



ChipLoaderNG

<https://www.chipsoft.com.ua/>

Модуль [51] Bosch MEDC17 - Bench

Document version 19.06.2020

Содержание

Назначение	2
Ограничения	2
Необходимое оборудование	2
Автоматическое управление питанием	3
Контроль записываемых данных	3
Идентификация типа процессора	4
Идентификация ЭБУ	6
Чтение Flash / EEPROM памяти	8
Запись Flash памяти	8
Запись EEPROM памяти	9
Извлечение пароля из прошивки	10
Отключение контроля цифровой подписи при записи диагностическим методом	11
Особенности работы с ЭБУ, использующий процессор без OTP областей во flash памяти	13
Особенности некоторых ЭБУ при использовании CHIPSOFT GPT адаптера	15
Возможные проблемы и способы их решения	16

Назначение

Модуль предназначен для работы с ЭБУ Bosch ME(D)17/EDC17 (CPU Tricore) на столе, без разборки и выполнения следующих операций:

1. [Идентификация процессора Tricore](#)
2. [Чтение внутренней и внешней flash памяти ЭБУ](#)
3. [Запись внутренней и внешней flash памяти ЭБУ](#)
4. [Чтение внутренней eeprom памяти Tricore](#)
5. [Запись внутренней eeprom памяти Tricore](#)
6. [Извлечение пароля из бинарного файла](#)
7. [Отключение контроля цифровой подписи при записи диагностическим методом](#)

Поддерживаются следующие типы процессора Tricore:

1. TC1762
2. TC1766
3. TC1792
4. TC1796
5. TC1724
6. TC1767
7. TC1797
8. TC1782
9. TC1793

Поддерживается внешняя flash память S29CD016G, S29CD032G, устанавливаемая в паре с процессором Tricore TC1796.

Ограничения

На данный момент не поддерживается:

1. Чтение, запись внешней флеш памяти в ЭБУ EDC17CP54, MED17.7.5, MED17.7.3.1
2. Работа с ЭБУ, которые не имеют внутренней flash памяти
3. ЭБУ Bosch, устанавливаемые на автомобили китайского производства
4. Часть ЭБУ, которые имеют высокую версию TPROT (MED17.5.5, MED17.1.1)

Необходимое оборудование

Для работы модуля необходимо следующее оборудование:

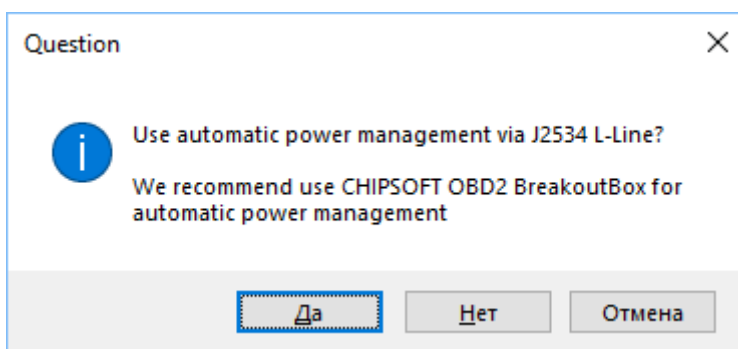
1. CHIPSOFT J2534 адаптер (Акрил/Lite/Mid/Pro). Адаптеры, произведенные до осени 2019 года необходимо доработать. Подробнее доработка адаптера описана в отдельном документе. Версия прошивки и драйвера адаптера должна быть не ниже 1.5
2. CHIPSOFT GPT адаптер. Адаптеры с платой Rev.A необходимо доработать и перепрошить, адаптеры с платой Rev.B никаких дополнительных подготовок не

требуют. Доработка и перепрограммирование GPT адаптера описано в отдельном документе.

3. Опционально CHIPSOFT OBD2 BreakOut Box

Автоматическое управление питанием

Модуль может использовать как автоматическое так и ручное управление питанием ЭБУ. Управление питанием осуществляется путем замыкания L-Линии CHIPSOFT J2534 адаптер на массу. Для автоматического управления питанием и удобного подключения к ЭБУ рекомендуем использовать CHIPSOFT OBD2 BreakOut Box. При старте работы с ЭБУ программа спросит предпочитаемый способ управления питанием.

