# Electric Car Deciphering

Weijia Ma, Shermaine Sue Ning Chew, Siwen Pan
Nanyang Girl's High School (As of 2013)
2 Linden Dr, Singapore 288683
Email: weijiama@outlook.com; shermainechew.1@gmail.com; wwp7767@gmail.com;

## I. Background and Purpose of Research Area

In the modern automobile industry, cars are becoming highly computerized which makes the security concern of vehicles top of the list. In order to have a deeper insight into the automotive systems and improve the security matter for vehicles, this project simulates the deciphering process and attempts to control the vehicle through reproducing the messages. Providing a better understanding into the issue, this project acts as a reference and guidance for those who want to improve the security system for automobiles.

Modern vehicle engines bear little resemblance to engines of the past. Within the past 20 years, vehicles have evolved to be embedded with a convoluted network consisting of many independent computers. The controller area network (CAN) message technology is largely used as the communication medium within the vehicle itself. CAN constitutes a system of controllers, which are called CAN nodes, being able to transmit and receive messages from the network [1]. As mentioned, today's vehicles may have up to 50 microprocessors that control various systems including those that unlock doors, start ignition, deploy airbags and optimize fuel efficiency [2].

As the CAN messages use broadcast communication, it becomes easier for an attacker to get remote code execution on the electronic control units (ECUs) in automotive vehicles via various interfaces such as the Bluetooth interface and the telematics unit and thus undermining the security of these electric vehicles [3]. More and more hackers are able to inject malicious code remotely to gain control over cars. In 2010, more than 100 drivers in Austin, Texas found their cars disabled or the horns honking out of control, after a hacker ran amok to intrude those vehicles and control critical systems [4]. Together, they bring about an unprecedentedly exciting challenge and unexplored frontier for criminal hackers itching to show their courage and prove their competence.

Due to the broadcast characteristics of CAN communication, when we capture CAN messages, we cannot locate their sources or their destinations, and hence it enhances the difficulty in deciphering the CAN messages. Additional difficulties are that the automotive manufacturer would not want to provide the detailed diagrams. Hence, we would have to figure out various components inside the vehicle. Moreover, the CAN messages do not follow any convention and are totally proprietary. It would be quite a task to decipher them.

## II. Hypothesis of the Research

If we successfully decipher the CAN messages, we would be able to take over the control of some functions of the vehicle by injecting the CAN messages into CAN network to control some vehicle ECUs. We hope this can raise security issue of vehicles and provide vehicle manufacturers and other researchers with insights of how to further improve vehicle security.

## III. Research Method and Materials

### *A. Passive Analysis Strategy*

In order not to damage the vehicle and not to affect its warrantee, we decide to apply the passive analysis strategy. Thus, we adopted the below methods into our research work

#### *Study, Survey and Collect Rich Information*

Firstly, we survey and collect as much information as possible related to the vehicle, as well as study how the CAN works. Thereafter, we try to figure out how the electric vehicle works. In this research project, an electric vehicle (EV) Mitsubushi i-MiEV is used as our testing target (Fig. 1.a). The main ECUs in the i-MiEV include Electronic Total Automobile Control System (ETACS), Electric Power Steering Control Unit (EPSCU), Active Stability Contl System, Combination Meter ECU, Battery Management Unit (BMU), EV-ECU, Aircon Control Unit and so on. We make use of OBD II port (designed to facilitate the diagnostic process) to connect to the CAN network for our testing (Fig. 1b).

Mitsubishu i-MiEV Electric Vehicle

Connecting laptop to the OBD II port via CAN adaptor

Figure 1. An electric vehicle and its testing setup

### i. Design Complete Test Cases

Based on the various car functions, we generate models, theories and hypotheses and designed the complete test cases.

### ii. Capture the Testing Data

Following the test cases, we collect empirical data by capturing the CAN messages carefully.

### iii. Analyze the Testing Data

After collecting empirical data, for the analysis of our data, we grouped the similar functions and studied the similarities and differences between the CAN messages under various scenarios.

### iv. Deduce, Guess and Check Methods in Analyzing Data

When analyzing the CAN messages, we deduce the trends, make use of guess and check, and other methods.

### v. Black Box Testing

We also did black box testing and created input intentionally to analyze the outcome, obtaining trends and different CAN messages corresponding to the various inputs.

