

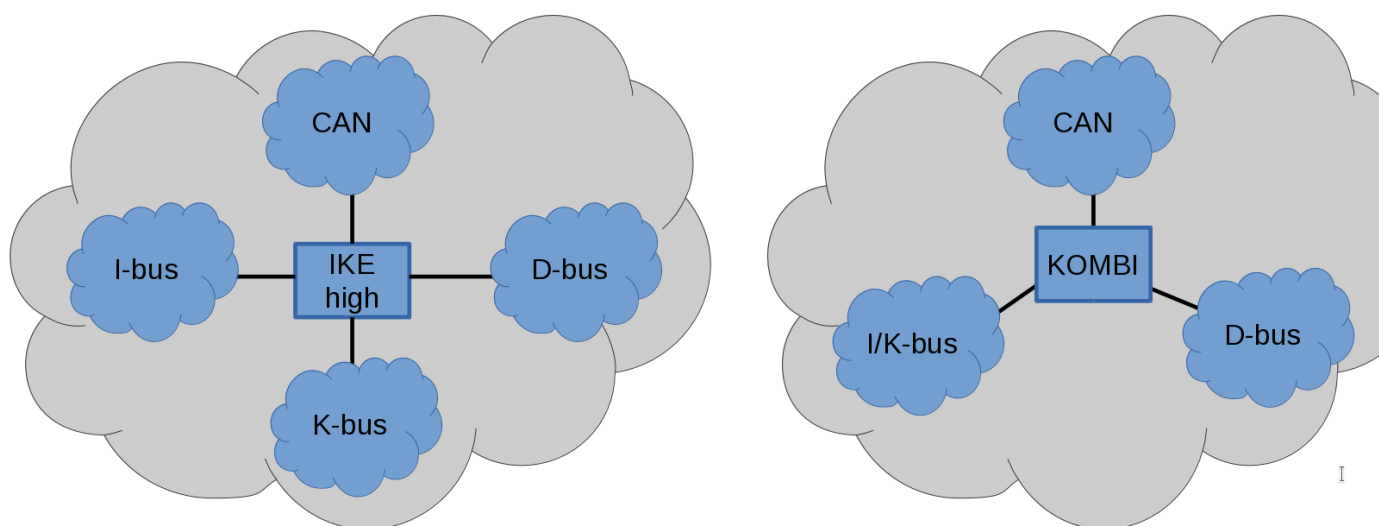
 kvova 13 июня 2016 в 08:53

Протокол управления CD-чейнджером

Реверс-инжиниринг, Программирование микроконтроллеров

Продолжаем начатое. В этот раз я расскажу о том, что содержится в полезной нагрузке кадра I/K-bus, кратко об устройстве информационно-развлекательной системы BMW e38, e39, e46, e53, и рассмотрим подробнее работу протокола на примере чейнджера компакт-дисков.

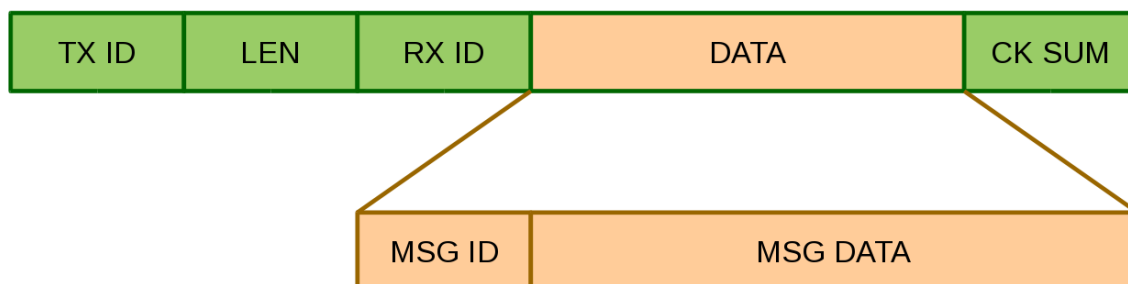
По логике вещей каналный уровень содержит в своих данных протоколы более высокого уровня. В I/K-bus так и происходит, только в нем протоколы сетевого и транспортного уровней на подобие TCP/IP. В кадре нигде нет информации об адресе сети, но межсетевое взаимодействие возможно. Выполняется оно посредством шлюза, который выполнен в блоке комбинации приборов. Суть работы шлюза проста — он знает в какой сети расположен тот или иной блок, в соответствии с этим пересылает кадр в другую сеть, если отправитель и получатель находятся в разных. Таким образом обеспечивается межсетевое взаимодействие на канальном уровне будто это единый сегмент сети. Рисунок ниже иллюстрирует подключение сетей в общей системе взаимодействия блоков управления.



