CONNECTED CAR SECURITY

Threat landscape and Potential Mitigation Strategies

Suresh Mandava
Cyber Security Lead
for IoT/BigData Practice
August 4, 2015

@sureshmandava

WIRED

Hackers Remotely Kill a Jeep on the Highway—With Me in It

July 21, 2015

Almost Year Before

MOTHERBOARD

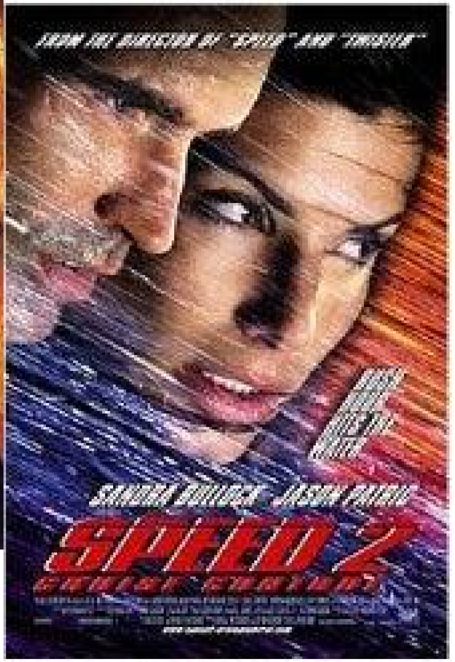
We Drove a Car While It Was Being Hacked, May 29, 2014

http://motherboard.vice.com/read/we-drove-a-car-while-it-was-being-hacked

Before Matrix there was Speed

1994

The film tells the story of the LAPD cop who tries to rescue civilians on a city bus rigged with a bomb programmed to explode if the bus slows down or if civilians try to escape.

