# Automobile Intrusion Detection


## Jun Li

Twitter： @bravo_fighter

**UnicornTeam**

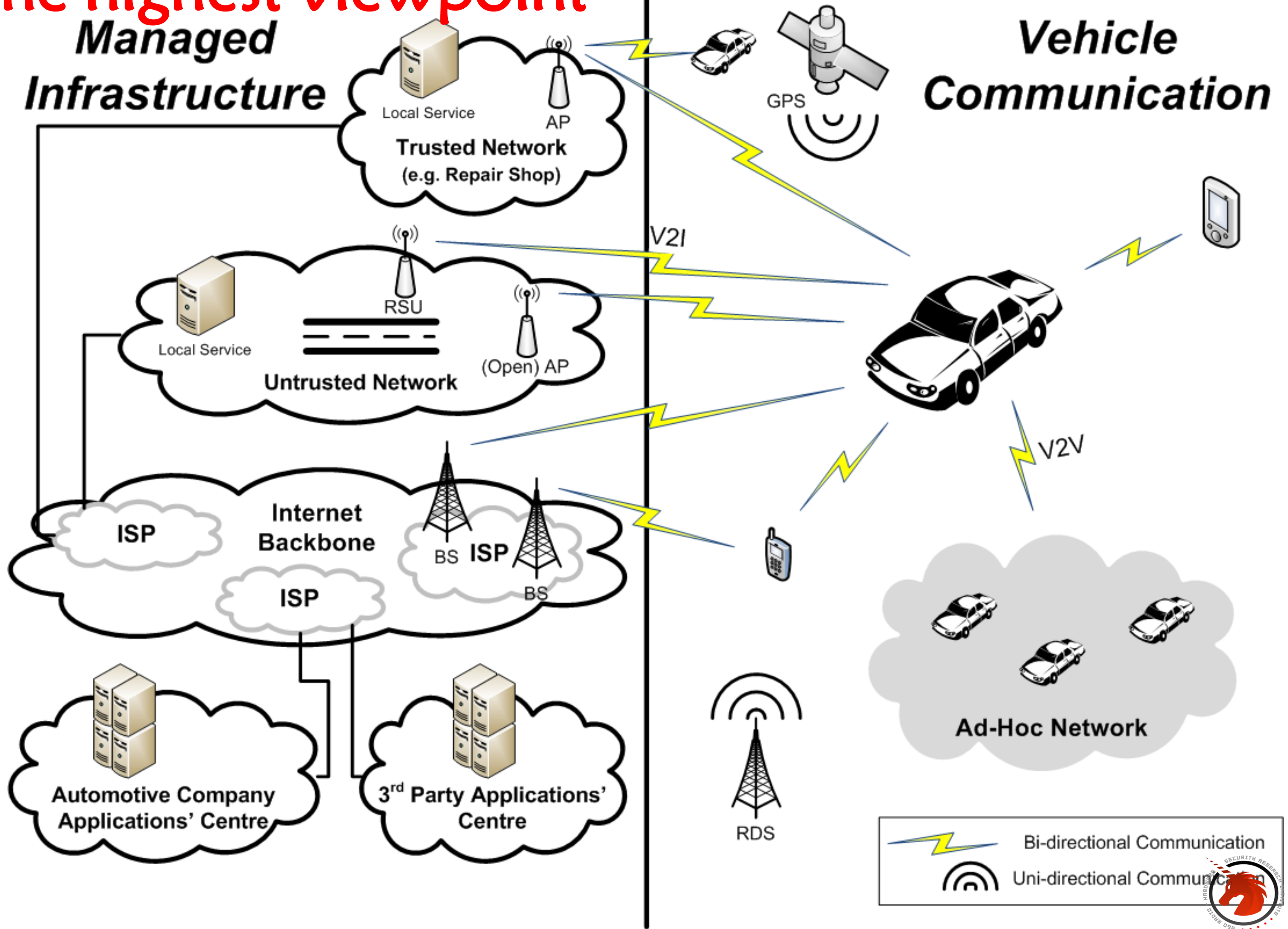
Qihoo360


360UNICORNTEAM

# Outline

- Quick recap of the status quo of connected vehicle security research
- Little bit about automobile working principle
- CAN bus anomaly detection

# From the highest viewpoint




360UNICORNTEAM

# Car hacking development

## CANSPY: A PLATFORM FOR AUDITING CAN DEVICES

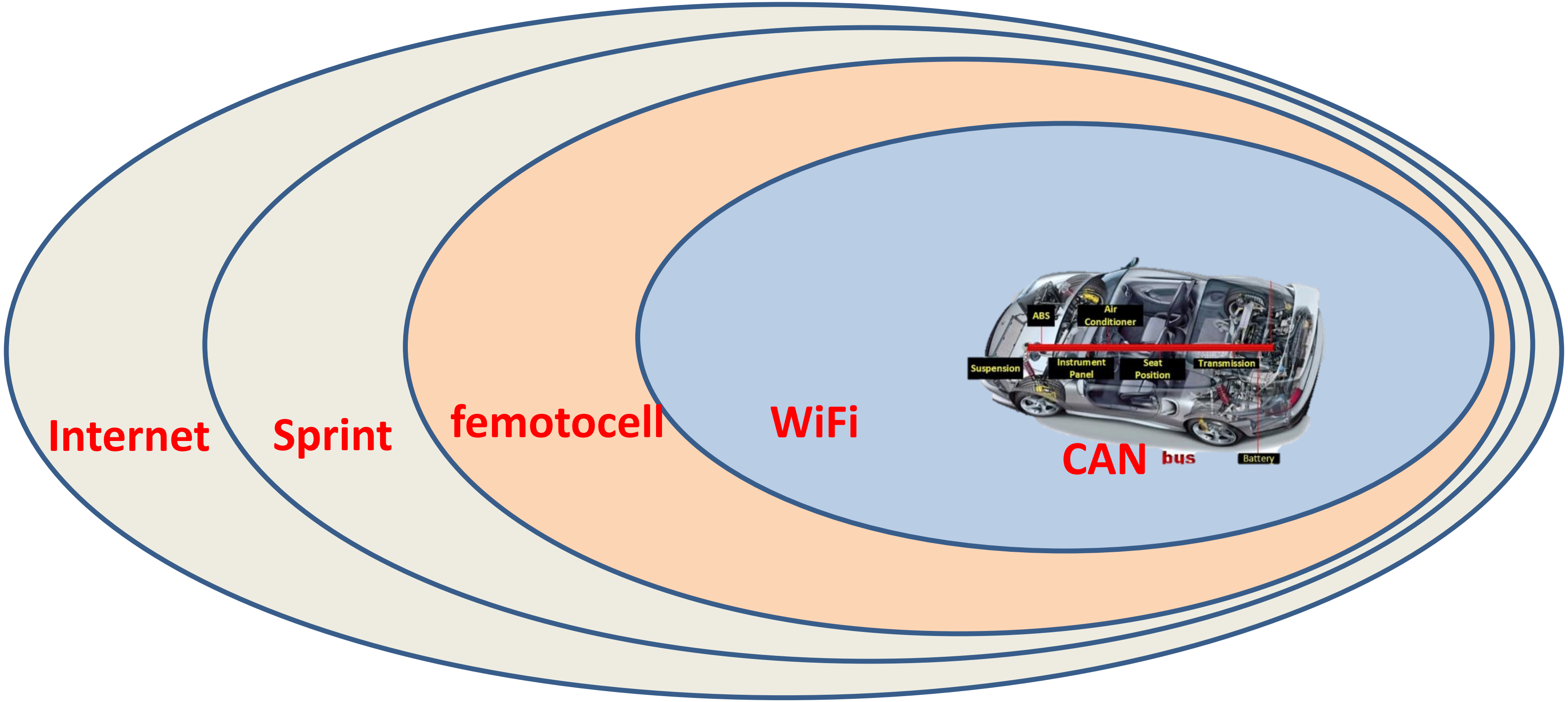
Arnaud Lebrun | Command and Control Engineer, Airbus Defence and Space
Jonathan-Christofer Demay | Penetration Testing Lead, Airbus Defence and Space

**Format**: 50 Minute Briefing
**Tracks**: Hardware/Embedded
Internet of Things

In the past few years, several tools have been released allowing hobbyists to connect to CAN buses found in cars. This is welcomed as the CAN protocol is becoming the backbone for embedded computers found in smartcars. Its use is now even spreading outside the car through the OBD-II connector: usage-based policies from insurance companies, air-pollution control from law enforcement or engine diagnostics from smartphones for instance. Nonetheless, these tools will do no more than what professional tools from automobile manufacturers can do. In fact, they will do less as they do not have knowledge of upper-layer protocols.

# Remote Attack Example

## Jeep Uconnect Vulnerability



# Sensor security

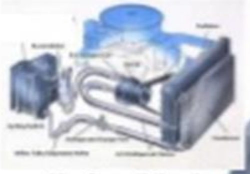
# Outline

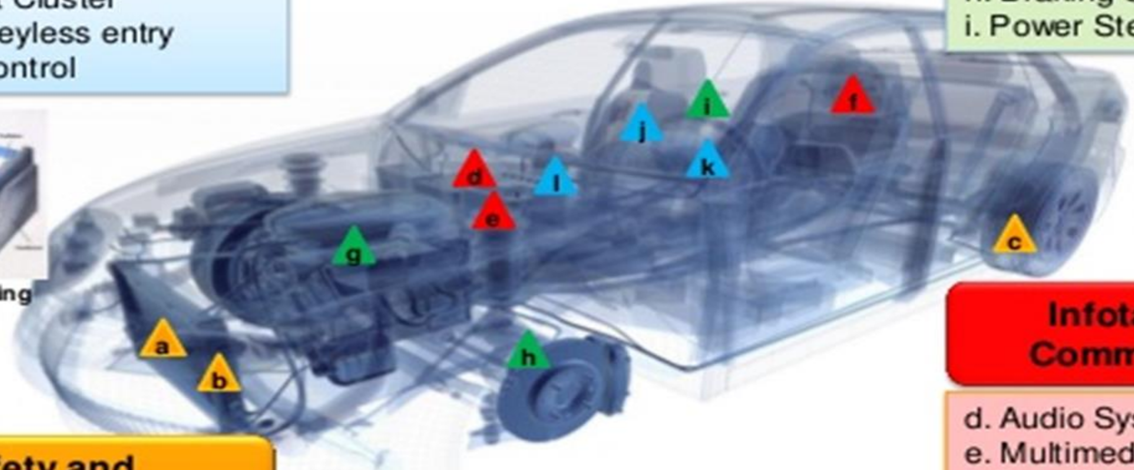
- Quick recap of the status quo of connected vehicle security research
- Little bit about automotive principles
- CAN bus anomaly detection

# Car explained

**Body Electronics - Comfort/Convenience**

j. Instrument Cluster
k. Remote keyless entry
l. Climate Control


Air Conditioning System




**Safety and Driver Assistance**

a. Adaptive Cruise Control
b. Collision Warning
c. Tire pressure monitoring

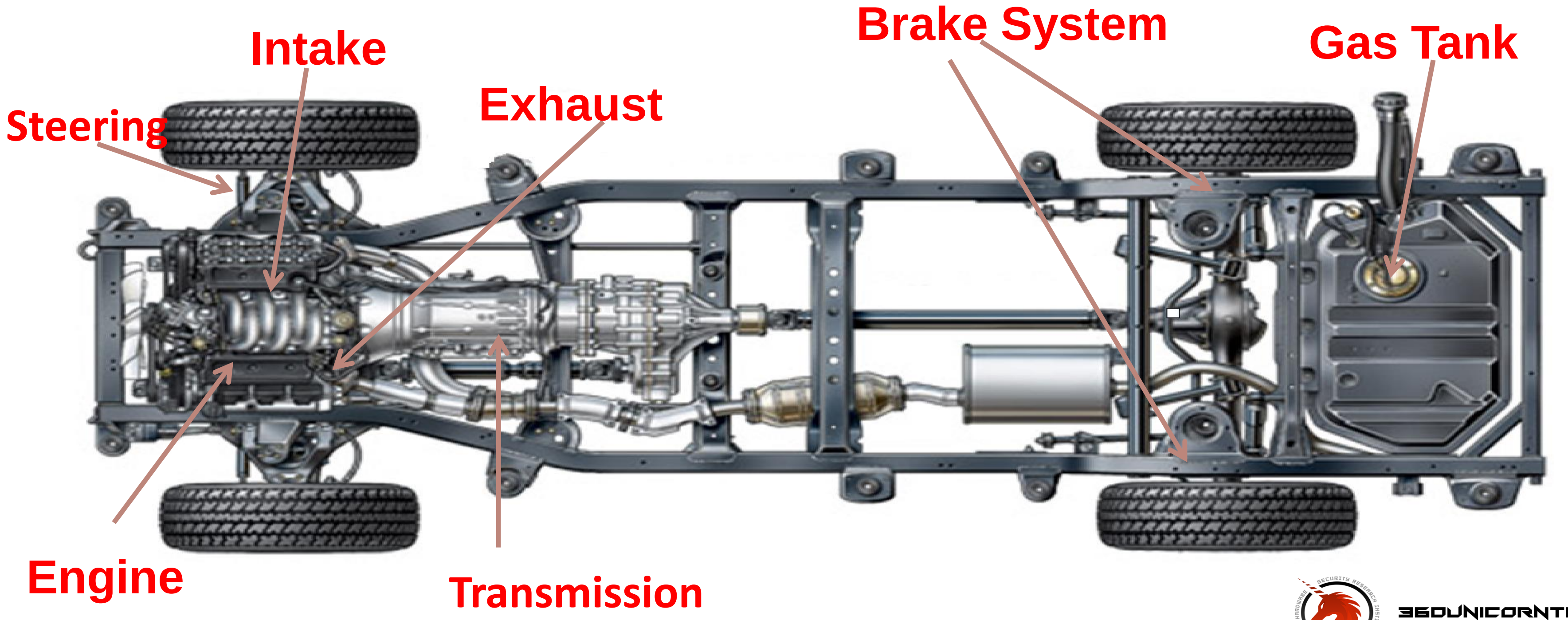
**Powertrain & Hybrid**

g. Engine management
h. Braking System
i. Power Steering

**Infotainment & Communications**

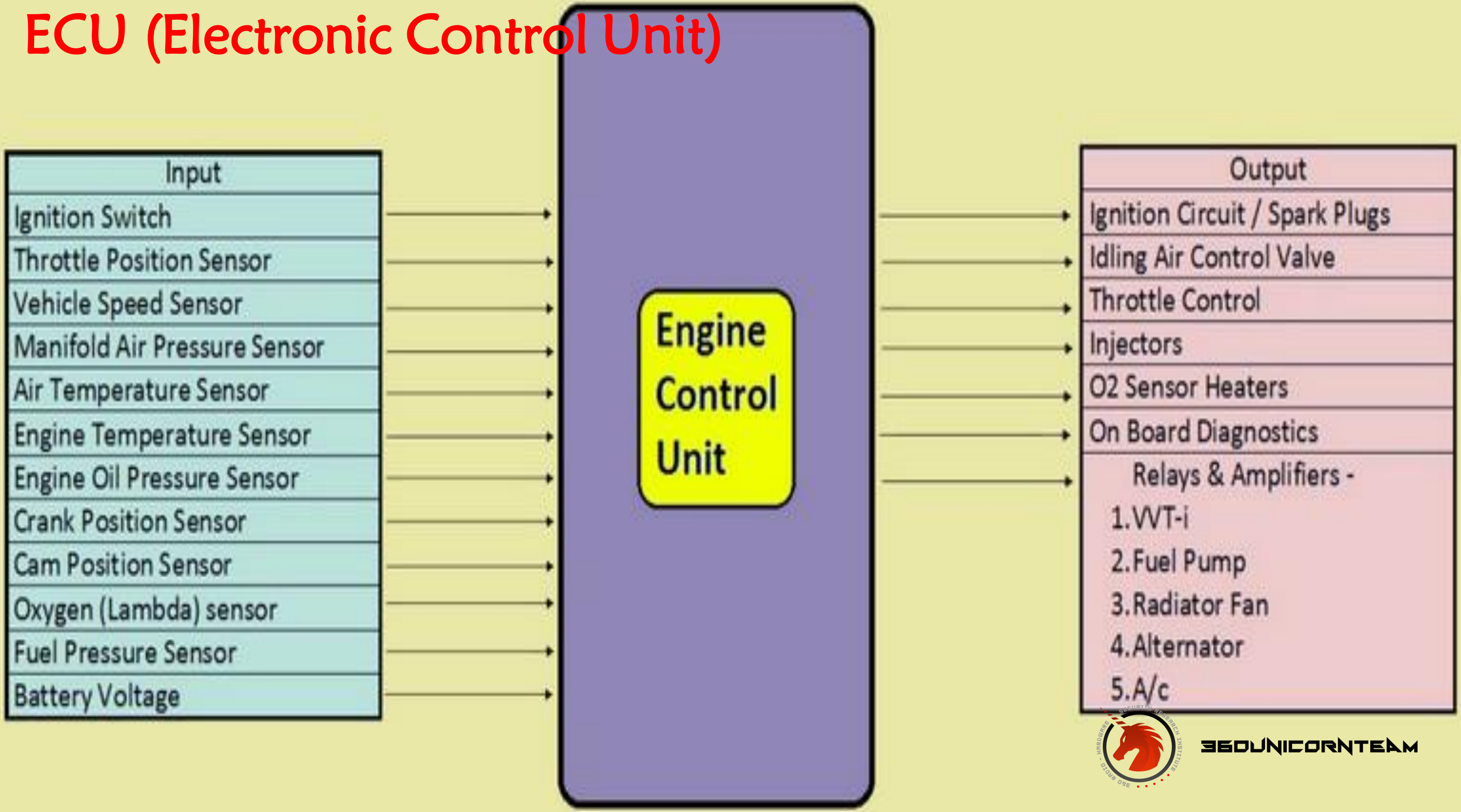
d. Audio Systems
e. Multimedia Systems
f. Rear Seat Entertainment