Следует уточнить, что левая схема справедлива для кузовов e38 и e39, e53 с блоком комбинации приборов повышенной функциональности (IKE high). В e39, e53 с базовым блоком комбинации приборов (KOMBI), а также в e46 шины I-bus и K-bus физически объединены в одну.

D-bus — это диагностическая шина (k-line). По ней подключается диагностическое оборудование. Эта шина не имеет физического подключения ко всем блокам управления, но через шлюз в IKE/KOMBI задача взаимодействия обеспечивается в полной мере. Для примера блок навигации подключён только к I-bus, но с помощью сервисного/диагностического оборудования мы можем считывать сервисную информацию, ошибки и производить кодирование.

То что содержится в полезной нагрузке кадра I/K-bus, я буду называть протоколом прикладного уровня. В основе своей он состоит из двух частей. MSG ID — идентификатор сообщения, занимает один символ. MSG DATA — информация дополняющая сообщение, может отсутствовать вовсе или занимать до 32 символов. На следующем рисунке показано, как это выглядит:

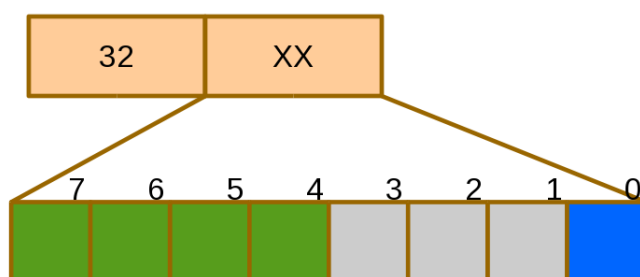


Так как символ состоит из 8 бит, получается возможных вариаций команд (CMD ID) 256. Немало, наверное даже с запасом, и мне извест

далеко не все. Но на некоторых ключевых я остановлю внимание.

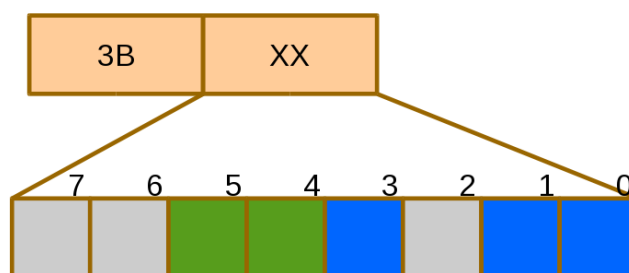
Сообщение с идентификатором MSG ID = **01** — запрос состояния устройства. Прежде чем взаимодействовать с каким-либо устройством необходимо убедиться в его наличии и исправности. Эта команда отправляется устройству, в состоянии которого необходимо убедиться этом поле MSG DATA не заполняется. Чтобы информация о состоянии устройств была актуальна все время, команда повторяется периодически. Рассмотрим этот вид сообщения на примере кадра **68 03 18 01 72** (здесь и далее содержимое кадра обозначается будучи цифрами в шестнадцатеричном исчислении). Кадр отправляется от радиоприёмника (идентификатор устройства **68**) к CD чейнджеру (**1** запросом о состоянии (идентификатор сообщения MSG ID = **01**). CD чейнджер, если он есть и исправен, отвечает сообщением, подтверждающим статус готовности (MSG ID = **02**). Полный фрагмент ответного кадра **18 04 FF 02 00 E1**. Ответ вещается всем в локальную сеть, так как адрес получателя **FF**. Здесь помимо идентификатора сообщения передаются дополнительные данные — MSG DATA = **00**. Если значение данных равно **01**, то это означает что устройство только включилось и это его первое сообщение о готовности. Такой вариант диалога наблюдается между многими блоками управления.

