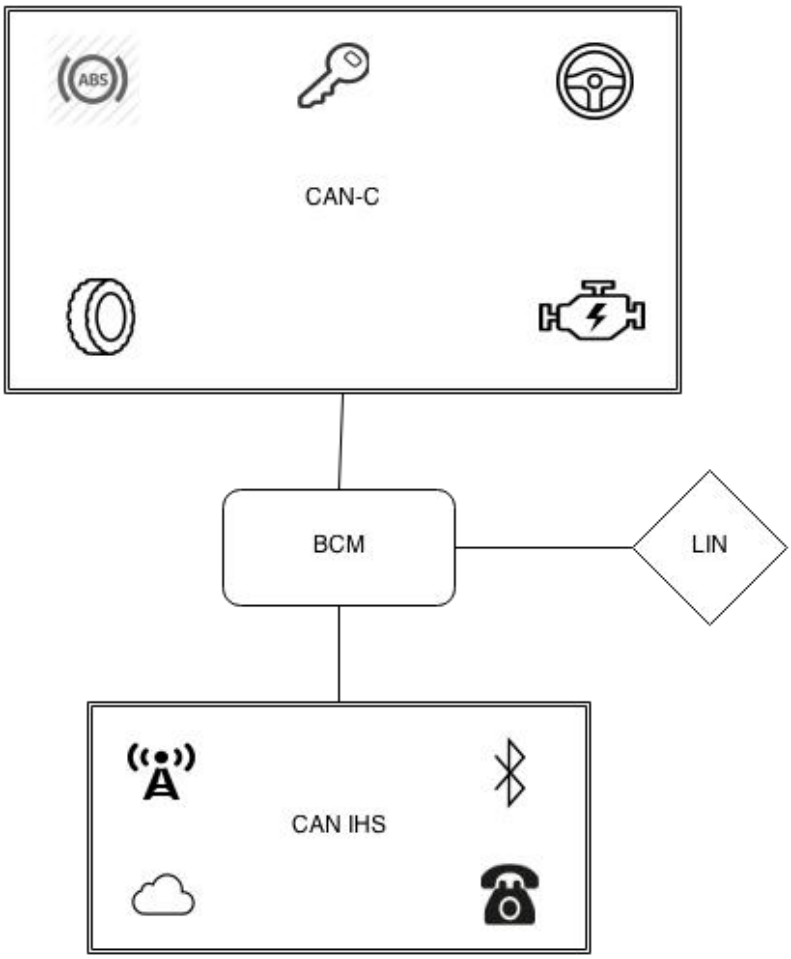
1. **BCM**
2. DDM
3. HSM
4. HVAC
5. MSM
6. PDM
7. **RADIO**

LIN Bus

1. AFLS
2. BCM
3. COM
4. DDM
5. LRSM
6. SCCM

Entry Point	ECU	Bus
RKE	RFH	CAN C
TPMS	TPM	CAN C
Bluetooth	Radio	CAN IHS
FM/AM/XM	Radio	CAN IHS
Cellular	Radio	CAN IHS
Internet / Apps	Radio	CAN IHS

Diagram



2014 Dodge Viper

http://www.drivesrt.com/news/wp-content/uploads/2013/09/TA-Color.jpg

Standards: CAN, LIN

Wireless Communications: Remote Keyless Entry, Bluetooth, AM/FM/XM Radio, Wi-Fi, Cellular, Proprietary Radio, Uconnect

Cyber Physical: Fast

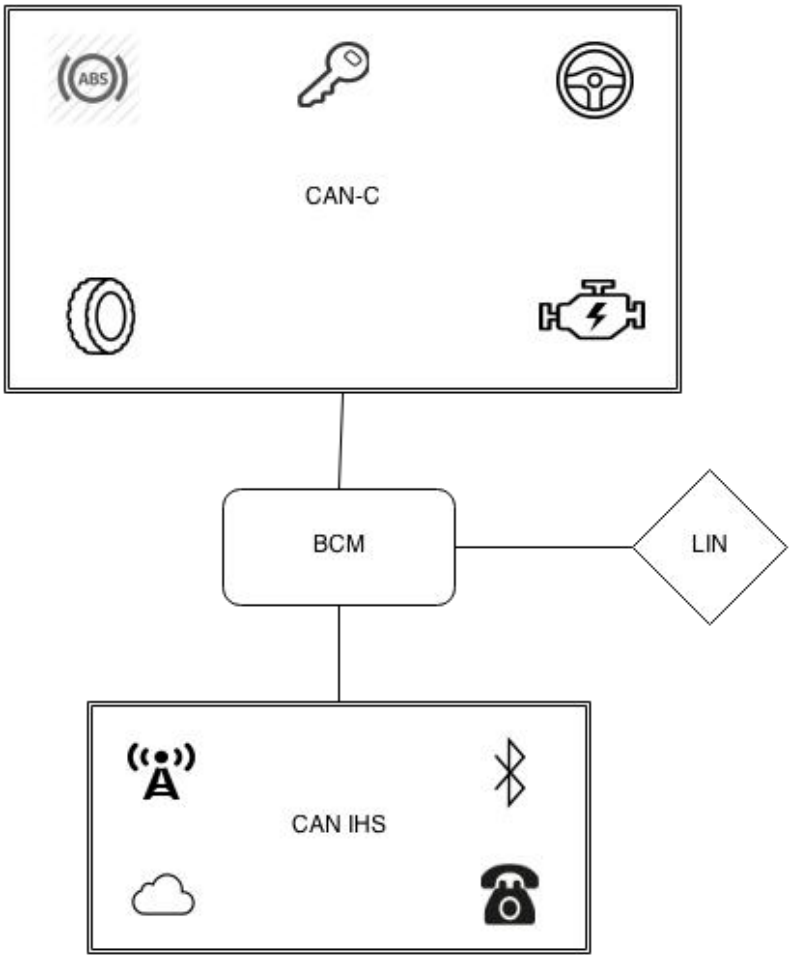
CAN C Bus
1. ABS
2. ADCM
3. **BCM**
4. ORC
5. PCM
6. RFH
7. SCCM
8. TPM

LIN Bus
1. BCM
2. DDM
3. SCCM

CAN IHS Bus
1. **BCM** 2. DDM 3. HVAC 4. ICS 5. PDM 6. RADIO

Entry Point	ECU	Bus
RKE	RFH	CAN C
TPMS	TPM	CAN C
Bluetooth	Radio	CAN IHS
FM/AM/XM	Radio	CAN IHS
Cellular	Radio	CAN IHS
Internet / Apps	Radio	CAN IHS

Diagram



2015 Cadillac Escalade AWD

http://image.motortrend.com/f/roadtests/suvs/1310_2015_cadillac_escalade_first_look/54528620/2015-cadillac-escalade-front-three-quarters-view.jpg

Standards: CAN, MOST, LIN

Wireless Communications Remote Keyless Entry, Bluetooth, AM/FM/XM Radio, Wi-Fi, Cellular, Proprietary Radio, OnStar

Cyber Physical: Front and rear automatic breaking, Automatic collision preparation, Full-speed adaptive cruise control

PT-CAN (power train controller area network)
1. DME **2.** ACSM **3.** KAFAS **4.** EKPS **5.** EGS **6.** GWS

Low Speed GMLAN (CAN)

1. info display module
2. radio
3. **telematics communication interface module (TCIM)**
4. HVAC
5. media disc player
6. instrument cluster
7. passenger presence module
8. **keyless entry control module (KECM)**
9. trailer interface control module
10. front and rear parking assist control module
11. side object sensor module left
12. active safety control module
13. **body control module**
14. lift gate control module
15. video processing control module
16. inflatable restraint sensing and diagnostic module
17. assist step control module

High Speed GMLAN (CAN)

1. distance sensing cruise control module
2. engine control module
3. transmission control module
4. active safety control module **
5. **telematics communication interface control module (TCIM)**
6. human machine interface control module
7. power steering control module
8. **body control module**
9. electronic brake control module
10. park brake control module
11. suspension control module
12. chassis control module

LIN

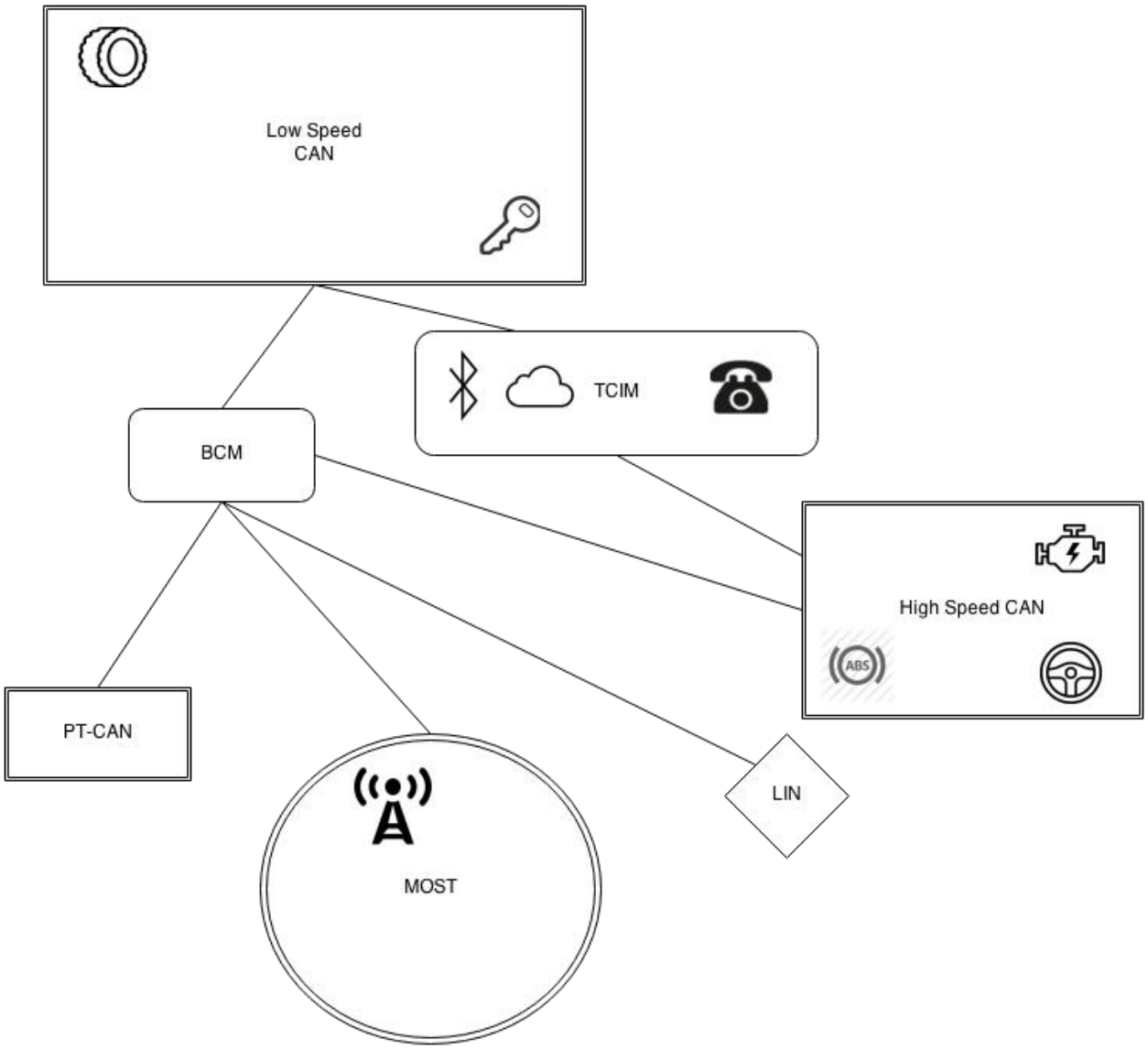
1. **BCM**
2. TPIM

MOST

1. **RADIO**
2. Instrument cluster
3. Amp
4. Media disk player
5. Human interface control module

