

В наших тяжелых российских условиях, когда нет доступа к фирменным деталям и диагностическому оборудованию, приходится довольствоваться "коленкой" и запчастями с разборки.

Одна из больших проблем возникает при замене и ремонте щитков приборов. Некоторые нюансы я опишу ниже.

1. BMW525i Simens ROM X2402PI

Эта машина обладает очень капризным характером, впервые мы столкнулись с такой проблемой, когда к нам приехала машина с мертвым щитком, с радующей глаз надписью CODE. Забегая вперед, скажу, причина в долгом игнорировании надписи INSPECTION, и часиков перед лицом водителя.

Вот пример прошивки чипа:

название машины BMW 520

VIN код WBAHB51040GG33360

показание спидометра 38874 мили

примечание:

неисп. датчик температуры и тахомет, звенит зуммер

□0000

□61

□60

□53

□10

□12

□0F

□FE

□FF

□DB

□78

□ 8D

□ 6C

□ 16

□ 02

□ FF

□ FF

□ 0010

□ FF

□ FF

□ FF

□ FF

□ FF

[FF

[FF

[FF

[00

[00

[08

[35

[93

[61

[D0

[FF

□020

□00

□00

□00

□00

□00

□00

□00

□00

□47

□47

□33

□ 36

□ 00

□ 01

□ 03

□ 5A

□ 0030

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 05

□ 42

□ FE

□ 4E

□ 24

□ 10

□ 01

□ C5

□ 0040

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 26

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 0050

□ 09

□ 8A

□ 68

□ 67

□ 69

□ 7A

□ DV

□ 65

□ BD

□ 31

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 0060

□63

□F4

□00

□00

□00

□00

□00

□00

□39

□40

□60

□80

□ 9F

□ BF

□ DF

□ FF

□ 0070

□ 64

□ F4

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ B7

□ B5

□ AC

□ 9A

□ 83

□ 65

□ 3C

□ 17

□ 0080

□ 65

□ F4

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ CD

□ 80

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 0090

□ 66

□ F4

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 5F

□ 42

□ 2E

□ 15

□ 0B

□ 00

□ 00

□ 00

□ 00A0

□ 5D

□ F4

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 29

□ 4B

□ 73

□ 9A

□ B5

□ C2

□ 3E

□ 02

□ 00B0

□ 5E

□ F4

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 78

□ 00

□ 00

□ 21

□ E0

□ 2E

□ 88

□ 8A

□ 00C0

□ 5F

□ F4

□00

□00

□00

□00

□00

□00

□DD

□01

□36

□01

□29

▣ 03

▣ CC

▣ 07

▣ 00D0

▣ 60

▣ F4

▣ 00

▣ 00

▣ 00

▣ 00

▣ 00

▣ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00E0

□ 61

□ F4

□ 00

□ 40

□ 51

□ 20

□ 00

□ 00

□ 00

□ 0C

□ 00

□ 00

□ 00

□ 00

□ 61

□ 20

□ 00F0

□ 62

□ F4

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□01

□11

□10

□10

□00

□00

□00

□39

Выявлено:

в ячейках

0028 47 47 33 36 00 vin GG33360

0018 00 00 08 35 93 61 номер щитка 8 359 361

003C 24 версия ключа

001F FF признак мили/км FF мили 06 км

002F 5A код процессора ; Когда не 5A парприз высвечивает CodE

0098 5F 42 2E 15 0B параметры термометра

00A3 00 00

00B3 00 00 Данные инспекцион и оил сервис

00C3 00 00

00D3 00 00

0008 делитель тахометра (1C - 3000 ОБ, BC - 500 ОБ, 5C - 900 ОБ при оборотах двигателя 800)

0060 63 F4 00 □

0070 64 F4 00 □ младшие 2 км спидометра

0080 65 F4 00 -

0090 66 F4 00

00A0 5D F4 00

00B0 5E F4 00

00C0 5F F4 00 0x00F45F = 62559 km - фактический километраж, без учета младшей части

00D0 60 F4 00

00E0 61 F4 00

00F0 62 F4 00

□ L-- старшие разряды спидометра

L----- младшие разряды спидометра

Для сравнения был взят дамп ПЗУ:

название машины BMW 524 TD

WIN код WBAHA51020BA80166

показание спидометра 180 177 km

□0000

□61

□60

□53

□10

□13

□0F

□FE

□FF

□BC

□78

□77

□55

□16

□02

□FF

□FF

□0010

□FF

□ FF

□ FF

□ FF

□ FF

□ FF

□ FF

□ FF

□ 00

□ 00

□ 08

□ 35

□ 93

□ 62

□ A0

□ 06

□ 0020

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 42

□ 4C

□ 40

□ 10

□ 80

□ 01

□ 04

□ 5A

□ 0030

□ 00

□ 00

□00

□00

□00

□00

□00

□00

□78

□FF

□16

□02

□12

□38

□92

□A7

□0040

□00

□00

□00

□00

□00

□00

□00

□00

□ 25

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 0050

□ 04

□ 8A

□ 7A

□ DV

□ 50

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 0060

□ 98

□ BF

□ 02

□ 00

□ 00

□ 00

□ 00

□ 00

□39

□40

□60

□80

□9F

□BF

□DF

□FF

□0070

□99

□BF

□02

□ 00

□ 00

□ 00

□ 00

□ 00

□ B7

□ B5

□ AC

□ 9A

□ 83

□ 65

□ 3C

□ 17

□ 0080

□ 90

□ BF

□ 02

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 2B

□ 73

□ 8C

□ FF

□ 00

□ 00

□ 00

□ 0090

□ 91

□ BF

□ 02

▣00

▣00

▣00

▣00

▣00

▣5F

▣42

▣2E

▣15

▣0B

▣00

▣00

□ 00

□ 00A0

□ 92

□ BF

□ 02

□ 00

□ 00

□ 20

□ 00

□ 00

□ 29

□4B

□73

□9A

□B5

□C2

□3E

□02

□00B0

□93

□BF

□02

□00

□ 00

□ 00

□ 00

□ 00

□ 96

□ 00

□ 00

□ 31

□ 10

□ 27

□ 88

□ 8A

□ 00C0

□ 94

□ BF

□ 02

□ 00

□ 00

□ 00

□ 00

□ 00

□ DD

□ 01

□ 57

□ 01

□ 3E

□ 03

□ F1

□ 06

□ 00D0

□ 95

□ BF

□ 02

□ 00

□ 00

□ 00

□ 00

□ 00

□ 30

□ 91

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00E0

□ 96

□ BF

□ 02

□ 80

□ 3E

□ 20

□ 00

□ 00

□ 00

□ 4E

□ 00

□ 00

□ 00

□ 00

□ 41

□ 25

□ 00F0

□ 97

□ BF

□ 02

□ 00

□ 00

□ 00

□ 00

□ 00

□ FF

□ FF

□ FF

□ FF

□ FF

□ 0A

□ 38

□ 97

Из этого дампа была переставлена строка:

0088 00 2B 73 8C FF

После перестановки термометр заработал корректно

Необходимо помнить, что все изменения в данных приводят к появлению ошибки 05 - false programming, устранить которую вы не сможете.

Вторая неприятность, которая вылезает примерно на 6 - 7 году службы автомобиля, превышение количества циклов записи EEPROM, здесь автоматом упираться в покупку нового чипа, поскольку чипы других производителей категорически или втихоря работать отказываются.