Управление воспроизведением музыкальных треков, радиостанций или изменение уровня громкости возможно как с рулевого колеса так центральной консоли. Эти органы управления передают информацию на радиоприёмник по той же I-bus. Сообщения регулировки уровня громкости идентифицируются номером **32**, а в данных содержится управляющая информация. Ниже приведена структура этого сообщения.



Данные состоят из одного байта, в котором синий бит отвечает за направление изменения уровня: 0 — убавить, 1 — добавить. А зелёные показывают силу относительного изменения от 1 до 15 дискретных уровней. Например кадр, отправляемый при нажатии клавиши «+» на рулевом колесе, выглядит так **50 04 68 32 11 1F**. Это сообщение заставляет радиоприёмник увеличить громкость на 1 дискретный уровень. Если резко крутнуть барашку управления громкости на центральной консоли по часовой стрелке, то в шину будет отправлен кадр **C0 C3 32 91 0F**. Здесь мультиинформационный дисплей сообщает о требовании увеличить громкость на 9 дискретных уровней.

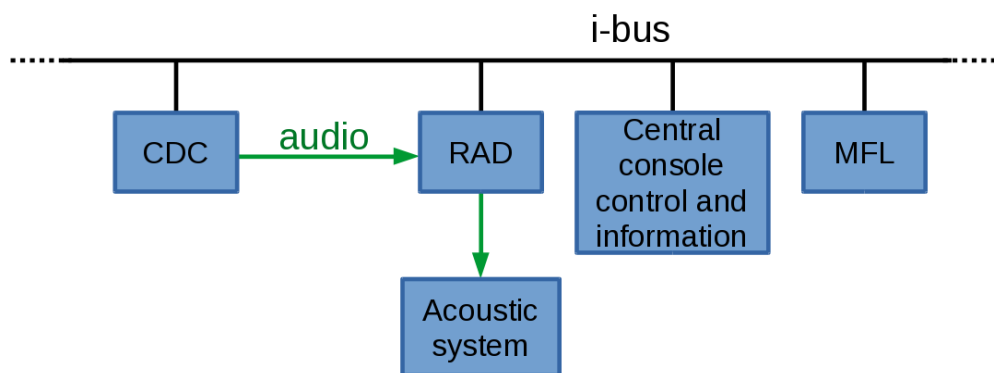
Для кнопочного управления характерны три вида сообщения: кнопка нажата, кнопка удерживается длительное время и кнопка отпущена. В данных сообщения, кроме состояния кнопки, передаётся её идентификатор. Например сообщение с MSG ID = **3B** означает, что передаётся информация об изменении состояния кнопок на рулевом колесе, отвечающих за управление радиоприёмником и телефоном. MSG DATA состоит из одного символа и содержит информацию о кнопке, подвергшейся воздействию.



В битах синего цвета обозначается кнопка. Если это 0-й бит, то было воздействие на кнопку «поиск вверх». Если 1-й бит, то кнопка «R/T». Если 3-й бит, то кнопка «поиск вниз». В битовой области зелёного цвета обозначается состояние кнопки. Если все биты равны 0, то это значит что кнопка нажата. Если 4-й бит равен 1, то было длительное удержание кнопки. Если 5-бит равен 1, то кнопка была отпущена. Рассмотрим ситуацию, когда мы переключаем музыкальный трек на следующий при нажатии кнопки на руле. В шину будет послано с небольшим интервалом два кадра: **50 04 68 3B 01 06** и **50 04 68 3B 21 26**. Первый кадр сообщает, что была нажата кнопка «поиск вверх». Второй сообщает, что была отпущена кнопка «поиск вверх».