# Components of an Automobile

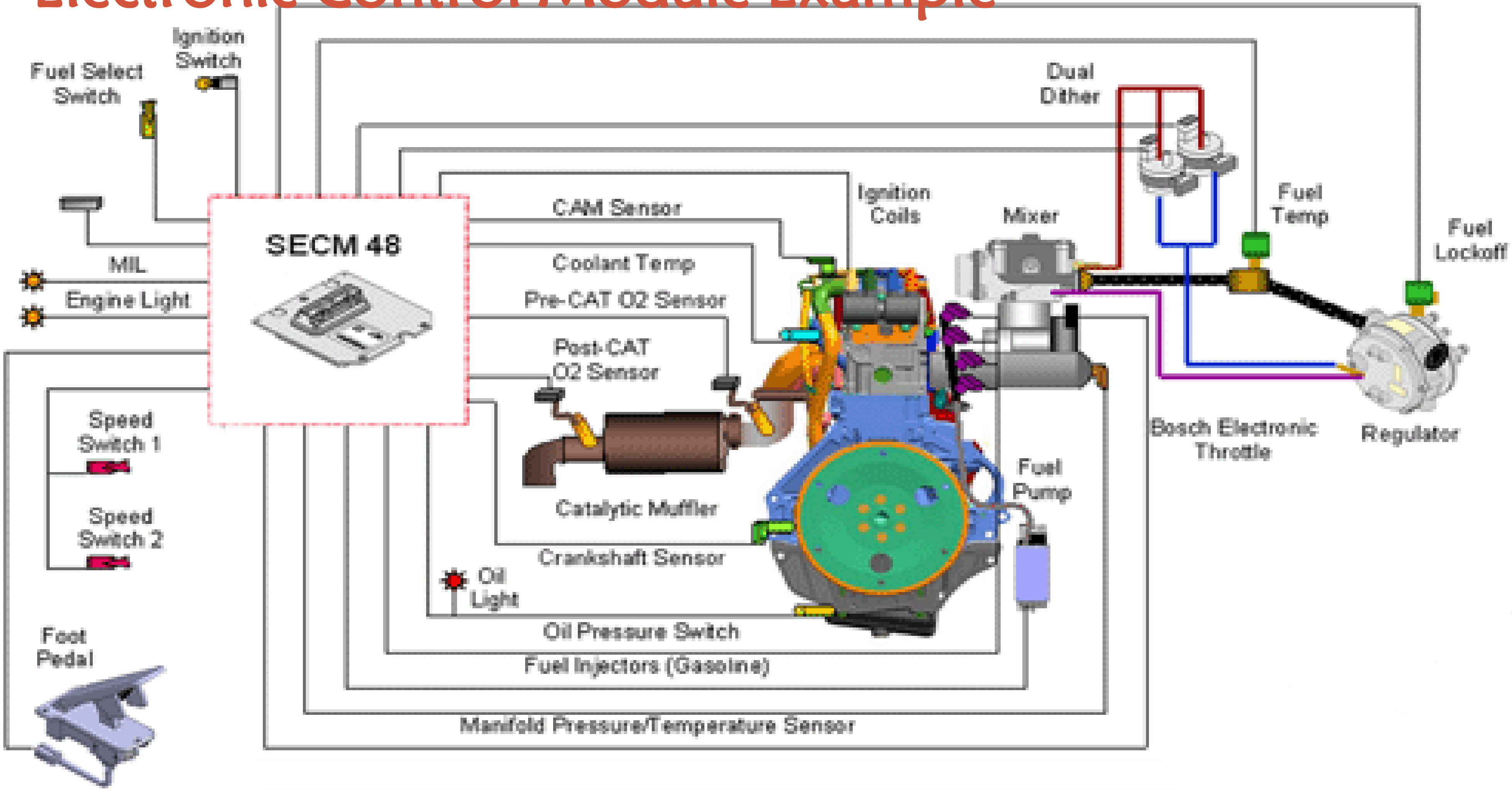



360UNICORNTEAM

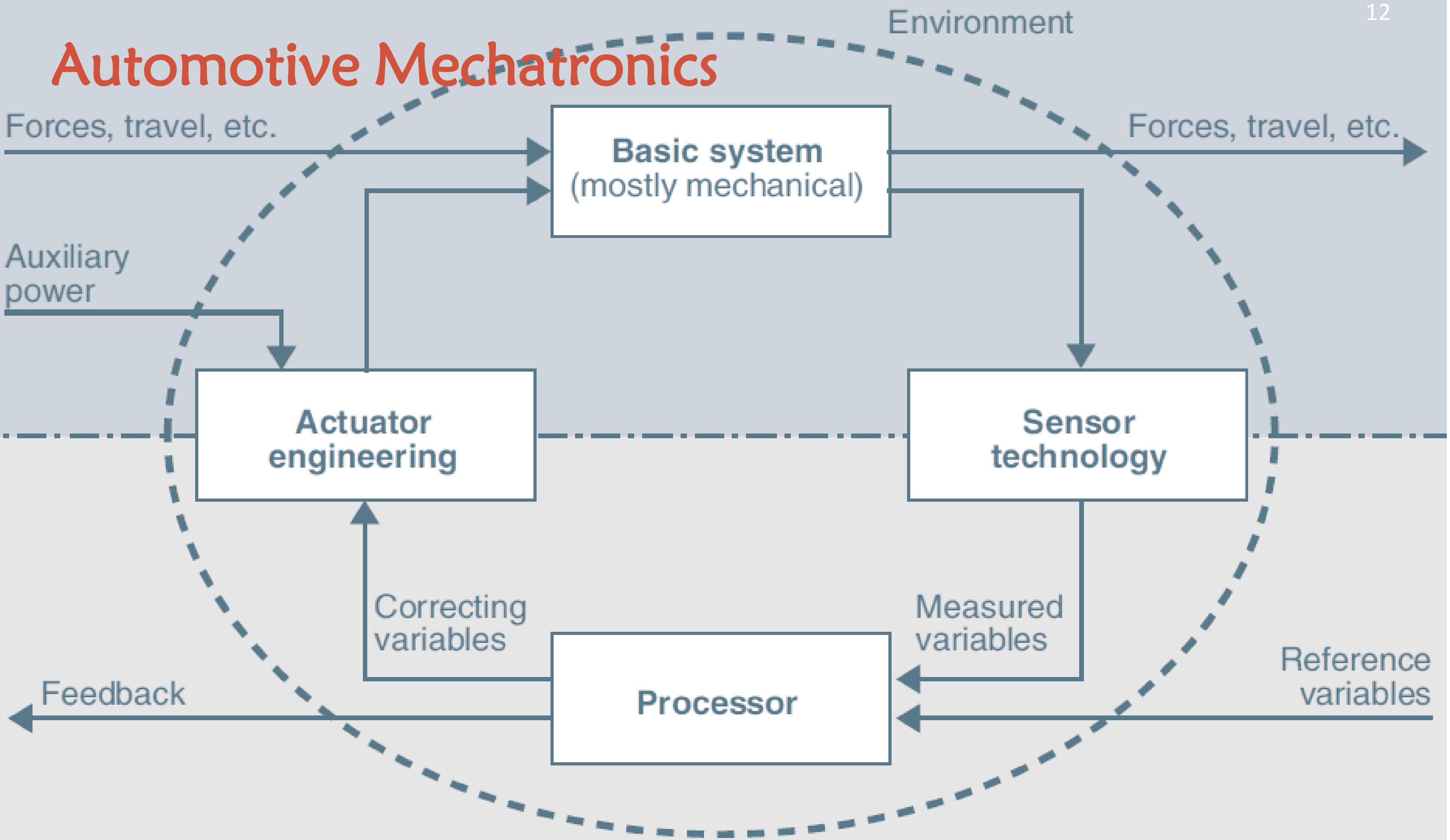
# ECU (Electronic Control Unit)



