black hat EUROPE 2018

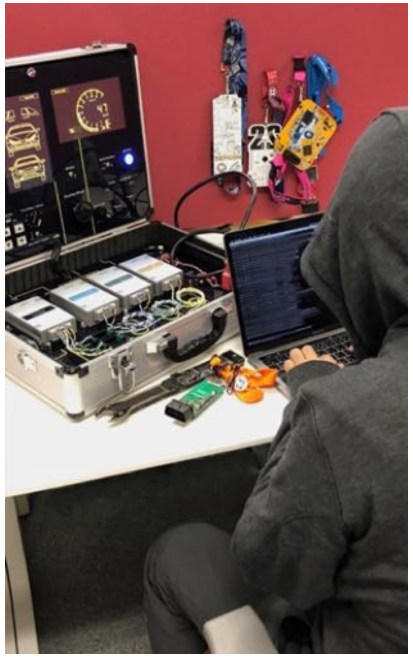
DECEMBER 3-6, 2018

EXCEL LONDON / UNITED KINGDOM

PASTA: Portable Automotive Security Testbed with Adaptability

Tsuyoshi Toyama, Takuya Yoshida, Hisashi Oguma, Tsutomu Matsumoto

Who are we?



Tsuyoshi Toyama — TOYOTA INFOTECH

Takuya Yoshida — TOYOTA INFOTECH

Hisashi Oguma — TOYOTA INFOTECH

Tsutomu Matsumoto — YNU YOKOHAMA National University

Agenda

□ Background of vehicular security

□ What is PASTA ?

□ Demo

□ Use cases

□ Roadmap

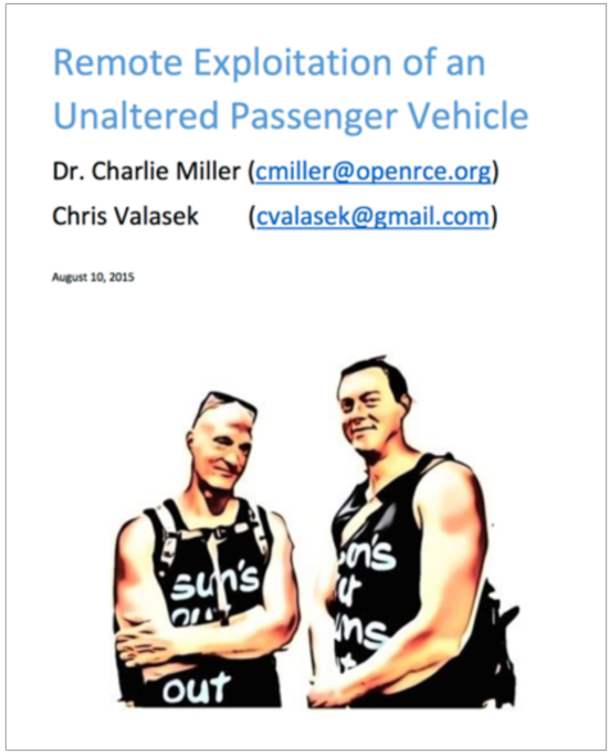
□ Take away

Background

- Lots of ECUs are in a vehicle to realize comfortable driving.
- ECUs interact with other ECUs, sensors, and actuators using CAN protocol, etc.
- CAN Protocol was developed with no concern about cyber security attacks.

Vehicle hacking is real threat

- □July 2015, two hackers presented that Jeep Chrysler can be remotely controlled.
  - □Controlling wipers, audio system, steering wheels, etc. of a running car.
  - □As a result, Chrysler recalled 1.4 million vehicles.

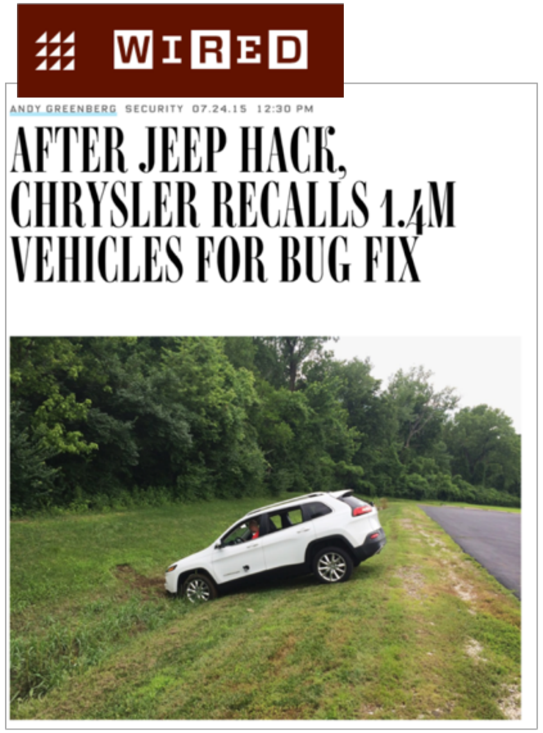


Remote Exploitation of an Unaltered Passenger Vehicle

Dr. Charlie Miller (cmiller@openrce.org)

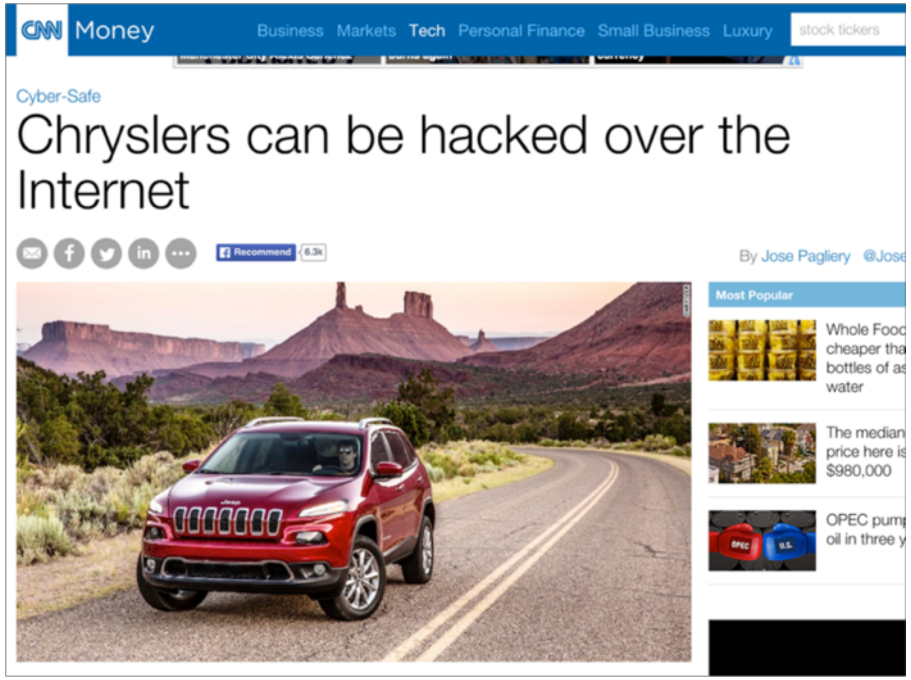
Chris Valasek (cvalasek@gmail.com)