Entry Point	ECU	Bus
RKE	KECM	Low Speed CAN
TPMS	KECM	Low Speed CAN
Bluetooth	TCIM	Low & High Speed CAN
FM/AM/XM	Radio	MOST
Cellular	TCIM	Low & High Speed CAN
Internet / Apps	TCIM	Low & High Speed CAN

Diagram



2006 Ford Fusion

http://www.blogcdn.com/www.autoblog.com/media/2006/03/Ford-Fusion-Crash-test-resized.jpg

Standards: CAN

Wireless Communications: Remote Keyless Entry, AM/FM Radio, Proprietary Radio

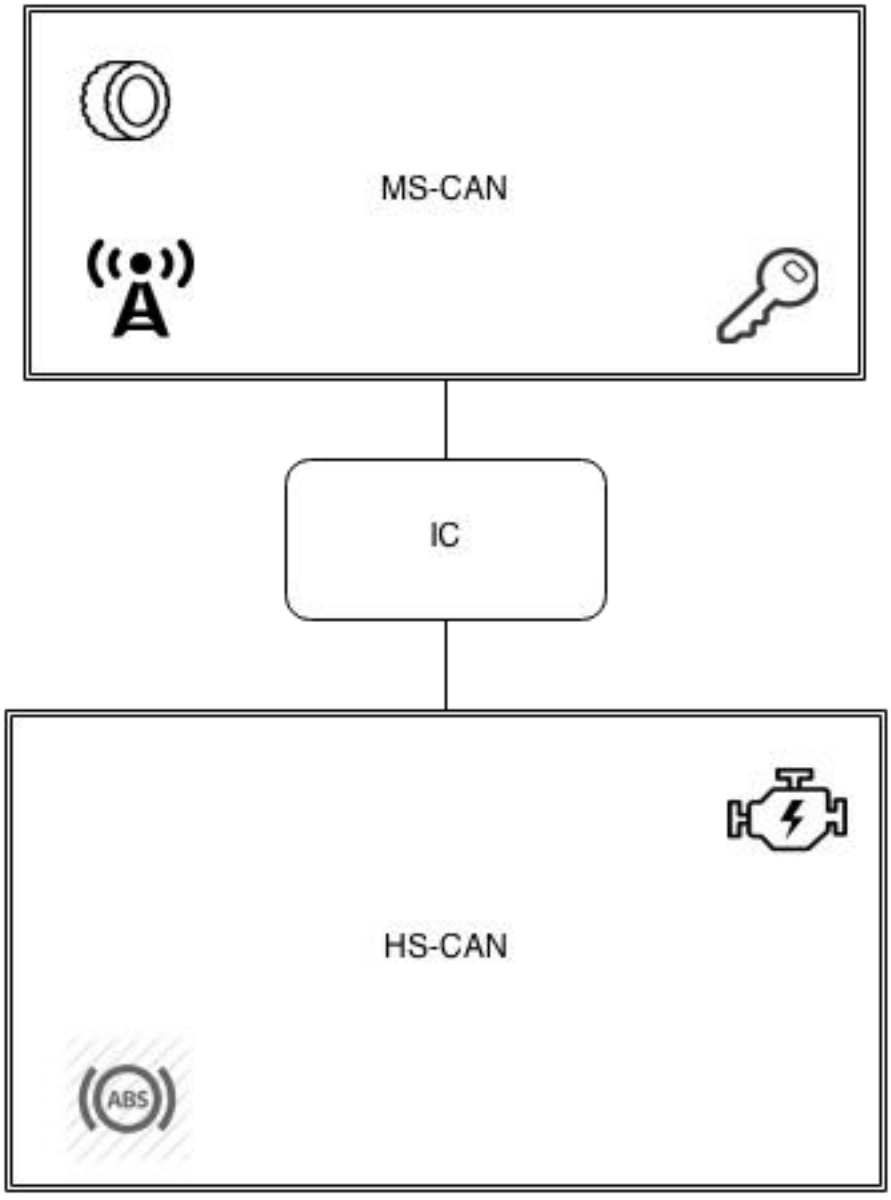
Cyber Physical: None

HS CAN
1. ABS 2. RCM 3. OCS **4. IC** 5. TCM 6. PCM

MS CAN
1. HCS (heated/cooled) 2. MM (mem module) 3. Dsp 4. Sjb 5. Ddm 6. Radio 7. Eatc 8. Datc **9. IC**

Entry Point	ECU	Bus
RKE	SJB	MS CAN
TPMS	SJB	MS CAN
Bluetooth	N/A	N/A
FM/AM/XM	Radio	MS CAN
Cellular	N/A	N/A
Internet / Apps	N/A	N/A

Diagram



2014 Ford Fusion

http://upload.wikimedia.org/wikipedia/commons/b/be/2013_Ford_Fusion_Titanium_--_2012_NYIAS.JPG

Standards: CAN

Wireless Communications: Remote Keyless Entry, Bluetooth, AM/FM/XM Radio, Wi-Fi, Cellular, Proprietary Radio, SYNC

Cyber Physical: Lane keeping assist, Adaptive cruise control with forward collision warning (collision warning only pre-charges brakes), Active Park assist

HS CAN 1
1. **APIM** 2. BCM 3. PCM 4. DC to DC converter control module 5. HCM (headlamp control) 6. **Gateway module**

HS CAN 2

1. RCM
2. OCSM
3. ADIM (auto dimming interior mirror)
4. Proximity warning radar unit
5. ABS
6. PSCM
7. SCCM (steering column)
8. HUDM heads up display
9. VDM Vehicle Dynamics
10. TRCM (transmission range control)
11. FSCM (front seat climate control)
12. PMCSM (passenger multi contour seat module)
13. CCM – cruise control module
14. **Gateway module**

HS CAN 3

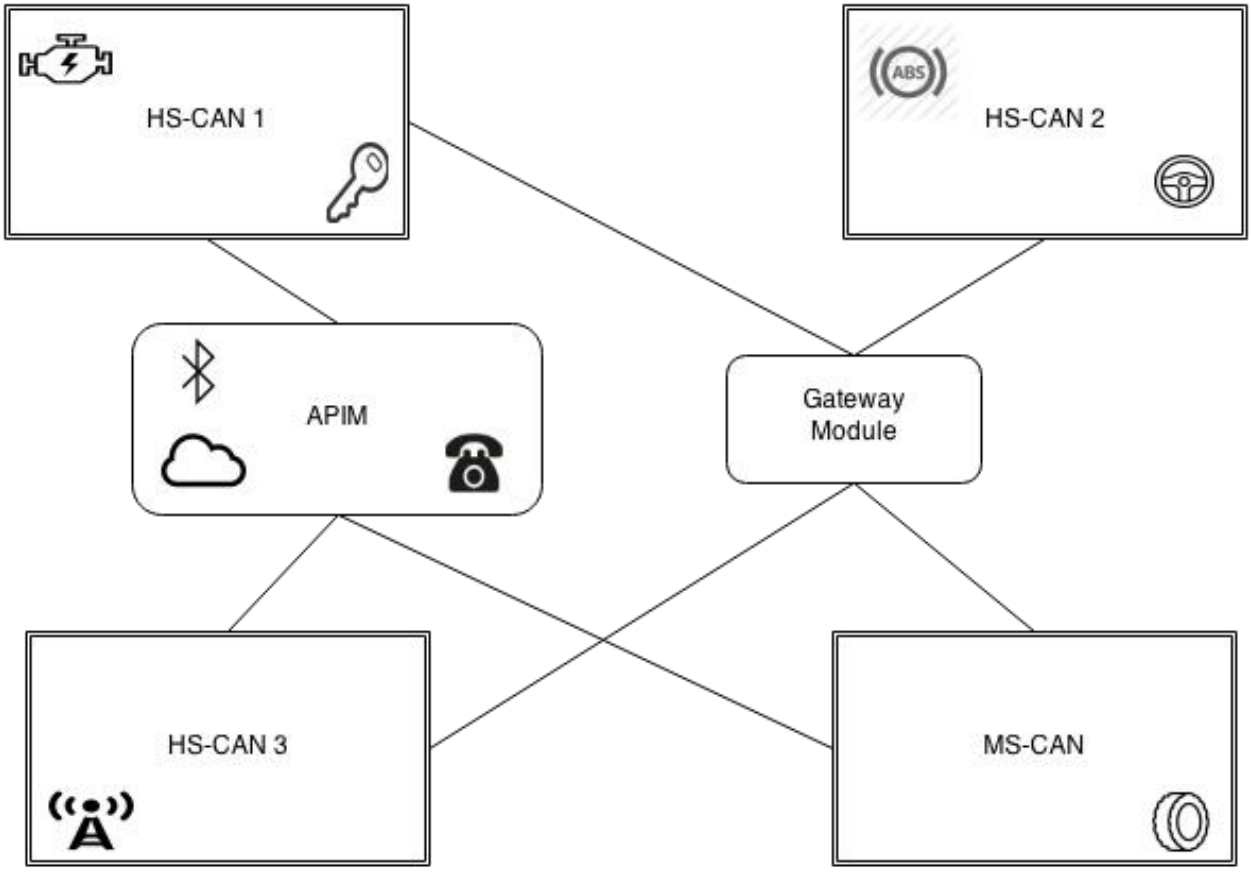
1. **APIM**
2. ACM
3. FCDM
4. IPC - instrument panel
5. ADSPM (audio digital processing)
6. CD
7. **Gateway module**

MS CAN

10. GPSM
11. **APIM**
12. FCIM (front control interface)
13. PCM
14. RTM (radio transceiver module)
15. DDM (driver door)
16. DSM (driver seat)
17. SODL (side obstacle detect left)
18. SODR
19. HSWM (heated steering wheel)
20. DMCSM (driver multi contour seat module)
21. DSM (driver seat module)
22. DDM (driver door module)
23. Rear gate trunk module
24. Side obstacle detection control module
25. **Gateway module**

Entry Point	ECU	Bus
RKE	BCM	HS CAN 1
TPMS	RTM	MS CAN
Bluetooth	APIM	MS CAN, HS CAN1, HS CAN3
FM/AM/XM	ACM	HS CAN 3
Cellular	APIM	MS CAN, HS CAN1, HS CAN3
Internet / Apps	APIM	MS CAN, HS CAN1, HS CAN3