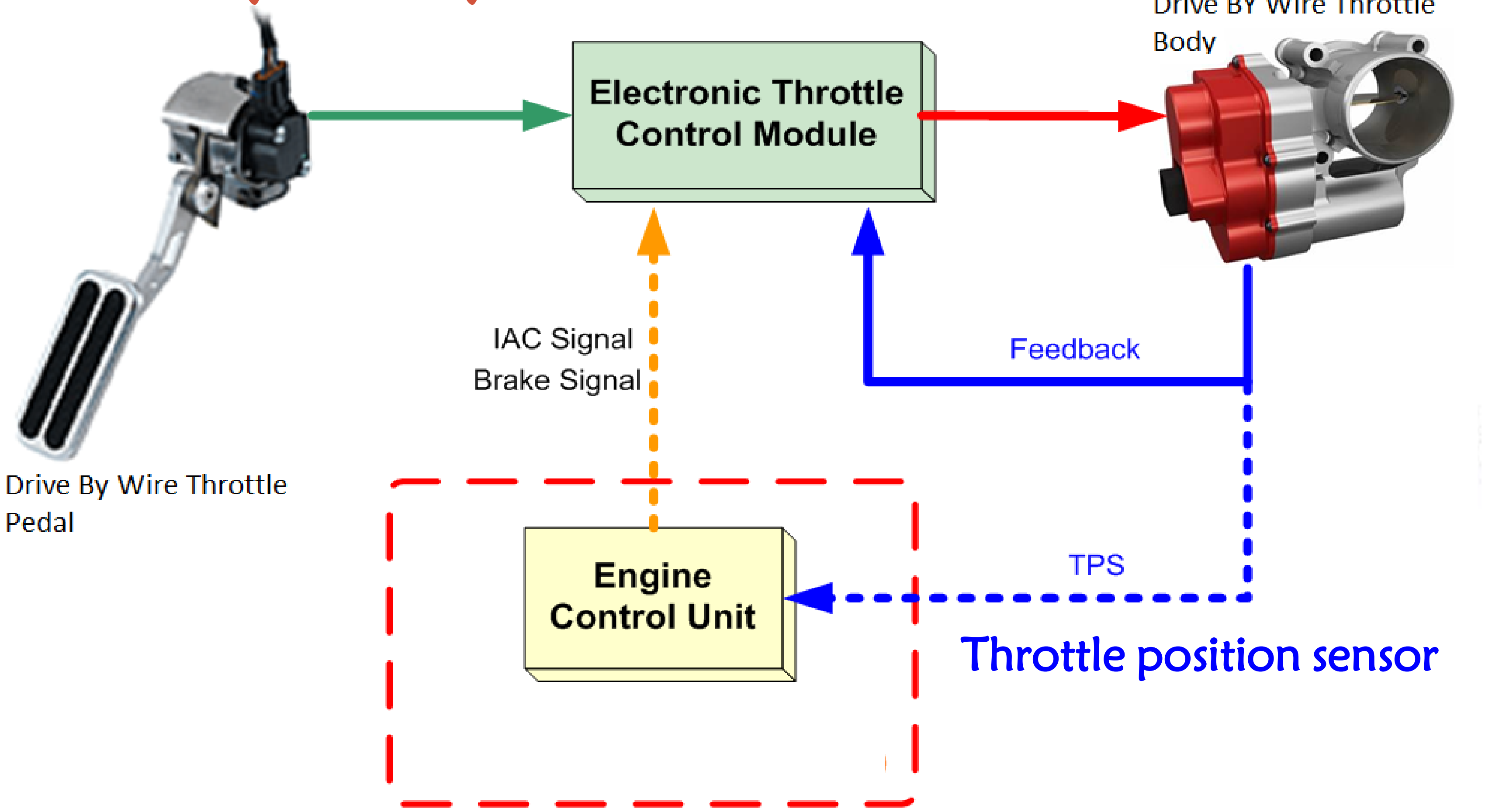
# Electronic Control Module Example



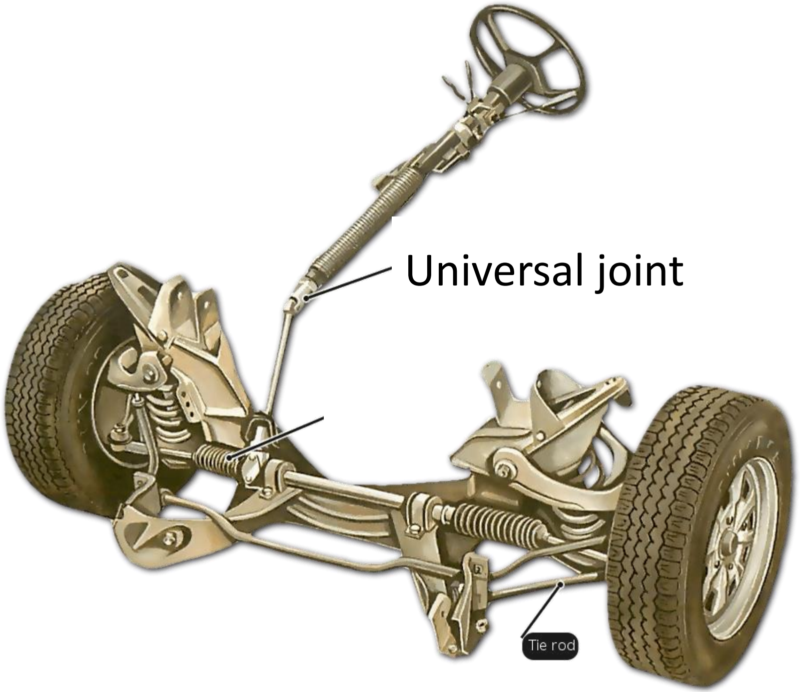
# Automotive Mechatronics



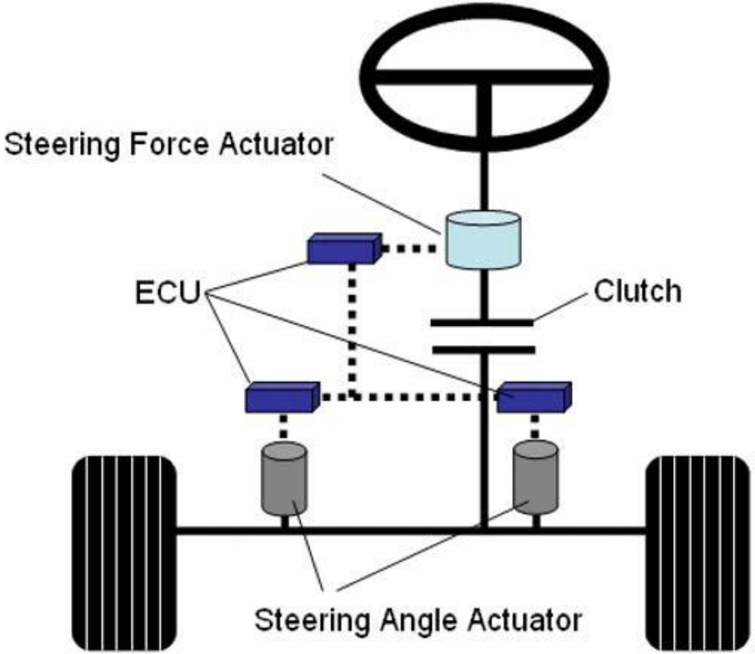
# Drive-by-wire system



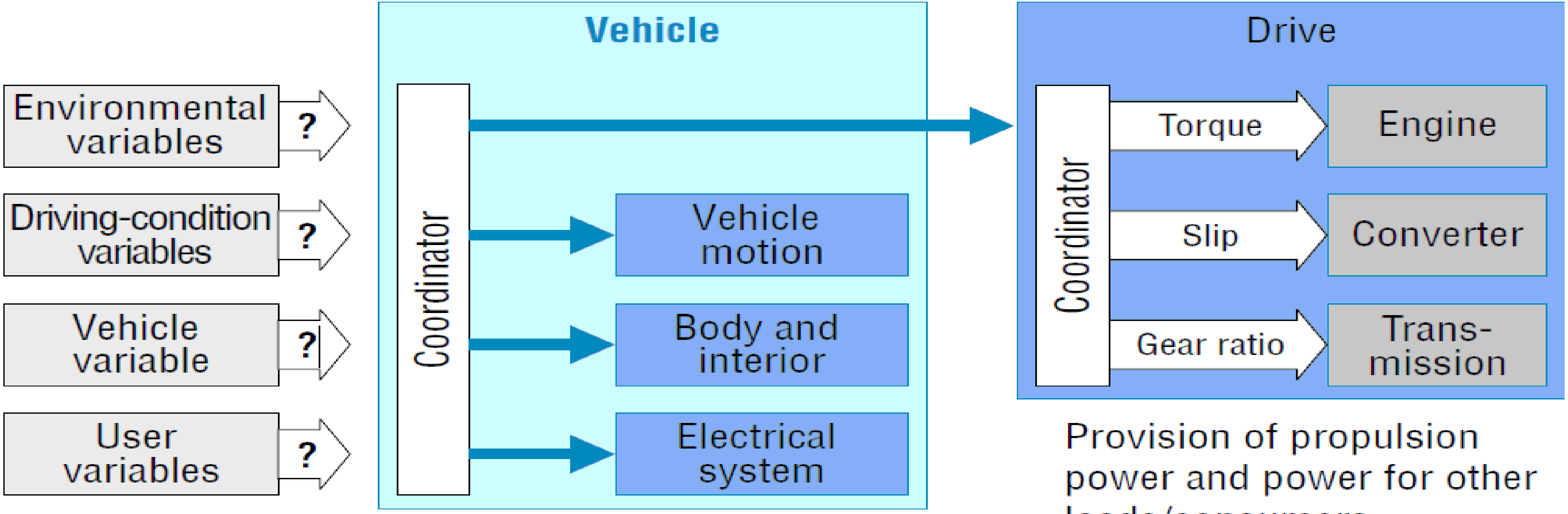
# Steering-by-wire system




Steer-by –wire
（with mechanical fallback clutch）

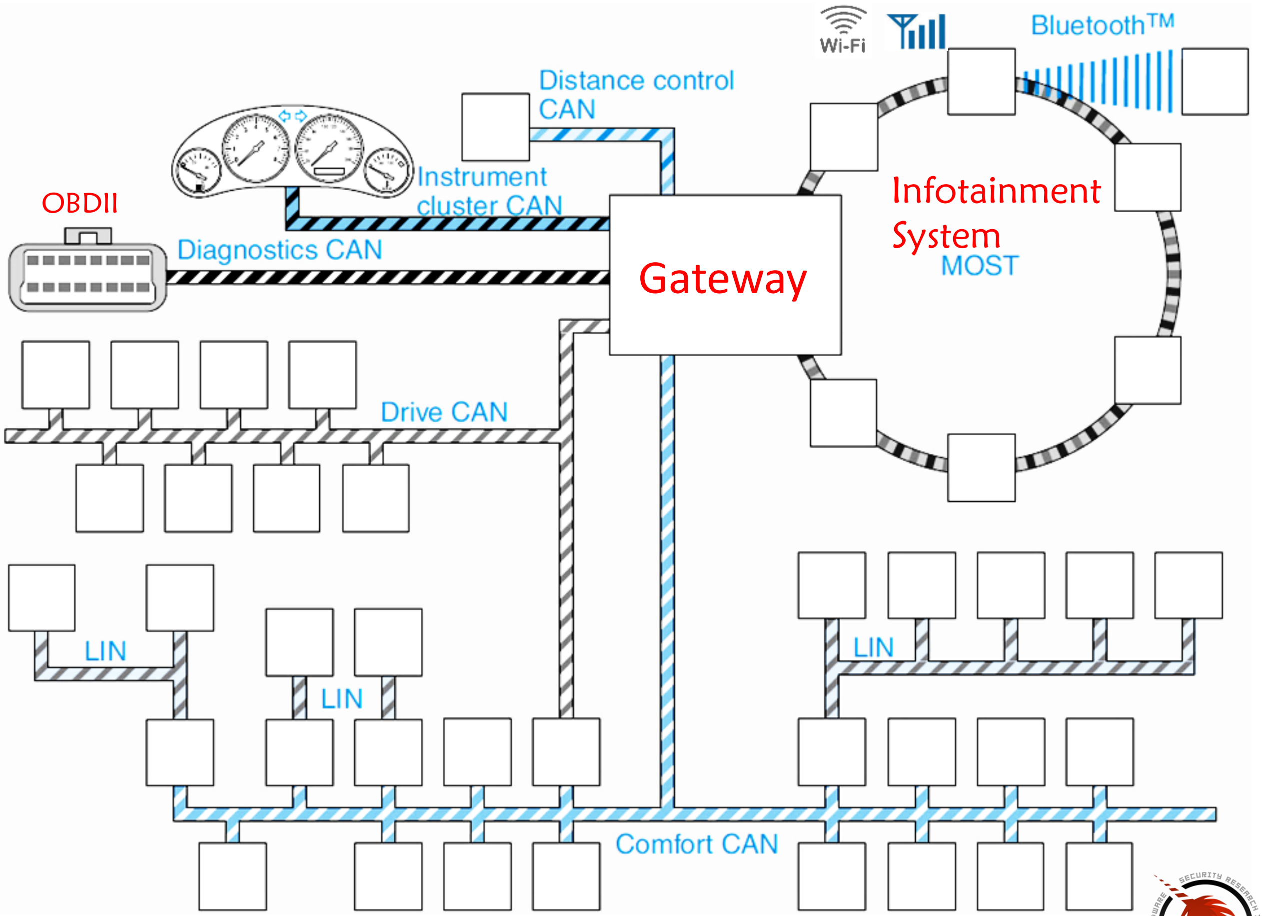


# Automotive Control System Architecture




Provision of propulsion power and power for other loads/consumers

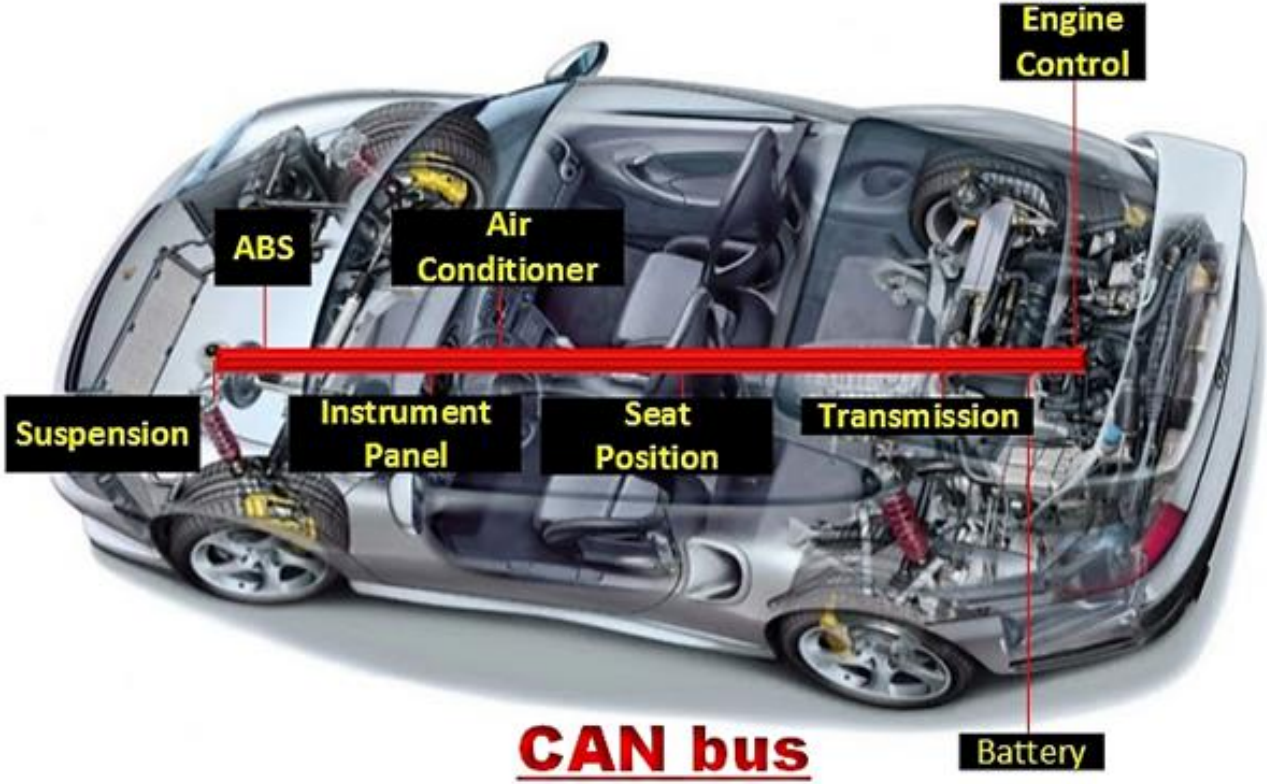
# Vehicle Communication System




MOST
LIN
CAN
FlexRay
Bluetooth
Wifi
SubGHz

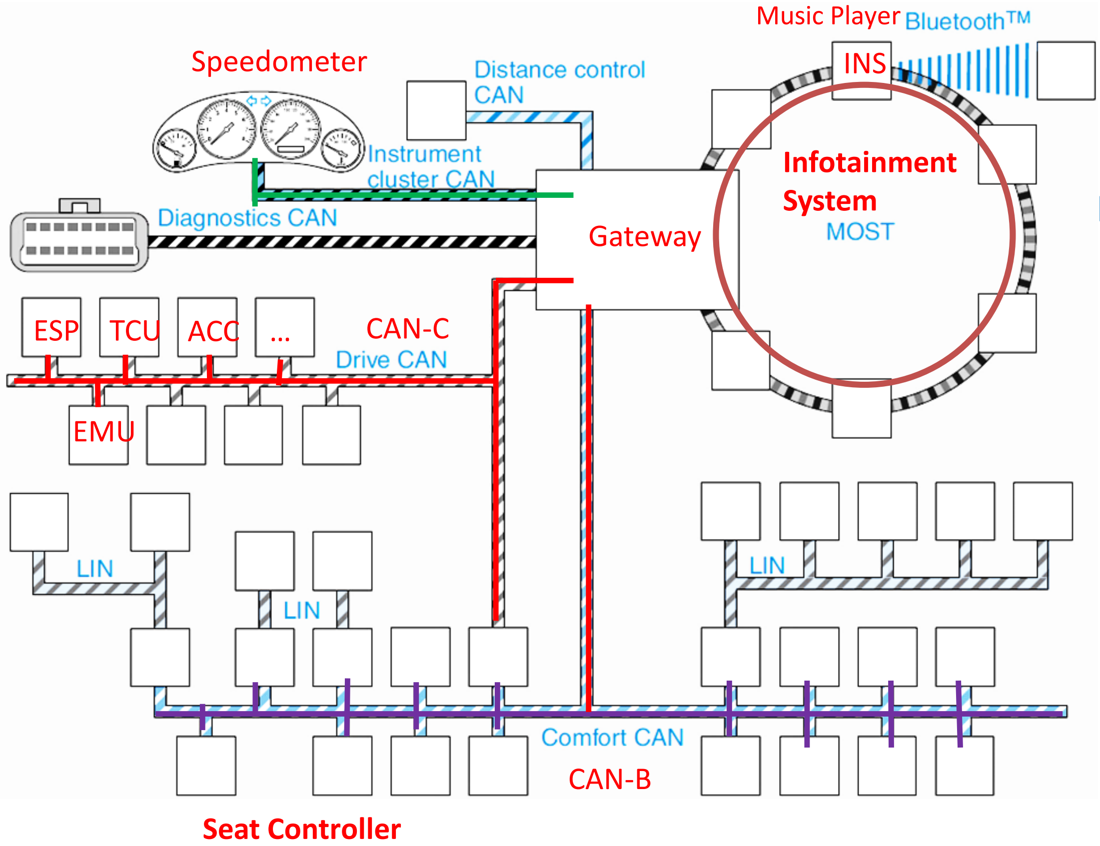
360UNICORNTEAM

# Vehicle CAN BUS System




360UNICORNTEAM

# Vehicle Communication System example




**ESP** （electronic stability program）

**EMU** （engine management system）

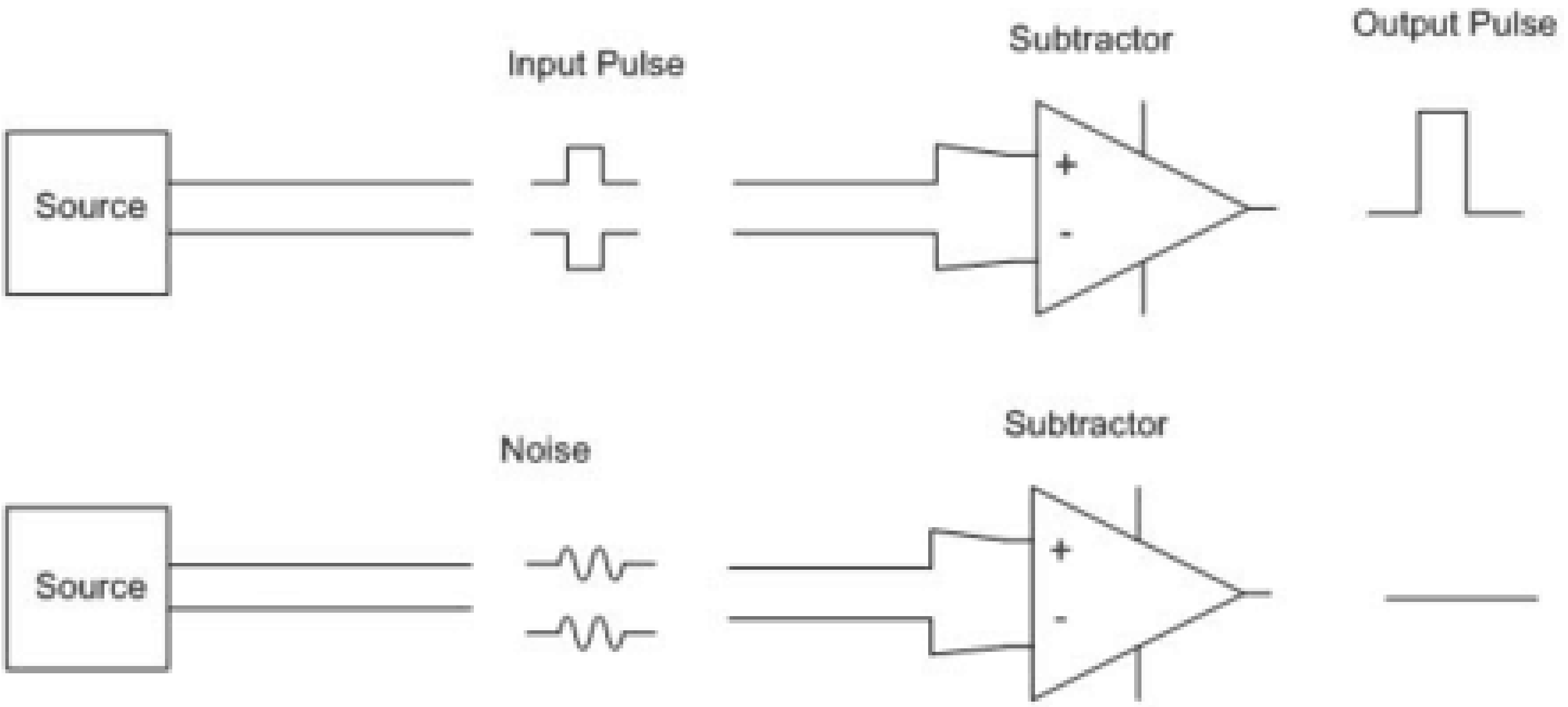
**TCU** （transmission control unit）

**ACC** （adaptive cruise control）

**INS** （Inertial navigation system）

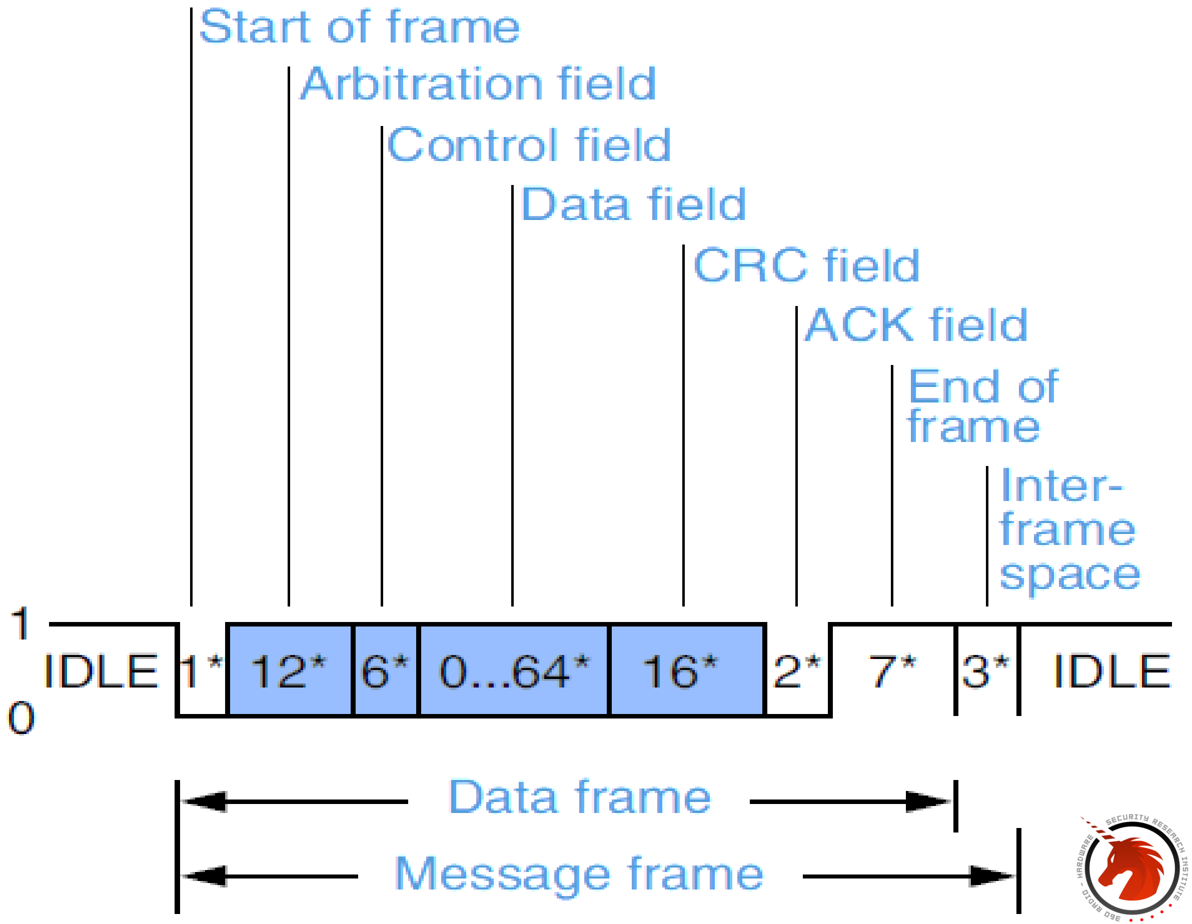
360UNICORNTEAM

# CAN BUS Signaling



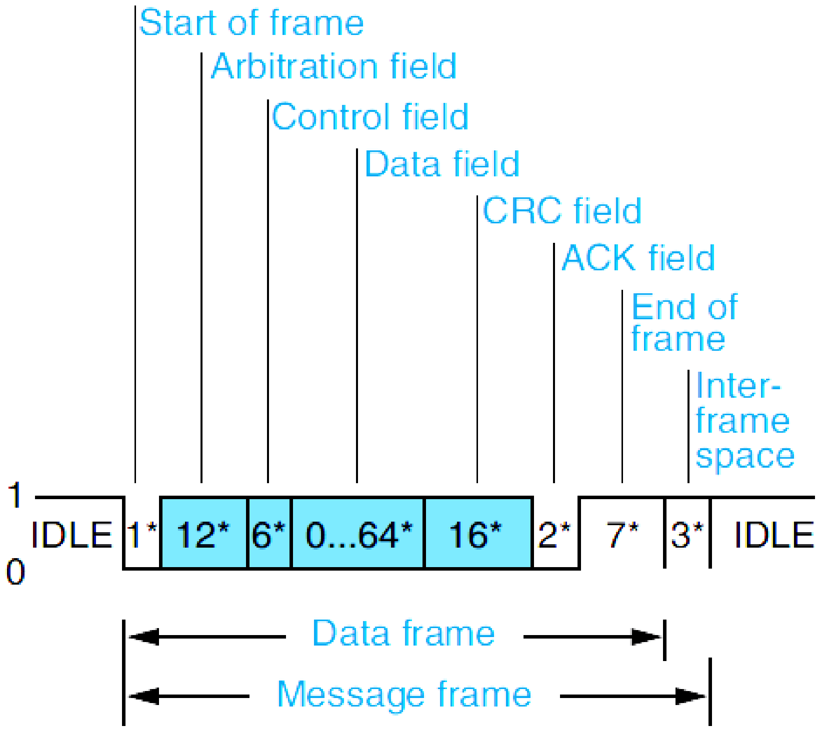

360UNICORNTEAM

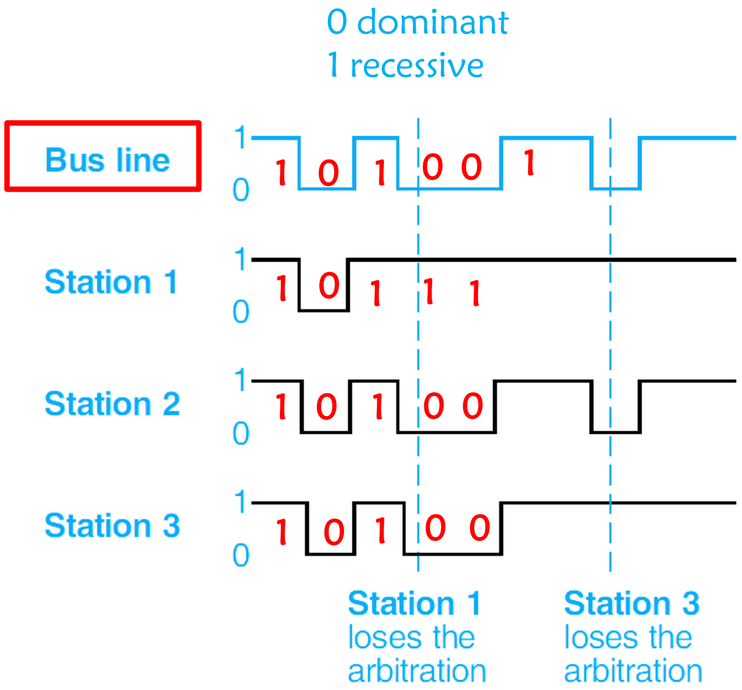
# CAN Frame Structure




360UNICORNTEAM

# CAN Bus Access Arbitration



# Difficulties of CAN bus defense

①Real time requirements
②Hard to trace back to sender
③High cost of false positive
④…

360UNICORNTEAM

# CAN BUS Attack

## ADVANCED CAN INJECTION TECHNIQUES FOR VEHICLE NETWORKS

Charlie Miller | Security engineer, Uber ATC
Chris Valasek | Security Lead, Uber ATC
**Format:** 50 Minute Briefing
**Tracks:** Hardware/Embedded
Smart Grid/Industrial Security

The end goal of a remote attack against a vehicle is physical control, usually by injecting CAN messages onto the vehicle's network. However, there are often many limitations on what actions the vehicle can be forced to perform when injecting CAN messages. While an attacker may be able to easily change the speedometer while the car is driving, she may not be able to disable the brakes or turn the steering wheel unless the car she is driving meets certain