August 10, 2015



ANDY GREENBERG SECURITY 07.24.15 12:30 PM

AFTER JEEP HACK, CHRYSLER RECALLS 1.4M VEHICLES FOR BUG FIX



Cyber-Safe

Chryslers can be hacked over the Internet

By Jose Pagliery @Jose

Whole Food cheaper tha bottles of a water

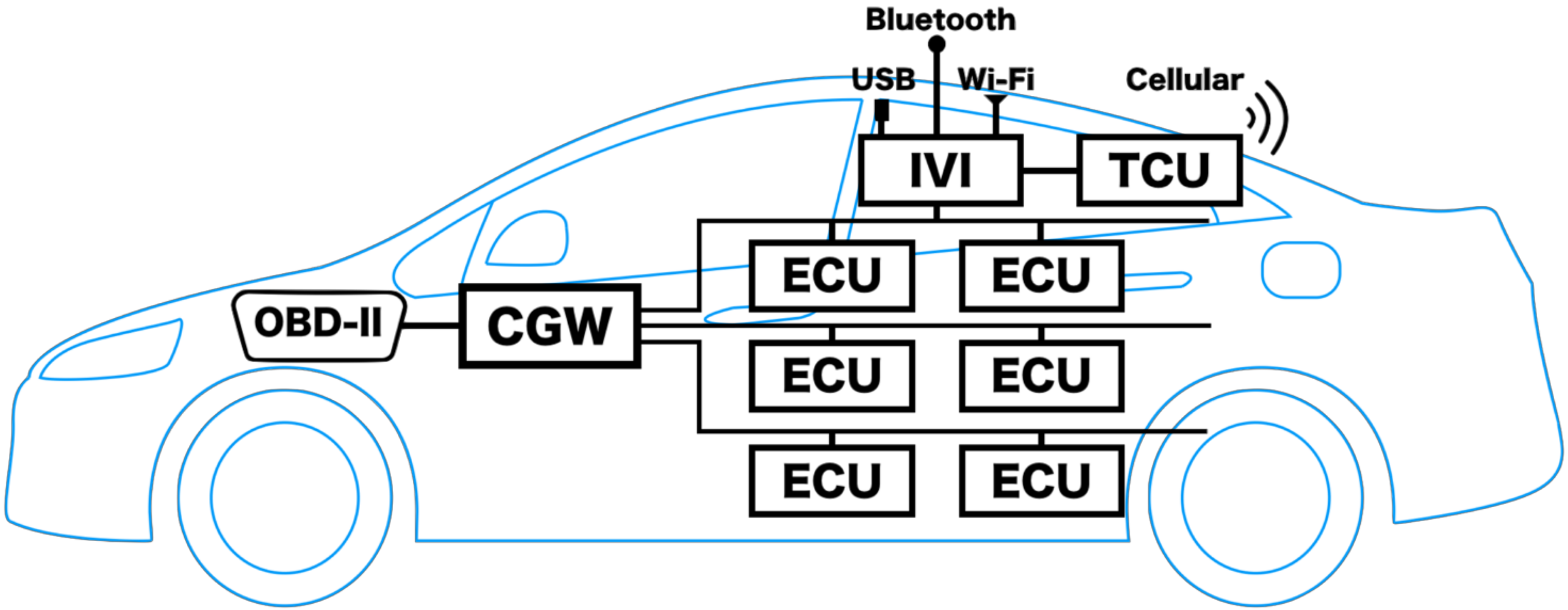
The median price here is $980,000

OPEC pum oil in three y

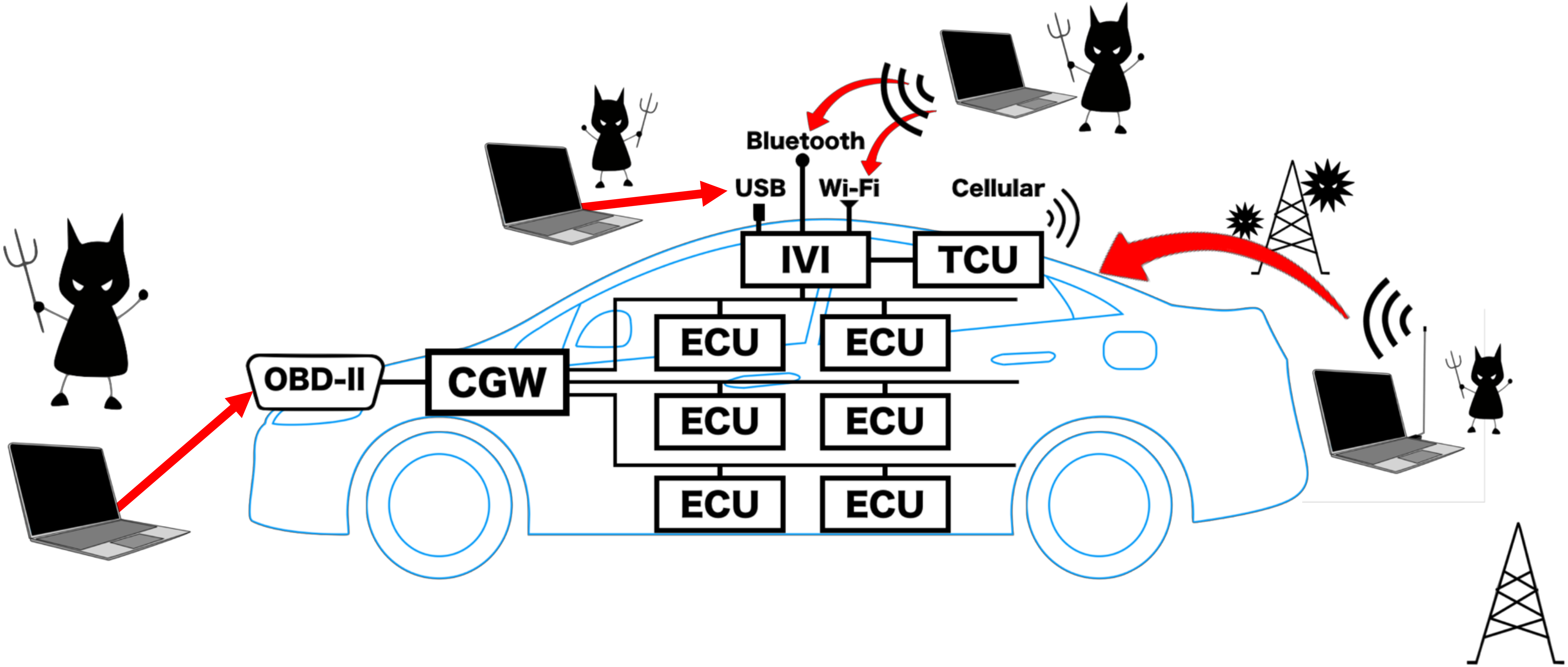
Problems in automotive industry

- □ Problems of cyber security technology for automobiles;
  - □ Delay in development of cyber security technology in automotive industry.
  - □ Lack of cyber security engineers in the automotive industry.

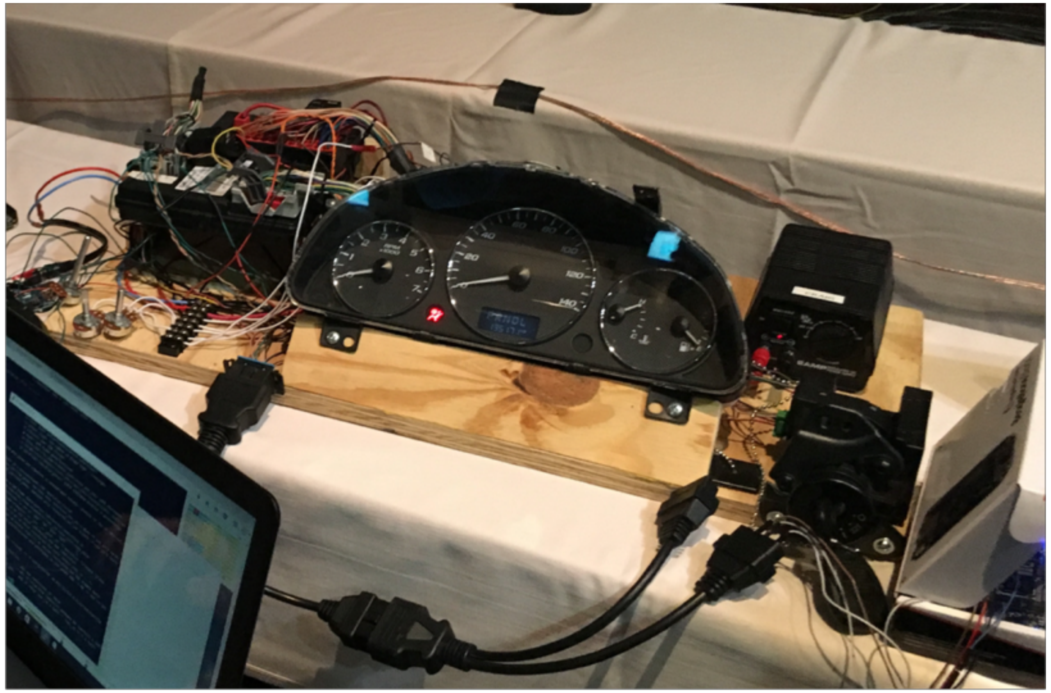
Typical architecture of a vehicle



Typical attack surfaces in recent vehicles



CAR HACKING VILLAGE in DefCon



Hacking event such as CTF is very fun! However, it is doubtful that it can be systematic way of learning vehicular security.

Motivation for developing platform

- □ There are no harmless real car for testers and no “generalized” one.
- □ We need to develop a platform not only for “Crack” but also “Hack”
  - □ Anyone can hack and study by “playground vehicle”
  - □ A newly proposed security technology can be evaluated its feasibility in common platform.

↓

Open, safe, and attractive platform for vehicular cyber security is required

Philosophy of PASTA

Philosophy of PASTA

Open

Safe

Adaptable

Portable

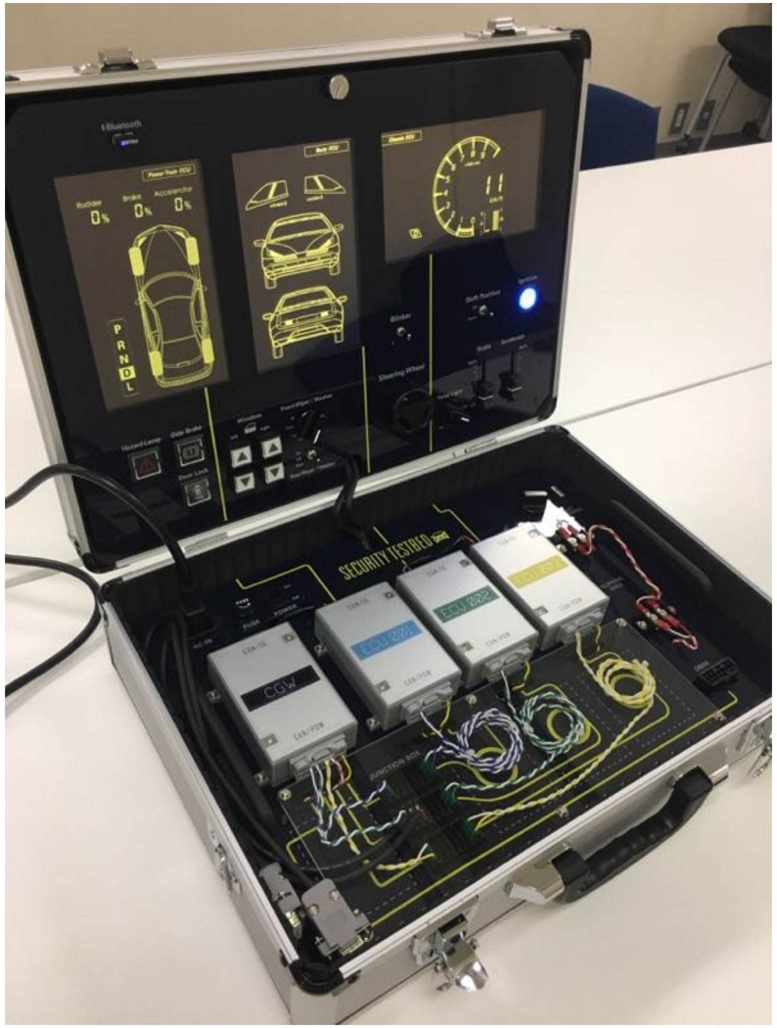
Philosophy of PASTA

- □ **Open**
  - □ It must be based on non-proprietary technologies.
- □ **Adaptable**
  - □ It must be designed with adaptability so that users can connect their own devices or rewrite the firmware of ECUs, for example.
- □ **Safe**
  - □ By realizing actuators such as meter, steering wheel and brake with a simulator rather than the real things, it can avoid incidents for the user.
- □ **Portable**
  - □ Vehicles are so large that users cannot prepare the environment easily. Platform is preferred to be small and portable so that users can study, research, and hack it anywhere.

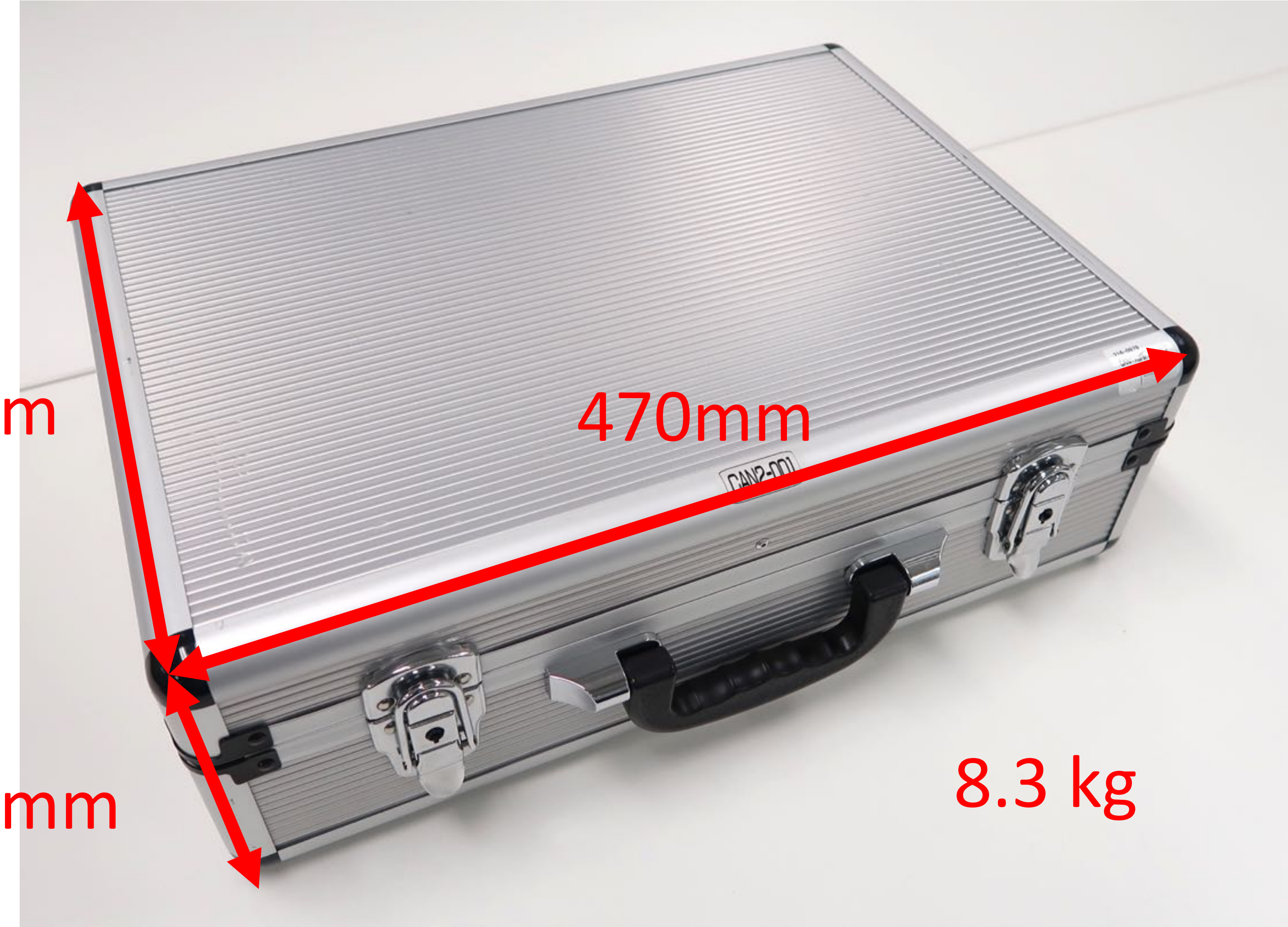
PASTA

It seems an ordinary attaché case…

Once it opened,
PASTA appears.