2. BOSCH BMW 730 ROM 9346

Пример прошивки

□ 0000

□ 11

□ FF

□ 5F

□ BF

□ A8

□ 82

□ D3

□ 47

□ E2

□ 00

□ 13

□ FF

□ 26

□ 8D

□ 4F

□ 73

□ 0010

□ 6E

□ 2B

□ D3

□ 00

□ 4A

□16

□F9

□E9

□5A

□C6

□AD

□38

□53

□D0

□00

□78

□0020

□ 00

□ 00

□ FF

□ 4F

□ 00

□ 1A

□ FF

□ 00

□ 98

□ 78

□ 50

□35

□10

□12

□63

□AF

□0030

□CB

□EA

□20

□00

□CB

□69

□ 23

□ 03

□ FF

□ FF

□ 92

□ 85

□ 5

□ 36

□ 95

□ 59

□ 0040

□ 31

□ 38

□ FF

□ 08

□ 00

□ 6A

□ D2

□ F0

□ D2

□ FA

□ D3

□ 04

□D3

□pE

□D3

□18

□0050

□D3

□22

□D3

□2C

□D2

□E6

□91

□EA

□32

□28

□FF

□FF

□91

□EA

□23

□47

□0060

□23

□ 46

□ 23

□ 46

□ 23

□ 46

□ 23

□ 46

□ 23

□ 46

□ 23

□ 46

□23

□46

□23

□46

□0070

□23

□46

□23

□46

□23

□46

□23

□46

□23

□46

□23

□46

□23

□46

□08

□FF

0xDF,0xE1,0xE3,0xE5,0xE7,0xE9,0xEB,0xED □ 0xEF,0xF1,0xF3,0xF5,0xF7,0xF9,0xFB,0xFD

- старшие разряды длинного счетчика. Увеличение байта на 1 увеличивает пробег примерно на 8000 Км.

003C, 003B, 003A - 58592 номер кузова

1-я буква по адресу 3D младший полубайт 5-B,7-C,9-D,...f-G

2-я буква по адресу 3C старший полубайт 1-A,2-B,3-C,...7-G

Сюрпризов не обнаружено, но кто знает.

3.BMW 316- 318 1994 г EEPROM 93LC56

счетчик пробега 215 740 Км

номер двигателя 387413 1

номер кузова 37204 4

0000 02C8 FD37 006E 788D A2CC 83E8 8721 0B5C

0010 0050 1400 3714 5325 8B4B BC70 EF9D 210D

0020 4F30 9671 0202 0202 2350 01C0 2850 FF50

0030 3111 9227 B054 D854 E77F DBFF A000 0000

0040 1310 **3874** 0022 **7204** 55C3 04FF 143C 111A

0050 0000 0000 0000 0402 FFFF FFFF 4077 2991

0060 C72B 1115 0000 0044 0000 0000 0000 3200

0070 0000 0000 3610 FFFF FFFF 47FF A739 FF00

0080 **F6E3 F6E4 F6E4 F6E4 F6E4 F6E4 F6E4 F6E4 F6E4**

0090 **F6E4 F6E4 F6E4 F6E4 F6E4 F6E4 F6E4 F6E4 F6E4**

00A0 FFB0 FFB0 FFB0 FFB0 FFB0 FFB0 FFB0 FFB0 FFB0

00B0 FE1F FE1A FFA2 FFFF FFFF FFFF FFFF FFFF

00C0 FFFF 7806 591A 5B6A 00F0 0000 0000 0000

00D0 0000 0000 FDEE 0F0F FF0F FFFF FFFF FFFF

00E0 FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF

00F0 FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF

0042, 0043, 0040 - номер двигателя

0049, 0046, 0047 - номер кузова

0081, 0083, 0085, 0087....008F, 0091, 0093, 0095, 0097....009F - старшие разряды
длинного счетчика. Увеличение байта на 1 уменьшает пробег примерно на 8 000
Км

0080, 0082, 0084, 0086....008F - средние разряды длинного счетчика

ПЗУ, с адреса 0000 до адреса 0060 защищена контрольной суммой. Любое изменение в этой области приводит к надписи PPPPP на индикаторе.