prerequisites, such as traveling below a certain speed. In this talk, we discuss how physical, safety critical systems react to injected CAN messages and how these systems are often resilient to this type of manipulation. We will outline new methods of CAN message injection which can bypass many of these restrictions and demonstrate the results on the braking, steering, and acceleration systems of an automobile. We end by suggesting ways these systems could be made even more robust in

# Outline

- Quick recap of the status quo of connected vehicle security research
- Little bit about automobile working principle
- Related Research
- CAN bus anomaly detection

- Researching and evaluating design processes and standards
  - Evaluating potential to adapt existing functional safety approaches
- Investigating Protective/Preventive solutions
  - Message authentication for communications Interfaces ( V2V project initiating)
  - Gateways, firewalls (project initiating)
- Researching Intrusion Detection Solutions
  - Vehicle bus monitoring for anomalous behavior; (project initiating)
- Assessing Treatment Solutions
  - Feedback loop for continuous improvements (Monitoring progress in standing up an Automotive ISAC ).
- Crosscutting Research:
  - Vulnerability Testing (Publish reports in 2016)
  - Software – including over the air updates

NHTSA
NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

# WHAT WE DO
# OUR SERVICES

## CAR DESIGN
## SECURITY TESTING

Our Auto Cybersecurity Testing Lab X-rays 80 + testing checkpoints :

- Telematics unit or IVI device
- ECU
- CAN Bus Networks
- Telematics platform



## FIREWALL AND SECURITY OTA
## CUSTOMIZED SDK APIS

- Security layer for easy deployment
- Defend Zero-day attacks
- Detection, alert and mitigation
- OTA for Vulnerability fixing and New security feature

## REAL-TIME MONITORING
## CYBER SECURITY DASHBOARD

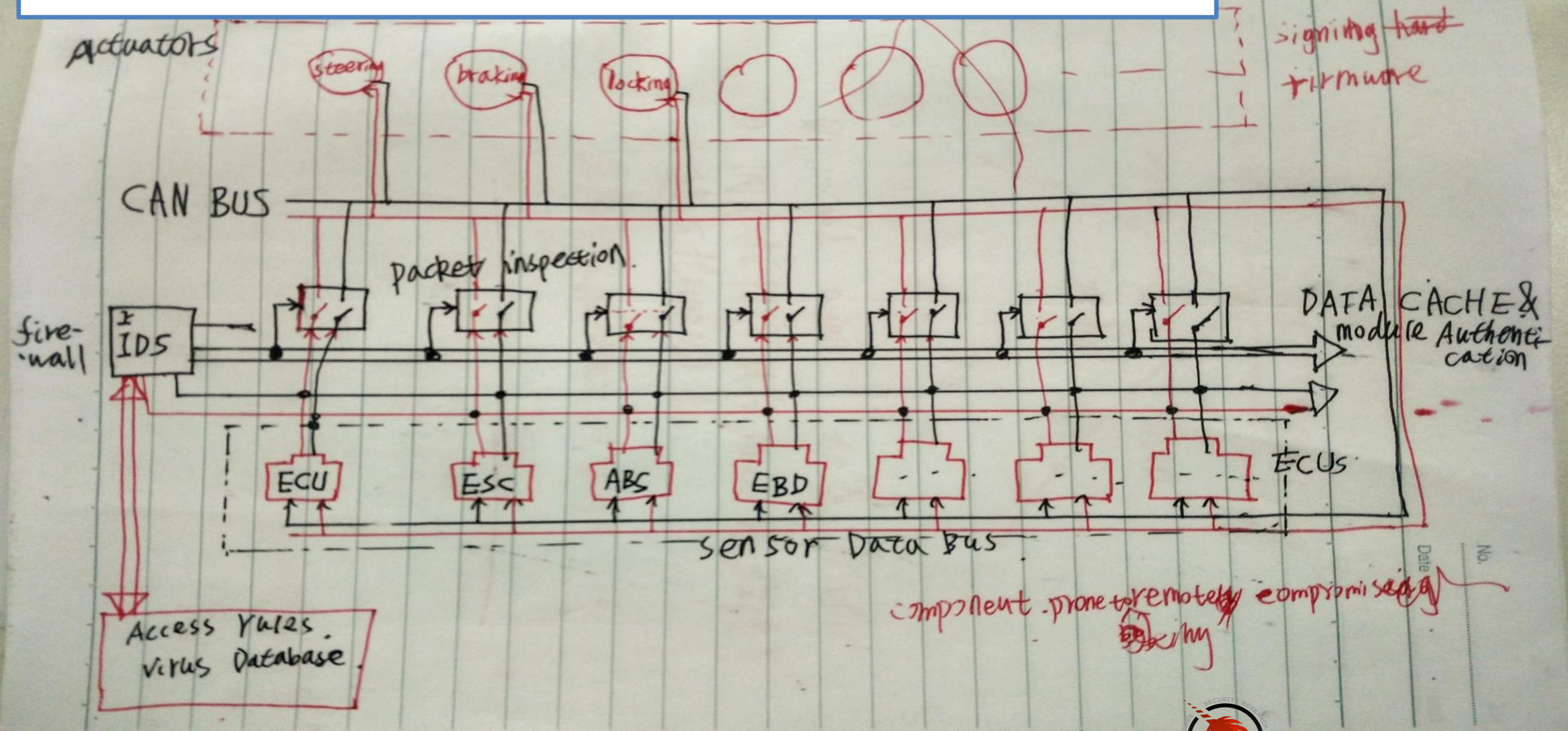
- SAE-J3061 standard

TOP

360UNICORNTEAM

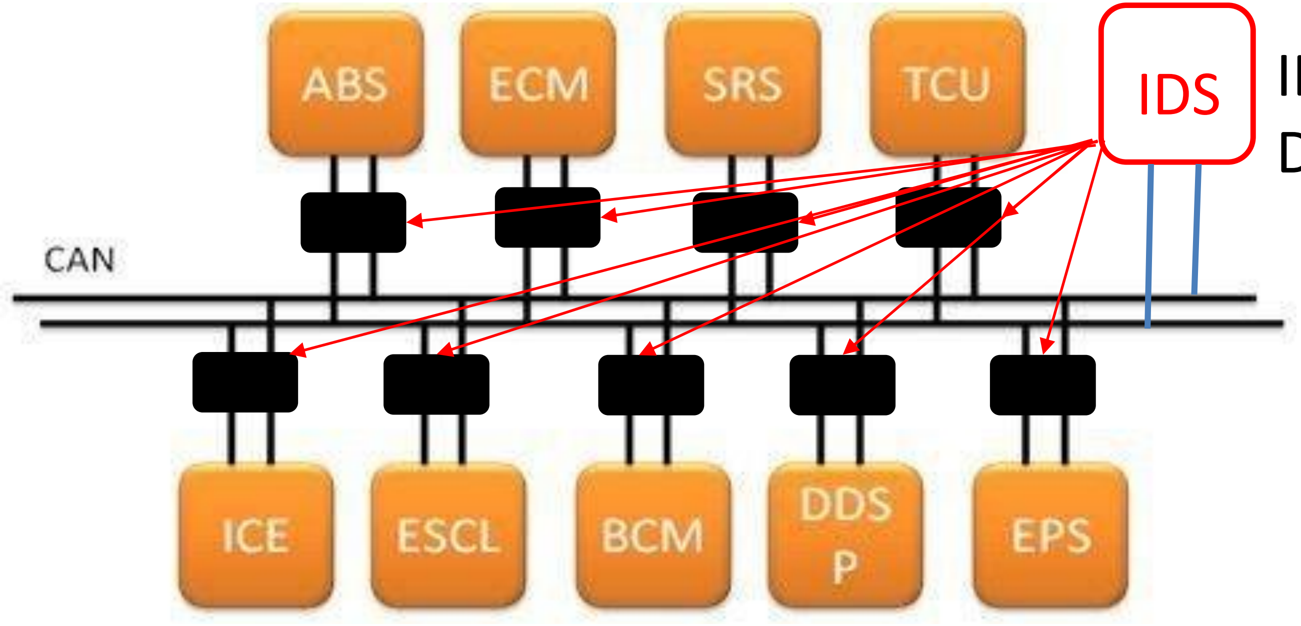
PROVEN, AFTERMARKET SOLUTIONS FOR USAGE-BASED INSURANCE, FLEET MANAGEMENT AND CONSUMER