Для кнопочного управления на центральной консоли, будь то мультиинформационный дисплей или бортовой монитор, подход тот же — передаётся информация об идентификаторе кнопки и её состоянии. Но структура сообщения построена по иному.

Теперь рассмотрим в общем как устроена информационно-развлекательная система на автомобилях e38, e39, e53. А именно та её часть отвечающая за воспроизведение музыки и радио. На рисунке ниже я представил схематично устройство этой части системы.



Центральную роль тут занимает радиоприёмник (RAD). Дело в том, что помимо функций приёма эфирных станций, этот блок выполняет функции усилителя. Если автомобиль не оборудован бортовым монитором, то в корпусе радиоприёмника располагается кассетный или проигрыватель. В таком варианте он располагается в центральной консоли. Если же автомобиль укомплектован бортовым монитором, то радиоприёмник располагается в багажном отделении и дооборудован аудио входом для кассетного проигрывателя. Кассетный проигрыватель вмонтирован в бортовой монитор.

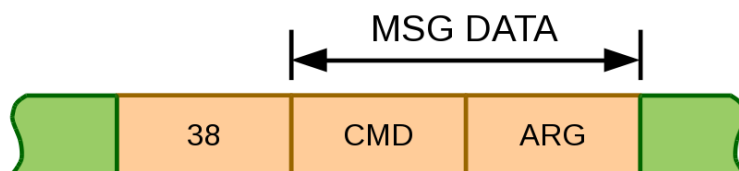
Акустическая система может быть в трёх исполнениях: простая стереосистема, Hi-Fi или Top Hi-Fi. В первом случае радиоприёмник непосредственно подключён к динамикам. В Hi-Fi акустической системе динамиков больше и они подключены к радиоприёмнику через дополнительный усилитель. Такой усилитель помимо повышения мощности аудио сигнала выполняет функции активной эквалаизации под автомобильную акустику и разделяет звук на диапазоны для соответствующих динамиков. Система top Hi-Fi ещё круче. В ней помимо всего выше перечисленного присутствует сабвуфер, а усилитель выполняет эквалаизацию в зависимости от скорости автомобиля, тем самым компенсируется шумность салона. Так же система дополнена эффектом объёмного звучания.

Отображение информации о выбранном источнике воспроизведения, номере трека, частоте радиостанции и прочее, а также управление выполняется на центральной консоли посредством бортового монитора или мультимедийного дисплея или чего-то ещё. Чтобы не отвлекаться от управления автомобилем, управление воспроизведением аудио может быть выполнено на многофункциональном рулевом колесе (MFL), о котором упоминалось выше.

CD-чейнджер (CDC) выполнен как дополнение к радиоприёмнику. Обмен управляющими командами и ответами производится только между радиоприёмником и CD-чейнджером. Делается это по I-bus, как видно на схеме. Аудио сигнал в аналоговой форме передаётся на линейный вход радиоприёмника, где усиливается и поступает далее на акустическую систему. Если акустическая система top Hi-Fi, то сигнал от CDC подаётся напрямую к усилителю в цифровой форме.

Теперь рассмотрим подробнее непосредственно сам диалог CD-чейнджера и радиоприёмника по шине I/K-bus. Как было описано ранее радиоприёмник периодически отправляет запросы о статусе CD-чейнджера. Если такой присутствует в автомобиле и он исправен, то незамедлительно в шину будет отослан ответ о присутствии. Получив ответ, радиоприёмник формирует в меню на центральной консоли дополнительный режим воспроизведения, в котором источником является CD-чейнджер. Водителю остаётся только нажать соответствующую кнопку, чтобы радиоприёмник запустил воспроизведение с CD-чейнджера, получил информацию о загруженном компакт диске, номер трека и отобразил эту информацию на центральной консоли.