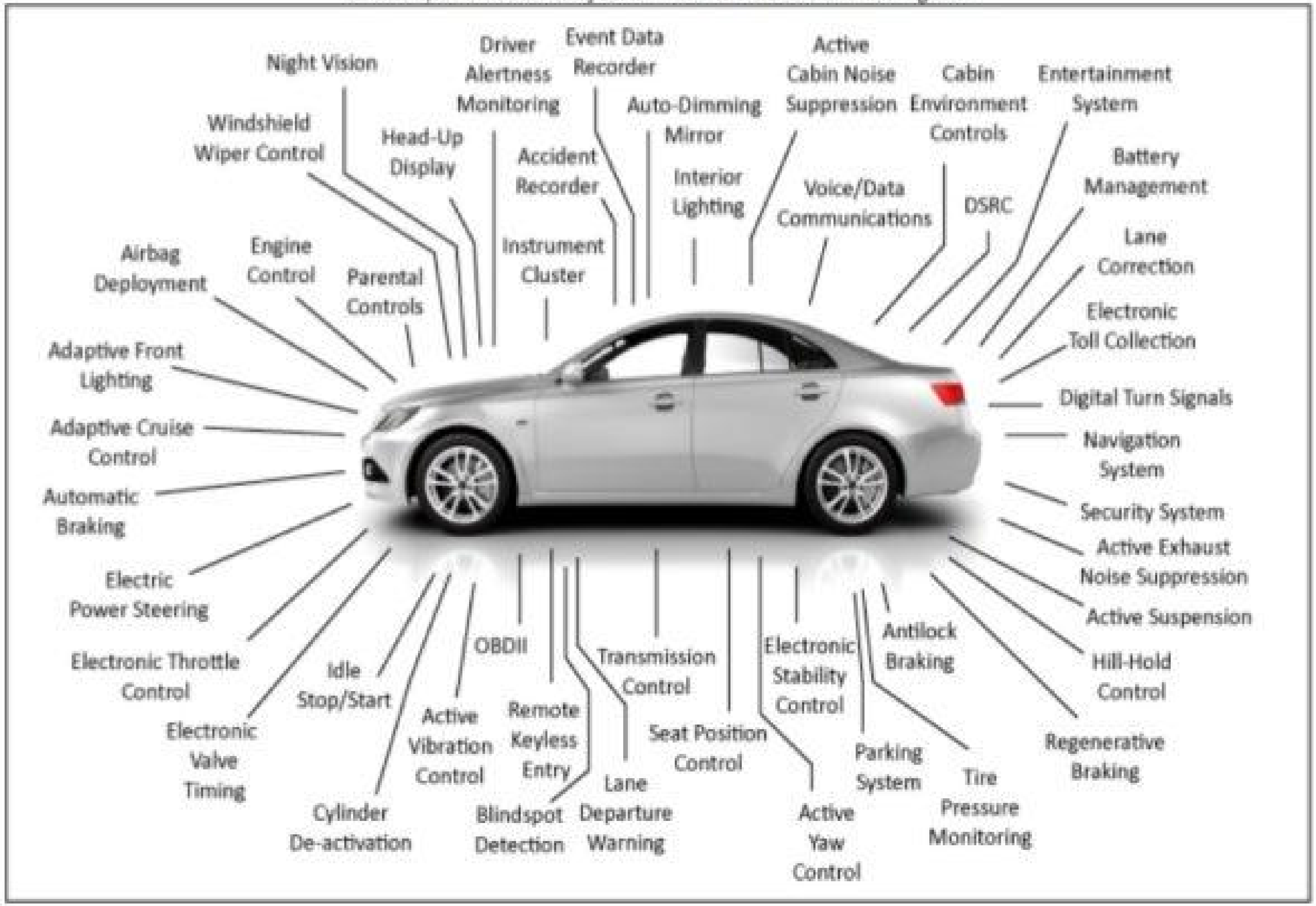

FROM THE DIRECTOR OF "SPEED" AND "TWISTER"
SANDRA BULLOCK JASON PATRIC
SPEED 2
CRUISE CONTROL

1997

Trapped aboard the ship, Annie and Alex work with the ship's first officer to try to stop the ship, which they discover is programmed to crash into an oil tanker.

Automotive Electronics Systems

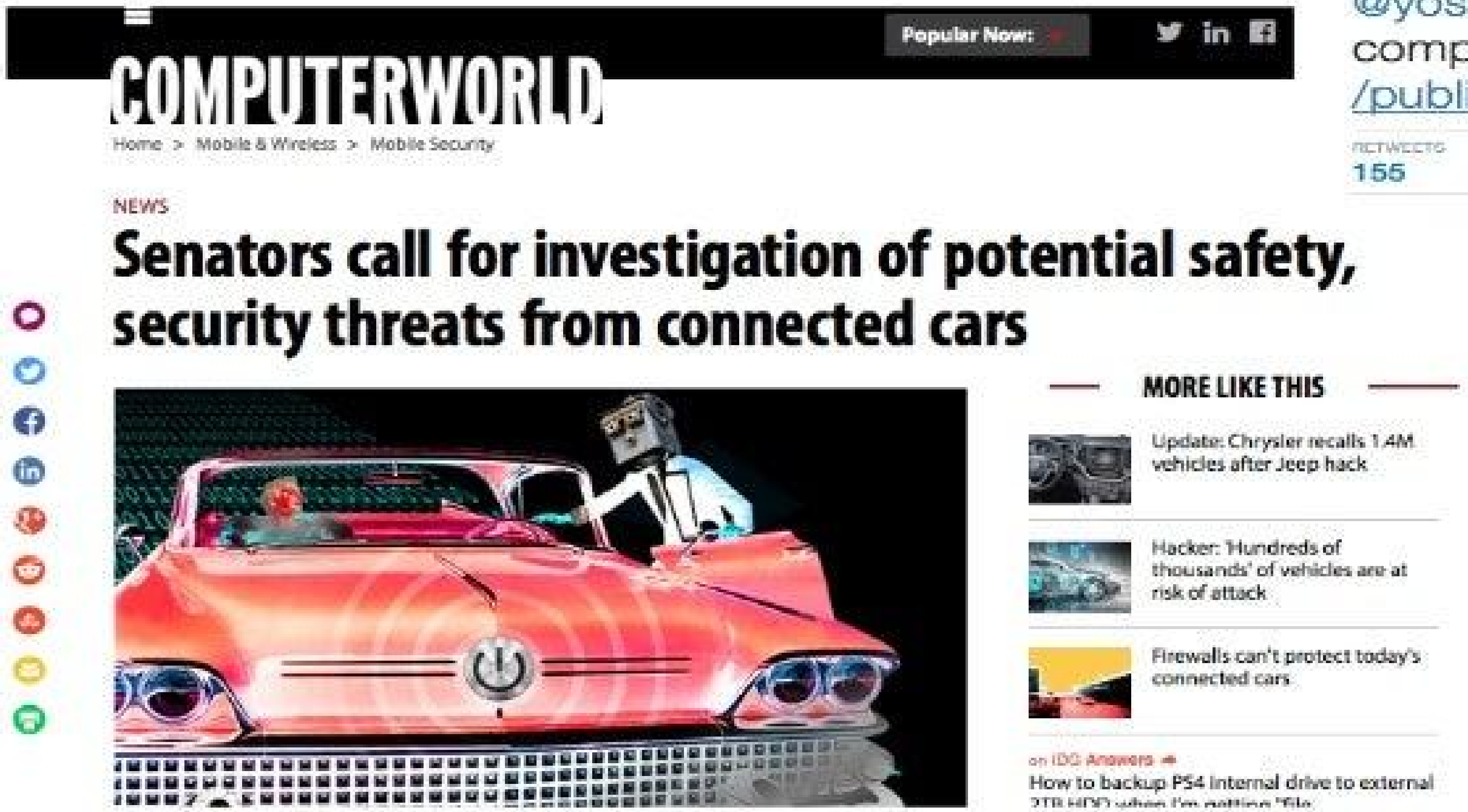
A typical automobile on the road today has dozens of computer controlled electronic systems. Click on a system in the figure below to learn more about it; or choose a system from the list below the figure.