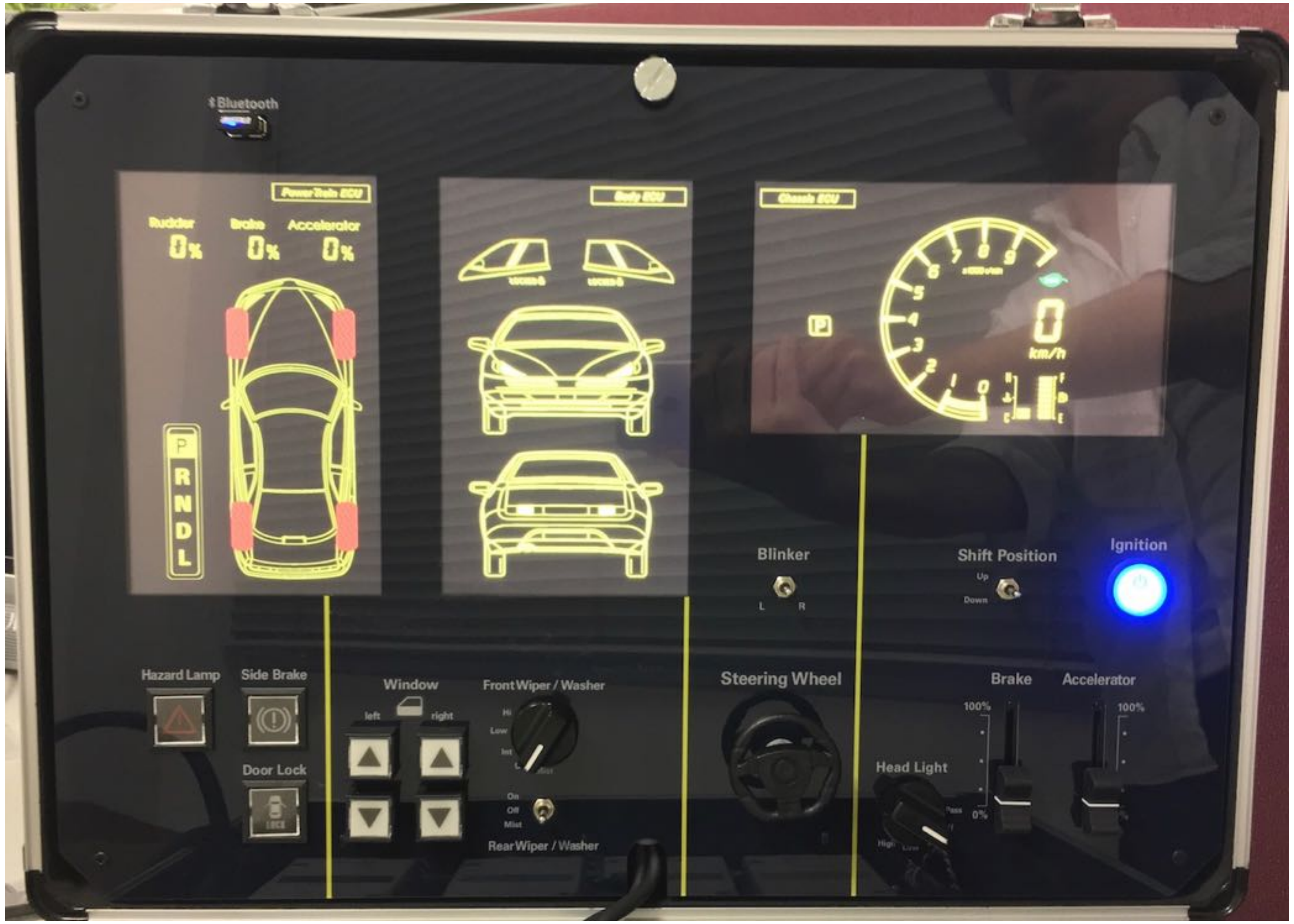


Portability of PASTA



Portable!

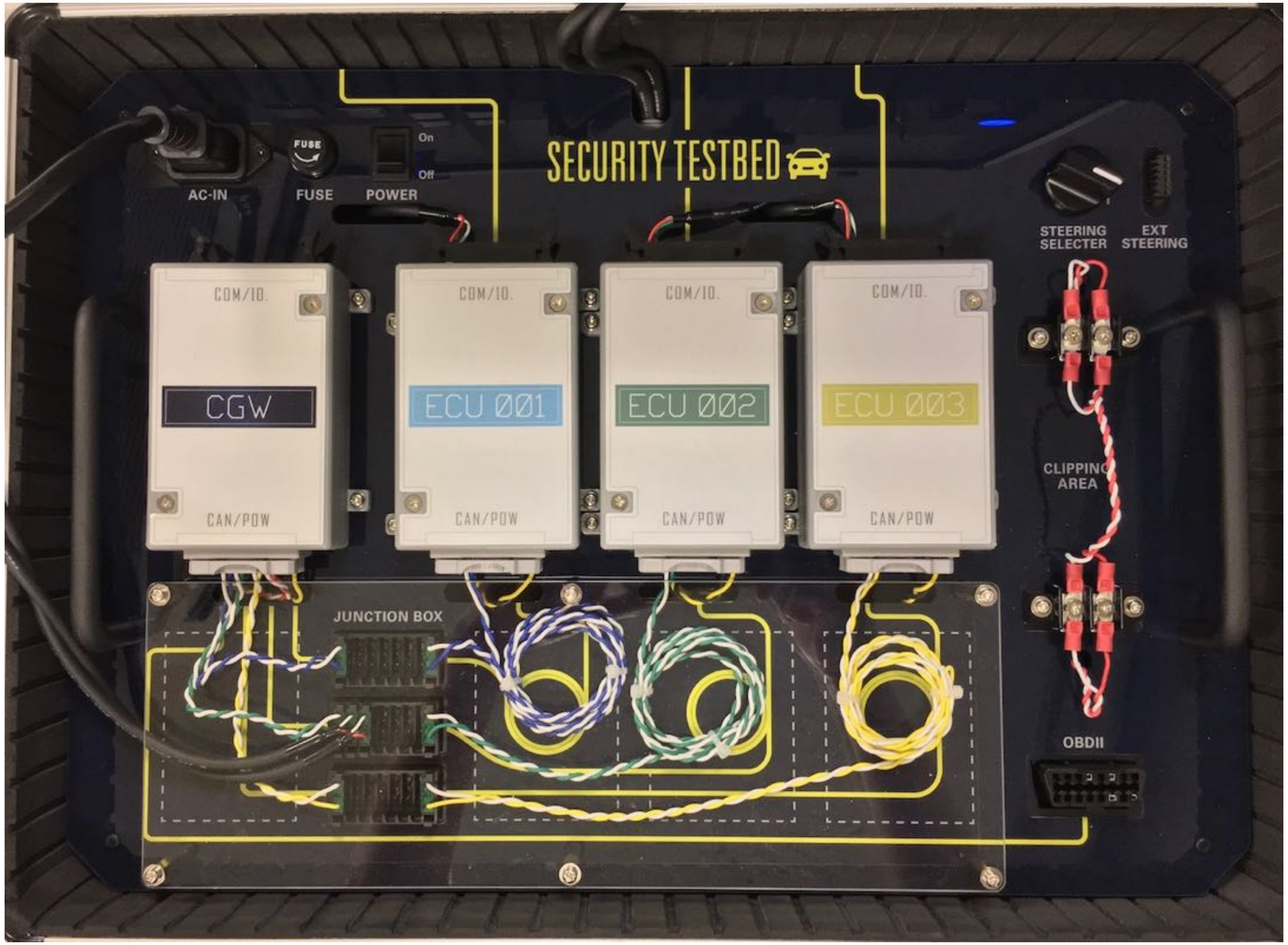
Upper side of PASTA



- □ There is a simple simulator in the attaché case, and it can be operated with the physical controller.
- □ The behavior by the operation can be confirmed from three monitors.

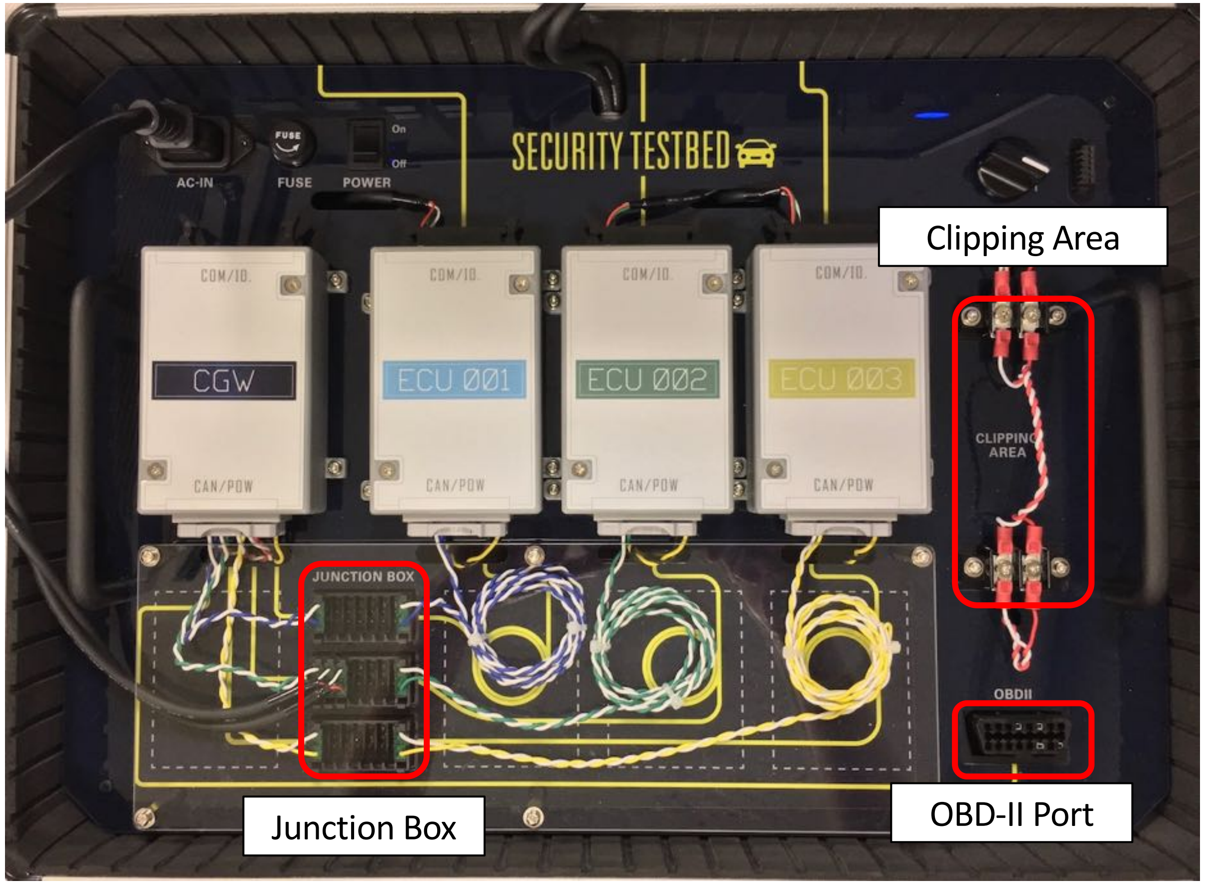
SAFE!

Bottom side of PASTA



- □ Frequently used attack surfaces are equipped.
  - □ Since if it is easy to simulate a CAN message injection, security evaluation is easy.
- □ You can modify the program of these ECUs in C language.