### vi. Repeat Tests and Verify the Decipher Results

Upon the CAN messages are decoded, the tests are repeated to double check the deciphered CAN messages.

## *B. First Experiment: Main Functions*

To test with the main functions of EV, we adopt the above methods into the below detail experiment with main functions.

a) Connect the laptop to the OBD II port inside the EV via a CAN adaptor. Use software to capture CAN messages under 35 different conditions. We take the condition of fully turning on the key (Appendix B) as bench mark and only change one variable at a time, solely carried out by the driver, so as to obtain the most accurate data.

b) Take down the effect of those 35 conditions. Group conditions that exhibit similar effects or are controlled by the same possible ECUs together.

c) Highlight the message data in each condition that is different from the message data of when the key is fully turned on (Table I).

d) Contrast the data of similar conditions to deduce the message ID and the data that controls those conditions.

e) After determining the particular data bytes controlling the different actions of the vehicle, we reproduce the condition and confirm the accuracy of our data.

## *C. Second Experiment: Battery Condition*

To understand the battery management system, we specially carry out the below test.

TABLE I. A SECTION OF THE HIGHLIGHTED DATA UNDER THE GROUPED CONDITIONS

| | Action | 374 | 384 | 3A4 | 418 | 424 |
|---|---|---|---|---|---|---|
| 1 | No power | 8B 8F 00 00 54 52 59 00 | 00 00 00 4A 00 78 77 00 | 85 13 B2 CA 68 70 00 8F | 50 00 00 00 00 00 00 00 | 40 00 01 00 00 23 01 FF |
| 2 | Charging | 8F 92 00 00 55 52 59 00 | 00 00 00 38 00 77 77 00 | 85 13 B5 C9 99 70 00 8F | 50 00 00 00 00 00 00 00 | 40 00 00 00 00 3A 01 FF |
| 3 | Charged for 30mins | A4 A7 00 00 56 52 59 00 | 09 60 16 59 00 7A 7A 03 | 85 13 B5 C9 99 70 00 8F | 50 00 00 00 00 00 00 00 | 40 00 00 00 00 54 01 FF |
| 4 | Insert Key | NIL | NIL | NIL | NIL | C0 00 88 00 27 1A 01 FF |
| 5 | Half turn on the key | 90 90 00 00 53 51 59 00 | 00 00 00 30 00 73 73 00 | 47 11 B4 BC AC 70 00 87 | 50 00 00 00 00 00 00 00 | C3 00 0C 00 27 1F 03 FF |
| 6 | Full on key | 90 90 00 00 53 51 59 00 | 00 00 00 30 00 73 73 00 | 47 10 B8 BD AD 70 00 87 | 50 00 00 00 00 00 00 00 | C3 00 0C 00 27 24 03 FF |
| 7 | P/P+ Brake | 4E 57 00 00 56 52 54 00 | 00 00 00 35 00 7F 7F 00 | 06 20 C0 CC B3 72 00 90 | 50 00 00 00 00 00 00 00 | C3 00 0C 00 C6 29 03 FF |
| 8 | Reverse / R+B | 4D 57 00 00 56 52 54 00 | 00 00 00 35 00 7F 7F 00 | 06 20 C2 CB B4 73 00 8F | 52 00 00 00 00 00 00 00 | C3 00 0C 00 C6 30 03 FF |
| 9 | Neutral / N+B | 4D 56 00 00 56 52 54 00 | 00 00 00 35 00 7F 7F 00 | 06 20 C2 CA B4 73 00 8F | 4E 00 00 00 00 00 00 00 | C3 00 0C 00 C6 30 03 FF |
| 10 | Drive /D+B | 4D 56 00 00 56 52 54 00 | 00 00 00 35 00 7F 7F 00 | 06 20 C2 C8 B4 73 00 8F | 44 00 00 00 00 00 00 00 | C3 00 0C 00 C6 41 03 FF |
| 11 | B/B+B | 4D 56 00 00 56 52 54 00 | 00 00 00 35 00 7F 7F 00 | 06 20 C2 CB B4 73 00 8F | 83 00 00 00 00 00 00 00 | C3 00 0C 00 C6 31 03 FF |
| 12 | Constant Speed / C+B | 4D 56 00 00 56 52 54 00 | 00 00 00 35 00 7F 7F 00 | 06 20 C2 CB B4 73 00 8F | 32 00 00 00 00 00 00 00 | C3 00 0C 00 C6 32 03 FF |
| 13 | P acceleration | 4E 57 00 00 56 52 54 00 | 00 00 00 35 00 7F 7F 00 | 06 20 C0 CD B2 72 00 91 | 50 00 00 00 00 00 00 00 | C3 00 0C 00 C6 28 03 FF |