Example:
Lexus LS-460

- Sep 2006
- +100 ECU's
- 7 Million Lines of Software Code

Year(s) apart…



COMPUTERWORLD

Popular Now:

Home > Mobile & Wireless > Mobile Security

NEWS

Senators call for investigation of potential safety, security threats from connected cars

MORE LIKE THIS

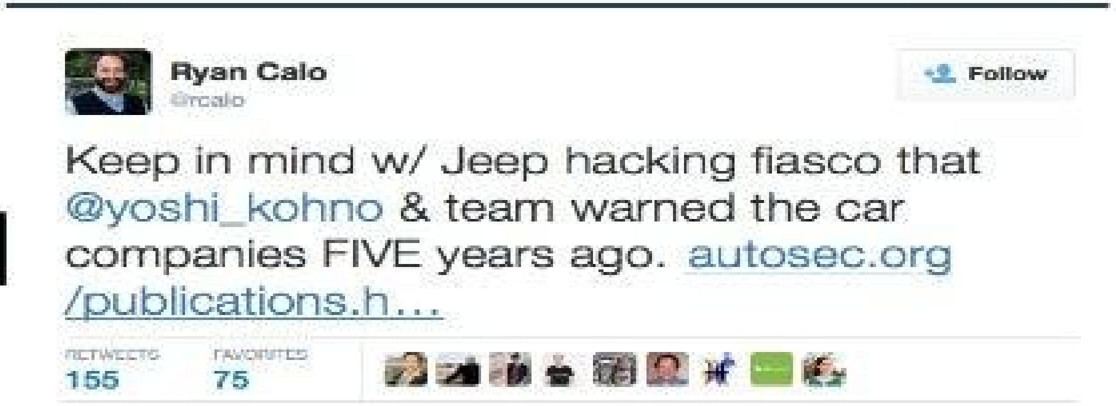
Update: Chrysler recalls 1.4M vehicles after Jeep hack

Hacker: 'Hundreds of thousands' of vehicles are at risk of attack

Firewalls can't protect today's connected cars

on IDG Answers

How to backup PS4 internal drive to external 2TB HDD when I'm getting "file



Ryan Calo
@rcalo

Follow

Keep in mind w/ Jeep hacking fiasco that @yoshi_kohno & team warned the car companies FIVE years ago. autosec.org/publications.h…

RETWEETS 155 FAVORITES 75

http://www.autosec.org/publications.html

SpyCar ACT
(July 21, 2015)

SPY Car Act, the legislation introduced by Markey and Blumenthal

The Security and Privacy in Your Car Act (the SPY Car Act) specifies that the NHTSA and FTC together issue

- Notices of Proposed Rulemaking within 18 months, and final regulations within three years of the act's enactment.
- The SPY Car Act will apply to vehicles made two years after final cybersecurity and privacy regulations are issued.

SpyCar ACT : Cybersecurity Standards

- **Vehicle System Security**. All entry points to a vehicle’s electronic systems must be equipped with reasonable measures to protect against cyberattacks, including isolation measures to separate critical and non-critical software systems;

- **Vulnerability Testing and Remediation**. Such reasonable security measures shall be evaluated for vulnerabilities following best security practices, including appropriate applications of techniques such as penetration testing, and must be adjusted and updated based on the results of such evaluation;

- **Data Security**. All driving data[9] collected by a vehicle’s electronic systems must be reasonably secured from unauthorized access while data is stored onboard the vehicle, in transit from the vehicle to another location, and in any offboard storage or use; and

- **Real-Time Attack Mitigation**. All entry points to a vehicle’s electronic systems must be equipped with capabilities to immediately detect, report, and stop unauthorized attempts to intercept driving data or control the vehicle.

Violation of such cybersecurity standards would result in liability to the federal government for civil penalties of no more than US$5,000 per violation.

SpyCar ACT : Privacy Standards

- **Transparency**. Foreclosing other notice mechanisms as legally viable, the act would require that each vehicle provide clear and conspicuous notice, in clear and plain language, to owners or lessees of a vehicle of the collection, transmission, retention, and use of any driving data collected;

- **Consumer Control**. Owners or lessees must be given the option to terminate the collection and retention of driving data without losing access to navigation tools or other features or capabilities, to the extent technically possible (with the exception of driving data stored as part of the electronic data recorder system or other safety systems required for post-incident investigations, emissions history checks, crash avoidance or mitigation, or other regulatory compliance);

- **Limitations on Driving Data Use**. Manufacturers may not use any driving data collected by a vehicle for advertising or marketing purposes without the affirmative and express consent of the owner or lessee, which must be obtained using a clear and conspicuous consent request in clear and plain language that does not make use of the driving data a condition for the consumer’s use of any nonmarketing feature, capability, or functionality of the vehicle.

With 'recall,' Fiat Chrysler makes its car hack worse

July 27, 2015

The decision of Fiat Chrysler to mail out USB sticks to customers directly to patch the recent vulnerability is the security equivalent of waving a red rag to a bull

Stuxnet delivered to Iranian nuclear plant on thumb drive

Citing U.S. intelligence sources, ISSSource says an infected memory stick was used to hit the facility with the worm that severely damaged Iran's nuclear program.