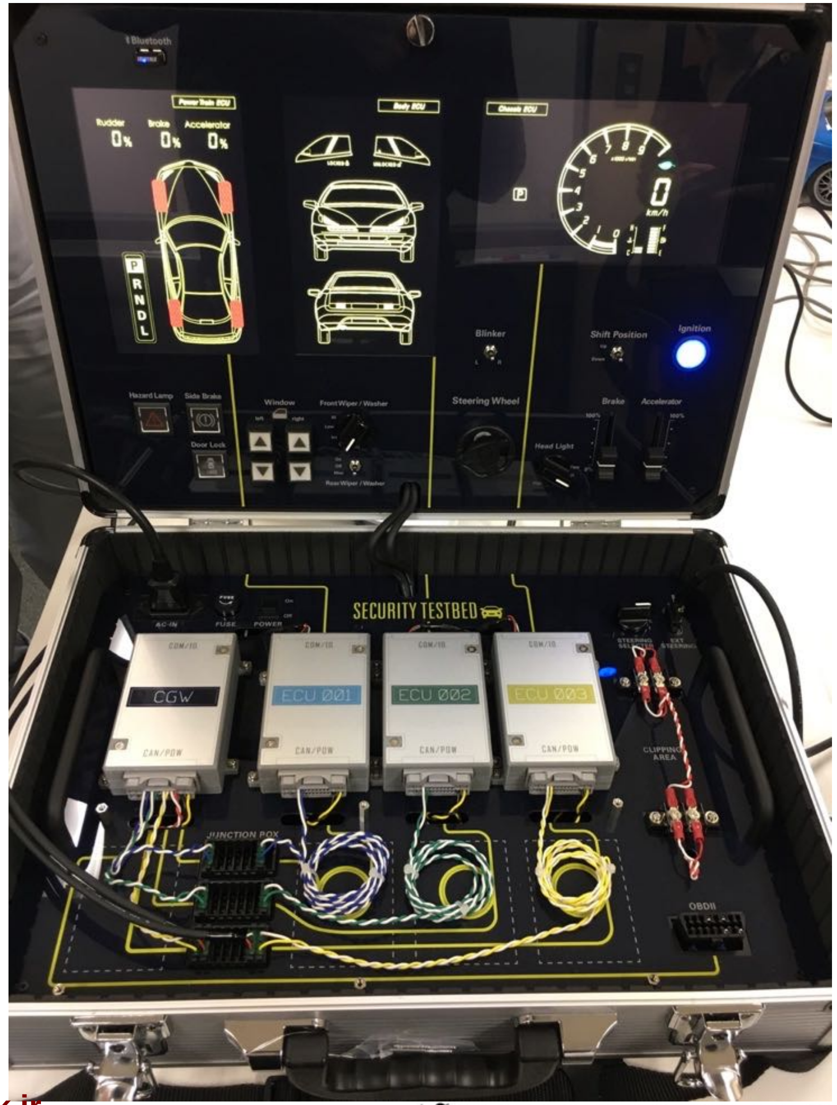
Attack surfaces in PASTA



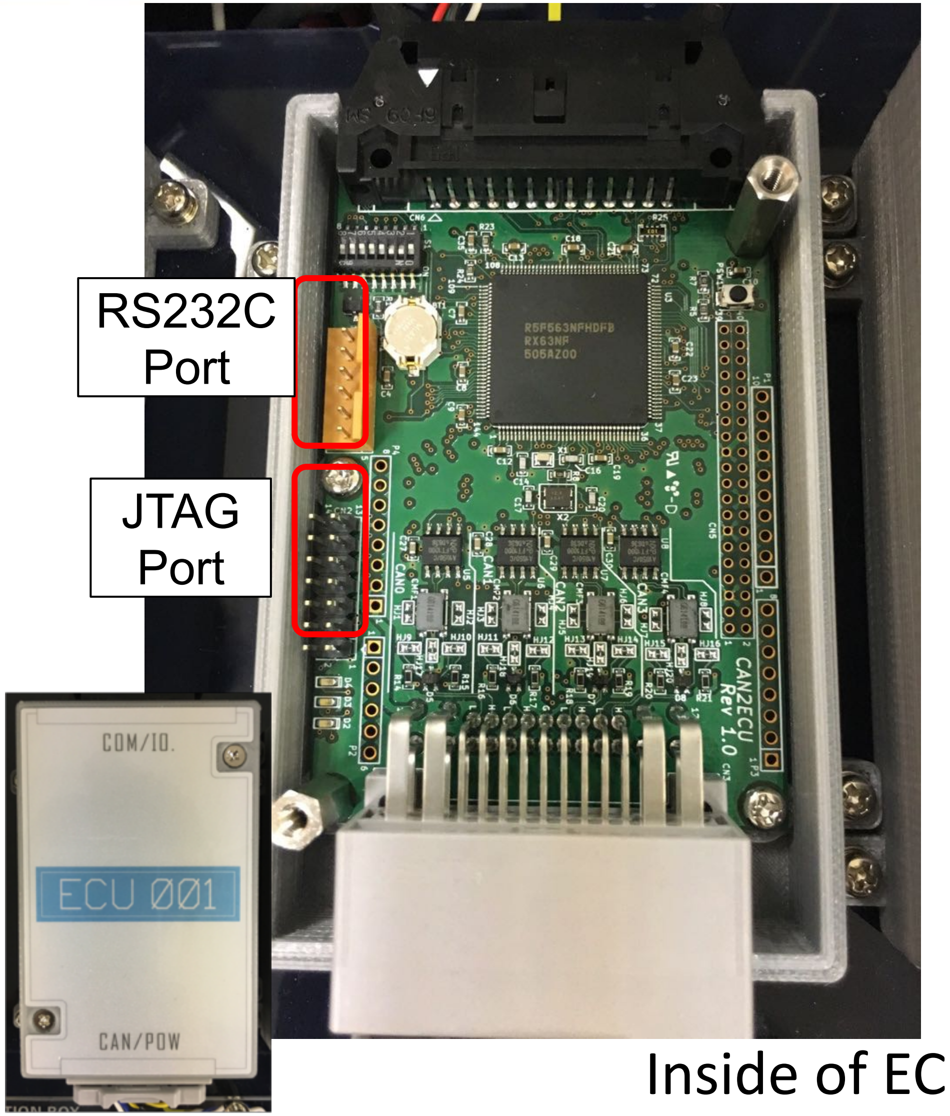
- □ Attack Surface are
  - □ OBD-II
  - □ Clipping Area
  - □ Junction Box

- □ Junction Box is implemented also for adaptability

Whole image of PASTA



Inside of the ECU

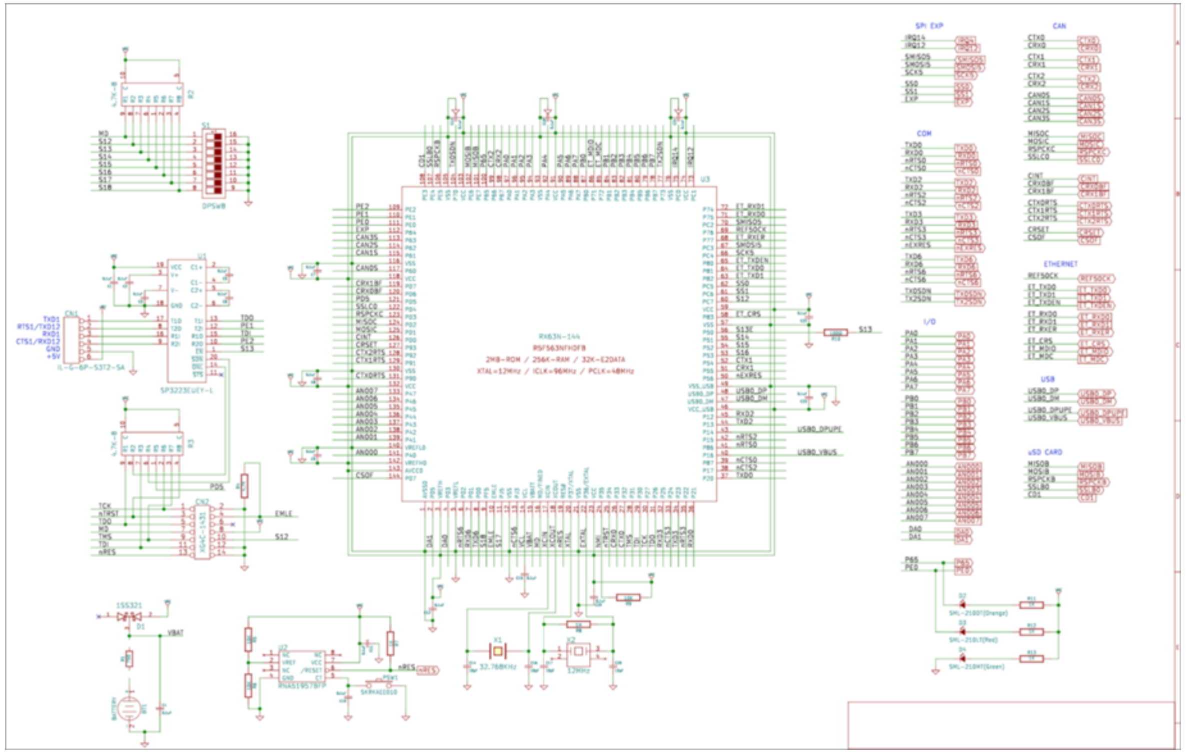


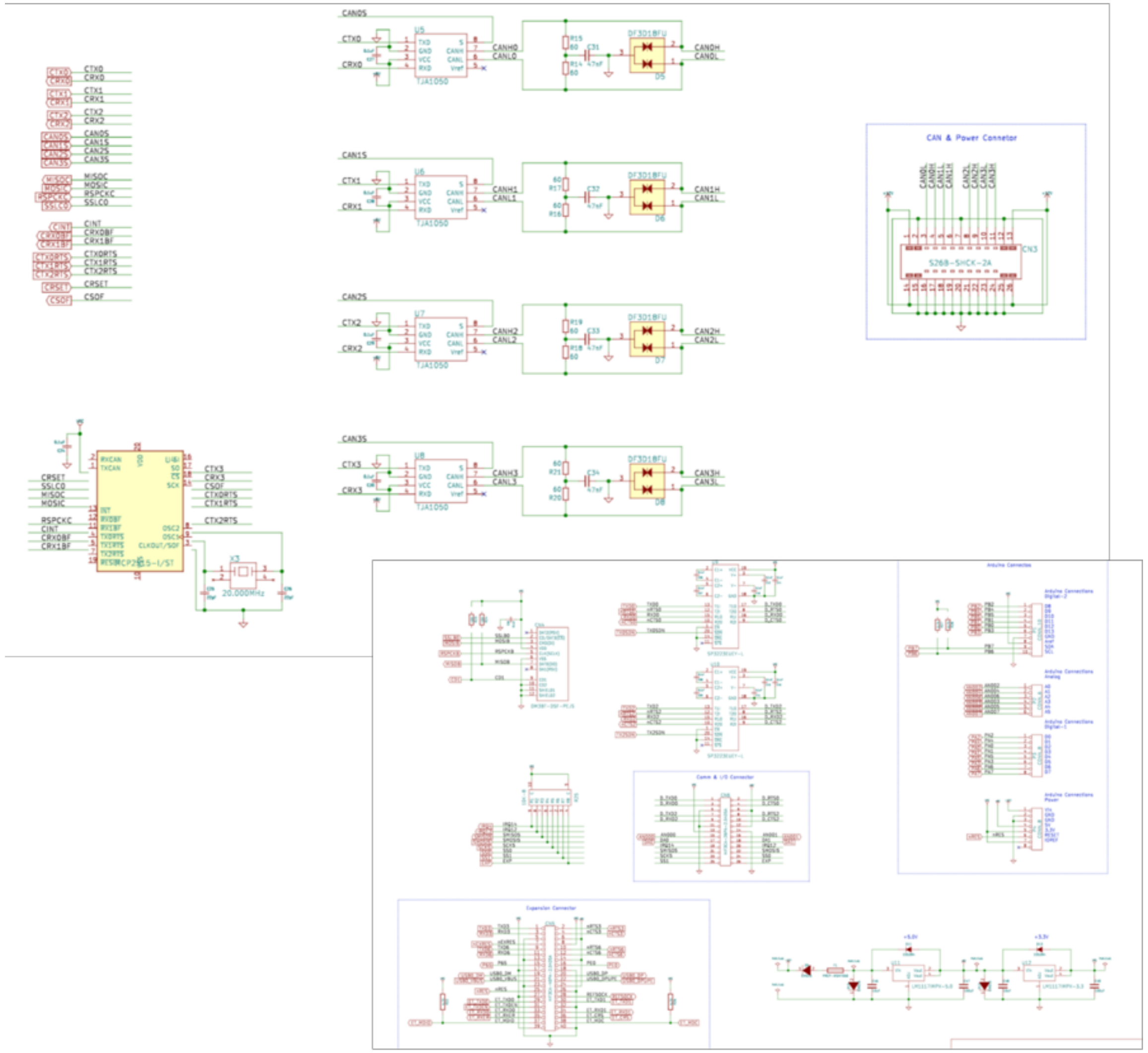
Inside of ECU

- □ Based on microcontroller(RX63N) by Renesas, we have designed and developed a ECU for PASTA from scratch.
- □ If you prepare for develop environment of Renesas microcontroller, You can apply your own program in C language.