| 14 | Shouzha | 4D 57 00 00 56 52 54 00 | 00 00 00 35 00 7F 7F 00 | 06 20 C1 CB B3 73 00 90 | 50 00 00 00 00 00 00 00 | C3 00 0C 00 C6 2E 03 FF |
| 15 | Turn left | 4F 58 00 00 56 52 54 00 | 00 00 00 34 00 7F 7F 00 | 06 20 BC CE AF 72 00 92 | 50 00 00 00 00 00 00 00 | C3 02 0C 00 C6 1E 01 FF |
| 16 | Turn right | 4E 58 00 00 56 52 54 00 | 00 00 00 34 00 7F 7F 00 | 06 20 BC CF B0 72 00 92 | 50 00 00 00 00 00 00 00 | C3 01 0C 00 C6 1E 01 FF |
| 17 | Warning | 4E 58 00 00 56 52 54 00 | 00 00 00 34 00 7F 7F 00 | 06 20 BC CE B0 72 00 92 | 50 00 00 00 00 00 00 00 | C3 03 0C 00 C6 1F 01 FF |
| 18 | Third light | 4E 57 00 00 56 52 54 00 | 00 00 00 35 00 7F 7F 00 | 06 20 C0 CC B3 72 00 90 | 50 00 00 00 00 00 00 00 | C7 40 0C 00 C6 2A 03 FF |
| 19 | Main light | 4D 56 00 00 56 52 54 00 | 00 00 00 35 00 7F 7F 00 | 06 20 C2 CA B4 73 00 8F | 50 00 00 00 00 00 00 00 | C3 24 0C 00 C6 33 01 FF |
| 20 | All three headlights | 4E 57 00 00 56 52 54 00 | 00 00 00 35 00 7F 7F 00 | 06 20 C0 CC B4 72 00 90 | 50 00 00 00 00 00 00 00 | C7 60 0C 00 C6 2A 03 FF |
| 21 | Rooftop light | 4E 57 00 00 56 52 54 00 | 00 00 00 35 00 7F 7F 00 | 06 23 BE CD AD 72 00 91 | 50 00 00 00 00 00 00 00 | C3 00 0C 00 C6 26 03 FF |
| 22 | Auto light | 4E 57 00 00 56 52 54 00 | 00 00 00 35 00 7F 7F 00 | 06 20 C0 CC B3 72 00 90 | 50 00 00 00 00 00 00 00 | C7 60 0C 00 C6 29 03 FF |
| 23 | Both seat belt fastened | 4D 56 00 00 56 52 54 00 | 00 00 00 35 00 7F 7F 00 | 06 20 C3 C9 B4 73 00 8F | 50 00 00 00 00 00 00 00 | 03 00 0C 00 C6 37 01 FF |
| 24 | Driver's Seat Belt Fastened | 4D 56 00 00 56 52 54 00 | 00 00 00 35 00 7F 7F 00 | 06 20 C2 CA B4 73 00 8F | 50 00 00 00 00 00 00 00 | 83 00 0C 00 C6 36 01 FF |
| 25 | Driver door open | 4D 56 00 00 56 52 54 00 | 00 00 00 35 00 7F 7F 00 | 06 20 C2 CB B4 73 00 8F | 50 00 00 00 00 00 00 00 | C3 00 0F 00 C6 34 01 FF |
| 26 | Lock door | 4E 57 00 00 56 52 54 00 | 00 00 00 35 00 7F 7F 00 | 06 20 C1 CC B2 72 00 90 | 50 00 00 00 00 00 00 00 | C3 00 4C 00 C6 2C 03 FF |
| 27 | Lock window | 4C 55 00 00 57 52 54 00 | 00 00 00 31 00 7F 7F 00 | 06 20 C5 CB 9D 73 00 90 | 50 00 00 00 00 00 00 00 | C3 00 0C 00 C6 45 01 FF |
| 28 | Roll down driver window | 4D 56 00 00 56 52 54 00 | 00 00 00 35 00 7F 7F 00 | 06 20 C4 C9 B4 73 00 8F | 50 00 00 00 00 00 00 00 | C3 00 0C 00 C6 38 01 FF |
| 29 | Roll up driver window | 4D 56 00 00 56 52 54 00 | 00 00 00 35 00 7F 7F 00 | 06 20 C4 CA B4 73 00 8F | 50 00 00 00 00 00 00 00 | C3 00 0C 00 C6 39 01 FF |
| 30 | Close Right Side Mirror Using Control | 4C 55 00 00 57 52 54 00 | 00 00 00 49 00 7F 7F 00 | 06 20 C5 CE 8B 73 00 91 | 50 00 00 00 00 00 00 00 | 03 00 0C 00 C6 41 01 FF |
| 31 | Close side mirror | 4E 57 00 00 56 52 54 00 | 00 00 00 35 00 7F 7F 00 | 06 23 BF CD AE 72 00 91 | 50 00 00 00 00 00 00 00 | C3 00 0C 00 C6 27 03 FF |
| 32 | Wiper | 4E 57 00 00 56 52 54 00 | 00 00 00 35 00 7F 7F 00 | 06 20 C1 CC B2 72 00 90 | 50 00 00 00 00 00 00 00 | C3 08 0C 00 C6 2B 03 FF |
| 33 | Seat heat | 4C 55 00 00 57 52 54 00 | 00 00 00 31 00 7F 7F 00 | 06 20 C4 CB 9F 73 00 8F | 50 00 00 00 00 00 00 00 | C3 00 0C 00 C6 47 01 FF |
| 34 | Aircon push to max | 4F 58 00 00 56 52 54 00 | 09 67 16 59 00 7F 7F 03 | A6 29 BB CF 84 72 00 92 | 50 00 00 00 00 00 00 00 | C3 00 0C 00 C6 20 01 FF |