# Distributed CAN bus defence architecture



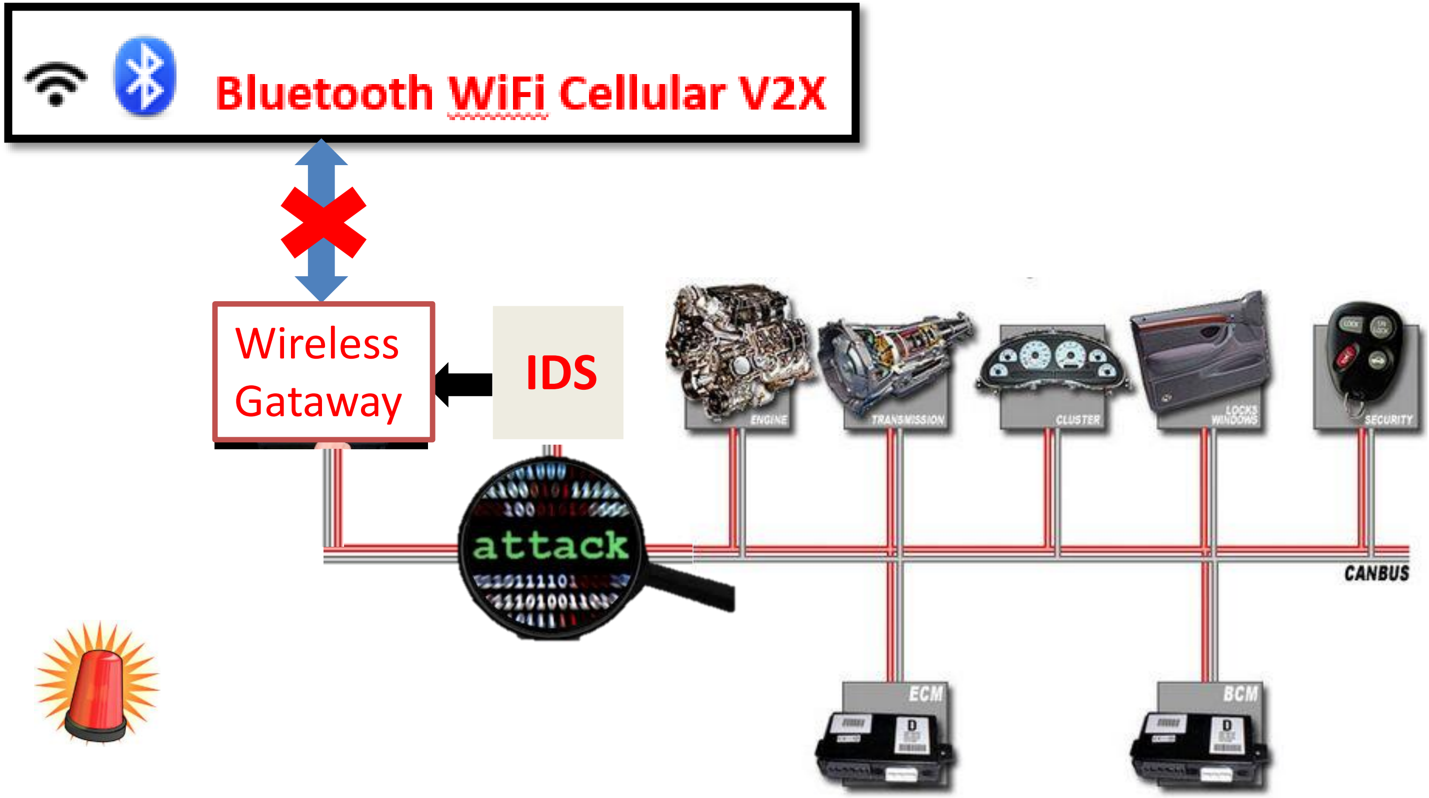

360UNICORNTEAM

# Distributed CAN bus defence architecture



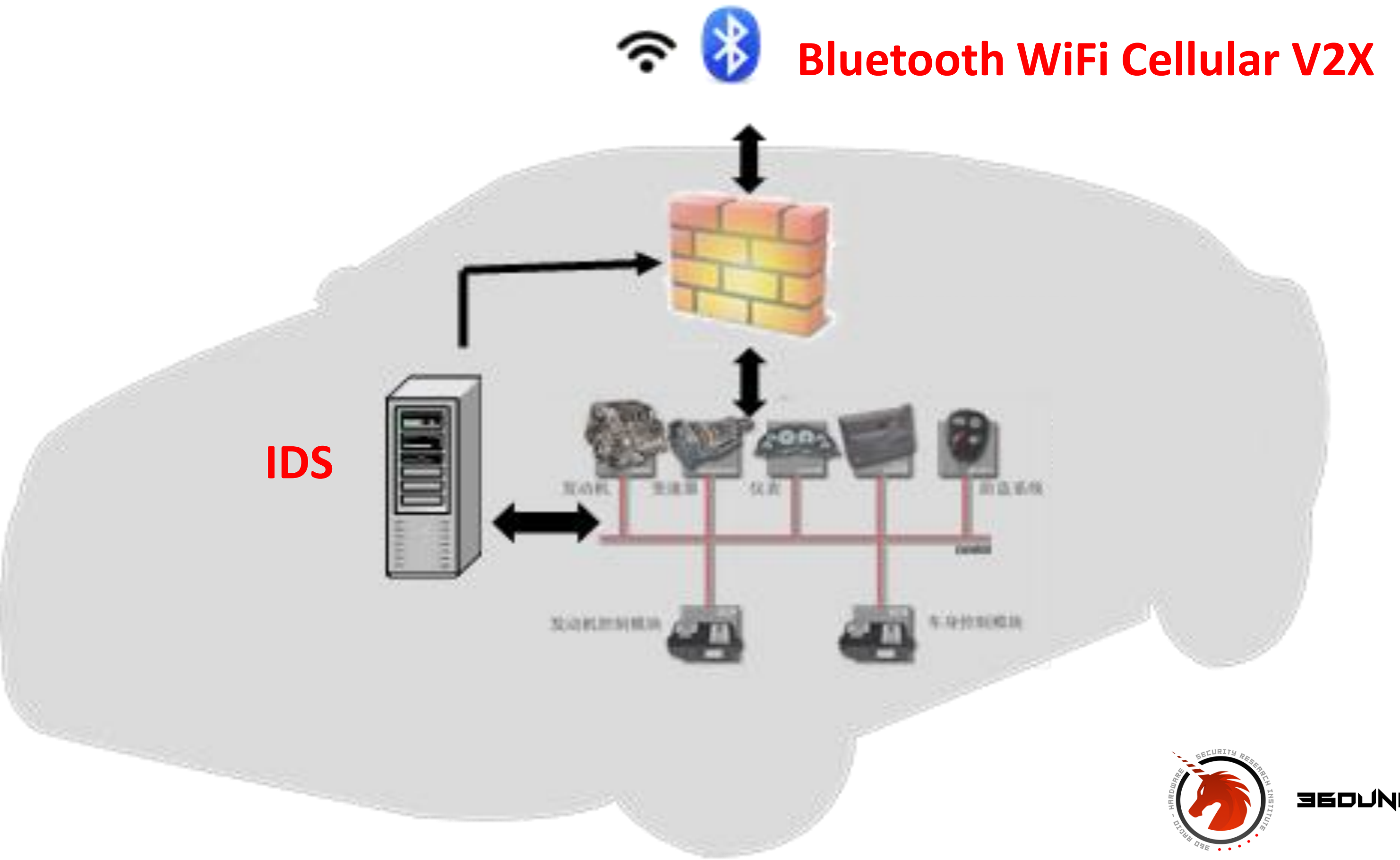

IDS（Intrusion Detection System）

# CAN bus defence




360UNICORNTEAM

# CAN security architecture

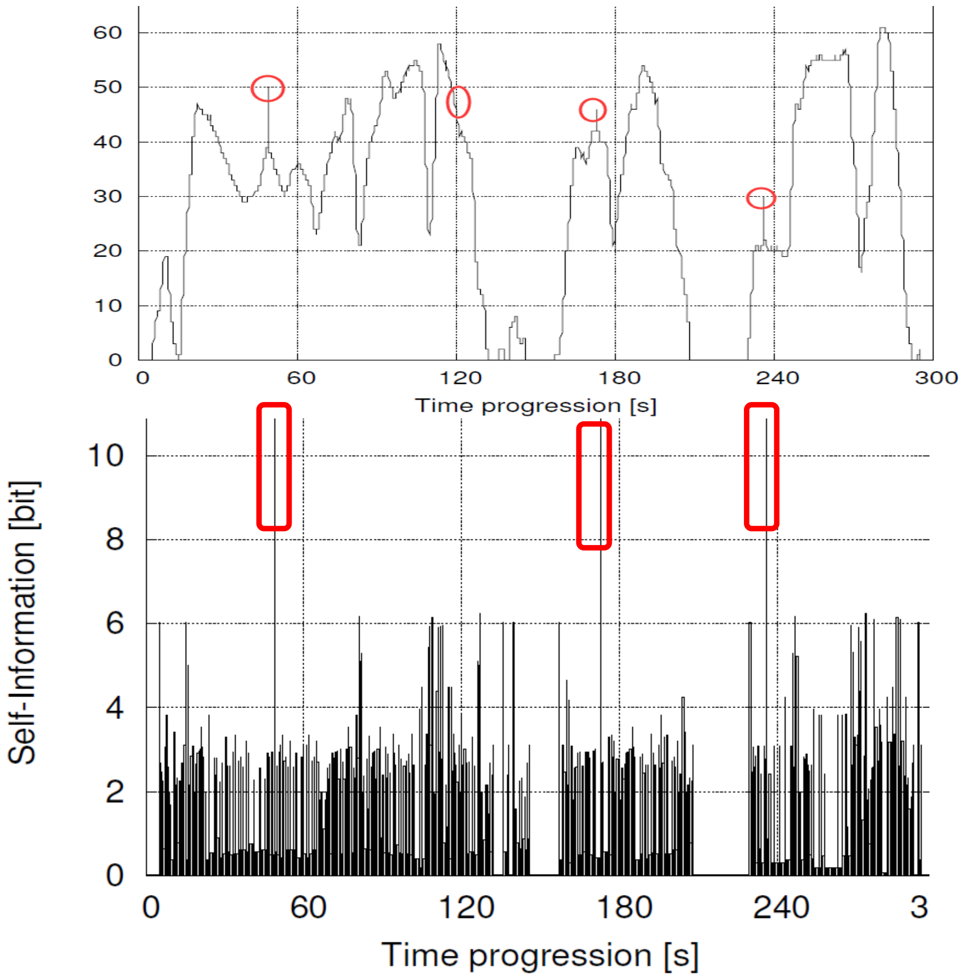


# Automotive intrusion detection researches

2011 IEEE Intelligent Vehicles Symposium (IV)
Baden-Baden, Germany, June 5-9, 2011

*Abstract*—**Due to an increased connectivity and seamless integration of information technology into modern vehicles, a trend of research in the automotive domain is the development of holistic IT security concepts. Within the scope of this development, vehicular attack detection is one concept which gains an increased attention, because of its reactive nature that allows to respond to threats during runtime. In this paper we explore the applicability of entropy-based attack detection for in-vehicle networks. We illustrate the crucial aspects for an adaptation of such an approach to the automotive domain. Moreover, we show first exemplary results by applying the approach to measurements derived from a standard vehicle's CAN-Body network.**

# Automotive intrusion detection researches



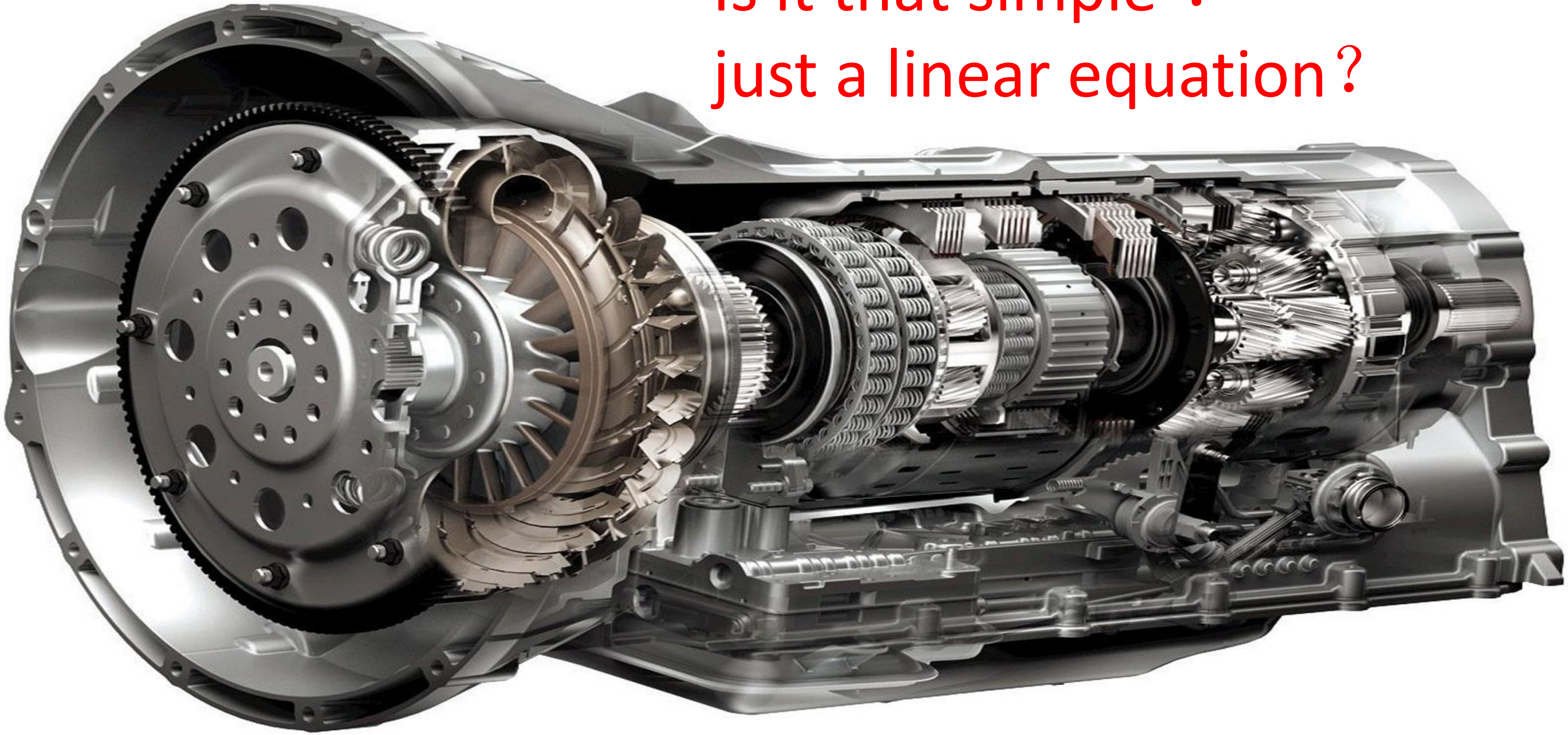

Not considering Temporal feature

360UNICORNTEAM

# My method（build a mathematical model）

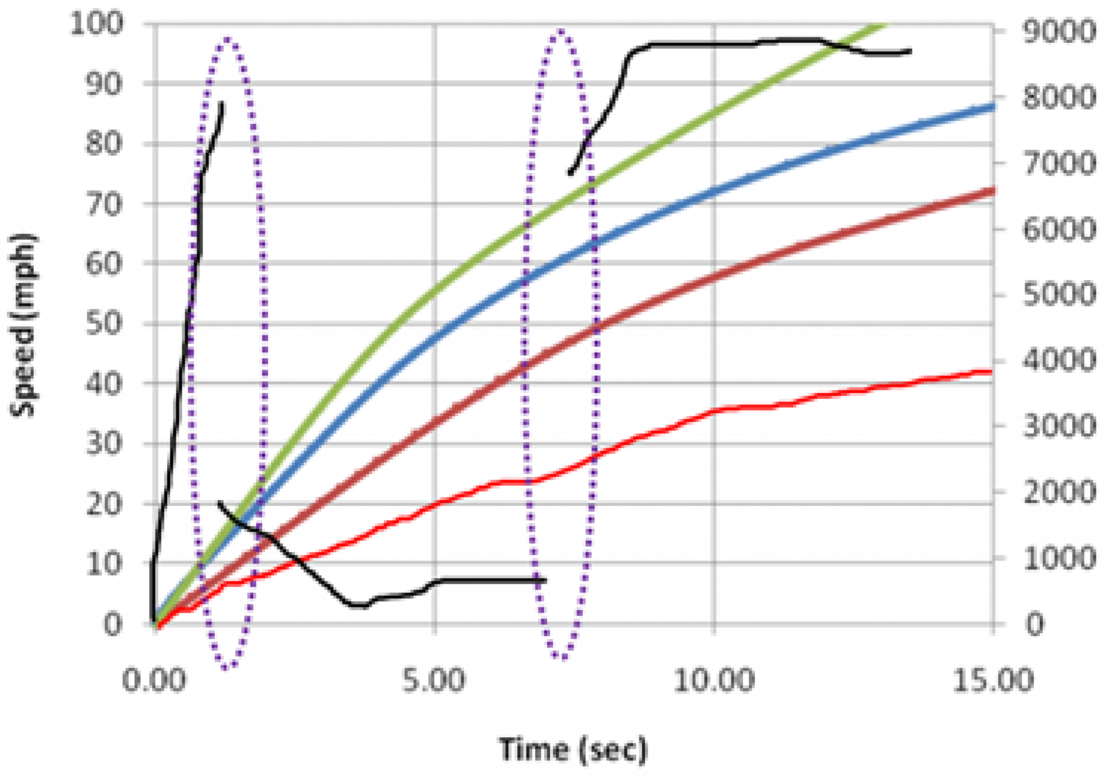
Is it that simple ？

just a linear equation？



You have clutches → Not linear

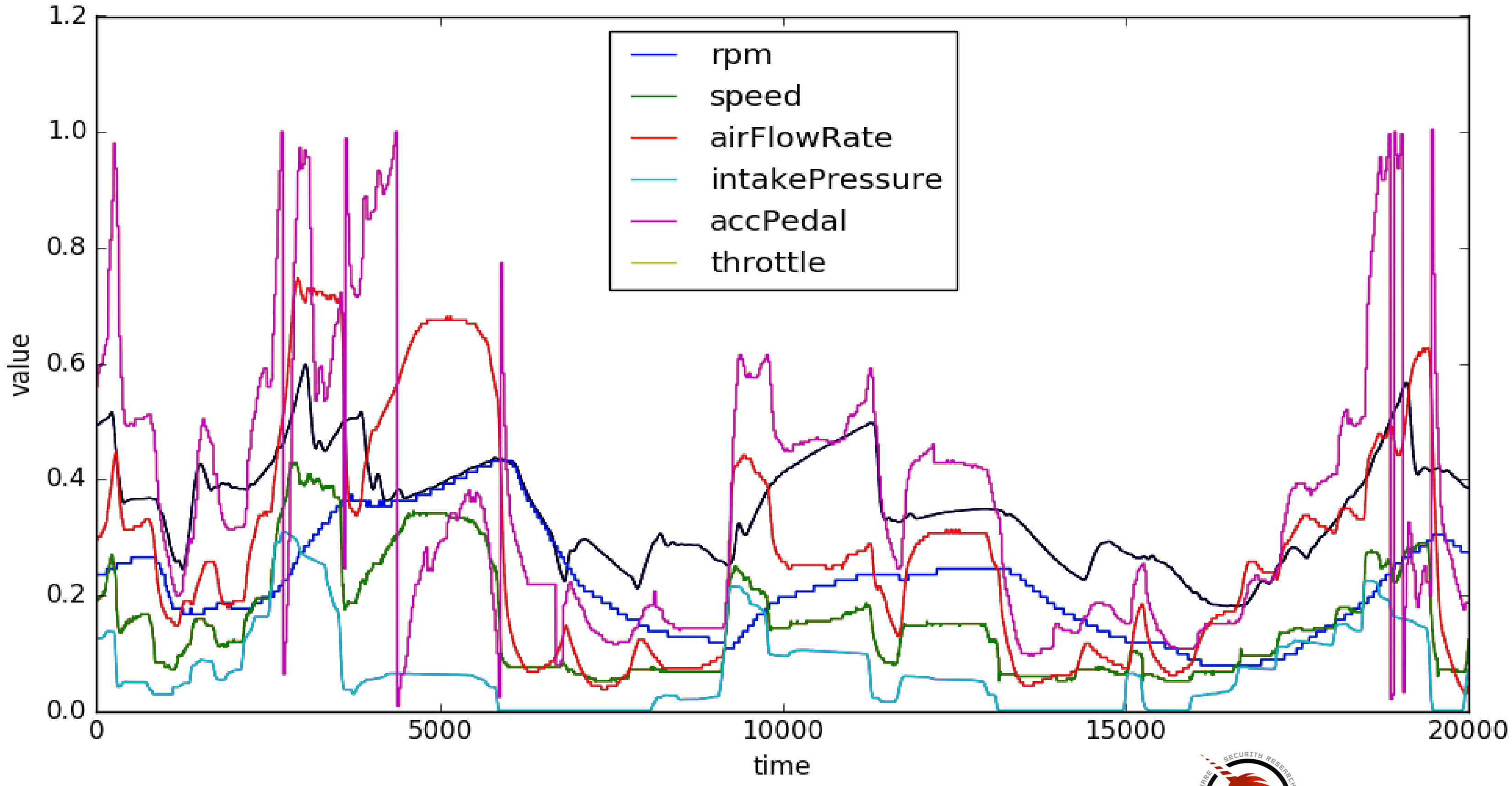
# System model requirements (We included temporal features)