Adr 0060:C72B - 2х байтовое слово коррекции контрольной суммы

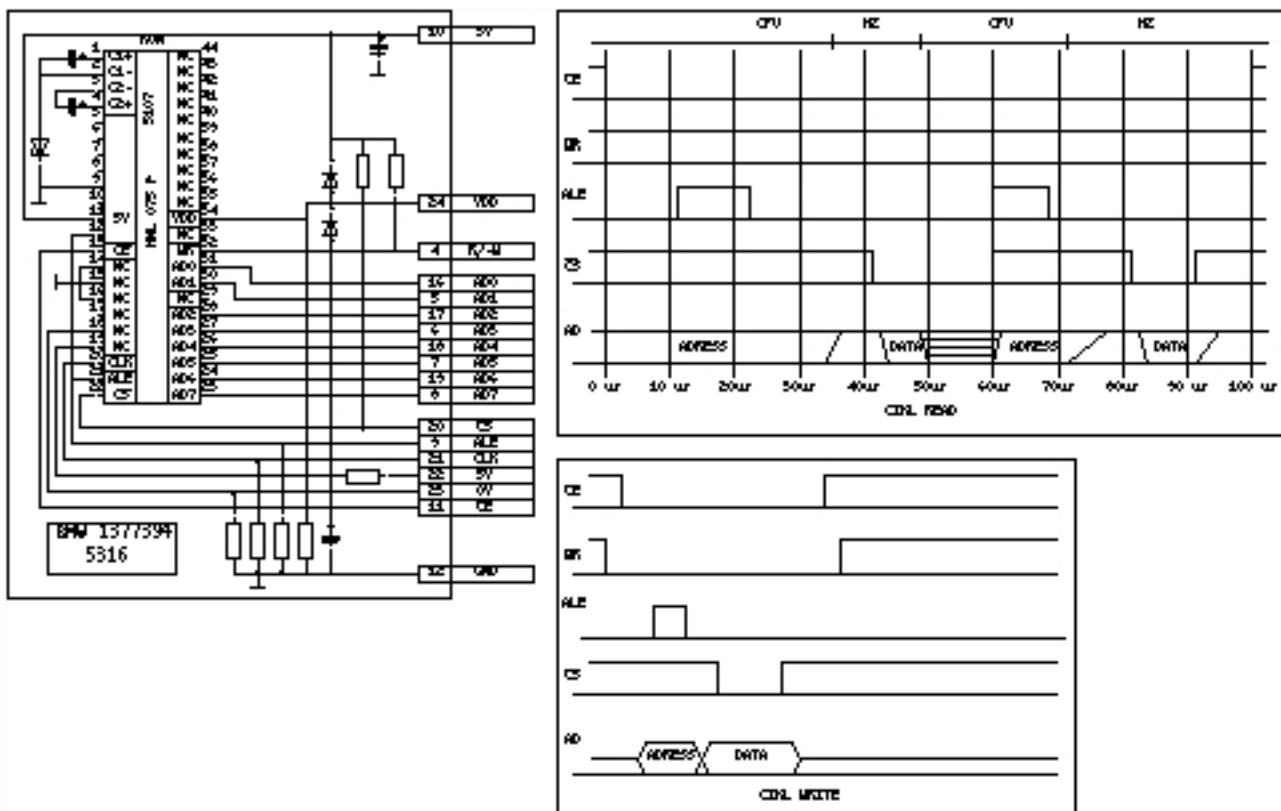
Контрольная сумма вычисляется как XOR 2х байтовых значений с адр 0000 до

адреса 005F и в месте с адресом 0060 дает значение 7F7F

Пример $02C8 \wedge FD37 \wedge 006E \wedge \dots \wedge 2991 \wedge C72B = 7F7F$

Пример программы корректировки бинарного файла "[xor.cpp](#)"

Данная программа корректирует дамп под контрольное число 0x7F7F, но необходимо учитывать, что могут быть другие контрольные числа. Просчитайте это число до внесения изменений, дабы не поиметь больших проблем.



4. Самый загадочный щиток с чипом в разъеме по имени HML 075 F

M/C HML075F представляет собой по видимому ПЛМ со встроенной FLASH.

M/C читается как область памяти 256x16, причем ст и мл байты читаются одинаково. В ней также содержится переписываемая область inspection, и аппаратный счетчик пробега с автосохранением данных в EEPROM

Пример прошивки для спидометра 292985 км приведена ниже.

Все данные представлены одним байтом, т.к. нет смысла повторять второй идентичный байт который однако обязателен к чтению, иначе произойдет пропуск данных.