a) Fully charge the battery
b) Connect the laptop to the BMU via the CAN adaptor
c) Slowly discharge it
d) Every 5 minutes during discharging:
   - Use the diagnosis software to measure the battery level in percentage as well as the temperature and voltage of the battery system
   - Capture the CAN messages

## IV. Interpretation of Data, Results and Findings

### A. First Experiment Interpretation

[0]~[7] represent the 8 bytes in a message. For example, 100H = 00 03 53 68 9A 10 37 25, then 100H [0] = 00 and 100H [3] = 68. We will elaborate on results relating to shift panel and other results from our first experiment can be seen in Appendix A.

#### *1) ID 4I8H (Shift panel Drive Mode Selector Lever)*

In the process of looking for the patterns of the bytes, we grouped different actions according to their similarities in operation. For example, while we were looking at the message IDs, we grouped the different shift panel choices, namely parking, reverse, neutral, drive, brake and constant speed. Since they should all be controlled by the same ECUs, there is very likely a message ID that has a few same data bytes only for these conditions. The rest of the data bytes in that ID for these five conditions should be different to differentiate their particular driving mode. In this way, we found message ID 418H (Table II).

TABLE II. CAPTURED DATA OF MESSAGE ID 418H UNDER DIFFERENT DRIVING MODE

| Condition | Data |
|---|---|
| Reverse | **52** 00 00 00 00 00 00 |
| Neutral | **4E** 00 00 00 00 00 00 |
| Drive | **44** 00 00 00 00 00 00 |
| Brake | **83** 00 00 00 00 00 00 |
| Constant Speed | **32** 00 00 00 00 00 00 |
| Parking | **50** 00 00 00 00 00 00 |

#### *2) ID 231H & 208H (Foot Brake related)*

*231H:* Without brake: 231H [4] = 00; With brake: 231H [4] = 02

*Comment: Indicator of brake (yes = 02; no = 00)*

*208H:* We found that the extent of foot brake is also shown in the CAN data and we had a retest when we kept varying the extent of foot brake and reached the following conclusion.

Without brake: 208H [3] = 02; Starting to brake: 208H [3] = XX. The value of XX increases from 02 (start value) to CX (around MAX) when the brake is applied to a greater extent

#### *3) ID 285H 288H (Foot brake & Shift panel)*

Based on our prior knowledge and observation, without foot brake applied, cars are supposed to be in stationary situation under the parking and neutral mode and with foot brake applied, the vehicle is going to stop or already in stationary situation whichever driving mode the car is under. Therefore, we look for other codes which change only when foot brake is applied which had similar data to the one under parking and neutral mode without foot brake. We managed to find message ID 285H and 288H shown in Table III.