Diagram



2014 BMW 3 Series (F30)

http://www.roadandtrack.com/cm/roadandtrack/images/zQ/001-3GT.jpg

Standards: CAN, Flexray, MOST

Wireless Communications: Remote Keyless Entry, Bluetooth, AM/FM/XM Radio, Wi-Fi, Cellular, Proprietary Radio, ConnectedDrive

Cyber Physical: Parking assist module, Collision detection (vibrate wheel), Lane warning (light)

K-CAN (body controller area network)
1. IHKA
2. CON
3. TRSVC
4. TPMS
5. SMFA
6. FEM – front electronics module

K-CAN2
1. Head unit
2. Combox
3. Rear electronic module
4. Fzd
5. Pma – parking maneuver assistant
6. Fla

PT-CAN (power train controller area network)

7. DME – digital motor electronics
8. ACSM
9. KAFAS
10. EKPS
11. EGS
12. GWS

Flexray

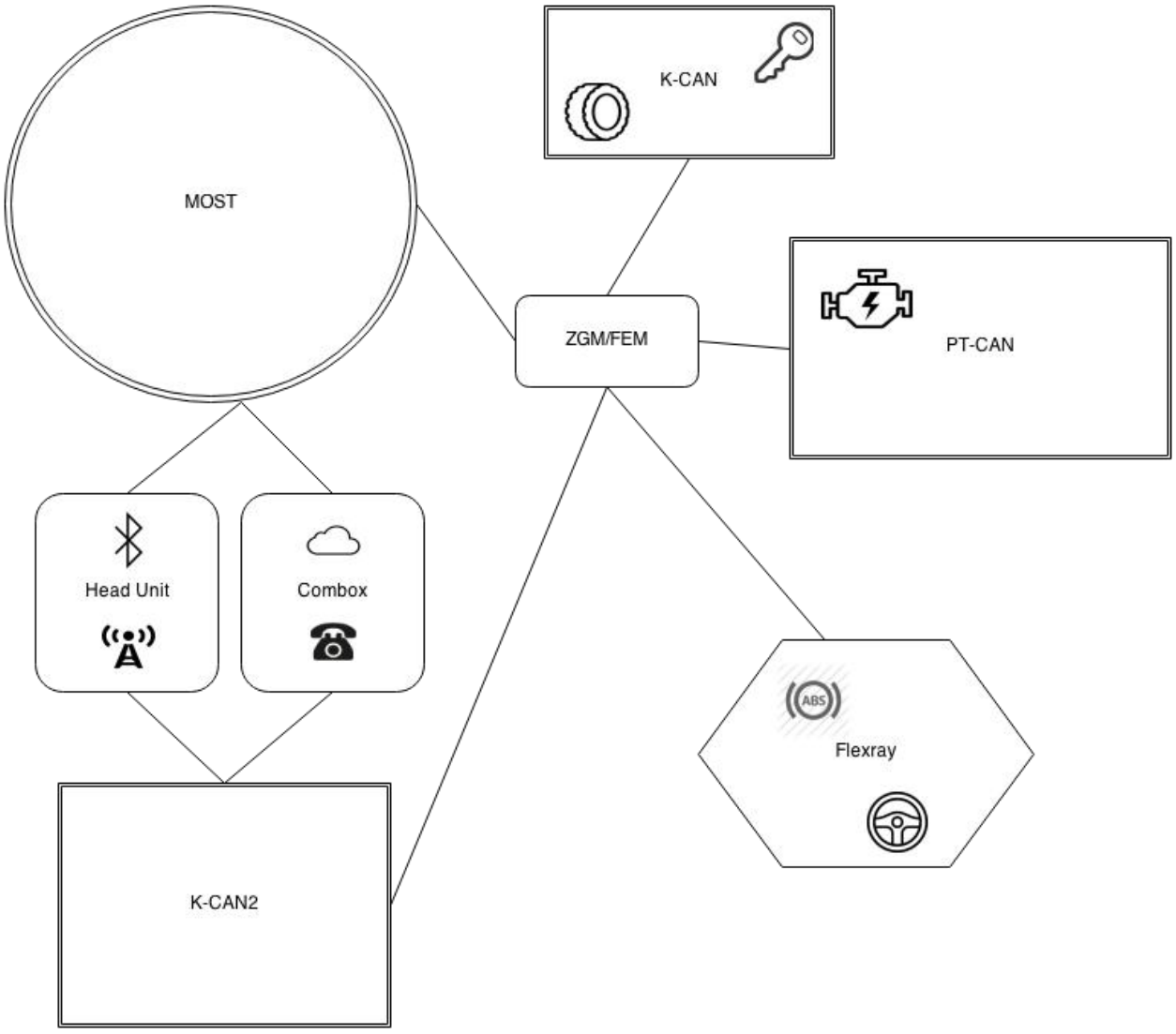
3. SWW
4. EPS – electromechanical power steering
5. VDM
6. DSC – dynamic stability control (brakes)
7. ICM
8. DME

MOST

6. Head unit
7. Combox – combox emergency call, multimedia combox
8. Kombi
9. Dvdc
10. Ampt

Entry Point	ECU	Bus
RKE	FEM	K-CAN
TPMS	TPMS	K-CAN
Bluetooth	Head unit	K-CAN2, MOST
FM/AM/XM	Head unit	K-CAN2, MOST
Cellular	Combox	K-CAN2, MOST
Internet / Apps	Combox	K-CAN2, MOST

Diagram



2014 BMW X3 (F25)

http://static.autoexpress.co.uk/sites/autoexpressuk/files/111061559231880430.jpg

Standards: CAN, Flexray, MOST

Wireless Communications: Remote Keyless Entry, Bluetooth, AM/FM/XM Radio, Wi-Fi, Cellular, Proprietary Radio, ConnectedDrive

Cyber Physical: Dynamic cruise control (includes braking), Parking assist module, Collision detection (vibrate wheel), Lane warning (light)

K-CAN (body controller area network)
1. IHKA 2. CON 3. CID 4. HUD 5. FLA 6. TRSVC 7. TPMS 8. SMFA 9. HKL **10. ZGM** **11. CIC**

K-CAN2

1. ZGM
2. FRM
3. FZD
4. JBE
5. CAS – car access system
6. RAD

PT-CAN (power train controller area network)

1. DME
2. ACSM
3. EKPS
4. EGS
5. GWS
6. EMF

Flexray

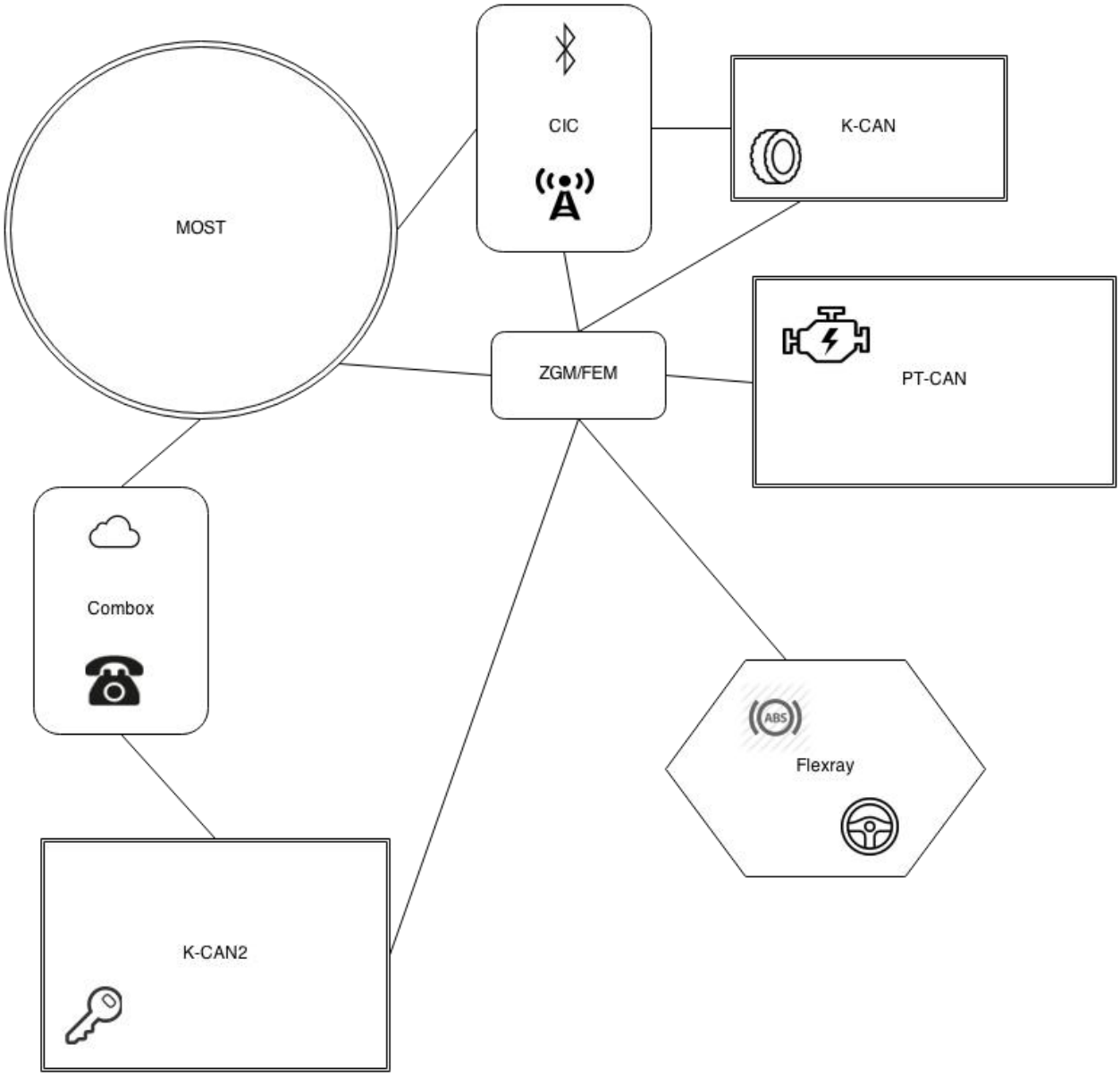
1. EPS
2. VDM
3. DSC
4. ICM
5. VTG

MOST

1. CIC
2. **Combox**
3. Kombi
4. Dvdc
5. ampt

Entry Point	ECU	Bus
RKE	CAS	K-CAN2
TPMS	TPMS	K-CAN
Bluetooth	CIC	MOST, K-CAN
FM/AM/XM	CIC	MOST, K-CAN
Cellular	Combox	MOST, K-CAN2
Internet / Apps	Combox	MOST, K-CAN2

Diagram



2014 BMW i12

http://upload.wikimedia.org/wikipedia/commons/d/db/BMW_Concept_Vision_Efficient_Dynamics_Front.JPG