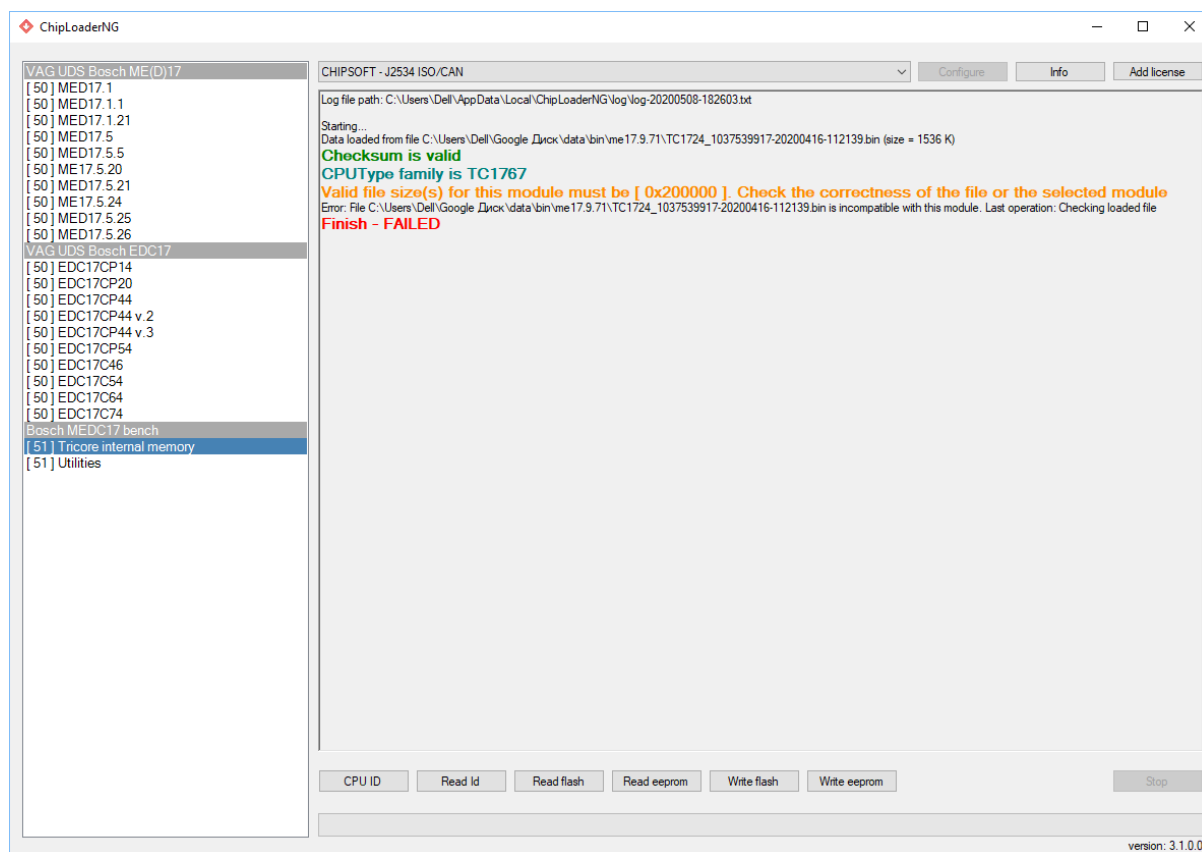


Есть возможность выбрать как ручное так и автоматическое управление питанием.

В процессе операций чтения и записи программа может несколько раз перегружать ЭБУ снятием/подачей питания.