Why Chrysler's car hack 'fix' is staggeringly stupid ZDNet

"It's like if after surgery the doctor forgets a pair of scissors in your stomach, and when you find out, he just sends you a scalpel to fix it yourself."

http://www.zdnet.com/article/chryslers-response-to-car-hack-was-slow-and-incredibly-stupid/

Recall Costs.

GM's total recall cost: $4.1 billion

Toyota's Out-of-Control Gas Pedals, cost of the blunder $5 billion

U.S. Department of Transportation's National Highway Traffic Safety Administration (NHTSA) sets the national safety standards and can influence -- or in some cases order -- an auto manufacturer to repair safety-related defects at no cost to the consumer. Even if the fix is something as minor as a missing washer or a faulty electrical connection, the manufacturer stands to lose millions of dollars in the process

In their interviews with manufacturers, some identified difficulties in notifying vehicle owners about safety defects. For example, there was mention that not all vehicle owners keep their address information up to date with state motor vehicle registration offices. In addition, the older the vehicle, the more changes of ownership and mailing addresses occur, making it more difficult to identify the current address of the current owner.

Will Autonomous Cars Be the Insurance Industry’s Napster Moment ?

Autonomous vehicles will make commuting a lot safer.

Consumers have to pay out a lot less money with the lower number of claims, but premiums will necessarily drop as well and the overall amount of money within the car insurance system will dwindle.

One opportunity for the industry could be selling more coverage to carmakers and other companies developing the automated features for cars.

When the technology fails, manufacturers could get stuck with big liabilities that they will want to cover by buying more insurance.

There's also a potential for cars to get hacked as they become more networked.

1996+ : Year the Matrix Started.

Modern automobiles are laced with a number of microcontrollers and sensors that monitor and control everything from the throttle position to the ambient air temperature.

These devices typically communicate over a wired in-vehicle network like a CAN bus.

CAN bus is one of five protocols used in the on-board diagnostics (OBD)-II vehicle diagnostics standard.

The OBD-II standard has been mandatory for all cars and light trucks sold in the United States since 1996