Standards: CAN, Flexray, MOST

Wireless Communications: Remote Keyless Entry, Bluetooth, AM/FM/XM Radio, Wi-Fi, Cellular, Proprietary Radio, ConnectedDrive

Cyber Physical: Collision warning with city braking function, Dynamic cruise control (includes braking)

K-CAN (body controller area network)
1. IHKA – Integrated automatic heating/air conditions 2. CON - controller 3. ASD – active sound design 4. AMP - amplifier 5. TBX - touchbox **6. TCB – telematics communication box**

K-CAN2
1. FZD – roof function center 2. TRSVC – top rear side view camera **3.** PDC – park distance control

K-CAN3

1. FLER – frontal light electronics right
2. FLEL – frontal light electronics left
3. VSG – vehicle sound generator

PT-CAN (power train controller area network)

1. LIM – charging interface module
2. DME – digital engine electronics
3. TFE – hybrid pressure refueling electronic control unit
4. GWS – gear selector switch
5. EGS – electronic transmission control
6. EMF – electmechanical parking rake
7. KAFAS – camera-based driver support systems
8. EME – electrical machine electronics

PT-CAN 2 (power train controller area network)

1. REME – range extender electrical machine electronics
2. SME – battery management electronics
3. DME – digital engine electronics
4. GWS – gear selector switch
5. EGS – electronic transmission control
6. EME – electrical machine electronics

Flexray

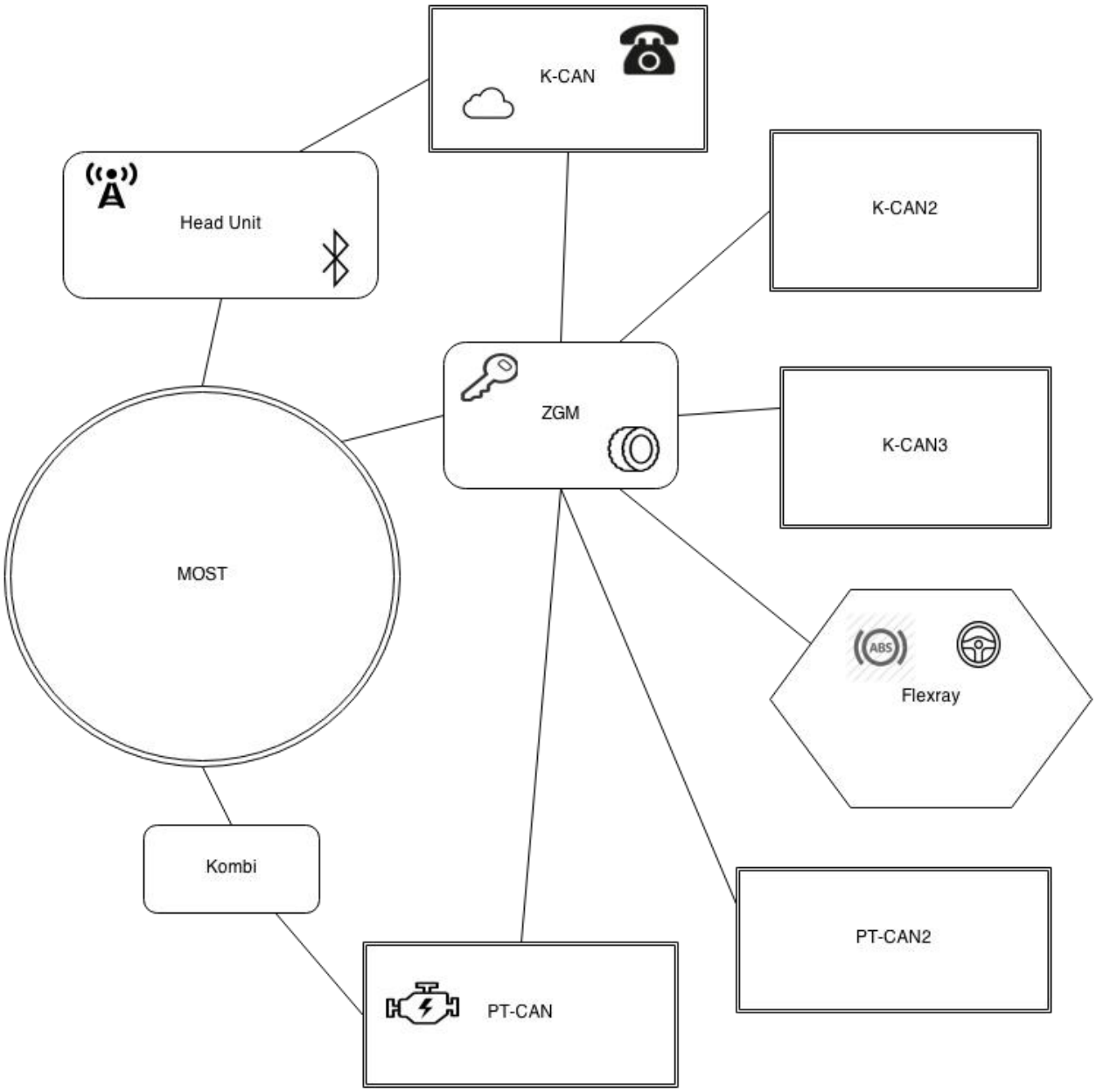
1. **ACSM – advanced crash safety module**
2. EPS – electornic power steering
3. SAS – optional equipment system
4. DSC – dynamic stability control
5. DME – digital engine electronics
6. EME – electrical machine electronics

MOST

1. Head unit
2. Kombi – instrument cluster

Entry Point	ECU	Bus
RKE	ZGM/BDC	ALL
TPMS	BDC	ALL
Bluetooth	Headunit	MOST
FM/AM/XM	Headunit	MOST
Cellular	TCB	K-CAN
Internet / Apps	TCB	K-CAN

Diagram


K-CAN
Head Unit
K-CAN2
ZGM
K-CAN3
MOST
ABS
Flexray
Kombi
PT-CAN2
PT-CAN

2014 Range Rover Evoque

http://evoque.landrover.com/static/images/content/l538-pure-models-930x530.jpg

Standards: CAN, LIN, MOST

Wireless Communications: Remote Keyless Entry, Bluetooth, AM/FM/XM Radio, Wi-Fi, Cellular, Proprietary Radio, InControl

Cyber Physical: Electronic Power Assisted Steering (EPAS), Adaptive Cruise Control, Automatic Self-Parking

CAN-HS Chassis System

1. Restraints Control Module
2. Module – Parking Aid Control
3. Module – AWD Control
4. Module – Damping-Continuously Variable
5. Module – General-Proximity Sensor
6. Switchpack-Terrain Response
7. Diagnostic Connector
8. **Module – Gateway**
9. Module – Power Steering
10. Module – Integrated Brake Control
11. Module – Steering Wheel

CAN-HS Powertrain System

1. **Junction box – Central (BCM)**
2. **Module – Gateway**
3. Module – Steering Column Lock
4. Restraints Control Module
5. Module – AWD Control
6. Diagnostic Connector
7. Instrument Cluster
8. Switch-Automatic Transmission
9. Module – Electric Park-Brake Control
10. **Module – Telematic Control**
11. Module – Control-Occupant Classification
12. Module – Control-Occupant Classification Sensor
13. Module – Integrated Brake Control
14. Module – Adaptive Speed Control
15. Module – Headlamp Leveling
16. Module – Transmission Control
17. ECM

CAN-MS Body System

1. **Junction Box – Central**
2. Diagnostic Connector
3. Module – Driver Door
4. **Module – Telematic Control**
5. Mirror – Rear View
6. Module – Passenger Door
7. Module – Seat Memory-Passenger
8. Module – Powered lid Luggage Compartment
9. **Keyless Vehicle Module**
10. Module – Seat Memory-Driver
11. **Module – Gateway**

CAN-MS Comfort and Convenience System

1. **Module – Gateway**
2. Fuel Fired Booster Heater
3. **Unit – Multi Information Display**
4. Touch Screen
5. Module – Climate Control
6. Integrated Control Panel
7. Diagnostic Connector
8. **Module – Navigation Control**
9. Module – Blind Spot Monitoring-Right
10. Camera – Rear View
11. Module – Bling Spot Monitoring-Left
12. Module – Image Processing
13. Instrument Cluster

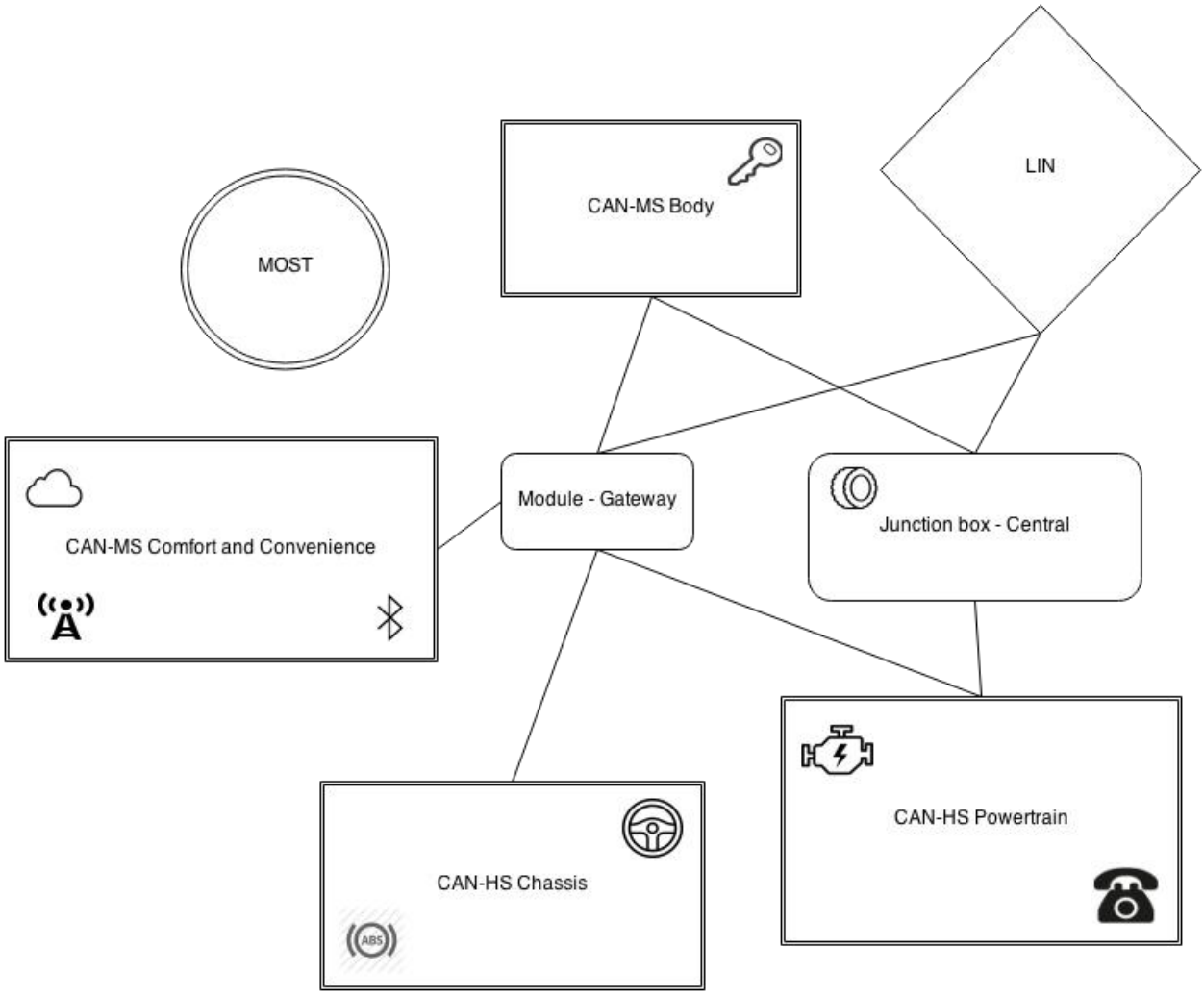
LIN (All LIN Subsystems)