Continuous Variable Acceleration/Deceleration Limit

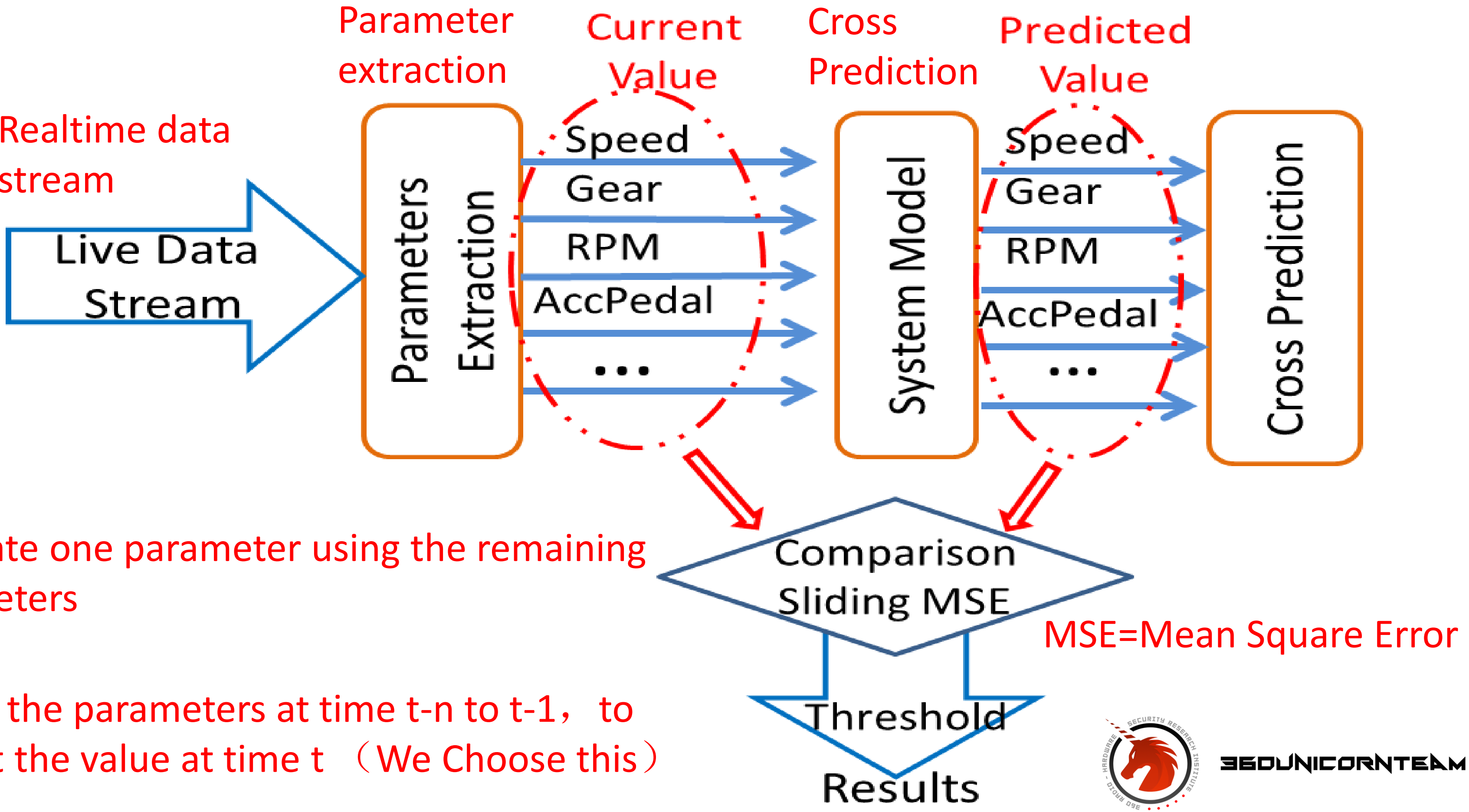
360UNICORNTEAM

# The parameters are related




360UNICORNTEAM

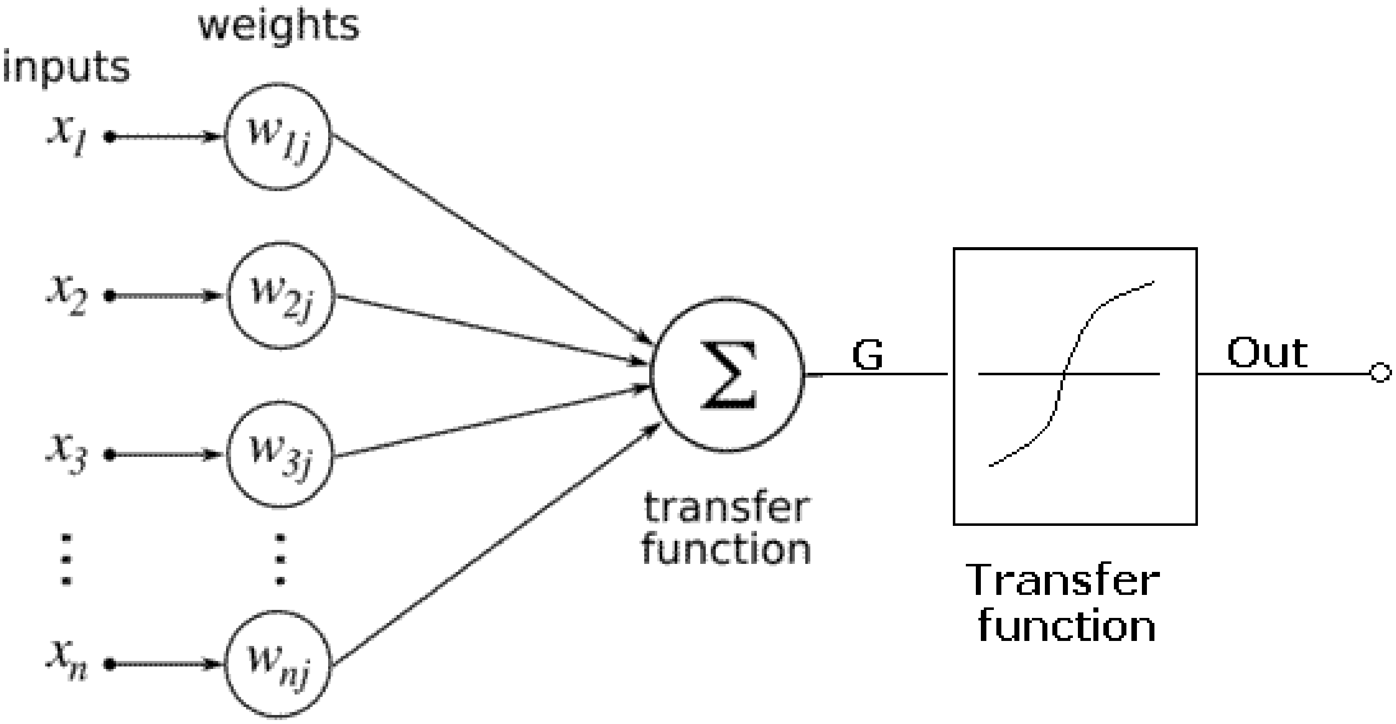
# Anomaly detection system




Calculate one parameter using the remaining parameters

Use all the parameters at time t-n to t-1， to predict the value at time t （We Choose this）

# Build a Model Using Deep Learing




http://playground.tensorflow.org/

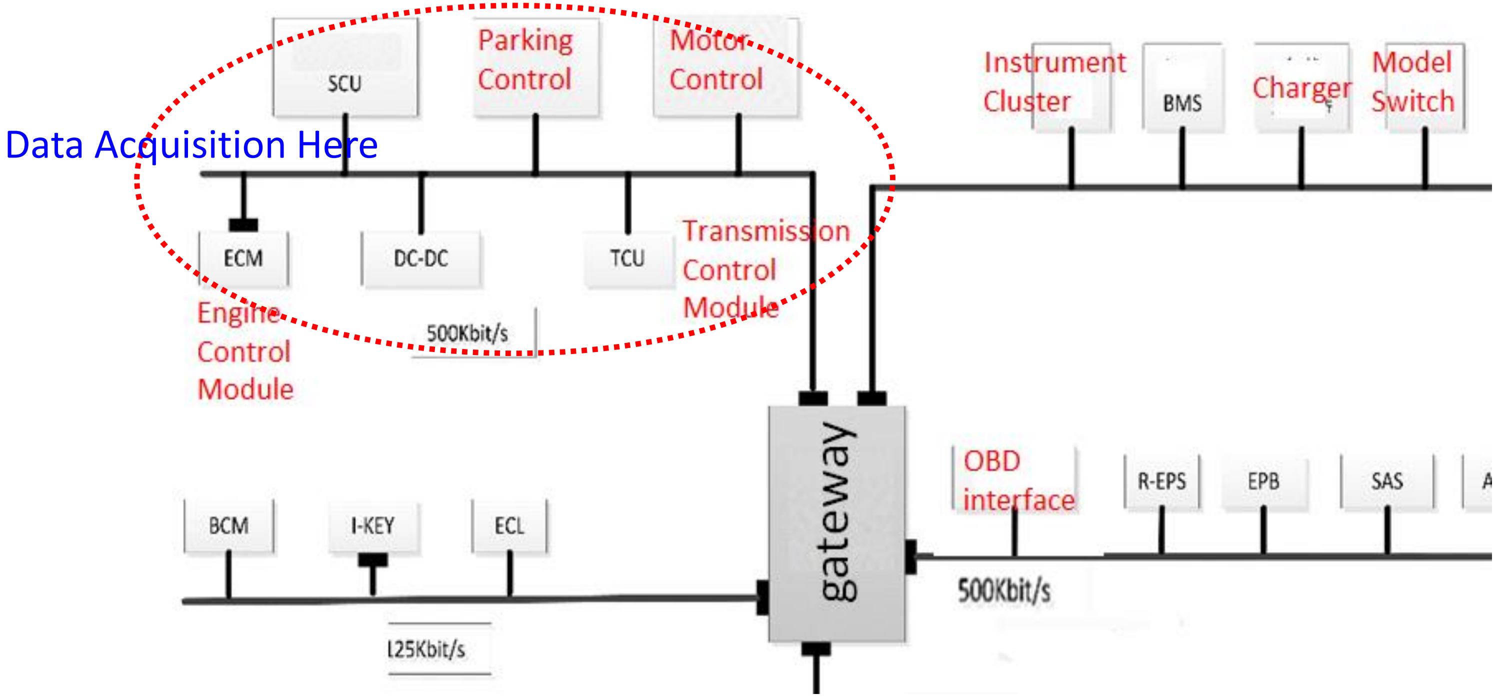
# Experiment Car

- Hybrid
- Electronic Brake
- Electric Power Steering
- Electronic Throttle
- Cellular Connection
- Cloud Service
- Bluetooth Key

360UNICORNTEAM

# Remotely control the car

# Experiment car’ s CAN network




360UNICORNTEAM

# The CAN database

## Message and Signal Information

### Message Details

Message Name: InstrumentStausLights

Message ID : 0x 133

Frame Format: Standard

Message Length(in: 8

Number of: 5

Data Format: Little Endian

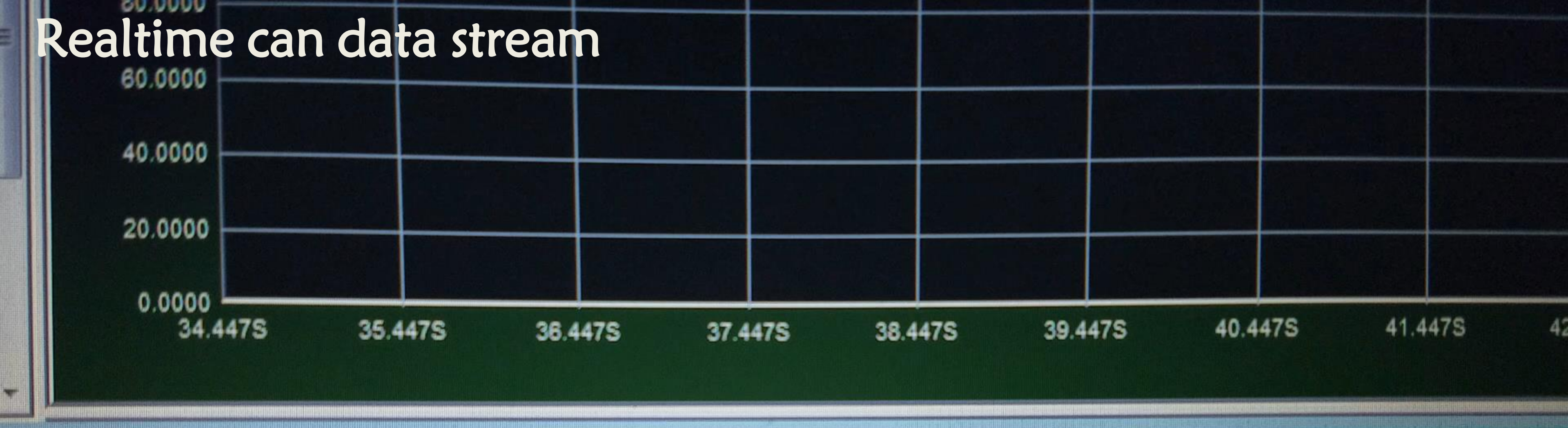
### Signal Details

| Name | Byte Index | Bit No | Length | Type | Max Val | Min Val | Offse |
|---|---|---|---|---|---|---|---|
| leftTurnSignal | 0 | 4 | 1 | bool | 1 | 0 | 0.00 |
| rightTurnSignal | 0 | 5 | 1 | bool | 1 | 0 | 0.00 |
| headLightStatus | 0 | 6 | 1 | bool | 1 | 0 | 0.00 |
| highBeam | 0 | 3 | 1 | bool | 1 | 0 | 0.00 |
| windowWiperSwitch | 1 | 0 | 8 | unsign... | FF | 0 | 0.00 |

- ModeSwitch
- InstrumentStausLights
- FrontHoodStatus
- Doorstatus

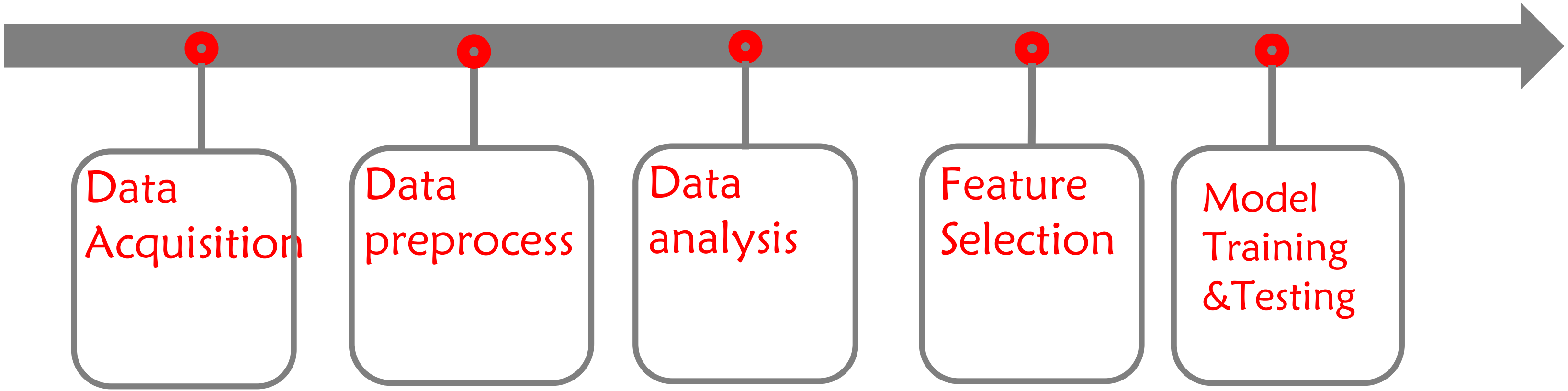
360UNICORNTEAM

# Realtime can data stream




| Msg | ID | Message | DLC | Data Byte(s) |
|---|---|---|---|---|
| s | 0x35C | 0x35C | 8 | 3E 01 00 00 FF FF FF C3 |
| s | 0x260 | 0x260 | 8 | 03 00 00 00 00 00 00 FC |
| s | 0x055 | 0x55 | 8 | 00 00 00 00 00 01 FF 04 |
| s | 0x394 | 0x394 | 8 | 80 73 5A 00 00 50 65 00 |
| s | 0x133 | InstrumentStausLights | 8 | 00 31 00 00 14 02 00 F0 |
| s | 0x1EB | FrontHoodStatus | 8 | AA 00 00 00 00 00 00 00 |
| s | 0x12D | Doorstatus | 8 | 01 50 00 10 04 [illegible] 02 FF |
| s | 0x180 | 0x180 | 8 | 00 00 04 00 00 [illegible] |