We found that '07 D0' signals the car being stationary. Comparing the codes for reverse, drive and constant speed, we found that reverse has '06 0E' which is a value smaller than '07 D0', while drive and constant speed have '09 02', a value larger than '07 D0'. As reverse mode makes the car to move back, and drive and constant speed give the car a forward motion, we presumed that a smaller value 06 0E signals the car to move backward, 07 D0 signals the car to be in a neutral state and a larger value 09 02 signals the car to move forward. This speculation is affirmed when we applied foot brake as the codes for all five modes became 07 D0 which indicates a neutral state of the car.

TABLE III. CAPTURED DATA OF MESSAGE ID 285H AND 288H UNDER DIFFERENT DRIVING MODE

| Condition | 285H | 288H |
|---|---|---|
| Parking<br>Parking with Foot Brake | **07 D0 14 00 8C FE 0C 10**<br>**07 D0 14 00 8C FE 0C 10** | **07 D0 27 10 AE 00 11 10**<br>**07 D0 27 10 AE 00 11 10** |
| Reverse<br>Reverse with Foot Brake | 06 0E 14 00 8C FE 0C 10<br>**07 D0 14 00 8C FE OC 10** | 06 0E 27 10 AE 00 11 10<br>**07 D0 27 10 AE 00 11 10** |
| Neutral<br>Neutral with Foot Brake | **07 D0 14 00 8C FE 0C 10**<br>**07 D0 14 00 8C FE OC 10** | **07 D0 27 10 AE 00 11 10**<br>**07 D0 27 10 AE 00 11 10** |
| Drive<br>Drive with Foot Brake | 09 92 14 00 8C FE 0C 10<br>**07 D0 14 00 8C FE OC 10** | 09 92 27 10 AE 00 11 10<br>**07 D0 27 10 AE 00 11 10** |
| Brake<br>Brake with Foot Brake | 09 92 14 00 8C FE 0C 10<br>**07 D0 14 00 8C FE OC 10** | 09 92 27 10 AE 00 11 10<br>**07 D0 27 10 AE 00 11 10** |
| Constant Speed<br>Constant Speed with Foot Brake | 09 92 14 00 8C FE 0C 10<br>**07 D0 14 00 8C FE OC 10** | 09 92 27 10 AE 00 11 10<br>**07 D0 27 10 AE 00 11 10** |

### B. Second Experiment Interpretation

#### *1) Battery System & Battery Cells*

After checking CAN messages captured, we deduce that there are 12 blocks of batteries among which 10 have 8 cells

and 2 have 4 cells. In total there are 88 cells. From captured CAN messages, 44 message ID ranging from 611h to 6C4h each contains 4 or 2 bytes of data that show the battery status. The second digit of ID represents the 12 blocks and the third digit ranges from 1 to 4.

### *2) Battery Level*

As shown in Table IV, the '5F' in 3C3H indicates the average percentage charge left in the whole battery system while the 8 bytes of highlighted data in 611H to 614H indicate the percentage charge left in each of the 8 individual cells in block 1. The data decrease while discharging and the data value of 3C3H is converted into the decimal value. We then plot the figure of battery power against the data value of 3C3H (Fig. 2).

TABLE IV. CAPTURED DATA OF BATTERY LEVEL

| Message ID | Data |
|---|---|
| 3C3H | 01 **5F** 00 02 00 00 00 00 |
| 611H | 01 00 50 51 01 **5F** 01 **5F** |
| 612H | 01 50 50 00 01 **5F** 01 **5F** |
| 613H | 01 50 50 00 01 **5F** 01 **5F** |
| 614H | 01 00 00 00 01 **5F** 01 **5F** |

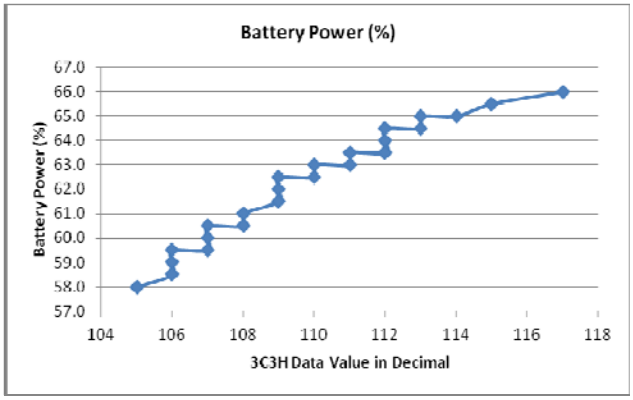


Figure 2. Relationship between value of 3C3H [1] and measured battery level in percentage