1. Unit – Immobiliser Antenna
2. **Junction Box-Central**
3. Motor – Roof Blind – Front
4. Console – Overhead-Front
5. Sensor – Rain
6. Sounder – Battery Backup
7. Module – Steering Wheel
8. Cruise Controls – Remote
9. Clockspring
10. Module – Heater Control – Steering Wheel
11. Switch – Remote – ICE
12. Module – Heated Seat-Passenger
13. Module – Climate Control
14. Sensor Humidity
15. RH Rear Seat Heater Module
16. RH ALR Temperature Door Motor
17. Screen Air Distribution Door Motor
18. Motor – Recirculation
19. LH Air Temperature Door Motor
20. Module – Climate Control
21. Motor – Air Distribution Feet / Face
22. Module – Heated Seat Driver
23. Switchpack – Rear Console
24. LH Rear Seat Heater Module
25. Module – Driver Door
26. Switchpack – Mirror Window-Driver
27. Module – Rear Door-Left
28. Module – Passenger Door
29. Module – Rear Door-Right
30. Module – Headlamp Leveling Control
31. Headlamp – Left
32. Headlamp – Right
33. **Module – Gateway**
34. Generator
35. **Receiver-RF**
36. Keyless Vehicle Module
37. Module – Voltage Quality
38. Module – Battery Monitoring System
39. Module – Control Quiescent Current

MOST Rings
1. Touch Screen 2. Connector MOST Diagnostic 3. Integrated Audio 4. Module Audio Amplifier 5. Entertainment Module 6. Module – TV Control **7.** Module Tuner DAB

Entry Point	ECU	Bus
RKE	Keyless Vehicle Module	CAN-MS Body System
TPMS	Junction Box Central	CAN-MS / CAN-HS
Bluetooth	Module – Navigation Control	CAN-MS Comfort & Convenience
FM/AM/XM	Module – Navigation Control	CAN-MS Comfort & Convenience
Cellular	Module – Telematic Control	CAN-HS Powertrain
Internet / Apps	Module – Navigation Control	CAN-MS Comfort & Convenience

Diagram


LIN
CAN-MS Body
MOST
CAN-MS Comfort and Convenience
Module - Gateway
Junction box - Central
CAN-HS Powertrain
CAN-HS Chassis
ABS

2010 Range Rover Sport

http://static.cargurus.com/images/site/2009/07/14/18/33/2010-land-rover-range-rover-sport-sc-pic-57937.jpeg

Standards: CAN, MOST

Wireless Communications: Remote Keyless Entry, Bluetooth, AM/FM/XM Radio, Proprietary Radio

Cyber Physical: Adaptive Cruise Control, Collision Restraint System

CAN-MS
1. Junction box-Central 2. Module – Passenger Door 3. Module – Driver Door 4. Memory Control Module **5. Keyless Vehicle Module** 6. Module – Climate Control 7. Module – Parking Aid 8. Module – Cameras 9. Mirror – Electrochromic 10. Fuel fired Booster Heater **11. Audio Head Unit** 12. Integrated Control Panel-Upper 13. Module – Climate Control 14. Diagnostic Socket **15.** Instrument Cluster

CAN-HS

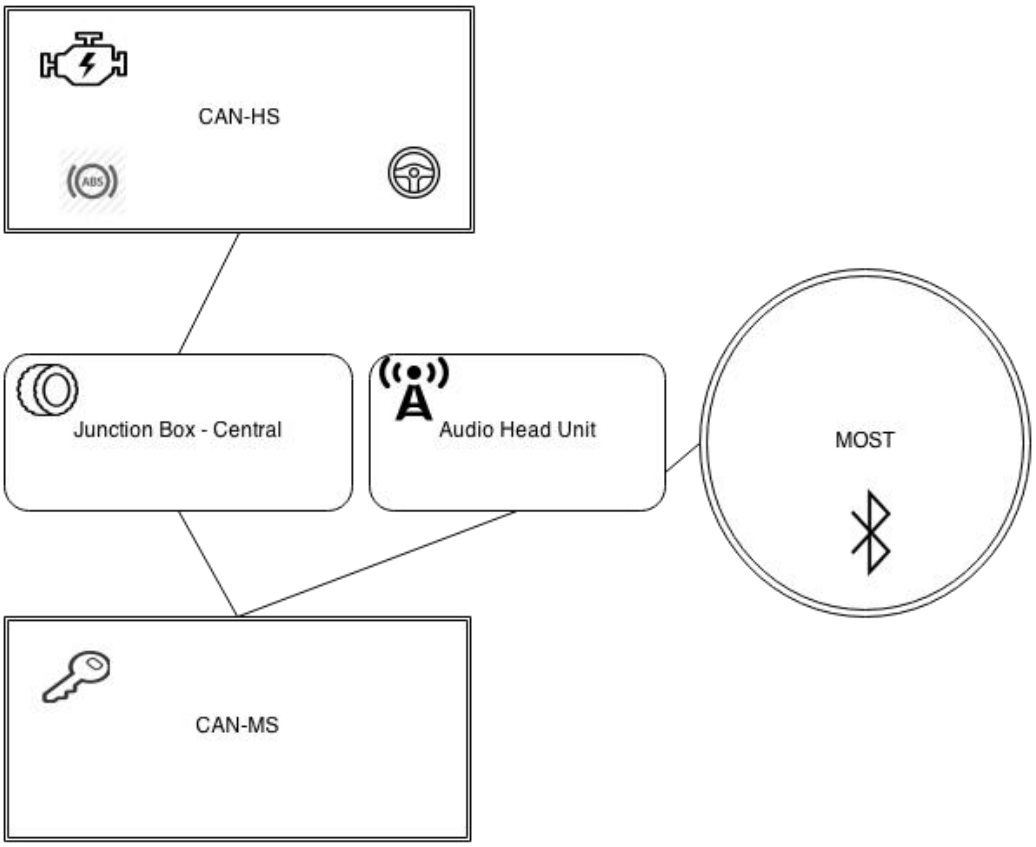
1. ECM
2. AFS Control Module
3. ABS Module
4. Module – Speed Control
5. Dynamic Response Module
6. TCM and Control Valve Body
7. Transfer Box Control Module
8. **Junction box-Central**
9. Diagnostic Socket
10. Instrument Cluster
11. Module – Steering Column Lock
12. Module – Air Suspension
13. Sensor – Occupancy Detector
14. Switch packet-Center Console
15. Restraints Control Module
16. Sensor – Steering Angle
17. Rear Differential Control Module
18. Module – Damping Continuously Variable
19. Module – Parking Brake

MOST Rings

1. Audio Head Unit
2. Touch Screen Display
3. Amplifier-Power
4. Module – Portable Audio Interface
5. Seat Entertainment Module
6. Module – Tuner
7. Module – Telephone

Entry Point	ECU	Bus
RKE	Keyless Vehicle Module	CAN-MS
TPMS	Junction Box Central	CAN-MS / CAN-HS
Bluetooth	Module – Telephone	MOST
FM/AM/XM	Audio Head Unit	CAN-MS
Cellular	N/A	N/A
Internet / Apps	N/A	N/A

Diagram



2006 Range Rover Sport

http://images.thecarconnection.com/med/2006-land-rover-range-rover-sport-4dr-wgn-white_100047815_m.jpg

Standards: CAN, MOST

Wireless Communications: Remote Keyless Entry, Bluetooth, AM/FM/XM Radio, Proprietary Radio

Cyber Physical: Adaptive Cruise Control

CAN-MS

1. **Instrument Cluster**
2. Diagnostic Socket
3. Fuel Fired Booster Heater
4. Tire Pressure Monitoring Control Module
5. **Audio Head Unit**
6. Automatic Temperature Control Module
7. Parking Aid Control Module
8. Central Junction Box

CAN-HS

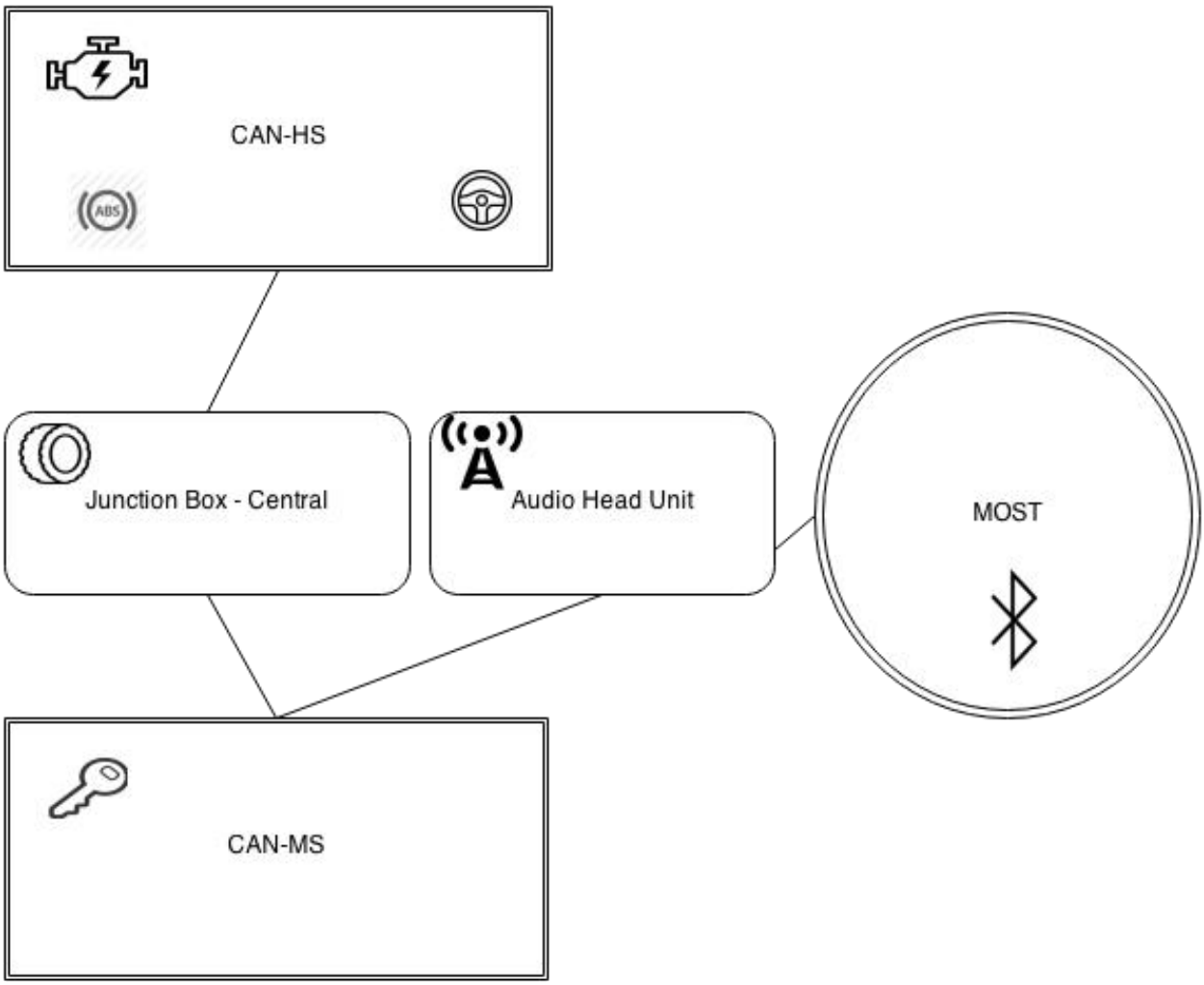
1. **Instrument Cluster**
2. Air Suspension Control Module
3. Sensor – Steering Angle
4. Diagnostic Socket
5. Switch pack-Center Console
6. Rear Differential Control Module
7. Parking Brake Module
8. Restraints Control Module
9. Speed Control Module
10. ECM
11. Generator
12. Transmission Control Module
13. Transfer Box Control Module
14. ABS
15. Dynamic Response Module
16. AFS ECU