Programmable!

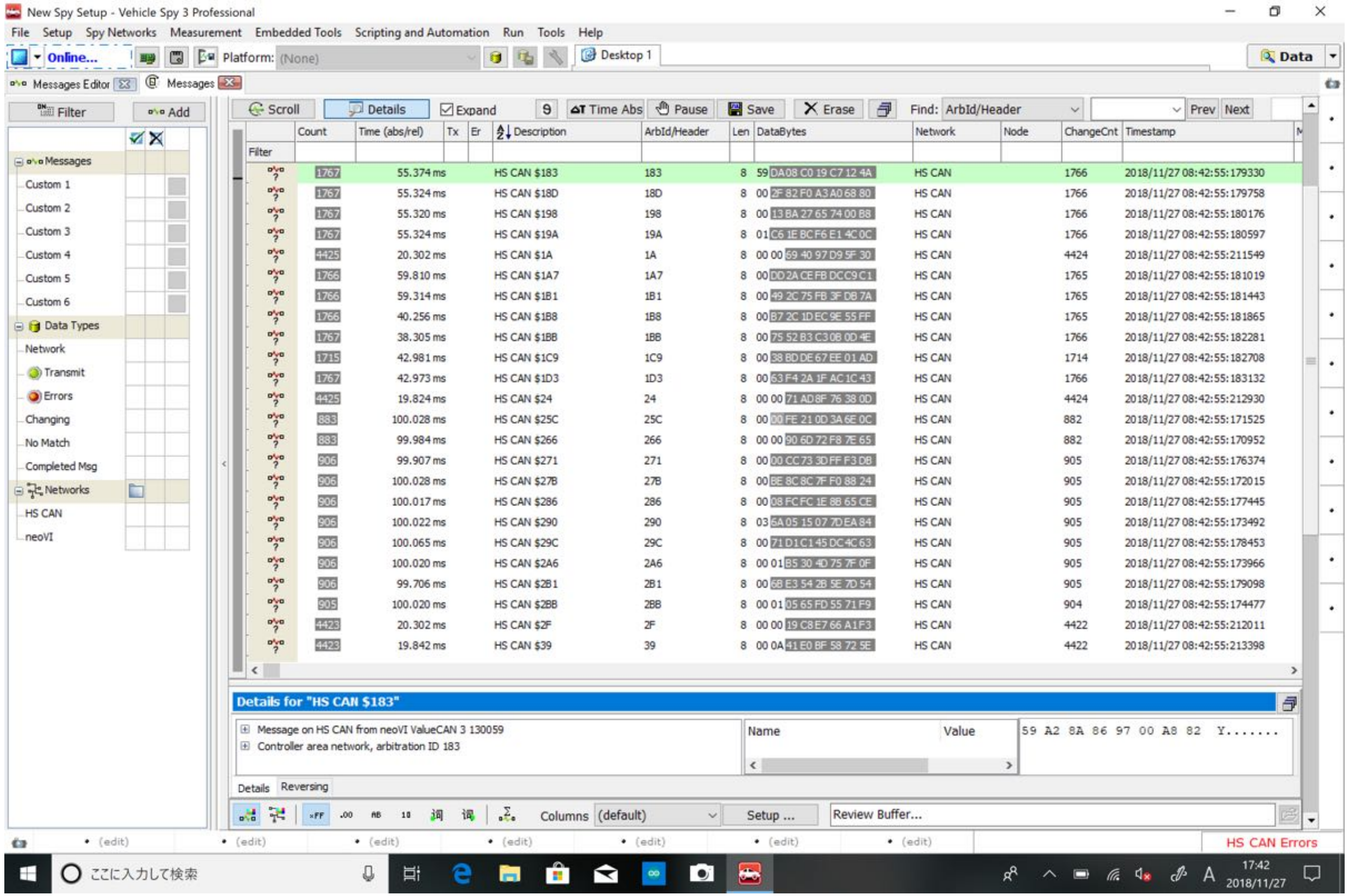
Design of the ECU





OPEN !

CAN IDs can be opened



Count	Time (abs/rel)	Tx	Er	Description	ArbId/Header	Len	DataBytes	Network	Node	ChangeCnt	Timestamp
1767	55.374 ms			HS CAN $183	183	8	59 DA 08 C0 19 C7 12 4A	HS CAN		1766	2018/11/27 08:42:55:179330
1767	55.324 ms			HS CAN $18D	18D	8	00 2F 82 F0 A3 A0 68 80	HS CAN		1766	2018/11/27 08:42:55:179758
1767	55.320 ms			HS CAN $198	198	8	00 13 BA 27 65 74 00 B8	HS CAN		1766	2018/11/27 08:42:55:180176
1767	55.324 ms			HS CAN $19A	19A	8	01 C6 1E BC F6 E1 4C 0C	HS CAN		1766	2018/11/27 08:42:55:180597
4425	20.302 ms			HS CAN $1A	1A	8	00 00 59 40 97 D9 5F 30	HS CAN		4424	2018/11/27 08:42:55:211549
1766	59.810 ms			HS CAN $1A7	1A7	8	00 DD 2A CE FB DC C9 C1	HS CAN		1765	2018/11/27 08:42:55:181019
1766	59.314 ms			HS CAN $1B1	1B1	8	00 49 2C 75 FB 3F D8 7A	HS CAN		1765	2018/11/27 08:42:55:181443
1766	40.256 ms			HS CAN $1B8	1B8	8	00 B7 2C 1D EC 9E 55 FF	HS CAN		1765	2018/11/27 08:42:55:181865
1767	38.305 ms			HS CAN $1BB	1BB	8	00 75 52 B3 C3 08 0D 4E	HS CAN		1766	2018/11/27 08:42:55:182281
1715	42.981 ms			HS CAN $1C9	1C9	8	00 38 8D DE 67 EE 01 AD	HS CAN		1714	2018/11/27 08:42:55:182708
1767	42.973 ms			HS CAN $1D3	1D3	8	00 63 F4 2A 1F AC 1C 43	HS CAN		1766	2018/11/27 08:42:55:183132
4425	19.824 ms			HS CAN $24	24	8	00 00 71 AD 8F 76 38 0D	HS CAN		4424	2018/11/27 08:42:55:212930
883	100.028 ms			HS CAN $25C	25C	8	00 00 FE 21 0D 3A 6E 0C	HS CAN		882	2018/11/27 08:42:55:171525
883	99.984 ms			HS CAN $266	266	8	00 00 90 6D 72 F8 7E 65	HS CAN		882	2018/11/27 08:42:55:170952
906	99.907 ms			HS CAN $271	271	8	00 00 CC 73 3D FF F3 DB	HS CAN		905	2018/11/27 08:42:55:176374
906	100.028 ms			HS CAN $27B	27B	8	00 BE 8C 8C 7F F0 88 24	HS CAN		905	2018/11/27 08:42:55:172015
906	100.017 ms			HS CAN $286	286	8	00 08 FC FC 1E 88 65 CE	HS CAN		905	2018/11/27 08:42:55:177445
906	100.022 ms			HS CAN $290	290	8	03 6A 05 15 07 7D EA 84	HS CAN		905	2018/11/27 08:42:55:173492
906	100.065 ms			HS CAN $29C	29C	8	00 71 D1 C1 45 DC 4C 63	HS CAN		905	2018/11/27 08:42:55:178453
906	100.020 ms			HS CAN $2A6	2A6	8	00 01 B5 30 4D 75 7F 0F	HS CAN		905	2018/11/27 08:42:55:173966
906	99.706 ms			HS CAN $2B1	2B1	8	00 6B E3 54 2B 5E 7D 54	HS CAN		905	2018/11/27 08:42:55:179098
905	100.020 ms			HS CAN $2BB	2BB	8	00 01 05 65 FD 55 71 F9	HS CAN		904	2018/11/27 08:42:55:174477
4423	20.302 ms			HS CAN $2F	2F	8	00 00 19 C8 E7 66 A1 F3	HS CAN		4422	2018/11/27 08:42:55:212011
4423	19.842 ms			HS CAN $39	39	8	00 0A 41 E0 BF 58 72 5E	HS CAN		4422	2018/11/27 08:42:55:213398

Details for "HS CAN $183"

Message on HS CAN from neoVI ValueCAN 3 130059
Controller area network, arbitration ID 183

Name	Value

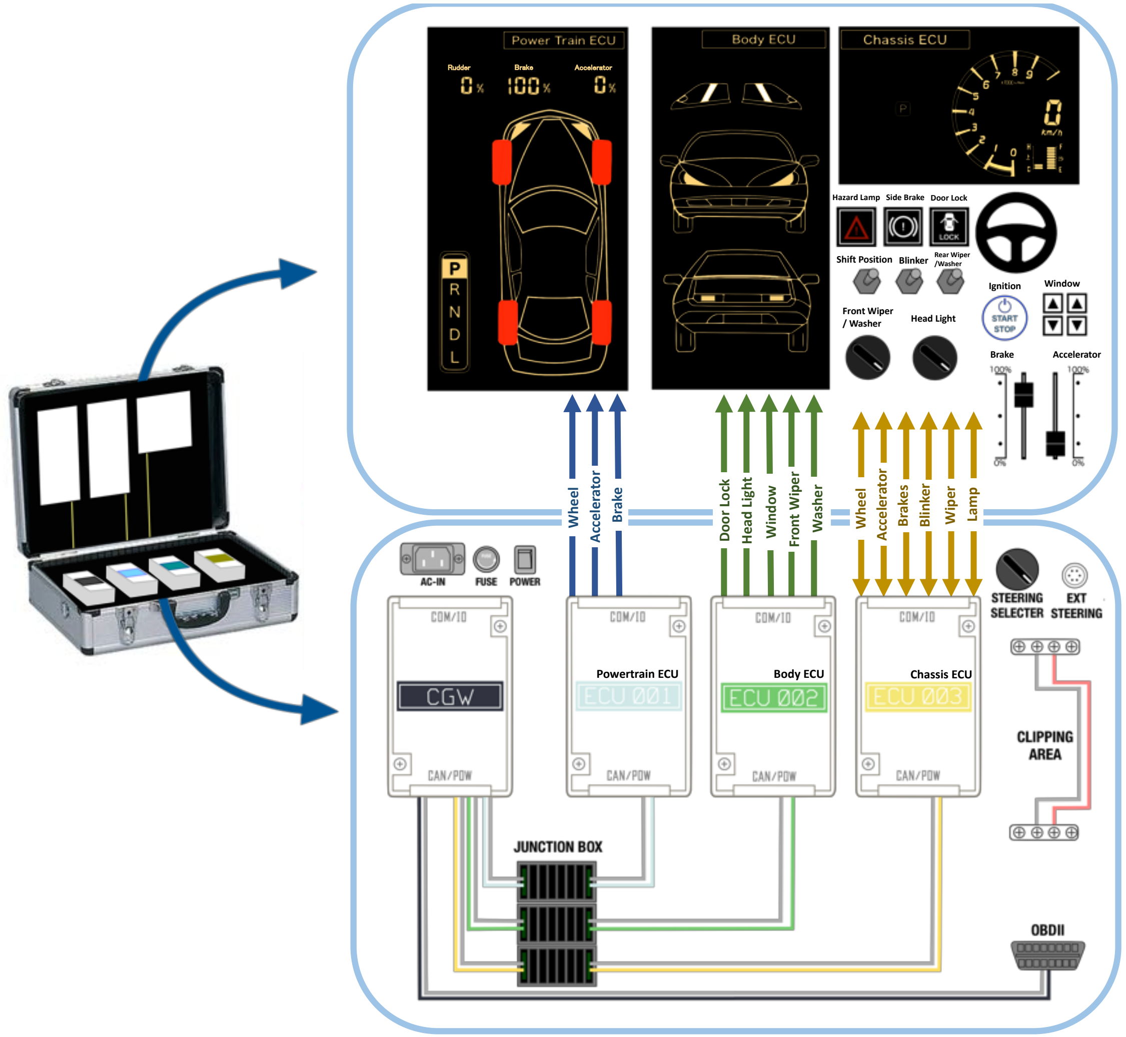
```
59 A2 8A 86 97 00 A8 82  Y.......
```

- □ 0x01A: Brake
- □ 0x02F: accelerator
- □ 0x1B1: headlight flashing
- □ 0x1B8: Ignition switch
- □ …

OPEN !