Network technology existed in E/E architecture

Mix of low data rate control or high-cost/proprietary solutions

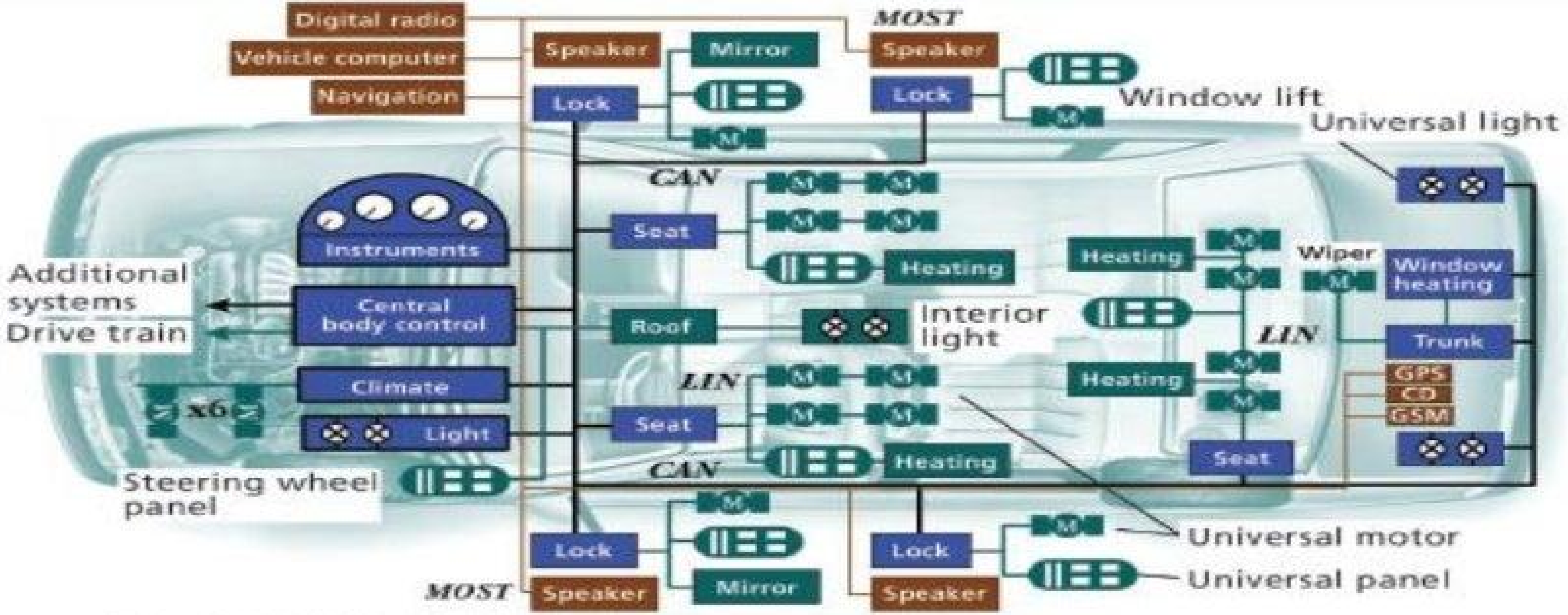
- Low data rate control

Technology	Data Rate	IP Ownership	Media	Topology	Usage
LIN	40kbps	LIN Consortium	Single wire	P2P	Body electronics
CAN	1Mbps	ISO-11898 Bosch	UTP	Shared	Power train (Engine, transmission, ABS)
CAN-FD	2.5Mbps	Bosch	UTP	Shared	Power train (Engine, transmission, ABS)
FlexRay	10Mbps	ISO-17458 FlexRay Consortium	UTP	Shared	High-perf power train, (Safety, drive-by-wire, active suspension, ACC)

- High cost/proprietary

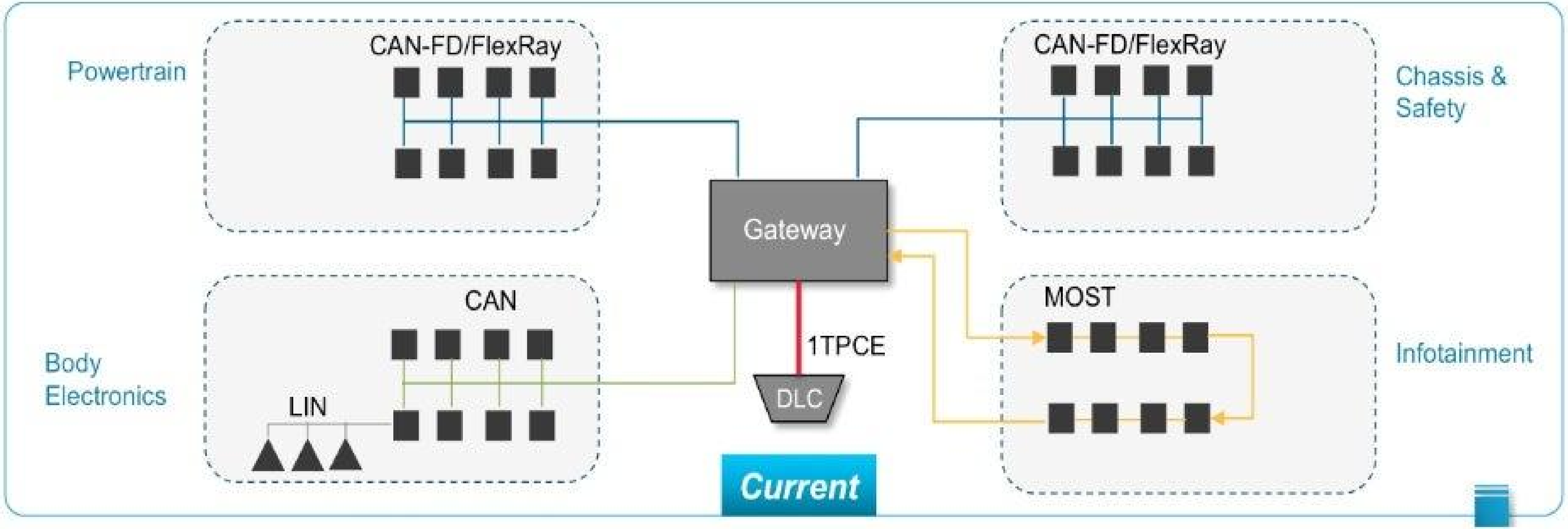
Technology	Data Rate	IP Ownership	Media	Topology	Usage
MOST	150Mbps	SMSC	POF	Ring	infotainment
FPDLink LVDS	655Mbps – 3Gbps	TI/National	Shield coax	P2P	Camera/display

Network Technology

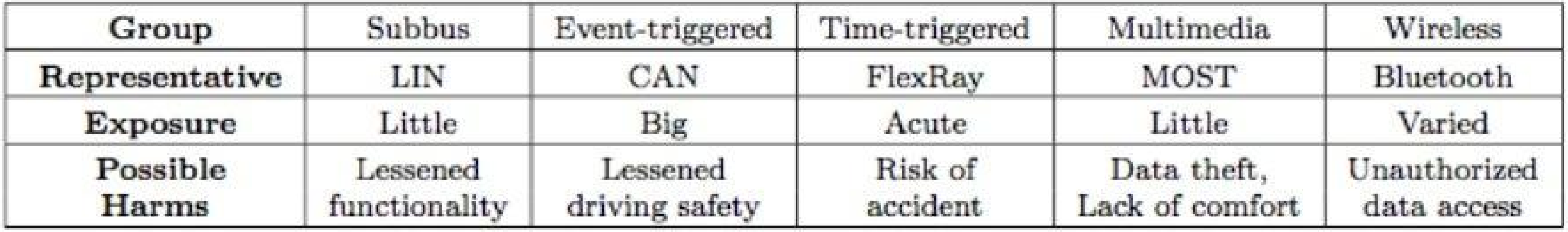


CAN	Controller area network
GPS	Global Positioning System
GSM	Global System for Mobile Communications
LIN	Local interconnect network
MOST	Media-oriented systems transport

Connected through Gateway.