MOST Rings

1. **Audio Head Unit**
2. Touch Screen Display
3. Amplifier-Power
4. Module – Portable Audio Interface
5. Seat Entertainment Module
6. Module – Tuner
7. Module – Telephone

Entry Point	ECU	Bus
RKE	Keyless Vehicle Module	CAN-MS
TPMS	Junction Box Central	CAN-MS / CAN-HS
Bluetooth	Module – Telephone	MOST
FM/AM/XM	Audio Head Unit	CAN-MS
Cellular	N/A	N/A
Internet / Apps	N/A	N/A

Diagram



2014 Toyota Prius

http://image.automobilemag.com/f/63379071+q100+re0/2014-toyota-prius-three-quarters-drivers-view-001.jpg

Standards: CAN, LIN, AVC-LAN

Wireless Communications: Remote Keyless Entry, Bluetooth, AM/FM/XM Radio, Cellular, Proprietary Radio, SafetyConnect

Cyber Physical: Adaptive Cruise Control, Self-Parking System, Pre-Collision System

LIN Power Windows and Sliding Roof

1. **Main Body ECU**
2. Power Window Regulation Motor Assembly (front passenger)
3. Power Window Regulation Motor Assembly (front driver)
4. Power Window Regulation Motor Assembly (rear passenger)
5. Power Window Regulation Motor Assembly (rear driver)
6. Sliding Roof ECU
7. Multiplex Network Master Switch Assembly

LIN Smart Key System

1. **Power Management Control ECU**
2. **Transmission Control ECU**
3. Immobiliser Code ECU
4. **Certification ECU**

LIN Air Conditioning System

1. **Air Conditioning Amplifier Assembly**
2. Air Conditioning Control Assembly

CAN v1 Bus

1. **Main Body ECU (LIN Also)**
2. ECM
3. Power Management ECU (LIN, Power Management Bus, CAN v2 Bus)
4. Transmission Control ECU (LIN Also)
5. **Navigation Receiver Assembly**
6. Main Body ECU
7. Power Steering ECU
8. Certification ECU
9. Yaw Rate and Acceleration Sensor
10. Airbag ECU Assembly
11. Steering Angle Sensor
12. **Skid Control ECU**
13. DLC3
14. Combination Meter

CAN Power Management Bus

1. ECM
2. Air Conditioning Amplifier Assembly
3. Skid Control ECU / ABS
4. **Power Management Control ECU**

CAN v2 Bus

1. **Power Management Control ECU**
2. Seat Belt Control ECU
3. Driving Support ECU

CAN Parking Assist Bus

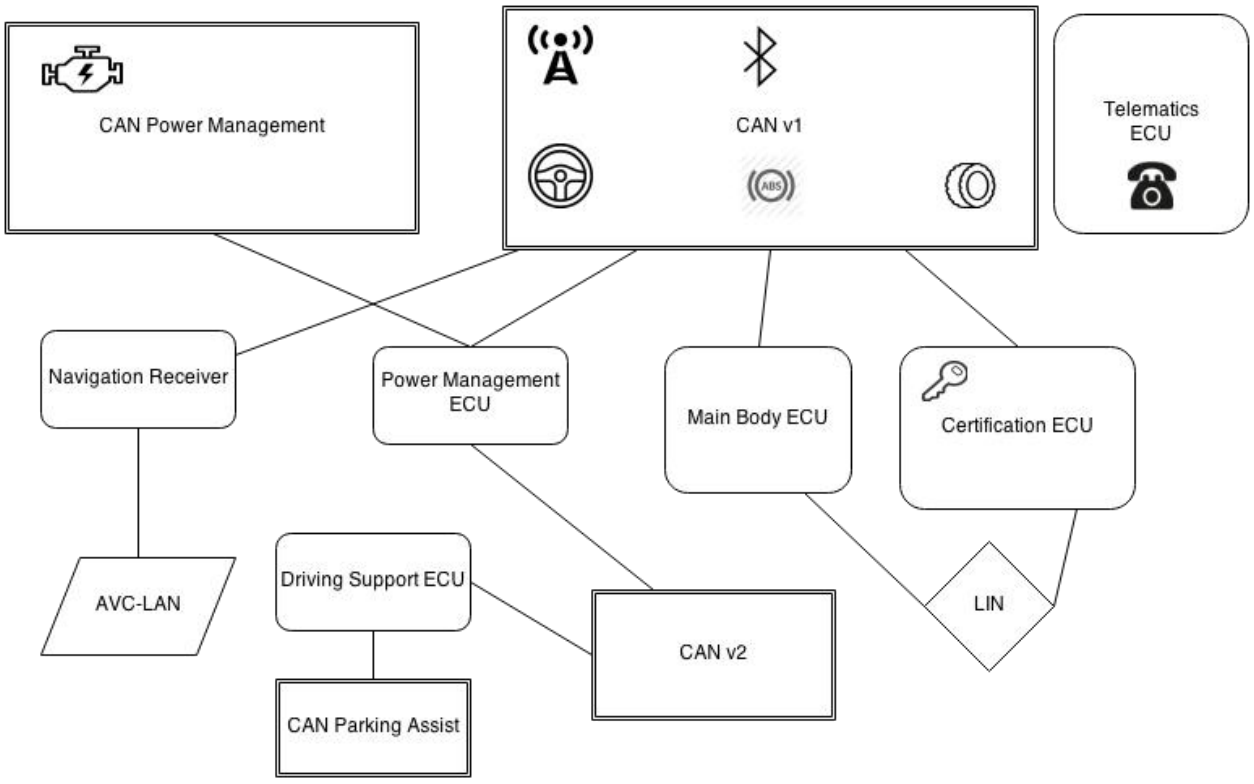
1. **Driving Support ECU**
2. Lane Recognition Camera
3. Millimeter Wave Sensor

AVC-LAN

1. Stereo Component Amplifier Assembly
2. XM Satellite Radio Tuner
3. **Navigation Receiver**

Entry Point	ECU	Bus
RKE	Certification ECU	LIN / CAN v1
TPMS	TPMS (Display light only)	CAN v1 (Display light only)
Bluetooth	Navigation Receiver Assembly	CAN v1
FM/AM/XM	Navigation Receiver Assembly	CAN v1
Cellular	Telematics ECU	None
Internet / Apps	N/A	N/A

Diagram



2010 Toyota Prius

Chris' Prius!

Standards: CAN, LIN, AVC-LAN

Wireless Communications: Remote Keyless Entry, Bluetooth, AM/FM/XM Radio, Cellular, Proprietary Radio, SafetyConnect

Cyber Physical: Adaptive Cruise Control, Self-Parking System, Pre-Collision System

LIN Power Windows and Sliding Roof

1. **Main Body ECU**
2. Power Window Regulation Motor Assembly (front passenger)
3. Power Window Regulation Motor Assembly (front driver)
4. Power Window Regulation Motor Assembly (rear passenger)
5. Power Window Regulation Motor Assembly (rear driver)
6. Sliding Roof ECU
7. Multiplex Network Master Switch Assembly

CAN Power Management Bus

1. ECM
2. Air Conditioning Amplifier Assembly
3. Skid Control ECU / ABS
4. **Power Management Control ECU**

CAN v2 Bus

1. **Power Management Control ECU**
2. Seat Belt Control ECU
3. **Driving Support ECU**

CAN v1 Bus

1. **Main Body ECU (LIN Also)**
2. ECM
3. Power Management ECU (LIN, Power Management Bus, CAN v2 Bus)
4. Transmission Control ECU (LIN Also)
5. **Navigation Receiver Assembly**
6. Main Body ECU
7. Power Steering ECU
8. Certification ECU
9. Yaw Rate and Acceleration Sensor
10. Airbag ECU Assembly
11. Steering Angle Sensor
12. **Skid Control ECU**
13. DLC3
14. Combination Meter

CAN Parking Assist Bus

1. **Driving Support ECU**
2. Lane Recognition Camera
3. **Millimeter Wave Sensor**

AVC-LAN

1. Stereo Component Amplifier Assembly
2. XM Satellite Radio Tuner
3. **Navigation Receiver**

LIN Smart Key System

1. **Power Management Control ECU**
2. **Transmission Control ECU**
3. Immobiliser Code ECU
4. **Certification ECU**