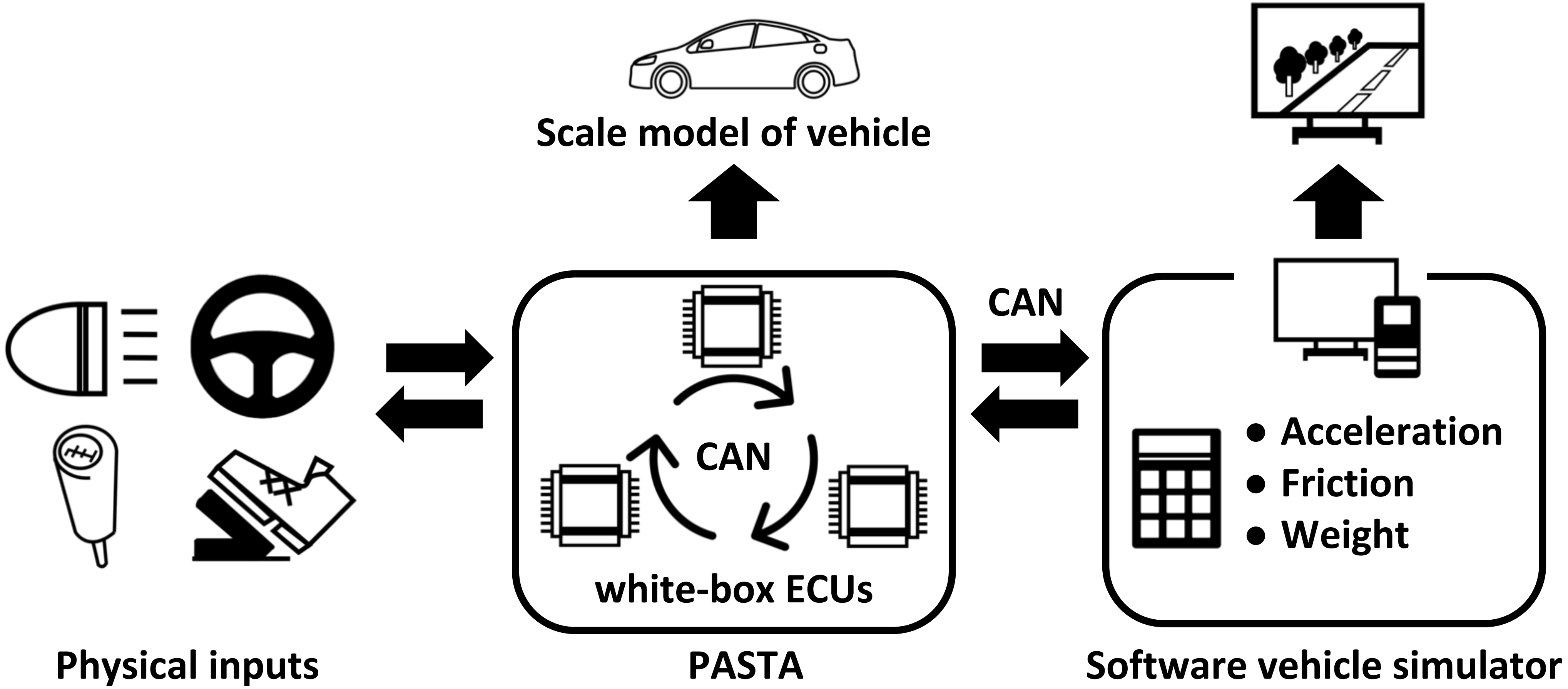
black hat EUROPE 2018

Information flow in PASTA



- □ In the attaché case, controller and vehicle simulator and ECUs are integrated.
- □ ECUs receive operations from controller, and ECUs send CAN messages. Thus ECUs share the information from operations and status of the vehicle.
- □ ECUs control actuators of simulator according to received CAN messages.