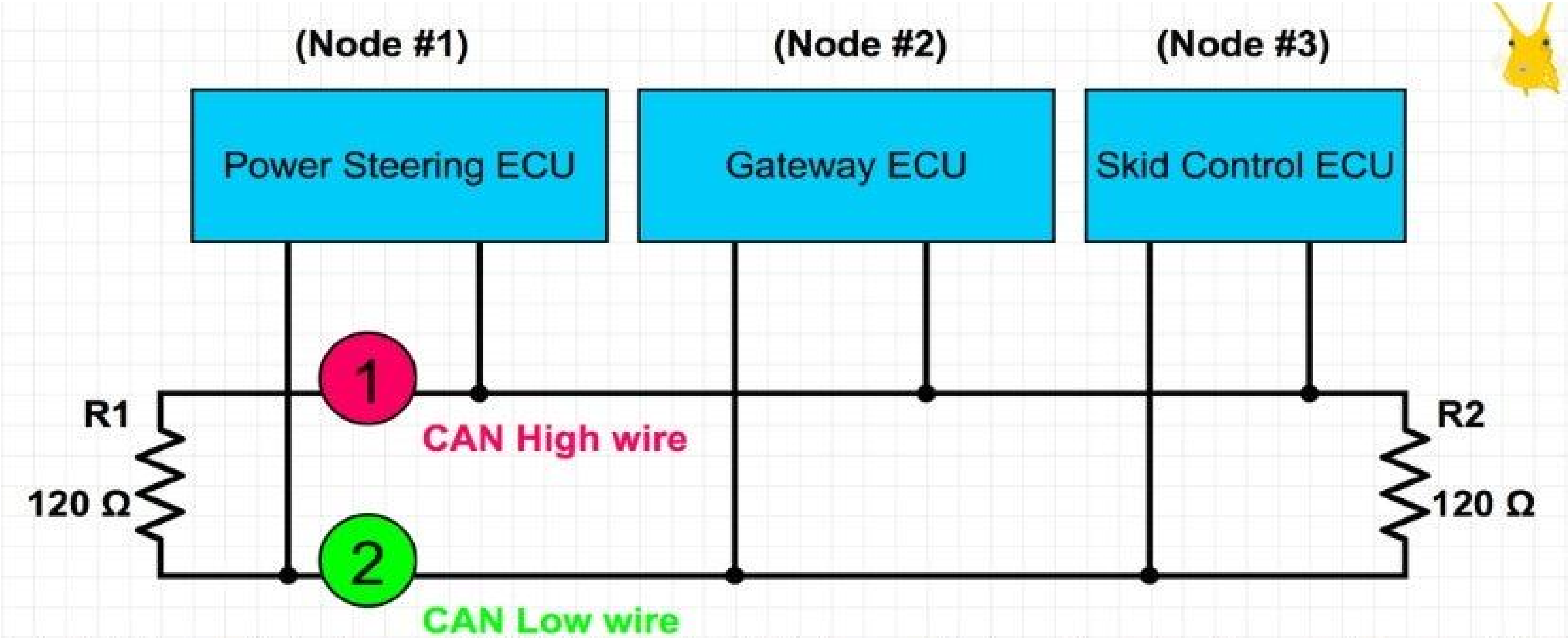
Endangerment of selected automotive bus systems



Group	Subbus	Event-triggered	Time-triggered	Multimedia	Wireless
Representative	LIN	CAN	FlexRay	MOST	Bluetooth
Exposure	Little	Big	Acute	Little	Varied
Possible Harms	Lessened functionality	Lessened driving safety	Risk of accident	Data theft, Lack of comfort	Unauthorized data access