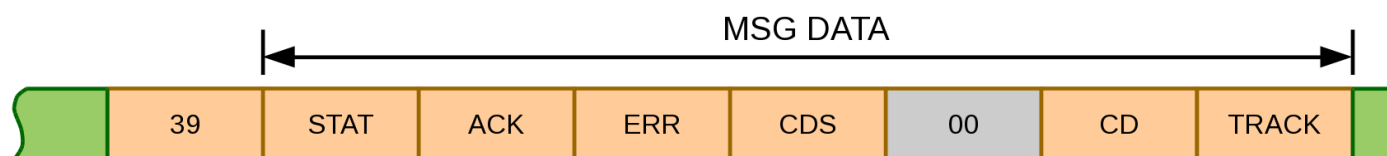
Управление воспроизведением CD-чейнджера выполняется сообщением с идентификатором MSG ID = **38**. Структура сообщения следующая:



Как видно, сообщение простое по структуре и содержит два ключевых параметра: CMD и ARG. В CMD передаётся код требуемого режима воспроизведения, а в ARG дополнительные данные. Для наглядности и простоты понимания, ниже представлена таблица, в которую сведены мне известные команды:

Наименование команды	Идентификатор команды (CMD), hex	Дополнительный аргумент (ARG), hex	Дополнительно
Запрос на текущее состояние	00	не учитывается	REFRESH
Остановить воспроизведение	01	не учитывается	STOP
Перевести воспроизведение на паузу	02	не учитывается	PAUSE
Начать воспроизведение	03	не учитывается	PLAY
Перемотка	04	00 — обратно	REWIND
		01 — вперёд	FAST FORWARD
Сменить трек	05	00 — следующий	NEXT
		01 — предыдущий	PREVIOUS
Сменить диск	06	Соответствует номеру требуемого диска	DISC
Режим сканирования треков (демонстрирования плейлиста)	07	00 — отключить	SCAN OFF
		01 — включить	SCAN ON
Режим случайного выбора треков	08	00 — отключить	RANDOM OFF
		01 — включить	RANDOM ON
	09		
Сменить трек	0A	00 — следующий	NEXT
		01 — предыдущий	PREVIOUS

Таким образом выполняется управление CD-чейнджером, а тот в свою очередь поддерживает обратную связь сообщениями с идентификатором 39:



В данном сообщении передаётся состояние CD-чейнджера и его режим воспроизведения. Более подробно о каждом символе сообщен следующей таблице:

Наименование символа сообщения	Описание	Возможные значения, hex
STAT	Сообщает о режиме проигрывателя	00 — STOP
		01 — PAUSE
		02 — PLAY
		03 — FAST FORWARD
		04 — REWIND
		07 — END
		08 — LOAD
		09 — CD CHECK
		0A — NO MAGAZINE
ACK	Индикатор текущего состояния воспроизведения	02 — молчание
		09 — обычное воспроизведение
		19 — воспроизведение в режиме сканирования треков
		29 — воспроизведение в случайном порядке
ERR	Маска ошибок	0-й бит — перегрев
		1-й бит — ошибка диска
		2-й бит — диск не найден
		3-й бит — диски не найдены
CDS	Маска загруженных дисков	0-й бит — первый диск
		1-й бит — второй диск
		2-й бит — третий диск
		3-й бит — четвертый диск
		4-й бит — пятый диск
		5-й бит — шестой диск
00	Неизвестно	всегда 0
CD	Номер текущего диска	значение в диапазоне возможного количества дисков, т.е. от 1 до 6
TRACK	Номер текущего трека	Двухзначное число в десятичном виде

Следует отметить, что есть команды управления от радиоприёмника, на которые CD-чейнджер должен отсылать незамедлительный ответ подтверждение принятия команды, иначе команды будут отправляться по таймауту 500 мс повторно. К таким командам относятся: «начать воспроизведение», «остановить воспроизведение», «перемотка», «режим случайного выбора треков» и «режим сканирования треков». Получив команду с соответствующим идентификатором CMD, CD-чейнджер на требуемый запрос изменяет индикатор состояния и отсылает сообщение радиоприёмнику. В случае команды «перемотка» индикатор остаётся в режиме простого проигрывания, только меняется статус на «FAST FORWARD» или «REWIND». Радиоприемник успокаивается, что команда принята успешно и перестаёт бомбить повторными сообщениями.