Таблица 1

□0000

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

0010

7F

7F

7F

7F

7F

7F

7F

7F

7F

7F

7F

□7F

□7F

□7F

□7F

□7F

□0020

□FF

□FF

□FF

□FF

□FF

▣FF

▣FF

▣FF

▣FF

▣FF

▣FF

▣FF

▣FF

▣FF

▣FF

▣FF

▣030

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□040

□00

□00

□00

□00

□00

□00

□ 1D

□ FF

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 1D

□ FF

□ 0050

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 1D

□ FF

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 1D

□ FF

□ 0060

□ FF

□ FF

□ FF

□ FF

□ FF

□ FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□070

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□080

□95

□F6

□C0

□5D

□B9

□01

□0A

□ 05

□ 4B

□ 13

□ 26

□ 4F

□ 6E

□ D3

□ FF

□ BF

□ 0090

□ 82

□47

□00

□1A

□00

□3F

□64

□00

□00

□00

□98

□78

□50

□35

□10

□12

□00A0

□63

□AF

□CB

□EA

□25

□05

□CB

□ 90

□ 01

□ 88

□ 11

□ 5F

□ A8

□ D3

□ E2

□ F8

□ 00B0

□ 14

□ EC

□pE

□D3

□p9

□AA

□p5

□7A

□p2

□p6

□p0

□p0

□4E

□55

□AA

□83

□00C0

□52

□20

□35

□97

□52

□20

□35

□97

□52

□20

□35

□97

□52

□20

□35

□97

□00D0

□52

□20

□35

□97

□52

□20

□35

□97

□52

□20

□35

□97

□52

□20

□ 35

□ 97

□ 00E0

□ FF

□ FF

□ FF

□ FF

□ FF

□ FF

□ FF

□ FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□00F0

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

□FF

Область 0040 - 0050h inspection, читается и пишется как 8 байт информации помноженные на 4 (0040 - 0047; 0047 - 004F; 0050 - 0057; 0058 - 005F) взаимосвязанных области, запись любого байта в любой области приведет к изменению соотв байта в остальных областях.

Это единственная область доступная по записи.

□040

□00

□00

□00

□00

□ 00

□ 00

□ 1D

□ FF

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 1D

□ FF

□ 0050

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 1D

□ FF

□ 00

□ 00

□ 00

□ 00

□ 00

□ 00

□ 1D

□ FF

Область 0080 - 00BF: служебная, изменение информации приводит к отказу панели работать с чипом.

□ 0080

□ 95

□ F6

□C0

□5D

□B9

□01

□0A

□05

□4B

□13

□26

□4F

□6E

□ D3

□ FF

□ BF

□ 0090

□ 82

□ 47

□ 00

□ 1A

□ 00

□ 3F

□ 64

□ 00

□ 00

□ 00

□ 98

□ 78

□ 50

□ 35

□ 10

□ 12

□ 00A0

□ 63

□ AF

□ CB

□ EA

□ 25

□ 05

□ CB

□ 90

□ 01

□ 88

□ 11

□ 5F

□ A8

□ D3

□ E2

□ F8

□ 00B0

□ 14

□ EC

□ 0E

□ D3

□ 09

□ AA

□ 05

□ 7A

□02

□06

□00

□00

□4E

□55

□AA

□83

Область 00C0 - 00DF непосредственно спидометр. Нарращивание показаний по тактам на входе CLK (455 импульсов на 100 м).

□00C0

□52

□ 20

□ 35

□ 97

□ 52

□ 20

□ 35

□ 97

□ 52

□ 20

□ 35

□ 97

□ 52

□ 20

□ 35

□ 97

□ 00D0

□ 52

□ 20

□ 35

□ 97

□ 52

□ 20

□ 35

□ 97

□ 52

□ 20

□ 35

□ 97

□ 52

□ 20

□ 35

□ 97

Пример расшифровки спидометра

□ 5

□ 2

□ 2

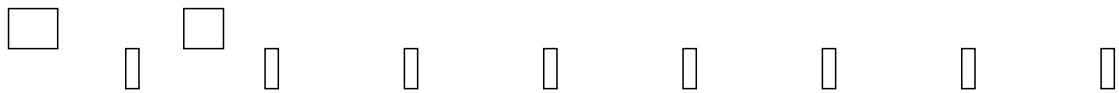
□ 0

□ 3

□ 5

□ 9

□ 7



□ not used

□ - 40 km = счетчику пробега

□

□ km x 10 000

□

□ km x 1 000

□

km x 100

km x 10

km x 1

km x 100 00

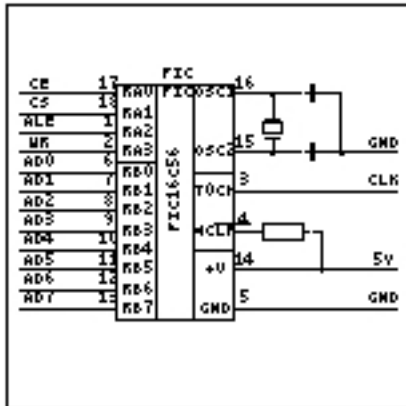
km x 0.1

Была попытка смотки спидометра методом его переброски через 0, подачей вход CLK импульсов КМОП уровня с частотой 100 кГц (эквивалентно скорости 000 км/ч). на 60