CANBUS

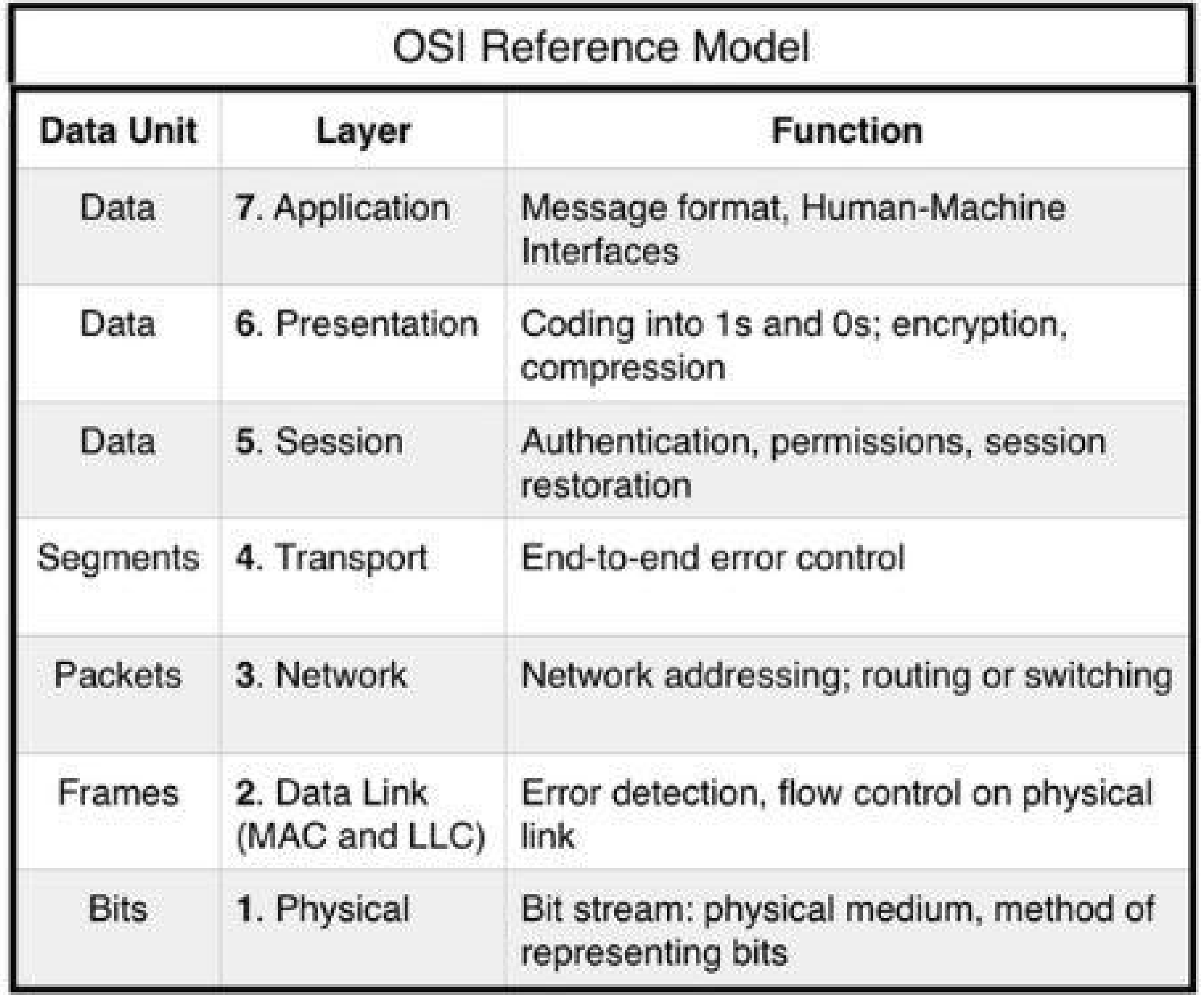
Can Topology



Two twisted differential wires, CAN high and CAN low, with two termination resistors of 120 ohm each. The bus has a maximum signaling rate of 1 Mbps with a bus length of 40 m with a maximum of 30 nodes.

http://www.cowfishstudios.com/blog/canned-pi-part1

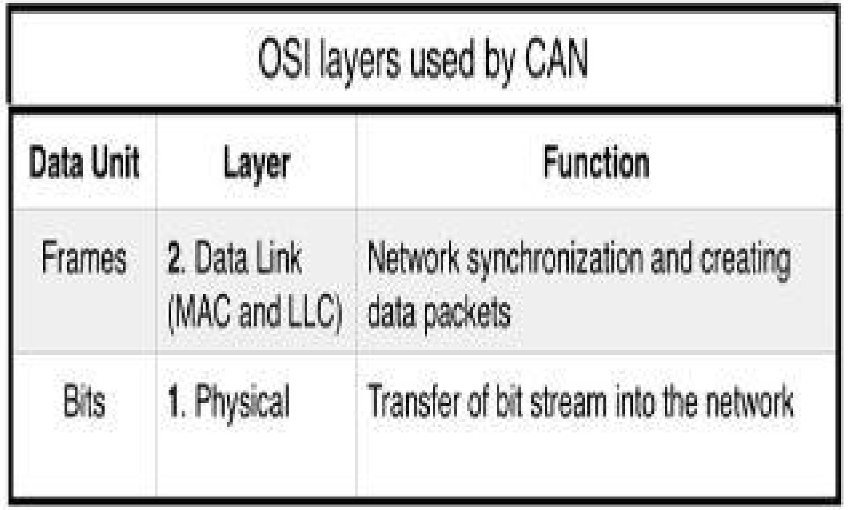
CAN specifies only the two basic layers: Data Link and Physical layer.