From Fig. 2 below, it indicates that 1H (1D) approximates equal to 1% of battery power. For example, when the data value of 3C3H is 6A (106 in decimal), the battery power is 59%, while the data value of 3C3H increases from 6A to 70 (from 106 to 112 in decimal), the battery power increases from 59% to 64%. From the above figure, we sketched a most fit line and calculated the approximate formula of battery level in percentage (B) using the CAN value of 3C3H [1] (x).

*B = 3C3H [1] (x) in decimal – 47*

In this way, we decipher the 45 CAN messages to obtain the battery level for the whole battery system and 88 individual battery cells.

### *3) Temperature*

As shown in Table V, there are 6 bytes of data in the first battery block related to temperature. There are 6 temperature sensors in each eight-cell block and the temperature is exhibited in the CAN messages for the self-diagnose system to make sure the battery system is not overheated or out of condition. Relationship between captured CAN value and measured temperature in degree Celsius is listed in Table VI. In total, we decipher the CAN messages for 66 battery temperatures from the 66 battery temperature sensors which are embedded in-between batteries.

TABLE V. CAPTURED DATA OF BATTERY TEMPERATURE FOR THE FIRST BATTERY BLOCK

| Message | Data |
|---|---|
| 611H | 01 00 **50 51** 01 5F 01 5F |
| 612H | 01 **50 50** 00 01 5F 01 5F |
| 613H | 01 **50 50** 00 01 5F 01 5F |
| 614H | 01 00 00 00 01 5F 01 5F |

TABLE VI. RELATIONSHIP BETWEEN CAPTURED CAN VALUE AND MEASURED TEMPERATURE IN DEGREE CELSIUS

| CAN values | Temperature (℃) |
|---|---|
| 50 | 30 |
| 51 | 31 |
| 52 | 32 |
| 53 | 33 |

From the table above, we can also deduce that
*Temperature in degree Celsius = the CAN value – 20*

## V. CONCLUSIONS AND RECOMMENDATIONS

In this research work, we apply the passive analysis strategy and adopt various methods into deciphering the main functions and battery condition of the electric vehicle. Throughout the project, we have gone deeper into the working of the automotive systems. We have deciphered the CAN messages for various main functions. For battery condition experiment, we have deciphered the 45 CAN messages about battery power for the whole battery system and 88 individual battery cells. We have also deciphered the CAN messages for 66 battery temperatures. Additionally, by reproducing the messages, we have attempted to gain control of some functions of vehicle. In this way, it would raise the concern of security issue with the vehicle.

We also have to deal with lots of difficulties and limitations. For example, when we tested the data under different panel shifts, we needed to apply foot brake for safety reasons. However, we did not keep the extent of the foot brake constant and did not know the extent of the foot brake would be shown in the message data either. Thus we mistook the message ID indicating the extent of foot brake as the message ID indicating shift panel at first. In addition,

we have not deciphered some message IDs which keep changing throughout the tests and which may suggest their relevance to the controlling of some basic functions. One way to overcome those limitations and difficulties is to search for more information on how vehicles function and all the effects of the conditions either visible or hidden before the experiment.

The deciphered CAN messages related to battery system may be used to improve battery management system via balancing the power of battery cells - this is another possible extension for further research.

## REFERENCES


[1] CANaerospace, Can introduction, available at: http://www.canaerospace.net/can_intro.pdf

[2] Future Crimes, 100 Cars Remotely Hacked: The Back-Door in Your Vehicle May Not Be the One You Think, available at: http://www.futurecrimes.com/article/100-cars-remotely-hacked-the-back-door-in-your-vehicle-may-not-be-the-one-you-think-2/

[3] Dr. Charlie Miller & Chris Valasek, Adventures in Automotive Networks and Control Units, available at: http://illmatics.com/car_hacking.pdf

[4] Kevin Poulsen, Hacker Disables More Than 100 Cars Remotely, available at: http://www.wired.com/threatlevel/2010/03/hacker-bricks-cars/