# Build the system model



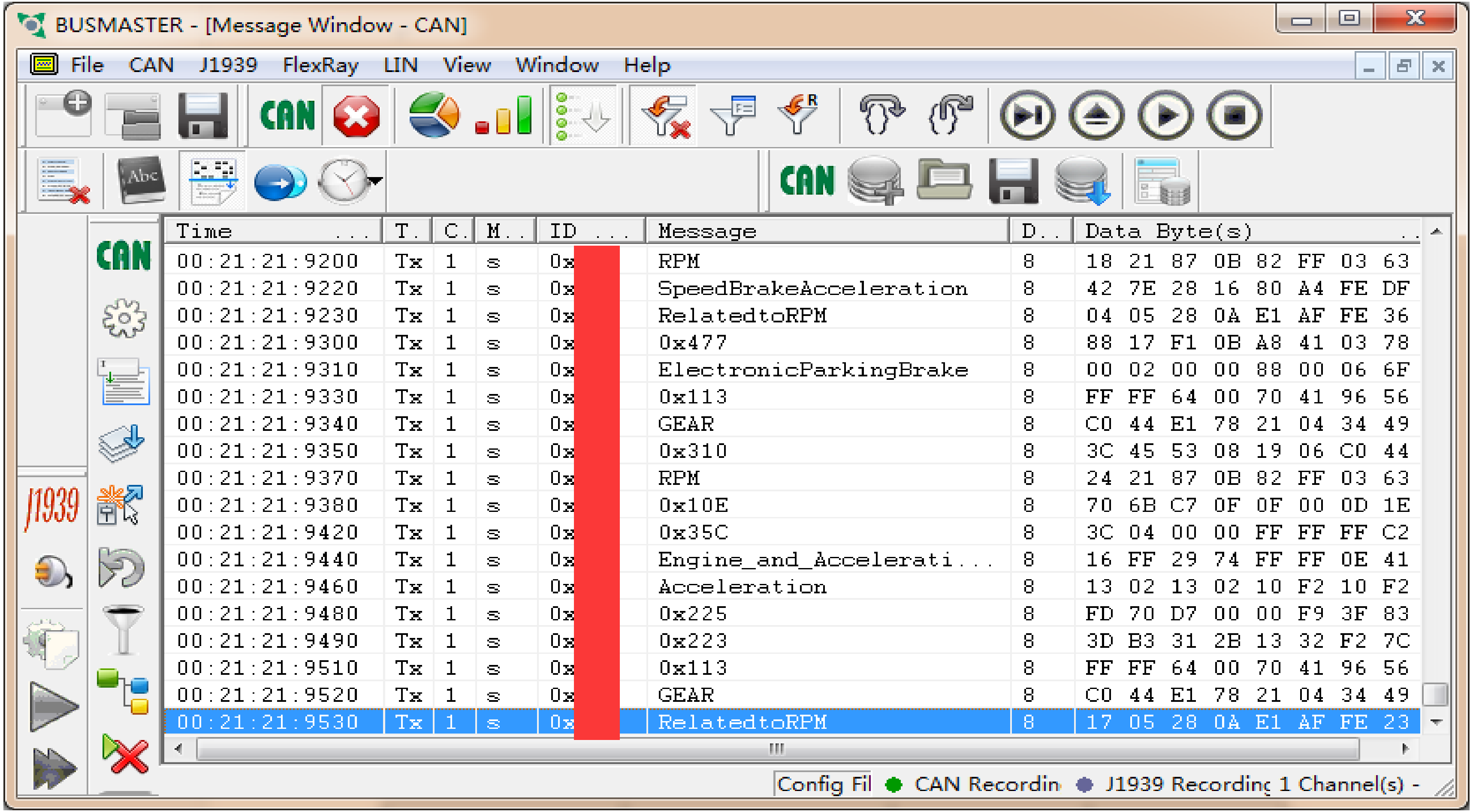

360UNICORNTEAM

# Data Acquisition Setup


360UNICORNTEAM

# Data Analysis

CAN database is kept highly confidential

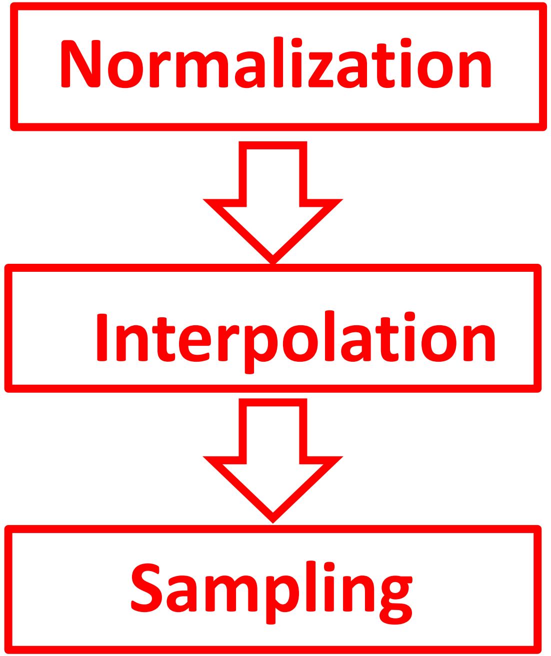



| Time | T. | C. | M.. | ID ... | Message | D.. | Data Byte(s) |
|---|---|---|---|---|---|---|---|
| 00:21:21:9200 | Tx | 1 | s | 0x[redacted] | RPM | 8 | 18 21 87 0B 82 FF 03 63 |
| 00:21:21:9220 | Tx | 1 | s | 0x[redacted] | SpeedBrakeAcceleration | 8 | 42 7E 28 16 80 A4 FE DF |
| 00:21:21:9230 | Tx | 1 | s | 0x[redacted] | RelatedtoRPM | 8 | 04 05 28 0A E1 AF FE 36 |
| 00:21:21:9300 | Tx | 1 | s | 0x[redacted] | 0x477 | 8 | 88 17 F1 0B A8 41 03 78 |
| 00:21:21:9310 | Tx | 1 | s | 0x[redacted] | ElectronicParkingBrake | 8 | 00 02 00 00 88 00 06 6F |
| 00:21:21:9330 | Tx | 1 | s | 0x[redacted] | 0x113 | 8 | FF FF 64 00 70 41 96 56 |
| 00:21:21:9340 | Tx | 1 | s | 0x[redacted] | GEAR | 8 | C0 44 E1 78 21 04 34 49 |
| 00:21:21:9350 | Tx | 1 | s | 0x[redacted] | 0x310 | 8 | 3C 45 53 08 19 06 C0 44 |
| 00:21:21:9370 | Tx | 1 | s | 0x[redacted] | RPM | 8 | 24 21 87 0B 82 FF 03 63 |
| 00:21:21:9380 | Tx | 1 | s | 0x[redacted] | 0x10E | 8 | 70 6B C7 0F 0F 00 0D 1E |
| 00:21:21:9420 | Tx | 1 | s | 0x[redacted] | 0x35C | 8 | 3C 04 00 00 FF FF FF C2 |
| 00:21:21:9440 | Tx | 1 | s | 0x[redacted] | Engine_and_Accelerati... | 8 | 16 FF 29 74 FF FF 0E 41 |
| 00:21:21:9460 | Tx | 1 | s | 0x[redacted] | Acceleration | 8 | 13 02 13 02 10 F2 10 F2 |
| 00:21:21:9480 | Tx | 1 | s | 0x[redacted] | 0x225 | 8 | FD 70 D7 00 00 F9 3F 83 |
| 00:21:21:9490 | Tx | 1 | s | 0x[redacted] | 0x223 | 8 | 3D B3 31 2B 13 32 F2 7C |
| 00:21:21:9510 | Tx | 1 | s | 0x[redacted] | 0x113 | 8 | FF FF 64 00 70 41 96 56 |
| 00:21:21:9520 | Tx | 1 | s | 0x[redacted] | GEAR | 8 | C0 44 E1 78 21 04 34 49 |
| 00:21:21:9530 | Tx | 1 | s | 0x[redacted] | RelatedtoRPM | 8 | 17 05 28 0A E1 AF FE 23 |

# Data Preprocessing

```
***BUSMASTER Ver 2.6.4***
***PROTOCOL CAN***
***NOTE: PLEASE DO NOT EDIT THIS DOCUMENT***
***[START LOGGING SESSION]***
***START DATE AND TIME 3:3:2016 22:42:21:222***
***HEX***
***SYSTEM MODE***
***START CHANNEL BAUD RATE***
***CHANNEL 1 - Kvaser - Kvaser Leaf Light v2 #0 (Channel 0), Serial Number- 0,
***END CHANNEL BAUD RATE***
***START DATABASE FILES (DBF/DBC)******START DATABASE FILES (DBF/DBC)***
***C:\Users\Administrator\Desktop\学校相关\BYD实验数据\BYD CAN DATABASE.DBF***
***END OF DATABASE FILES (DBF/DBC)******END OF DATABASE FILES (DBF/DBC)***
***<Time><Tx/Rx><Channel><CAN ID><Type><DLC><DataBytes>***
22:42:21:2045 Rx 1 0x243 s 8 00 00 28 0A D1 AF FE 4F
22:42:21:2065 Rx 1 0x20F s 8 12 3F 64 E0 77 33 00 00
22:42:21:2075 Rx 1 0x10D s 8 0C 0C 4B 00 A0 FF 03 67
22:42:21:2075 Rx 1 0x10E s 8 0A 00 C7 0F 0F 00 0D 1E
22:42:21:2075 Rx 1 0x218 s 8 00 02 00 00 08 00 0C E9
22:42:21:2085 Rx 1 0x26C s 8 00 40 04 06 FC FF FF BB
22:42:21:2095 Rx 1 0x342 s 8 00 FF 29 74 FF FF 0E 57
22:42:21:2115 Rx 1 0x344 s 8 20 00 0F 20 4E 00 1E 44
22:42:21:2125 Rx 1 0x113 s 8 FF FF 5E 00 F8 00 3F 6C
22:42:21:2135 Rx 1 0x212 s 8 C0 14 F1 0C 00 00 14 2A
```

# Data Preprocessing



# Normalization

$$X^* = \frac{x - \min}{\max - \min}$$

Must make sure the maximum and minimum values are not calculated from the training data

# Interpolation

p

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| speed | 0.2 | 0.2 | *0.1* | 0.1 | 0.1 | 0.1 | 0.1 |
| rpm | 0.3 | *0.5* | 0.5 | 0.5 | 0.5 | 0.5 | *0.8* |
| accpedal | *0.7* | 0.7 | 0.7 | 0.7 | 0.7 | *0.9* | 0.9 |
| ... | 0.1 | 0.1 | 0.1 | 0.1 | *0.3* | 0.3 | 0.3 |
| | 0.4 | 0.4 | 0.4 | *0.5* | 0.5 | 0.5 | 0.5 |

t

● Observation

● Interpolation

# Sub-Sampling

| Time_ms | RPM | Speed | MAP | MAF | AccPedal | Throttle |
|---|---|---|---|---|---|---|
| 138973 | 0.2879838 | 0.1342592 | 0.0590551 | 0.1675675 | 0.6971070 | 0.1377952 |
| 138974 | 0.2873125 | 0.1342592 | 0.0551181 | 0.1675675 | 0.6971070 | 0.1377952 |
| 138975 | 0.2873125 | 0.1342592 | 0.0511811 | 0.1675675 | 0.6971070 | 0.1377952 |
| 138976 | 0.285970 | 0.1342592 | 0.0472440 | 0.1675675 | 0.6971070 | 0.1377952 |
| 138977 | 0.285970 | 0.134259 | 0.0511811 | 0.1675675 | 0.6971070 | 0.1377952 |

360UNICORNTEAM

# The Training Data

Input Vector
10x7=70

Output Vector
1x7=7

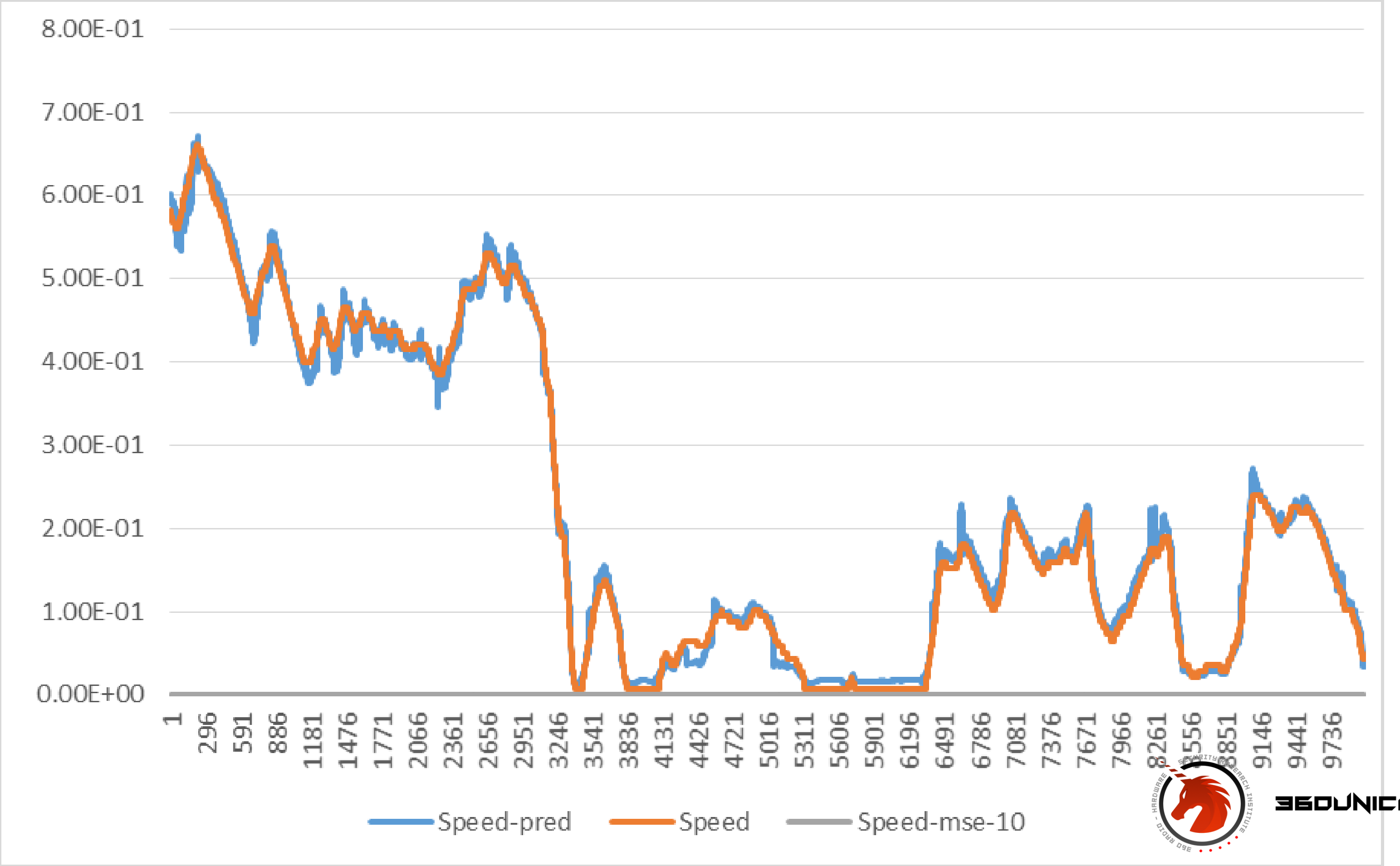
| | 1 | … | 7 |
|---|---|---|---|
| | RPM | … | Gear |
| 1 | 1.52E-01 | … | 0.00E+00 |
| … | … | … | … |
| 10 | 1.52E-01 | … | 0.00E+00 |
| 11 | 1.52E-01 | … | 0.00E+00 |