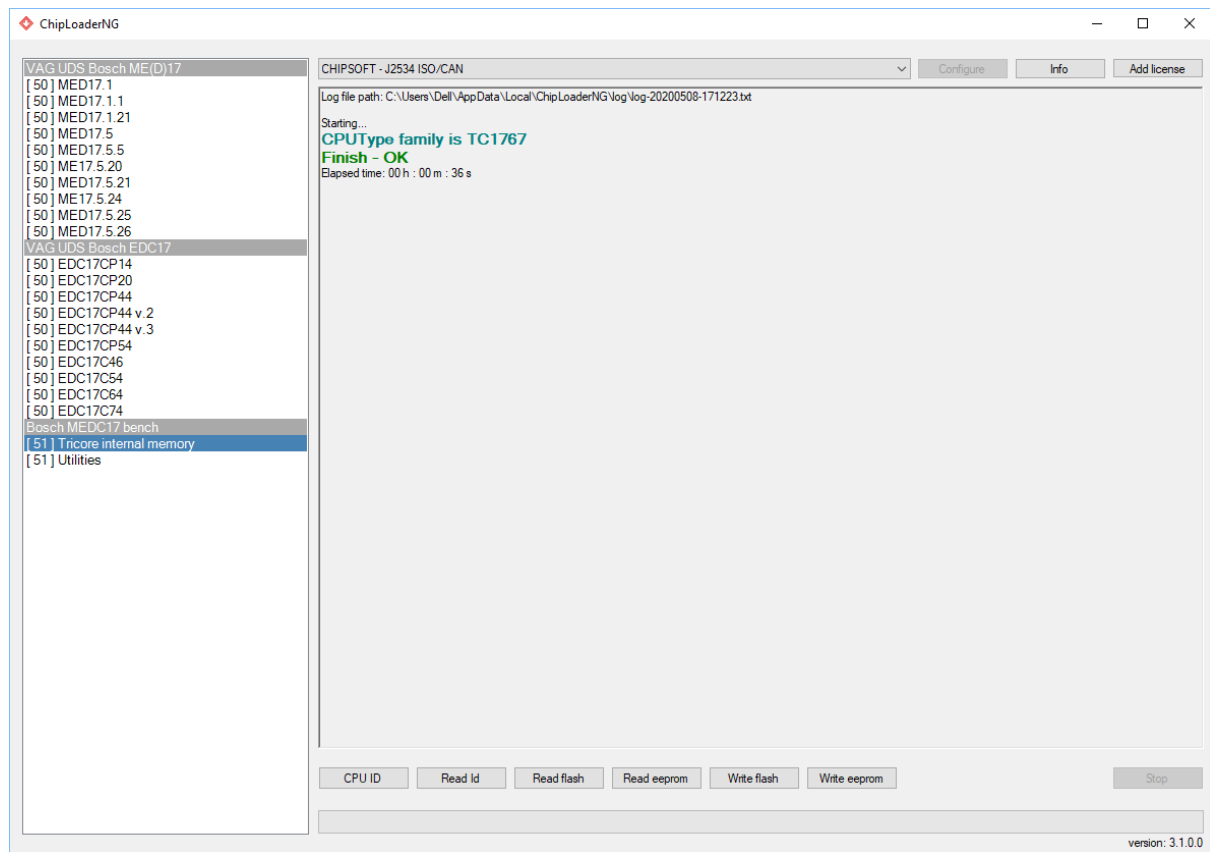
Контроль записываемых данных

Программа осуществляет различные контроли файла прошивки, перед тем, как он будет записан. Если по какой-то причине, программа считает файл некорректным она выведет об этом сообщение.