OSI Reference Model

Data Unit	Layer	Function
Data	7. Application	Message format, Human-Machine Interfaces
Data	6. Presentation	Coding into 1s and 0s; encryption, compression
Data	5. Session	Authentication, permissions, session restoration
Segments	4. Transport	End-to-end error control
Packets	3. Network	Network addressing; routing or switching
Frames	2. Data Link (MAC and LLC)	Error detection, flow control on physical link
Bits	1. Physical	Bit stream: physical medium, method of representing bits

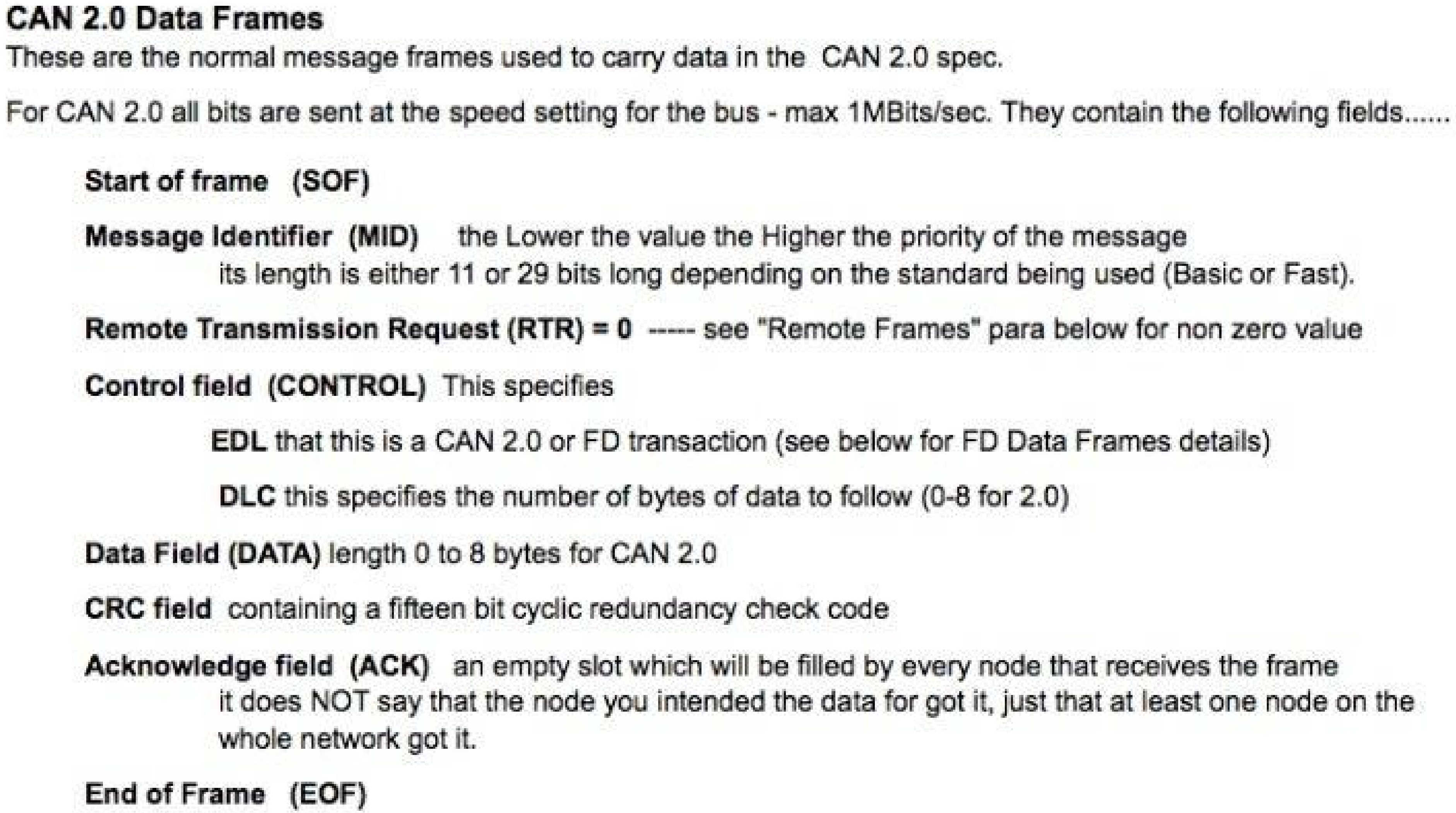
Only 2 Layers



OSI layers used by CAN

Data Unit	Layer	Function
Frames	2. Data Link (MAC and LLC)	Network synchronization and creating data packets
Bits	1. Physical	Transfer of bit stream into the network

CAN Frames



CAN 2.0 Data Frames
These are the normal message frames used to carry data in the CAN 2.0 spec.

For CAN 2.0 all bits are sent at the speed setting for the bus - max 1MBits/sec. They contain the following fields......

Start of frame (SOF)

Message Identifier (MID) the Lower the value the Higher the priority of the message
its length is either 11 or 29 bits long depending on the standard being used (Basic or Fast).

Remote Transmission Request (RTR) = 0 ----- see "Remote Frames" para below for non zero value

Control field (CONTROL) This specifies

EDL that this is a CAN 2.0 or FD transaction (see below for FD Data Frames details)

DLC this specifies the number of bytes of data to follow (0-8 for 2.0)

Data Field (DATA) length 0 to 8 bytes for CAN 2.0

CRC field containing a fifteen bit cyclic redundancy check code

Acknowledge field (ACK) an empty slot which will be filled by every node that receives the frame
it does NOT say that the node you intended the data for got it, just that at least one node on the whole network got it.

End of Frame (EOF)