360UNICORNTEAM

# Model training

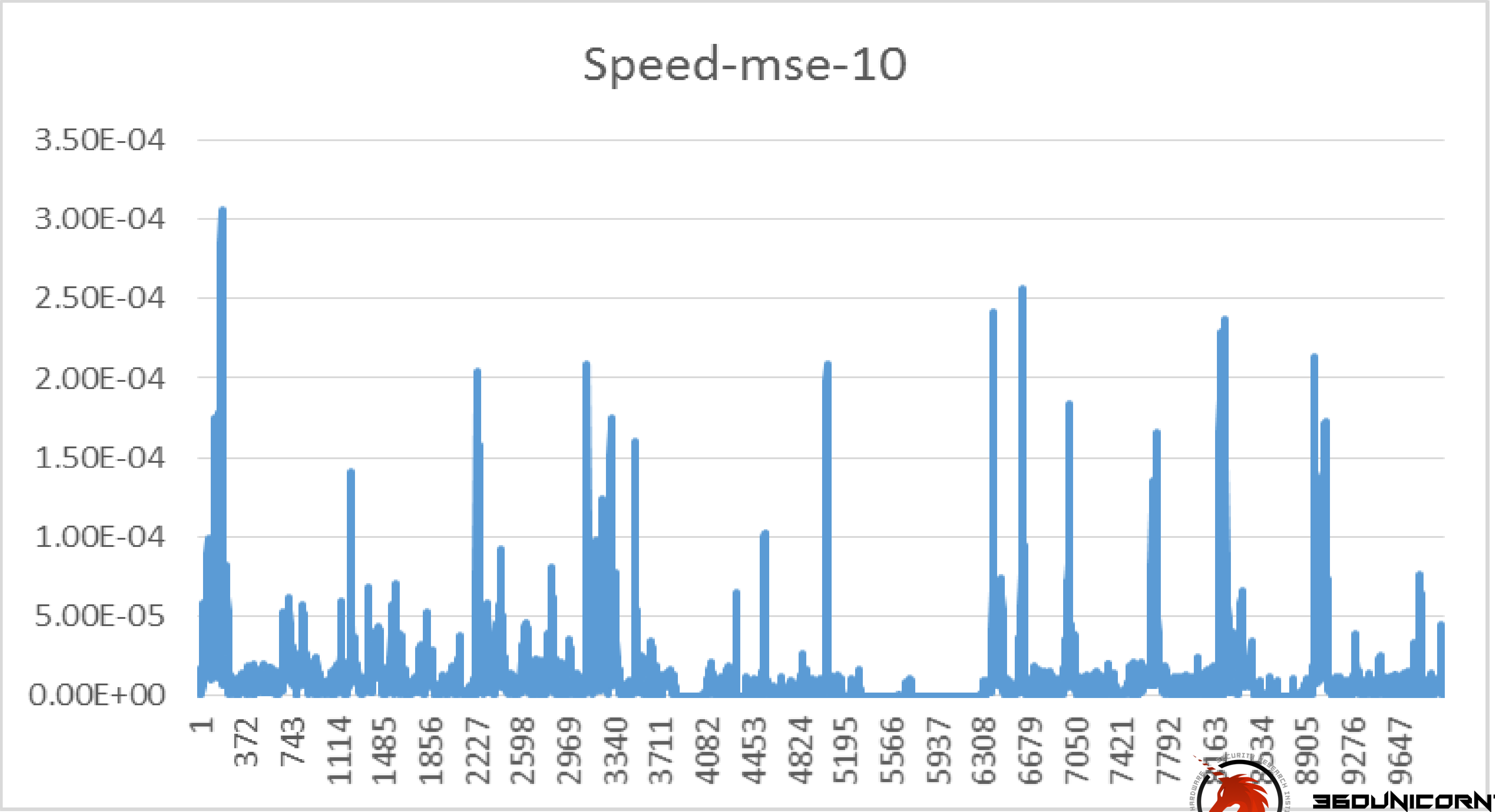
I will publish the code， the CAN traffic data later

# Results



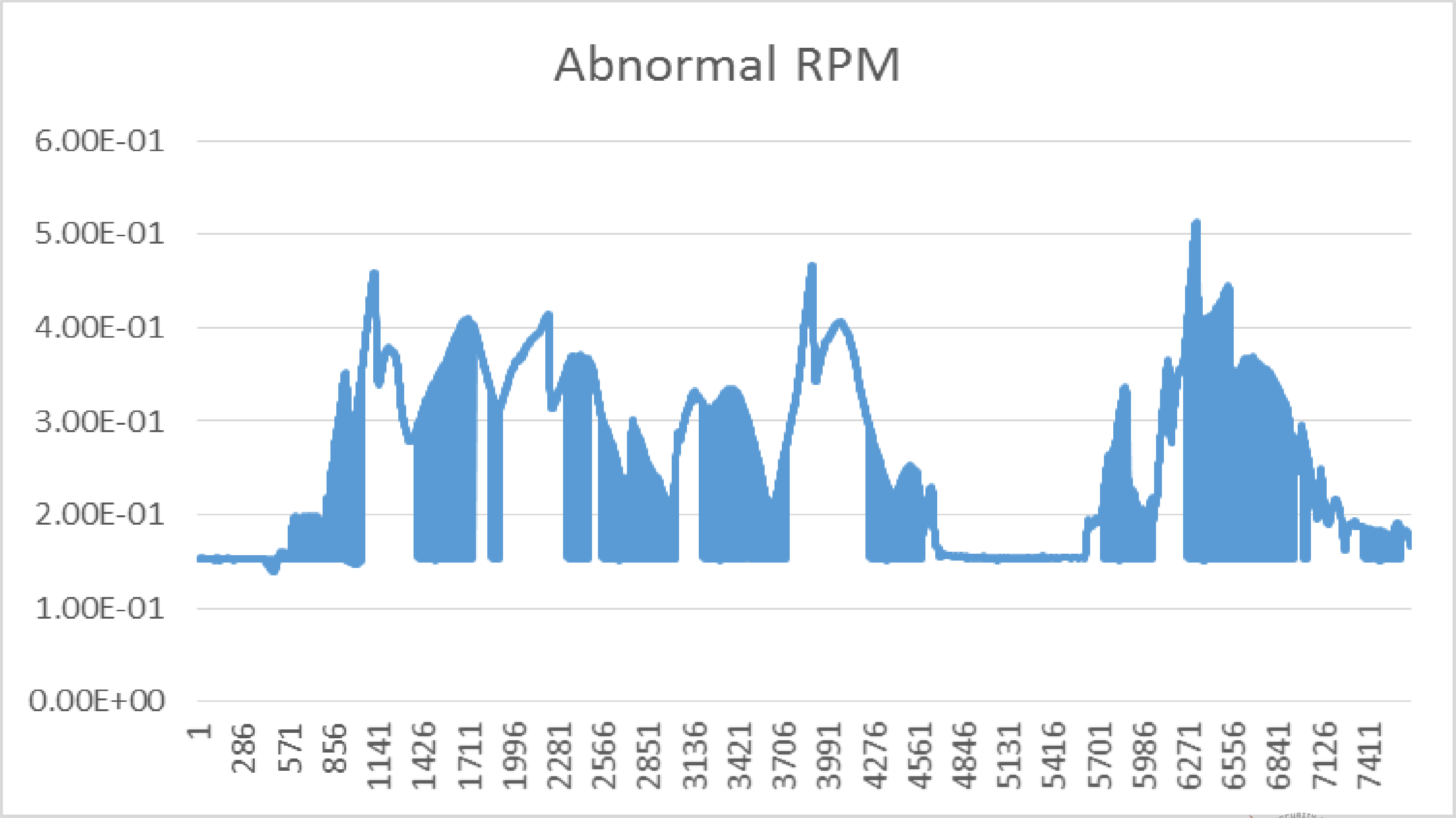

360UNICORNTEAM

# Result



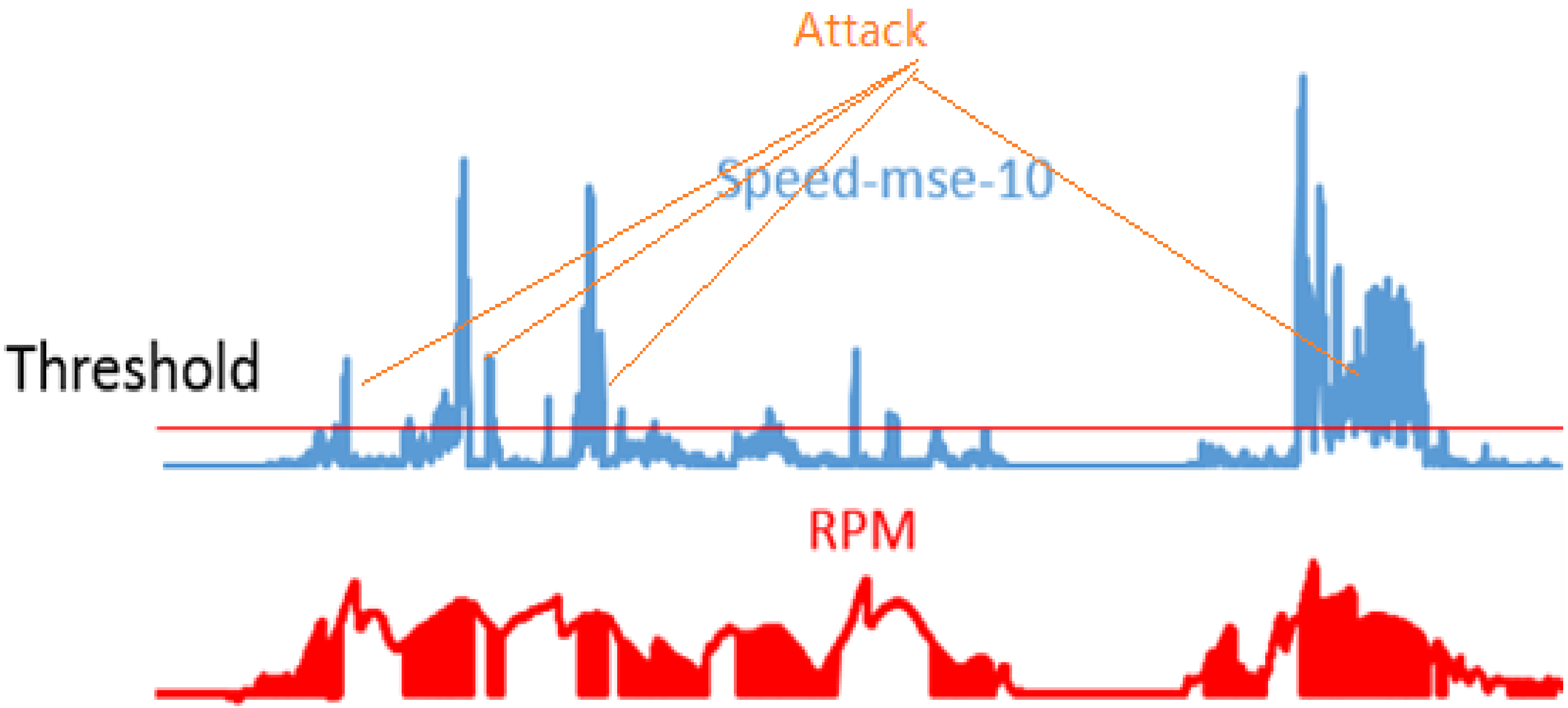

360UNICORNTEAM

# Model testing




360UNICORNTEAM

# Model testing




360UNICORNTEAM

# CAN Anomaly Detection

McAfee&Intel

**Software and Services**

| | | |
|---|---|---|
| Anti-malware | Network enforcement | Biometrics |
| Cryptographic services | Anomaly detection | Over-the-air updates |

Owners of computers are painfully familiar with security patches and software update processes. Interrupting a drive for a weekly security scan or urgent update is not realistic. Forcing a patch at the wrong time may be dangerous to the vehicle occupants. Processes will need to be developed to determine when and how to inform the owner that an update is required, how and when to enforce the update, and how do deal with unpatched systems. Memory monitoring and anomaly warning solutions are possible that model the normal operation of the vehicle and create a unique fingerprint. Significant deviation from the model can trigger alerts and even a safe mode with sufficient but diminished functions to enable the car to get home.

**Hardware Security Building Blocks**

| | | |
|---|---|---|
| Platform boot integrity and chain of trust | Secure storage (keys and data) | Secure communication |
| Secure debug | Tamper detection and protection from side channel attacks | |

**Figure 3.** Defense-in-depth building blocks.

360UNICORNTEAM

# Acknowledgements

Professor Shuicheng Yan @360 Institute of Artificial Intelligence
Doctor Ming Lin @360 Institute of Artificial Intelligence
Doctor Zhanyi Wang @360 Skyeye lab
Doctor Lin Huang @ 360 UnicornTeam

360UNICORNTEAM

# References

1. Karl Koscher, Alexei Czeskis, Experimental Security Analysis of a Modern Automobile, 2010
2. Stephen Checkoway,Damon McCoy，Brian Kantor, Comprehensive Experimental Analyses of Automotive Attack Surfaces，2011.
3. Charlie Miller，Chris Valasek，Adventures in Automotive Networks and Control Units，2013.
4. Charlie Miller，Chris Valasek，Remote Exploitation of an Unaltered Passenger Vehicle，2015
5. Dieter Spaar，Sicherheitslücken bei BMWs ConnectedDrive/ Beemer, Open Thyself! – Security vulnerabilities in BMW's ConnectedDrive,2015.
6. Iamthecarvalry.org , Five Star Automotive Cyber Safety Framework，2015.
7. Pierre Kleberger，Security Aspects of the In-Vehicle Network in the Connected Car，IEEE Intelligent Vehicles Symposium，2011
8. Jeff Moser，The First Few Milliseconds of an HTTPS Connection，2009.
9. 安天实验室，乌克兰电力系统遭受攻击事件综述分析报告，2016
10. Stamatis Karnouskos, Stuxnet Worm Impact on Industrial Cyber-Physical System Security,2011
11. Marc Rogers，Kevin Mahaffey，How to Hack a Tesla Model S，DEF CON 23,2015

1. Nobuyasu Kanekawa,X-by-Wire Systems,Hitachi Research Lab.2011
2. Paul Yih, Steer-by-Wire: Implication For Vehicle Handling and Safety，Stanford PHD Dissertation，2005
3. Luigi Coppolion，Dependability aspects of automotive x-by-wire technologies，2008.
4. NPR,Sniffs out vulnerability in Bluetooth devices，2005
5. Jonas Zaddach,Andrei Costin,Embedded Devices Security and Firmware Reverse Engineering，Blackhat Workshop,2013.
6. Andrei costin，Jonas Zaddach，A large-Scale Analysis of the Security of Embedded Firmwares，EURECOM，2014.
7. Samy Kamkar，Drive It Like You hacked It，DEF CON23，2015
8. David A Brown, Geoffrey Cooper, Automotive Security Best Practices, White Paper by Intel & McAfee,2014.
9. OpenGarages, Car Hacker’s Handbook，openGarage.org,2014.
10. Henning Olsson, OptimumG，Vehicle Data Acquisition Using CAN,2010
11. Varun Chandola，Arindam Banerjee，Vipin Kumar，Anomaly Detection ：A Survey，2009

1. Park, Ming Kuang, Neural learning of driving environment prediction for vehicle power management, Joint Conf. on Neural Networks, 2008.
2. Taylor, P., Adamu-Fika, F., Anand, S., Dunoyer, A., Griffiths, N., and Popham, T. Road type classification through data mining，2012.
3. Michael Muter, Naim Asaj，Entropy-based anomaly detection for in-vehicle networks", IEEE Intelligent Vehicles Symposium (IV), 2011.
4. Ulf E. Larson, Dennis K. Nilsson,An Approach to Specification-based Attack Detection for In-Vehicle Networks, IEEE Intelligent Vehicles Symposium,2008.
5. Y. L. Murphey, Zhi Hang Chen, L. Kiliaris, Jungme ,I. Tang and T. P. Breckon, Automatic road environment classication, IEEE Trans. on Intelligent Transportation Systems, 2011.
6. Salima Omar, Asri Ngadi, Hamid H.Jebur, Machine Learning Techniques for Anomaly Detection: An Overview.
7. Jiawei Han, Micheline Kamber, Data mining: concepts and techniques, 2011.
8. Perter Harrington，Machine Learning In Action，2013.
9. Jurgen Schmidhuber， Deep learning in neural networks: An overview， 2015.
10. Kaiserslautern，Comparison of Unsupervised Anomaly Detection Techniques，German Research Center for Artificial Intelligence, 2011

1. Sepp Hochreiter, Jurgen Schmidhuber, Long short-term memory,Neural computation, 1997.
2. Michael Husken, Peter Stagge,Recurrent neural networks for time series classifcation, Neurocomputing, 2003.
3. Felix A Gers, Jurgen Schmidhuber, Fred Cummins, Learning to forget:Continual prediction with LSTM, Neural computation, 2000.
4. David E Rumelhart, Geo_rey E Hinton, and Ronald J Williams.，Learning internal representations by error propagation，1985.
5. Christopher M Bishop,Pattern recognition and machine learning, springer, 2006.
6. Simon Haykin and Neural Network. A comprehensive foundation. Neural Networks, 2004.
7. Eleazar Eskin,Andrew Arnold,Michael Prerau, A Geometric Framework for Unsupervised Anomaly Detection-Detecting Intrusions in Unlabeled Data tection-Detecting Intrusions in Unlabeled Data,2002.
8. Kingsly Leung, Christopher Leckie, Unsupervised Anomaly Detection in Network Intrusion Detection Using Clusters, 2005
9. Ronan Collobert, Clement Farabet, Koray Kavukcuoglu, and Soumith Chintala Torch，Scientic computing for lua，2015.

# Thank You !

# Q&A

360UNICORNTEAM