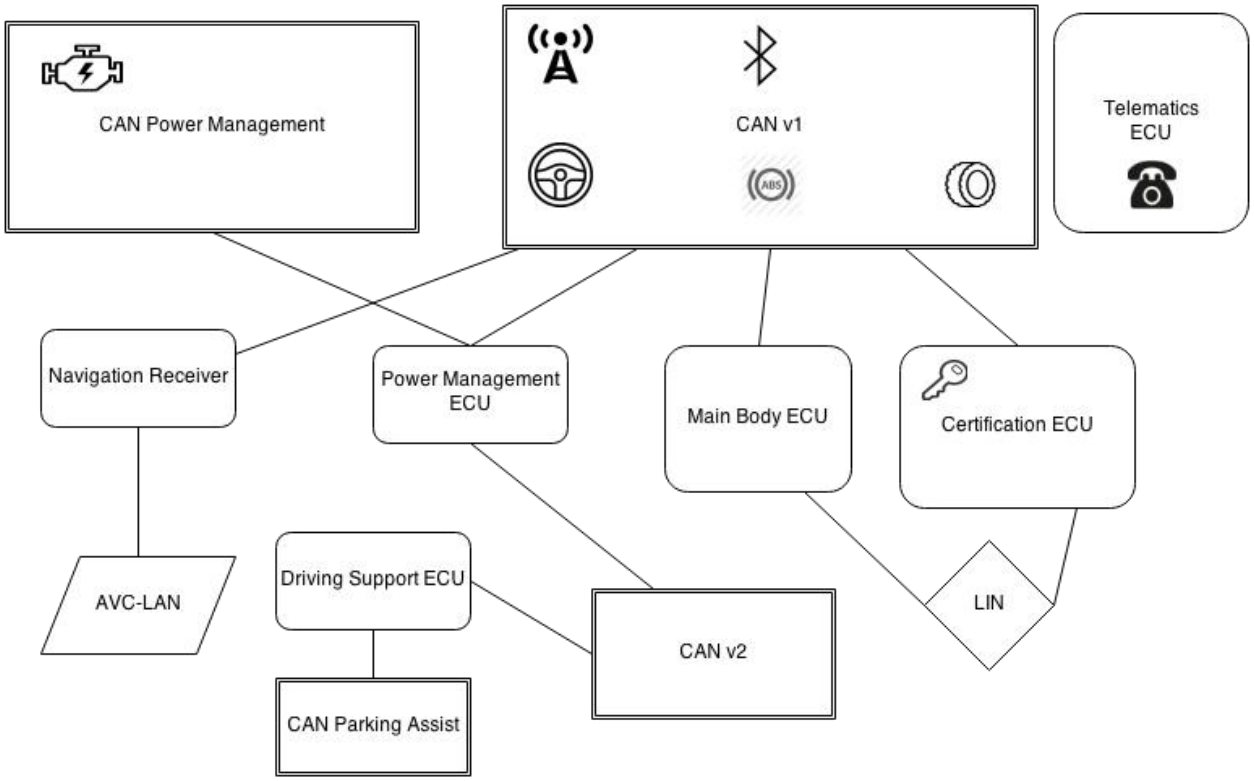
LIN Air Conditioning System

1. **Air Conditioning Amplifier Assembly**
2. Air Conditioning Control Assembly

LIN Advanced Parking Guidance
1. **Parking Assist ECU** 2. Ultra Sonic Sensor LH

Entry Point	ECU	Bus
RKE	Certification ECU	LIN / CAN v1
TPMS	TPMS ECU (Display light only)	CAN v1 (Display light only)
Bluetooth	Navigation Receiver Assembly	CAN v1
FM/AM/XM	Navigation Receiver Assembly	CAN v1
Cellular	Telematics ECU	N/A
Internet / Apps	N/A	N/A

Diagram



2006 Toyota Prius

http://upload.wikimedia.org/wikipedia/commons/6/60/2006_Toyota_Prius.jpg

Standards: CAN, BEAN, AVC-LAN

Wireless Communications: Remote Keyless Entry, Bluetooth, AM/FM/XM Radio, Proprietary Radio

Cyber Physical: None

CAN Bus
1. ECM 2. HV ECU 3. Yaw Rate and Deceleration Sensor 4. Battery ECU 5. ABS ECU 6. Electronic Power Steering (EPS) ECU 7. Steering Angle Sensor 8. DLC3 **9. Gateway ECU**

BEAN Bus

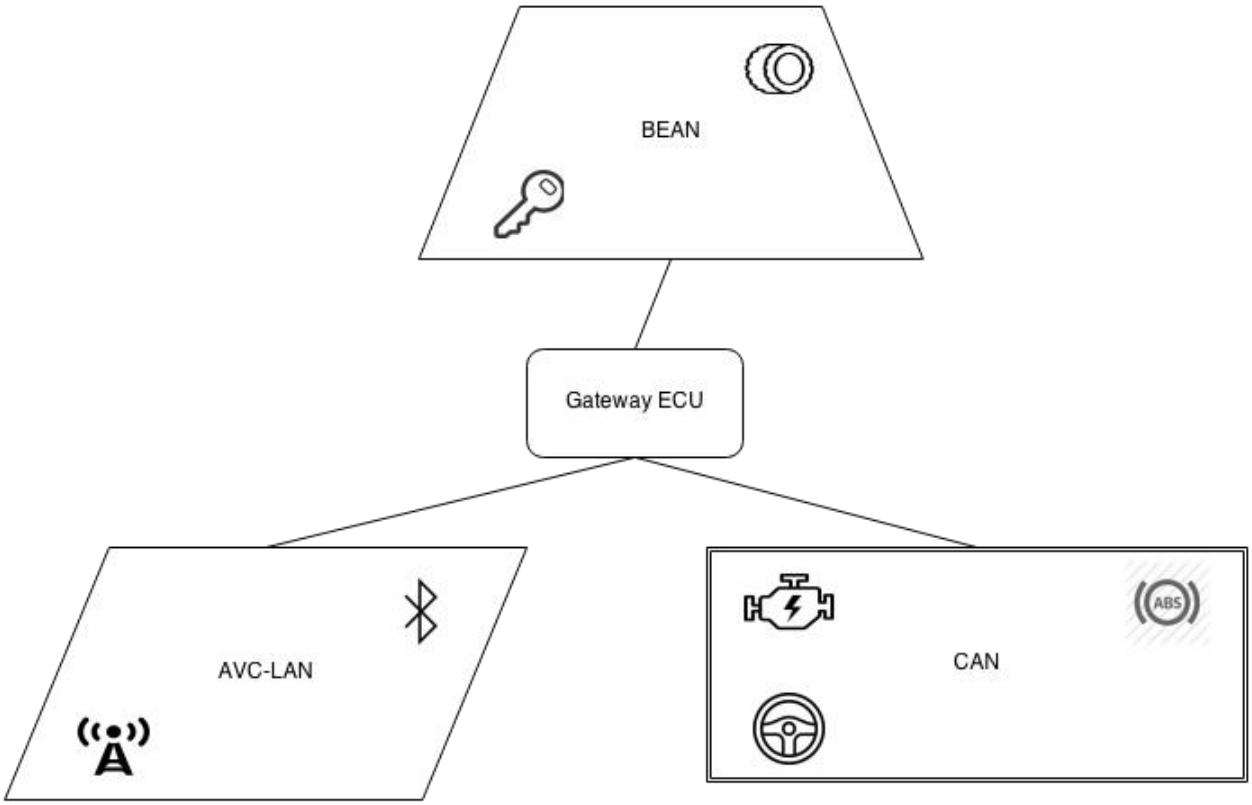
1. Power Source Control ECU
2. Combination Meter
3. Tire Pressure Monitor ECU
4. Certification ECU
5. Transmission Control ECU
6. Transponder Key ECU
7. Driver Side Junction Block
8. A/C ECU
9. **Gateway ECU**

AVC-LAN

1. Navigation ECU
2. Audio Amplifier
3. Radio and Media Player
4. Multi-Display
5. **Gateway ECU**

Entry Point	ECU	Bus
RKE	Transponder Key ECU	BEAN
TPMS	Tire Pressure Monitor ECU	BEAN (Display light only)
Bluetooth	Navigation ECU	AVC-LAN
FM/AM/XM	Navigation ECU	AVC-LAN
Cellular	N/A	N/A
Internet / Apps	N/A	N/A

Diagram



Analysis of automotive networks

As you can see, each manufacturer differs not only in remote communications and cyber physical systems, but also network architecture. This means that remote compromises will generally be different for each manufacturer and each car.

Analysis

- The number of **ECUs** have **increased** over time
  - Infiniti went from 11 in 2006 to 34 in 2014
  - Jeep went from 7 in 2010 to 17 from 2014
  - Range Rover went from 41 in 2010 to 98 in 2014
  - Toyota Prius went from 23 in 2006 to 40 in 2014

- There are a large number of **ECUs** in 2014 vehicles from 19 (Dodge Viper) to **98** (Range Rover)

- The **remote** attack surface and the number of cyber physical features has **increased** as time has gone on.

- The number of different **networks** in cars (complexity of architecture) has **increased** over time.

- The **addition** of ECUs over time is a result of manufacturers requiring more technology, specifically around user experience and safety, which is most easily added to the vehicle by patching it into the **multiplex** systems available, instead of adding new wiring or networks.

- Vehicles are having common **desktop** technology, such as web browsers and in-car apps, providing a familiar attack surface known to **attackers** for many years [12].

- The **TPMS** and **RKE** are the **most** likely ECUs with remote attack surface on the same segment as cyber physical ECUs.

- **6** out of 14 (42%) of the 2014 vehicles we looked at have **no separation** between at least one cyber physical ECU and one with remote attack surfaces.

- The diagrams of the cars examined (above) show network **topologies** with a large degree of **variance**. Some vehicles separate certain functionality while others had most of the technology and cyber physical components on the same bus.

- On the other hand, Cars manufactured in the same **region** tend to have **similar** network topologies. We've seen common architectures in Japanese (Toyota & Infiniti), German (Audi/VW & BMW), and American (GM & Ford) automobiles. This could be due to similar thought process or engineer turnover.

- **Cyber physical** controls, such as Adaptive Cruise Control, are more prevalent in **newer** automobiles. Much of the new technology has to do with customer demand for more safety conscious automobiles. Permitting computers to perform physical actions make the driver safer,

but at the same time, give an attacker built-in functionality of which to **abuse** to bring potential harm to the passenger and vehicle.

- Our survey shows **newer** cars have **more cyber physical** features but many times are segmented on different computer networks. Since we did not have all of the cars reviewed in this paper we cannot say definitely how big of an obstacle segmented networks would put in front of an attacker. From our perspective, we have **rarely** seen segmentation used for **security boundaries**, instead network segmentation is used for non-communicable network buses.

- 'How **patchable** is the modern automobile'? Right now, we've received several recall notices for the 2010 Ford Escape and the 2010 Toyota Prius. All of them **required** us to bring the vehicle to a local dealership. It does not appear that many manufacturers support Over-the-Air (OTA) update as this time (July 2014). We've seen patching wasn't nearly as effective until Microsoft **automated** the Windows **Update** functionality and assume vehicles will not be any different.