Далее хочу привести лог трафика I/K-bus, где к шине подключены три устройства: мультиинформационный дисплей, радиоприемник и программный эмулятор CD-чейнджера. Эту простую сеть я собрал у себя на столе, чтобы проводить анализ работы взаимодействия блока управления и отлаживать программный CD-чейнджер.

```
1464451769.645053 18 04 FF 02 00 E1
1464451773.449266 18 04 FF 02 00 E1
1464451774.095554 C0 06 68 31 00 00 0C 93
1464451774.246175 C0 06 68 31 00 00 4C D3
1464451774.260696 68 05 18 38 0A 01 46
1464451774.609043 18 0A 68 39 02 09 00 01 00 01 00 48
1464451774.627934 C0 03 80 01 42
1464451776.518986 C0 06 68 31 00 00 0D 92
1464451777.130483 C0 03 68 01 AA
1464451777.137252 68 04 FF 02 00 91
1464451777.252071 18 04 FF 02 00 E1
1464451777.261962 C0 06 68 31 00 00 2D B2
1464451777.279240 68 05 18 38 04 01 48
1464451777.324026 18 0A 68 39 03 09 00 01 00 01 00 49
1464451777.343397 68 10 C0 23 C0 20 43 44 20 31 2D 20 20 20 20 BC BC 40
1464451778.719662 68 03 18 01 72
1464451778.754030 18 04 FF 02 00 E1
1464451780.357435 C0 06 68 31 00 00 4D D2
1464451780.372239 68 05 18 38 03 00 4E
1464451780.425673 68 10 C0 23 C0 20 43 44 20 31 2D 20 20 20 20 20 20 40
1464451780.476647 18 0A 68 39 02 09 00 01 00 01 00 48
1464451781.053624 18 04 FF 02 00 E1
1464451784.607437 C0 06 68 31 00 00 09 96
1464451784.624009 68 05 18 38 08 01 44
1464451784.653874 68 10 C0 23 C0 20 43 44 20 31 2D 20 20 20 52 4E 44 38
1464451784.676392 C0 03 80 01 42
1464451784.699230 68 0A C0 21 00 00 09 2A 52 4E 44 F8
1464451784.712321 C0 04 68 22 00 8E
1464451784.753545 18 0A 68 39 02 29 00 01 00 01 00 68
1464451784.788999 C0 06 68 31 00 00 49 D6
1464451784.854543 18 04 FF 02 00 E1
1464451786.873157 C0 06 68 31 00 00 09 96
1464451786.888385 68 05 18 38 08 00 45
1464451786.933176 18 0A 68 39 02 09 00 01 00 01 00 48
1464451786.953783 68 10 C0 23 C0 20 43 44 20 31 2D 20 20 20 20 20 20 40
1464451786.968580 68 0A C0 21 00 00 09 20 52 4E 44 F2
1464451786.991598 C0 04 68 22 00 8E
1464451787.060769 C0 06 68 31 00 00 49 D6
1464451787.130785 C0 03 68 01 AA
1464451787.137541 68 04 FF 02 00 91
```

Цветом здесь выделены сообщения управления CD-чейнджером и ответы на них.

- Желтый — это переключение на предыдущий трек.
- Зеленый — включение и выключение перемотки
- Синий — включение и выключение режима произведения треков в случайном порядке.

Подводя итог, хочу сказать, что применив данный протокол на простейшем программно-аппаратном решении, можно «легально» вкли в штатную информационно-развлекательную систему автомобиля. Как самый простой пример создать свой функциональный по современным меркам медиа проигрыватель, который будет получать управляющие команды с рулевого колеса, центральной консоли и издавать звучание по штатной акустической системе.