PASTA is adaptable



Scale model of vehicle

CAN

CAN

white-box ECUs

- Acceleration
- Friction
- Weight

Physical inputs

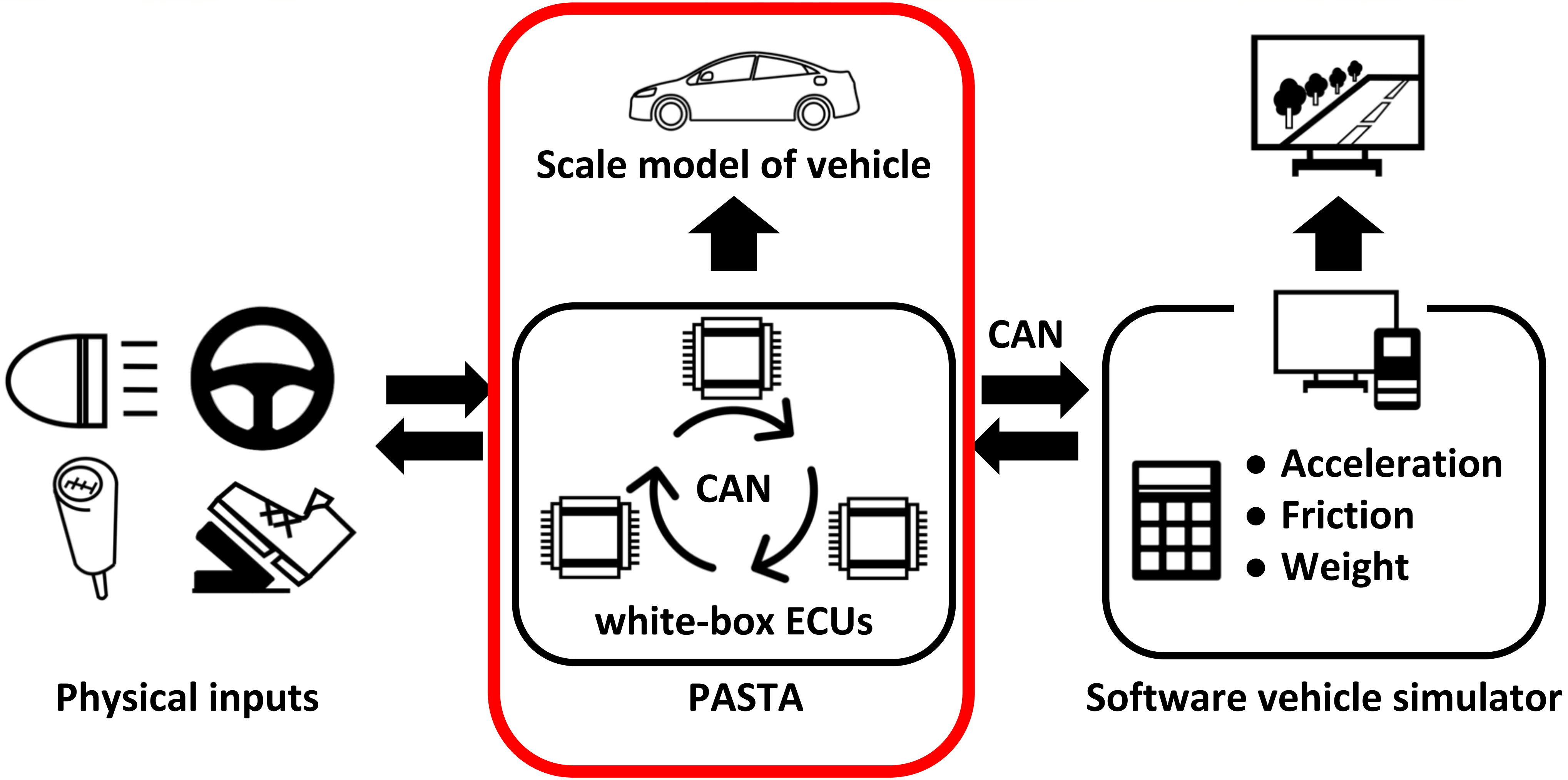
PASTA

Software vehicle simulator

Demo

Demo: normal

Demo of adaptability 1



Scale model of vehicle

CAN

CAN

white-box ECUs

- Acceleration
- Friction
- Weight

Physical inputs

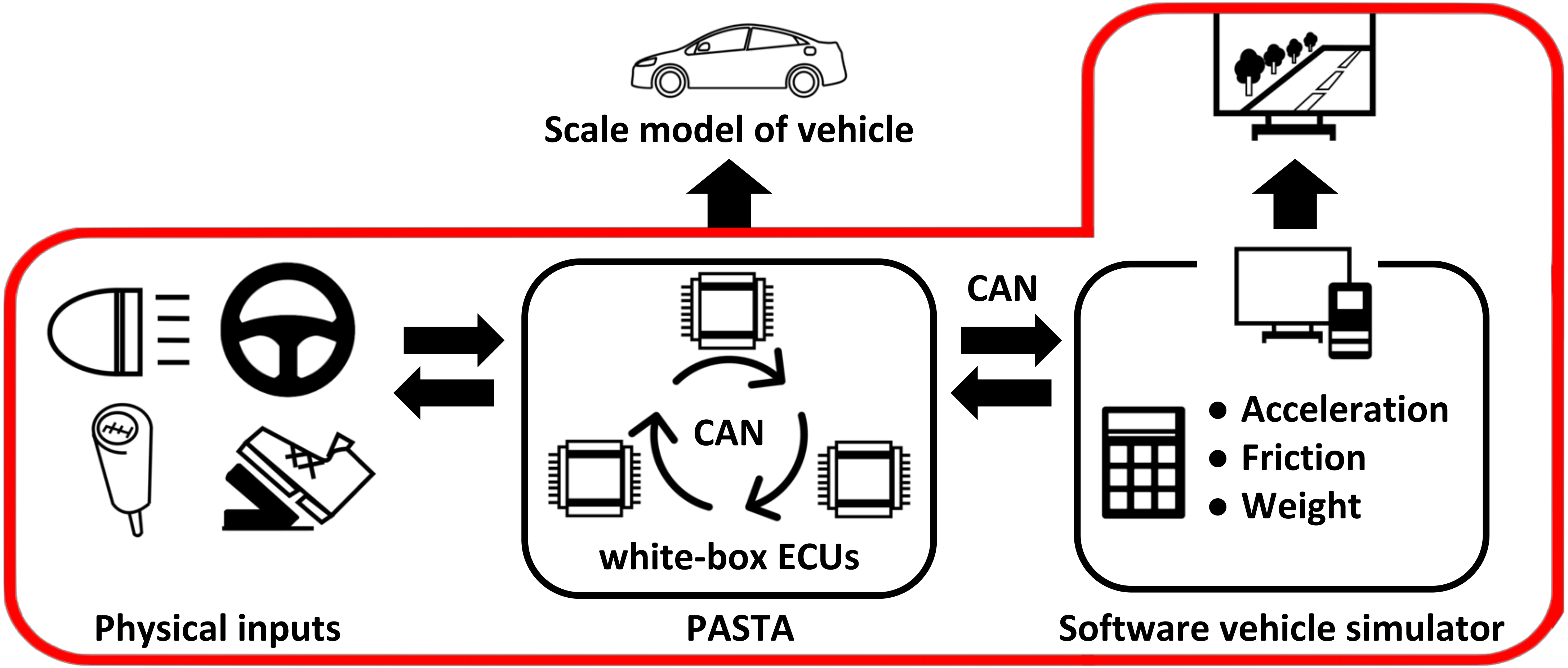
PASTA

Software vehicle simulator

PASTSA with miniature vehicle

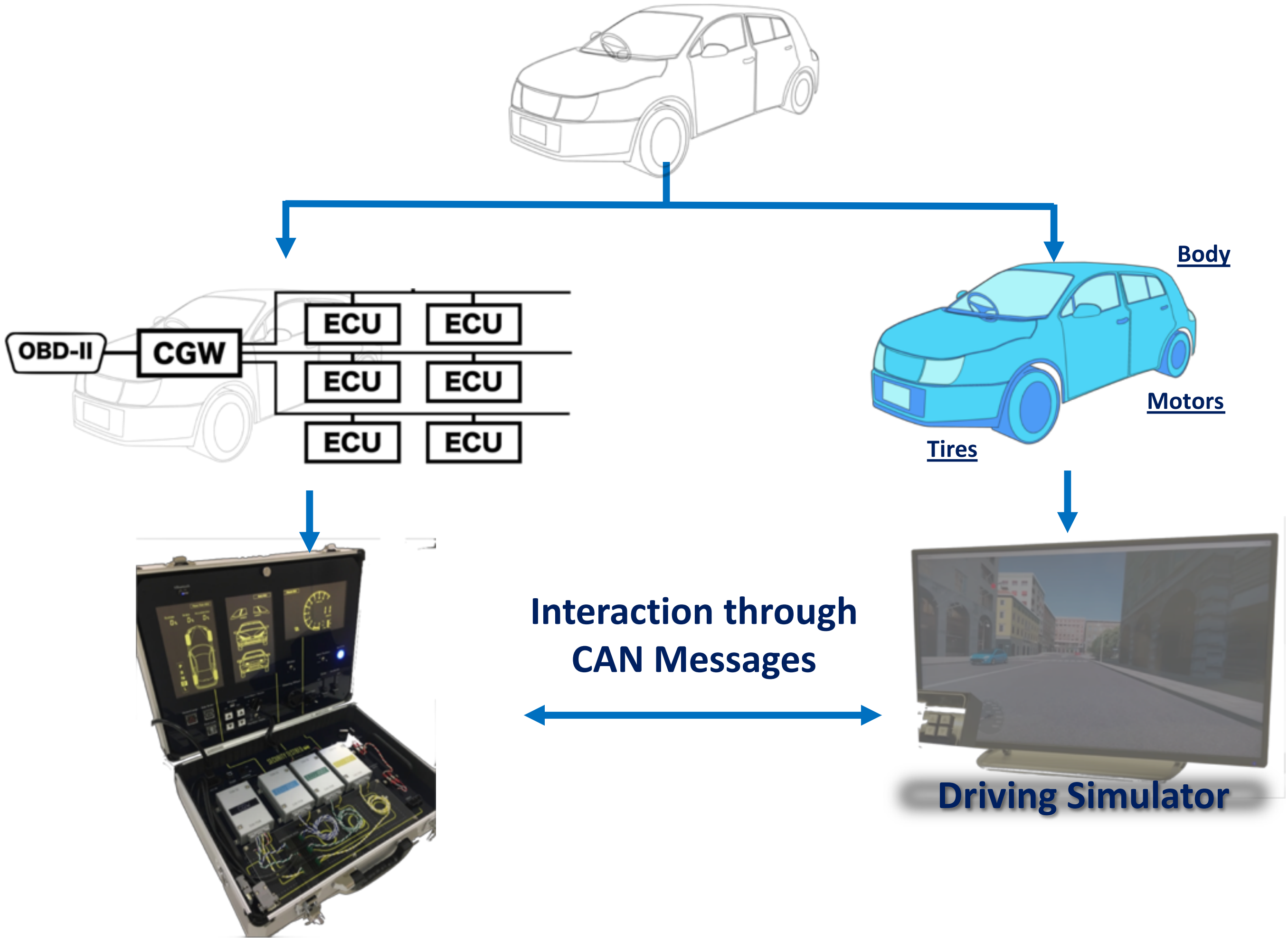
(video – with miniature vehicle)

Demo of adaptability 2



- Acceleration
- Friction
- Weight

Integration of drive simulator with PASTA



Interaction through CAN Messages

PASTA

Driving Simulator

Real behavior by connection with a drive simulator

(video – with a drive simulator)

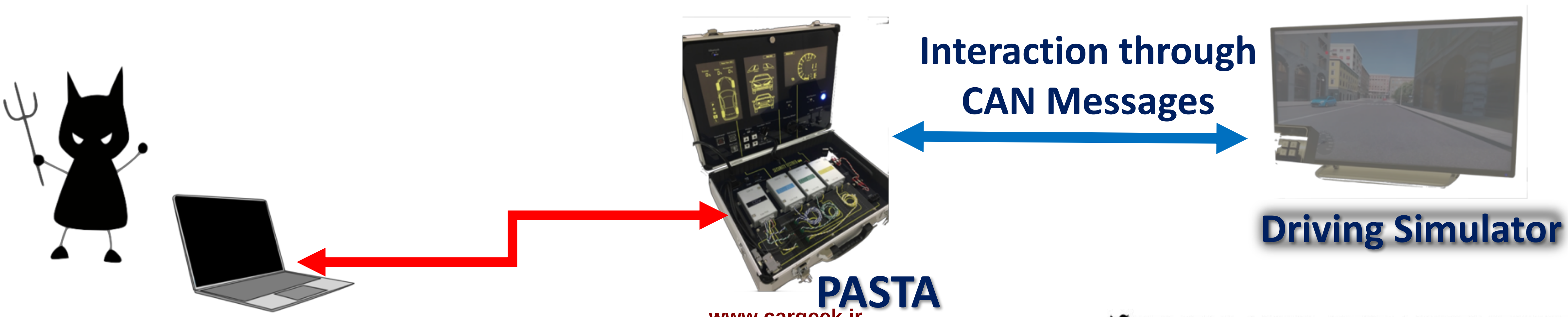
Demo: Incident…

Demo and caution!!!

□ Typical attack demonstration via OBD-II port: an attacker injects malicious CAN packets via OBD-II port.

□ The effect of attack is noticeable, because, we have not implement enough safety function in software of ECUs in PASTA.

□ However real vehicles have safety functions, it is difficult to reproduce the result of following demo.



Interaction through CAN Messages

Driving Simulator

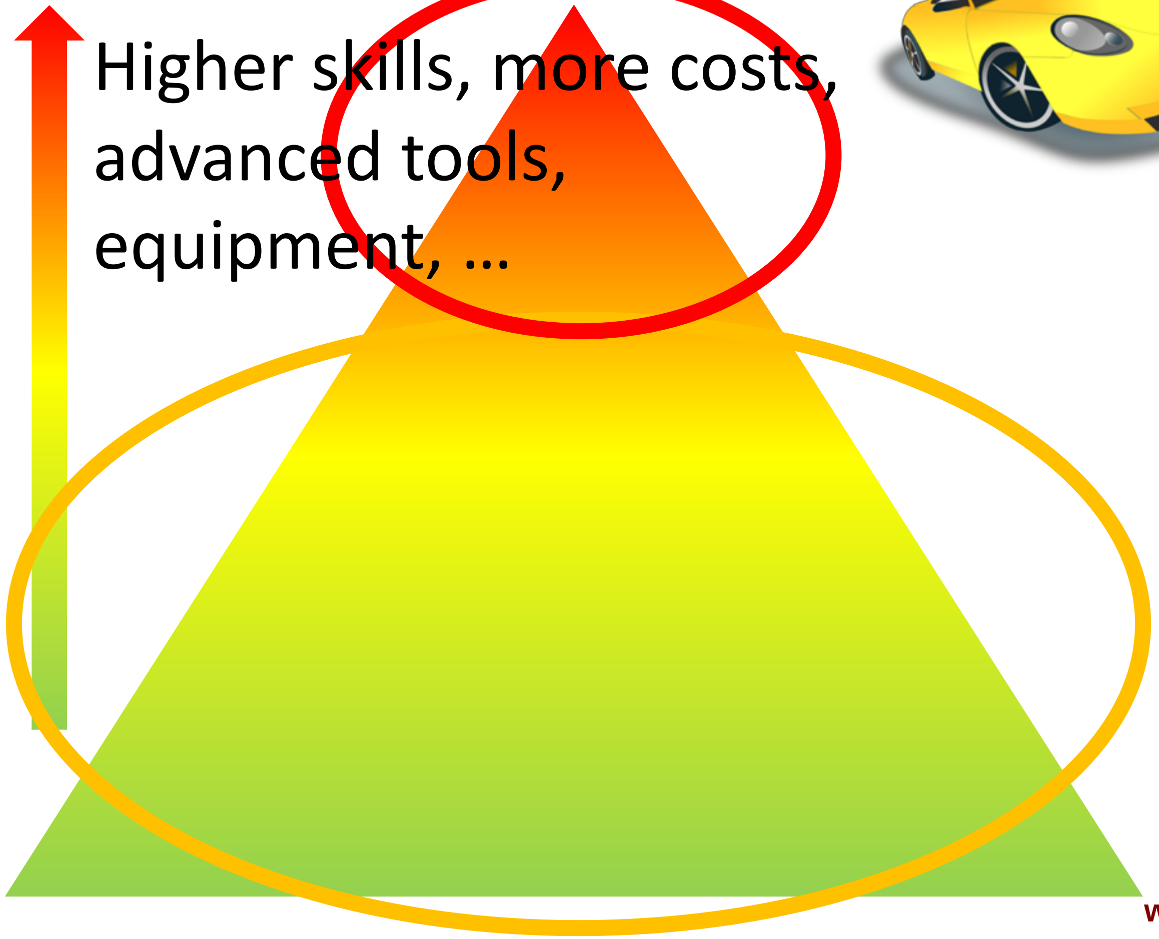
PASTA

Demo: Incident…

(Video - incident)

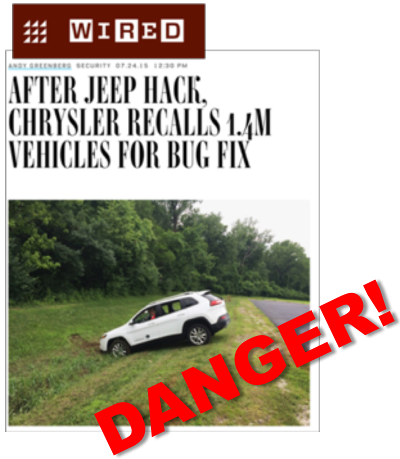
Use Cases

Use Cases



Higher skills, more costs, advanced tools, equipment, …

Real Vehicle



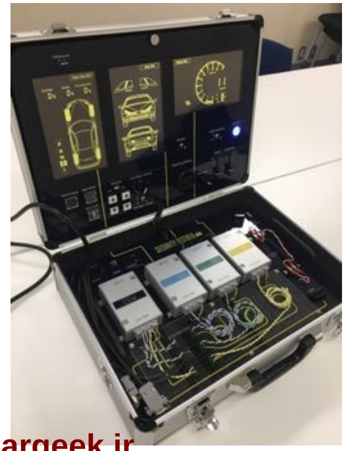
WIRED

ANDY GREENBERG SECURITY 07.24.15 12:30 PM

AFTER JEEP HACK, CHRYSLER RECALLS 1.4M VEHICLES FOR BUG FIX

NOT for Everyone …

PASTA



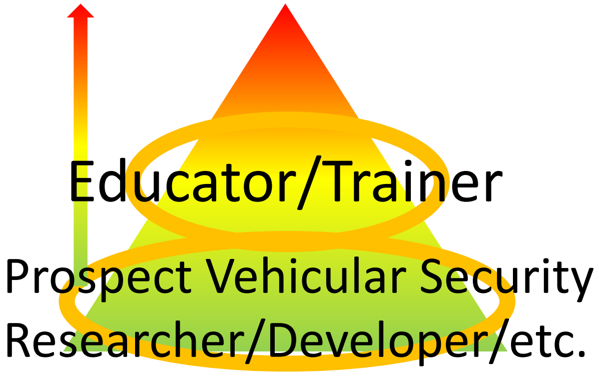
You can start if you have:
- Some space on desk
- An outlet