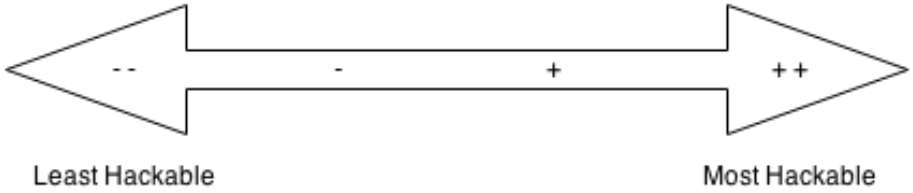
Most Hackable

1. 2014 Jeep Cherokee
2. 2015 Cadillac Escalade
3. 2014 Infiniti Q50

Least Hackable

1. 2014 Dodge Viper
2. 2014 Audi A8
3. 2014 Honda Accord

C&C Car Ratings



Car	Attack Surface	Network Architecture	Cyber Physical
2014 Audi A8	++	--	+
2014 Honda Accord LX	-	+	+
2014 Infiniti Q50	++	+	+
2010 Infiniti G37	-	++	+
2014 Jeep Cherokee	++	++	++
2014 Dodge Ram 3500	++	++	--
2014 Chrysler 300	++	-	++
2014 Dodge Viper	++	-	--
2015 Cadillac Escalade	++	+	+
2006 Ford Fusion	--	--	--
2014 Ford Fusion	++	-	++
2014 BMW 3 series	++	--	+
2014 BMW X3	++	--	++
2014 BMW i12	++	--	+
2014 Range Rover Evoque	++	-	++
2010 Range Rover Sport	-	--	-
2006 Range Rover Sport	-	--	-
2014 Toyota Prius	+	+	++
2010 Toyota Prius	+	+	++
2006 Toyota Prius	-	--	--

Defending Against Remote Attacks

Now that we understand the entire chain of events necessary to go from remotely communicating with vehicle to controlling cyber physical features, we can have an informed discussion about how to defend these attacks. As such an attack is necessarily multi-stage in nature, it is our opinion that the defense should be layered as well, making each stage of such an attack difficult to achieve. Below is a list of such ideas.

Secure Remote Endpoints

First, minimize the attack surface and lock down remote services as much as possible. This probably goes without saying. However, as the history of software security shows, complete security is not achievable. Engineering powerhouses like Microsoft and Google still haven't been able to make a web browser that can go a few months without a critical security patch, so there is no reason to think that we'll have a 100% secure Bluetooth stack anytime soon. Nonetheless, trying to minimize the number of vulnerabilities is still an important step. On top of all the secure engineering issues, more and more technology is being added every year, creating additional attack surface. While we condone securing remote end points, we don't believe it should be the only process used in securing the modern automobile.

CAN Injection Mitigations

Once an attacker gets code running on an ECU, it is possible to make it harder to for the attacker to inject CAN messages immediately. For example, the Bluetooth stack probably does not need the ability to send CAN messages (but we can't completely rule anything out). It seems telematics units in the future may run Android which would have this capability. However, as we've seen with other sandbox technologies (and Android in particular), there is always a way to escape these sandboxes or elevate privileges, say through a Linux kernel exploit, to bypass these mechanisms.

Message Cryptography

One idea often suggested is to cryptographically verify CAN messages to make injection difficult. The idea is that only the ECUs (and mechanics tools) have the keys and so a random attacker wouldn't be able to send valid CAN messages on the compromised automotive network. This idea may present obstacles for attackers who add rogue devices to automotive networks, but in the context of a remote attack, the attacker is executing code on a compromised ECU. At this point, the keys are also compromised, or at least the ability to send valid CAN messages. So this idea doesn't seem to present much of an obstacle in the remote attack scenario, which is most concerning to consumers and manufacturers alike.

Network Architecture

As we've seen by looking at existing automotive architectures, some automotive networks present more of a challenge to attack safety critical ECUs than others. This forwards the idea that manufacturers should design their automotive networks in such a way to isolate those ECUs with remote functionality from those that control safety critical features. This is a great idea and is definitely recommended.

However, it is not a panacea and does not solve all the problems. First, major architectural changes like this are expensive, take years to implement, and most likely aren't going to be happening anytime soon. One of the underlying problems is that while you can isolate these two types of ECUs, some communication between them is likely. This means there will have to be some kind of bridge/gateway between them. This bridge ECU then opens up the possibility of being tricked into forwarding messages or straight up becoming the target of compromise. While this does add an additional barrier (for example, the academic researchers cited throughout this work were able to move from one network to the other by compromising the bridge), it is not going to be perfect, and may even become the single point of failure.

Additionally, with more connectivity technology, including Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I), becoming more prevalent, there seems to be the requirement of remote communications devices talking to cyber physical components. For example, for V2V collision avoidance systems to work correctly a wireless component must receive a signal and send messages that control braking and/or steering.

Attack Detection

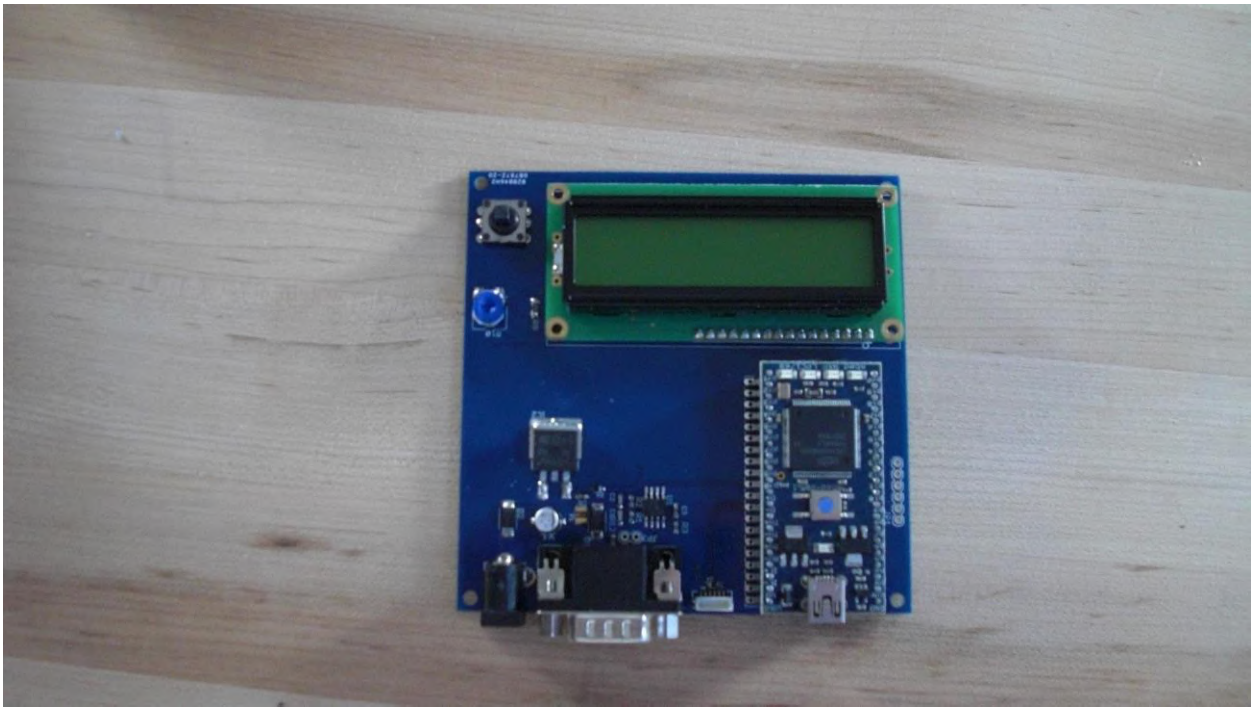
A final suggestion is to add attack detection and prevention technology into critical CAN networks. This represents an inexpensive and accurate way to greatly improve the security of CAN networks and can be added to vehicles immediately, especially since most major cyber physical components rely on CAN (although Flexray and other communications protocols are gaining traction).

While attack detection typically doesn't work well in enterprise network environments, initial data shows that it works quite well in automotive networks. The primary difference is that automotive networks are highly regular and only involve computers talking with computers, without human interaction. Furthermore, while typical software exploits can vary widely and can be designed to be stealthy, this doesn't appear possible in automotive networks. All known CAN injection attacks (both ours and the academic researchers) all take one of two forms. They are either CAN diagnostic messages or they are standard message with a highly inflated send rate.

While it is obvious why diagnostic messages might be dangerous, it may need a quick discussion of why normal messages used for attack must bet transmitted at a much higher rate than normal. The rate must be higher because there are always messages going from ECUs to ECUs. Unless the attacker happens to be on the ECU that sends the particular message the attacker wishes to inject, the original ECU will still be sending the original message along with the attacker.

That means the attacker can send the same message but the target ECU will be receiving messages from the original ECU and the attacker. At this point, the rate of the CAN messages are higher than normal. But, even more so, in practice, the way an attacker ensures the target ECU listens to the injected messages and not the original ones is to send them even faster than the original ECU. Regardless of the normal message injection attack, the rate of messages will be twice as high as normal and in practice 20-100x higher than normal. The point is that abnormal messages occur whether the attacker is sending diagnostic messages or normal messages at an increased rate, permitting easy detection and possible prevention of attacks.

The other interesting aspect of detection, unlike the other possibilities mentioned here, is that individual researchers can build and test these devices. All of our attacks are published and important aspects of the academics are public as well. As a proof of concept, we built a small device that plugs into the OBD-II port of a car, learns traffic patterns, and then detects anomalies. When the device does detect something, it short circuits the CAN bus, thus disabling all CAN messages, see Figure below.



CAN defense and protection mechanism

While this particular device plugs into the OBD-II port, it could just as easily be wired directly into the CAN bus or manufacturers could easily integrate these simple algorithms into existing ECUs at almost no cost.

Conclusions

Remote attacks against vehicles having physical implications will typically need three stages. These three stages are remote compromise; sending injected messages to cyber-physical components, and making the destination ECU perform some unsafe action. In this paper, for a large variety of vehicles, we identified the remote attack surface to estimate how difficult remote compromise might be. We then examined the architecture of the internal networks of each vehicle, identifying the location of ECUs which process external inputs as well as ECUs that contain capabilities to cause physical changes to the vehicle. This will give an indication on how easy it would be to get messages from the former to the latter. Finally, we identify the features that the car possesses which may help in taking physical control of the vehicle. Combining this data, we can make rough estimates on the difficulty of remote exploitation for these vehicles. Since these types of remote attacks will necessarily be multi-stage, we recommend a defense in depth strategy that includes detection of message injection as part of an overall safety strategy.

References

[1] http://bwrcs.eecs.berkeley.edu/Classes/icdesign/ee241_s05/Projects/Midterm/VictorWen.pdf
[2] http://ftp.cse.sc.edu/reports/drafts/2010-002-tpms.pdf
[3] http://www.autosec.org/pubs/cars-usenixsec2011.pdf
[4] http://networksasia.net/article/f-secure-warns-against-htc-bluetooth-exploit-1247839201
[5] http://www.defcon.org/images/defcon-15/dc15-presentations/dc-15-barisani_and_bianco.pdf
[6] http://datasheets.maximintegrated.com/en/ds/MAX1471.pdf
[7]http://www.codenomicon.com/resources/whitepapers/codenomicon_wp_Fuzzing_Bluetooth_20110919.pdf
[8] http://en.wikipedia.org/wiki/Radio_Data_System
[9] http://illmatics.com/car_hacking.pdf
[10] http://www.f-secure.com/vulnerabilities/SA201106648
[11] http://www.networkworld.com/article/2231495/cisco-subnet/defcon---hacking-tire-pressure-monitors-remotely.html
[12] http://en.wikipedia.org/wiki/Pwn2Own