Испльзованные источники:

- Bus System Troubleshooting, 2001
- I-BUS Inside, Franck Touanen, 2002

Метки: [bmw](#), [i-bus](#)

↑

+13

↓

🔖

55

👁

12k

💬

9

17,0

0,0

24

Карма

Рейтинг

Подписчики

Владимир Король @kvova

Инженер-программист

Github

Поделиться публикацией

21.02.2018

Протокол управления CD-чейнджером / Хабрахабр

ПОХОЖИЕ ПУБЛИКАЦИИ

16 июня 2014 в 21:44

Nissan и BMW присоединятся к планам Tesla по развитию электрозаправок

↑ +49

👁 27,9k

📌 31

💬 123

24 апреля 2014 в 15:15

Пользовательские типы в Qt по D-Bus

↑ +6

👁 6,7k

📌 32

💬 2

1 октября 2013 в 19:03

BMW Connected Drive как тренд

↑ +17

👁 28,8k

📌 19

💬 87

ЗАКАЗЫ ДЛЯ ФРИЛАНСЕРОВ	Фриланс
Контекстная реклама в Яндекс.Директ 21.02.2018 • 0 откликов	Цена догово
Написать обработку для загрузки XML-файла из сторонней системы в 1C 21.02.2018 • 1 отклик	5000 руб./за пр
Js 21.02.2018 • 1 отклик	Цена догово
Все заказы	<div>Зарегистрироваться</div> <div>Разместить з</div>



Реклама

Комментарии 9

- DAT540

13.06.16 в 22:59

🔒

📌

↑

В радиомодуле BM54 появилось расширение данного протокола, при подключении CDC 7го и выше годов, умеющего играть MP3 диски, данное расширение обеспечивает передачу данных о MP3 тэгах. Вот хотелось бы найти информацию об этом расширении. Ну или хотя бы машину стар 7го года и помониторить шину на предмет протоколирования этого протокола. Ни у кого нет инфы?
- kvova

14.06.16 в 07:15

🔒

📌

🔗

🔄

↑

Мне никогда не попадались такие CDC, только китайские эмуляторы, которые воспроизводят MP3 с USB носителя. Но они шлют тэги от имен телефонного аппарата на приборную панель.
- DAT540

14.06.16 в 13:34

🔒

📌

🔗

🔄

↑

Если поискать, можно найти на разборках, но барыги знают про них и цену ломают совершенно не гуманную. Либо ебау, но там они тоже не дешевы.
- gryberg

14.06.16 в 15:38

🔒

📌

↑

Недавно занимался ревер-инжинерингом протокола P-Bus от того же Pioneer и даже «вклинился» в штатную систему. Протокол очень похожий кстати, да и на некоторых e38 ставились именно P-Bus changer-ы
- kvova

14.06.16 в 18:08

🔒

📌

🔗

🔄

↑

Про P-Bus changer-ы не слышал. В BMW WDS документации P-Bus называется «Периферийная шина», используется на кузовах e38, e39, e53 помощью нее осуществляется коммуникация основного модуля (его функциональной части ZKE) с модулями памяти положения сидений,

 gryberg 14.06.16 в 18:13

 alex_kag 14.06.16 в 18:09

 kvova 14.06.16 в 18:24

 **DAT540** 14.06.16 В 19:03  

Только [полноправные пользователи](#) могут оставлять комментарии. [Войдите](#), пожалуйста.

Что это такое – BPM, и как компании его строить

 +6
  144
  6
  0

Внедрение IdM. Часть 3.2. Как построить модель доступа?

 +7
 127
 2
 0

Флаги в аргументах функций



 +8
  1,2k
  15
  1

Корпорация Samsung начала массовое производство корпоративных SSD объемом в 30 ТБ

 +9
 4,5k
 6
 21

Иерархия IT-систем и выбор программного обеспечения для организации труда

 +13
 1,5k
 6
 5

Аккаунт	Разделы	Информация	Услуги	Приложения
Войти	Публикации	О сайте	Реклама	 Загрузите в App Store  доступно в Google Play
Регистрация	Хабы	Правила	Тарифы	
	Компании	Помощь	Контент	
	Пользователи	Соглашение	Семинары	
	Песочница	Конфиденциальность		