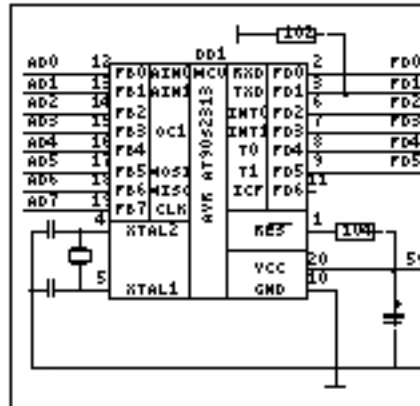
Первая попытка прошла удачно, но все последующие приводили к остановке счетчика пробега на значении 299 960 км (300 000 внутреннее значение).

Для работы с этим типом панелей были сделаны два эмулятора, один на PIC16C84(раскачан до 12 мГц), второй на ATMEL AVR90S2313.

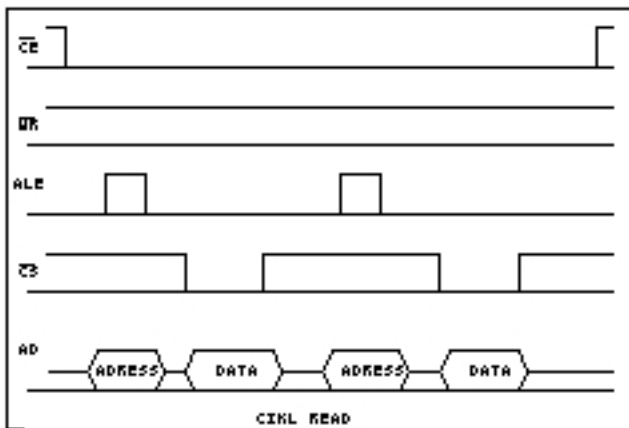
□ Как победить щиток прибора BMW.



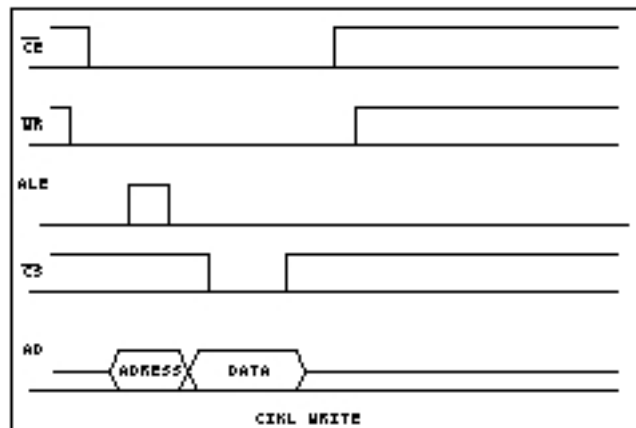
5V	10	5V	30
	22	5V	15
	24	VDD	
	23	0V	
AD0	16	AD0	
AD1	5	AD1	
AD2	17	AD2	
AD3	6	AD3	
AD4	18	AD4	
AD5	7	AD5	
AD6	19	AD6	
AD7	8	AD7	
WR	4	R/-M	
ALE	9	ALE	
CE	11	CE	
CS	20	CS	
CLK	21	CLR	
GND	12	GND	



5V	10	5V	30
FD1	22	5V	15
	24	VDD	
	23	0V	
AD0	16	AD0	
AD1	5	AD1	
AD2	17	AD2	
AD3	6	AD3	
AD4	18	AD4	
AD5	7	AD5	
AD6	19	AD6	
AD7	8	AD7	
FD0	4	R/-M	
FD1	9	ALE	
FD2	11	CE	
FD3	20	CS	
FD5	21	CLK	
	12	GND	



CYCLE READ



CYCLE WRITE

Адреса и данные изображены в виде



Ну а без этого никак не обойтись, поэтому рекомендую посмотреть видео на support@diakom.ru Удачи.