Open **Safe**

Adaptable **Portable**

Use Cases: Education/Training

TARGET



OBJECTIVE

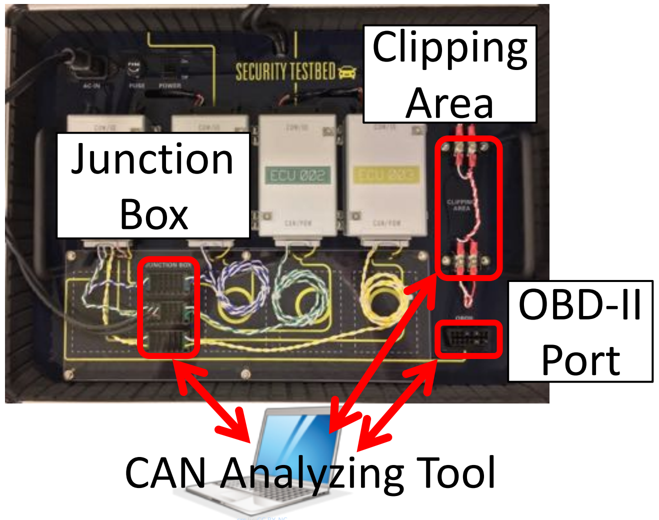
- Educate or learn vehicle security

REQUIRMENTS

- Open (e.g. known answers)
- Flexibility (e.g. intentionally embed vulnerabilities)
- Typical architecture
- Typical attack surfaces

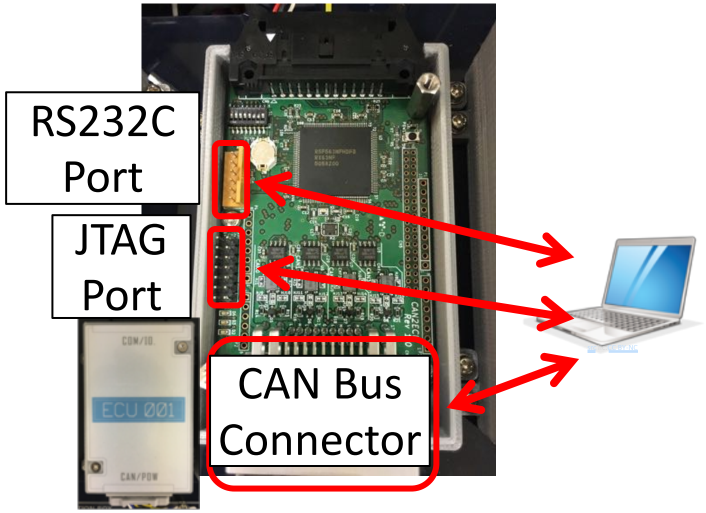
EXAMPLES

Hacking CAN bus messages



- Wire-tap, analyze, and inject CAN messages

Hacking ECU/CGW



- Read, analyze, and reprogram firmware

NOTES

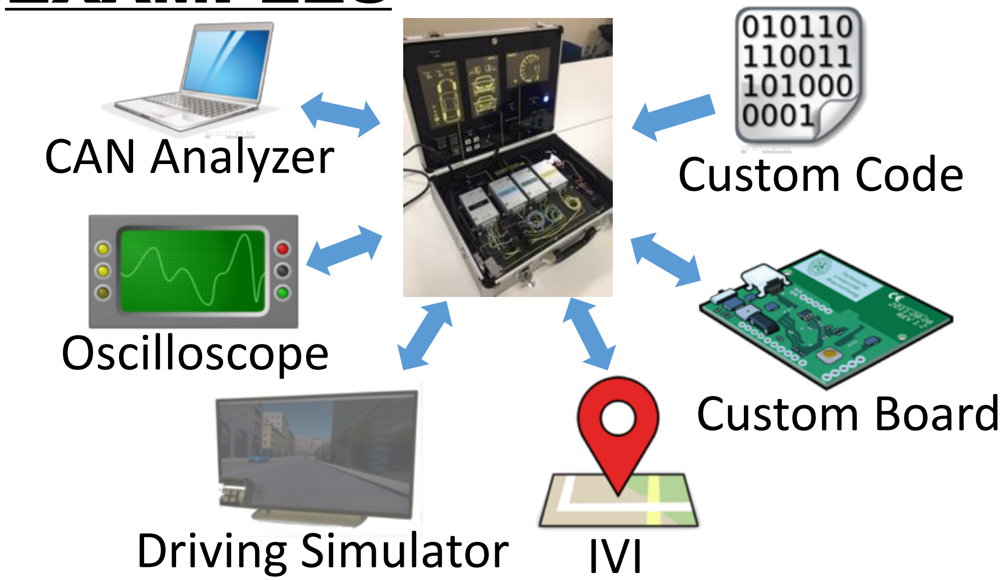
- More to come:
  - LIN, CAN FD, IVI, Wireless I/F support, etc.
  - On going or on roadmap
- Joint work with YNU

Use Cases: Research

TARGET

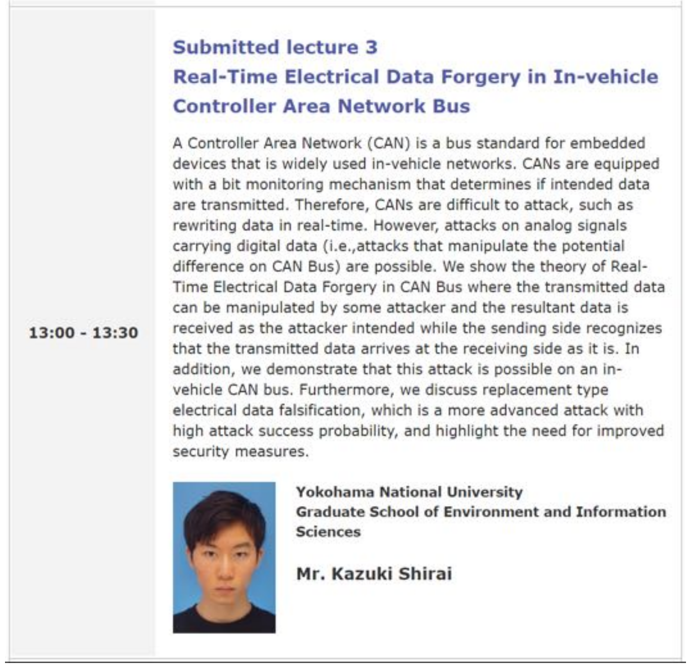
Researcher

EXAMPLES



OBJECTIVE

- Open research from various perspective



13:00 - 13:30

Submitted lecture 3
Real-Time Electrical Data Forgery in In-vehicle Controller Area Network Bus

A Controller Area Network (CAN) is a bus standard for embedded devices that is widely used in-vehicle networks. CANs are equipped with a bit monitoring mechanism that determines if intended data are transmitted. Therefore, CANs are difficult to attack, such as rewriting data in real-time. However, attacks on analog signals carrying digital data (i.e.,attacks that manipulate the potential difference on CAN Bus) are possible. We show the theory of Real-Time Electrical Data Forgery in CAN Bus where the transmitted data can be manipulated by some attacker and the resultant data is received as the attacker intended while the sending side recognizes that the transmitted data arrives at the receiving side as it is. In addition, we demonstrate that this attack is possible on an in-vehicle CAN bus. Furthermore, we discuss replacement type electrical data falsification, which is a more advanced attack with high attack success probability, and highlight the need for improved security measures.

Yokohama National University
Graduate School of Environment and Information Sciences

Mr. Kazuki Shirai

REQUIRMENTS

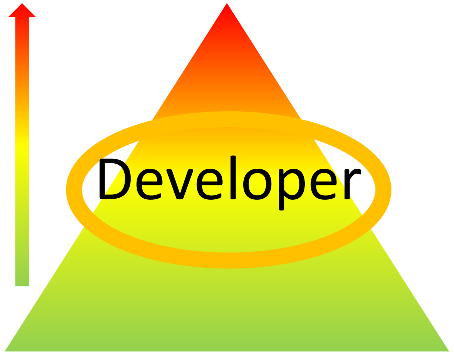
- Publish the results
- Reproduce environments and results
- Physical/Logical, HW/SW, Analog/Digital
- Adaptability

RESULTS

- **“Real-time Electrical Data Forgery in In-vehicle Controller Area Network Bus”** @ escar Asia 2018
  by K. Shirai, T. Kiyokawa, J. Sakamoto, T. Toyama, T. Matsumoto
  https://tech.nikkeibp.co.jp/cp/2018/escar2018e/

Use Cases: Development

TARGET



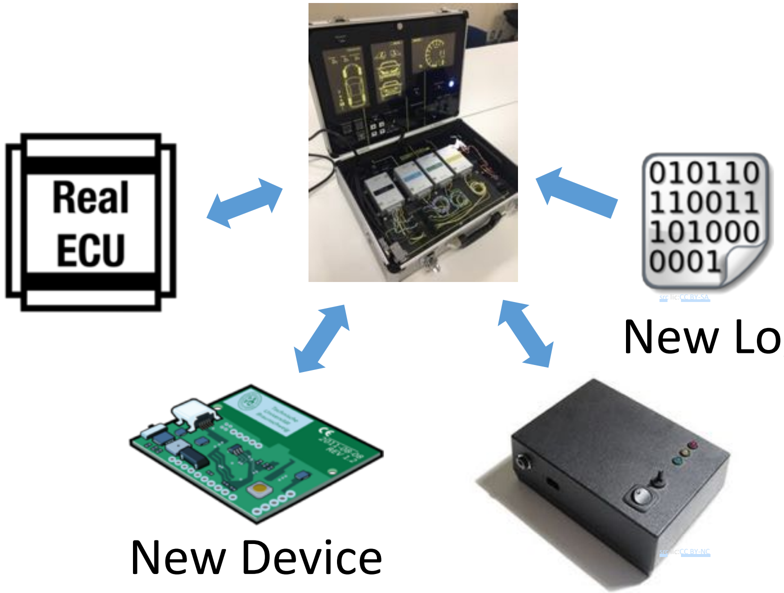
OBJECTIVE

- Prototyping and PoC
  of new technologies and products

REQUIRMENTS

- Simulates real vehicle
- Verify the effect
- Support various devices
- Adaptability

EXAMPLES



New Logic

New Device

New Security Product

NOTES

- Require real vehicle in final process
- Can be used for evaluation of technologies and products

Roadmap

- For more advanced and realistic architecture:
  - Support **more protocols**
    - LIN, CAN FD, Ethernet, etc.
  - Support **wireless** interfaces
    - Wi-Fi, Bluetooth, Cellular
  - **IVI**
  - **More domains**
    - In-Vehicle Network of vehicles currently available are more complicated and have more domains.
  - Support **AUTOSAR** system
    - The ECUs in PASTA do not support any OS for vehicles and AUTOSAR system.
- Make specifications **OPEN** on GitHub

Take away

- □ In spite of vehicular security importance, any common platform for research has not been developed.

- □ PASTA is open, portable, safe, adaptable.
  - □ Apparently portable!
  - □ The design of PASTA is open; anyone can program and change the ECUs behavior.
  - □ PASTA is harmless for students, researchers, hackers, and so on because actuators are simulated in software.

- □ The testbed can be a common platform for…
  - □ Automotive cyber security research and development.
  - □ Educational tools.
  - □ etc…

For more information

@pasta_auto

GitHub https://github.com/pasta-auto

mail pasta_auto@jp.toyota-itc.com