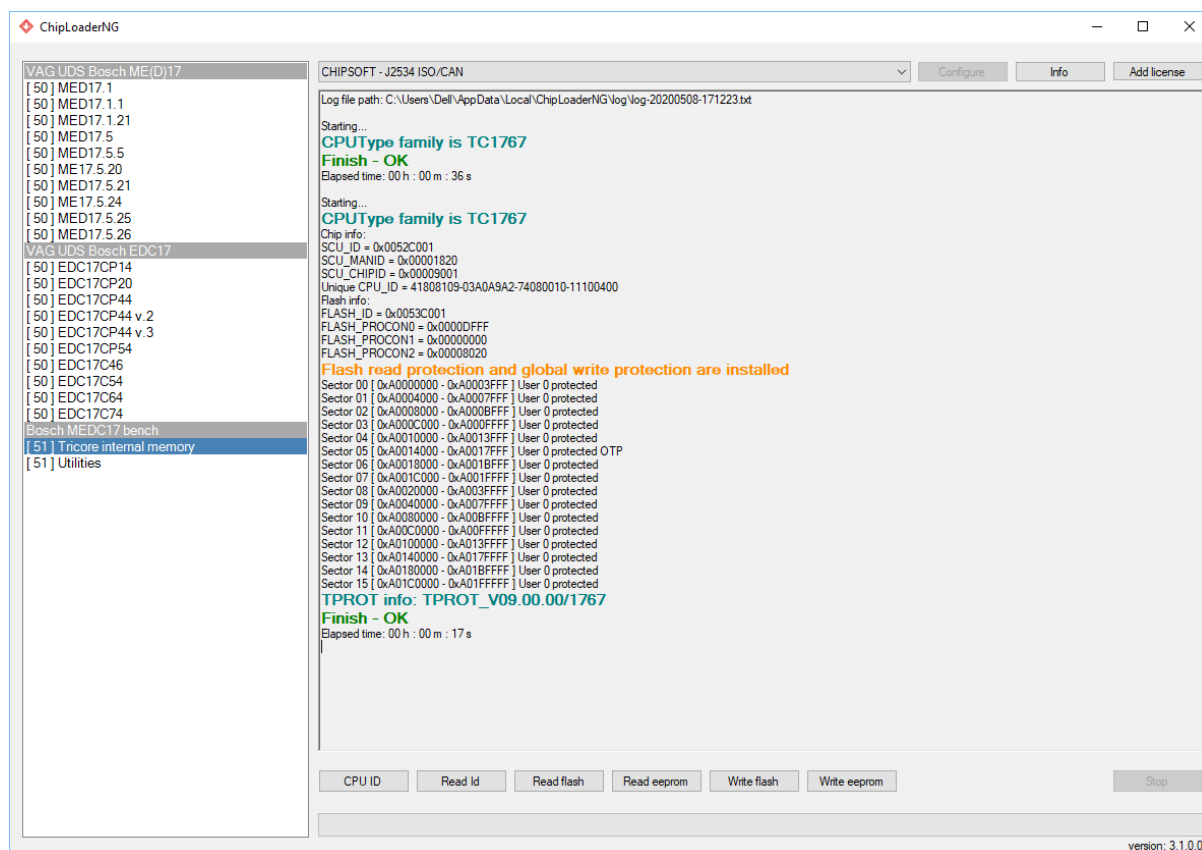


Идентификация типа процессора

Операция **CPU ID** доступна без наличия лицензии на модуль и может использоваться для проверки работоспособности оборудования при работе с модулем.



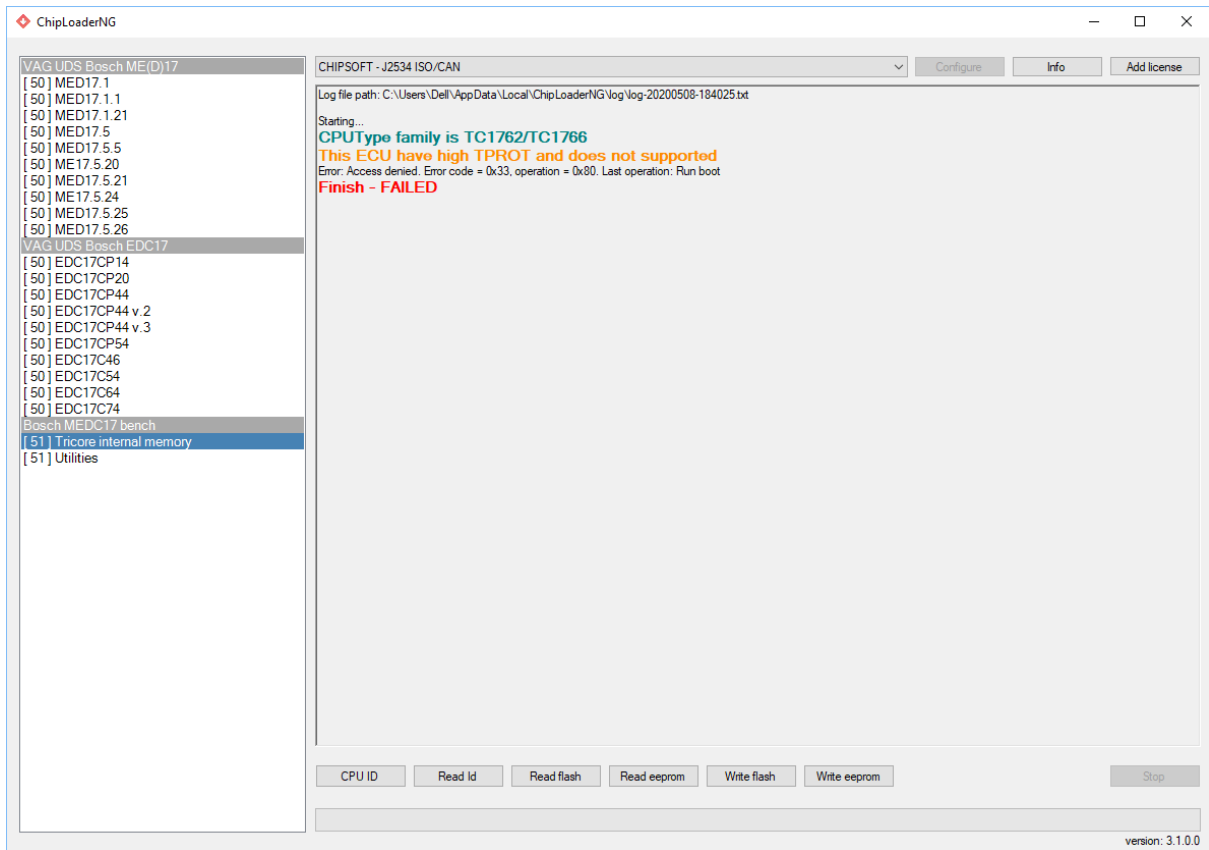
Идентификация ЭБУ



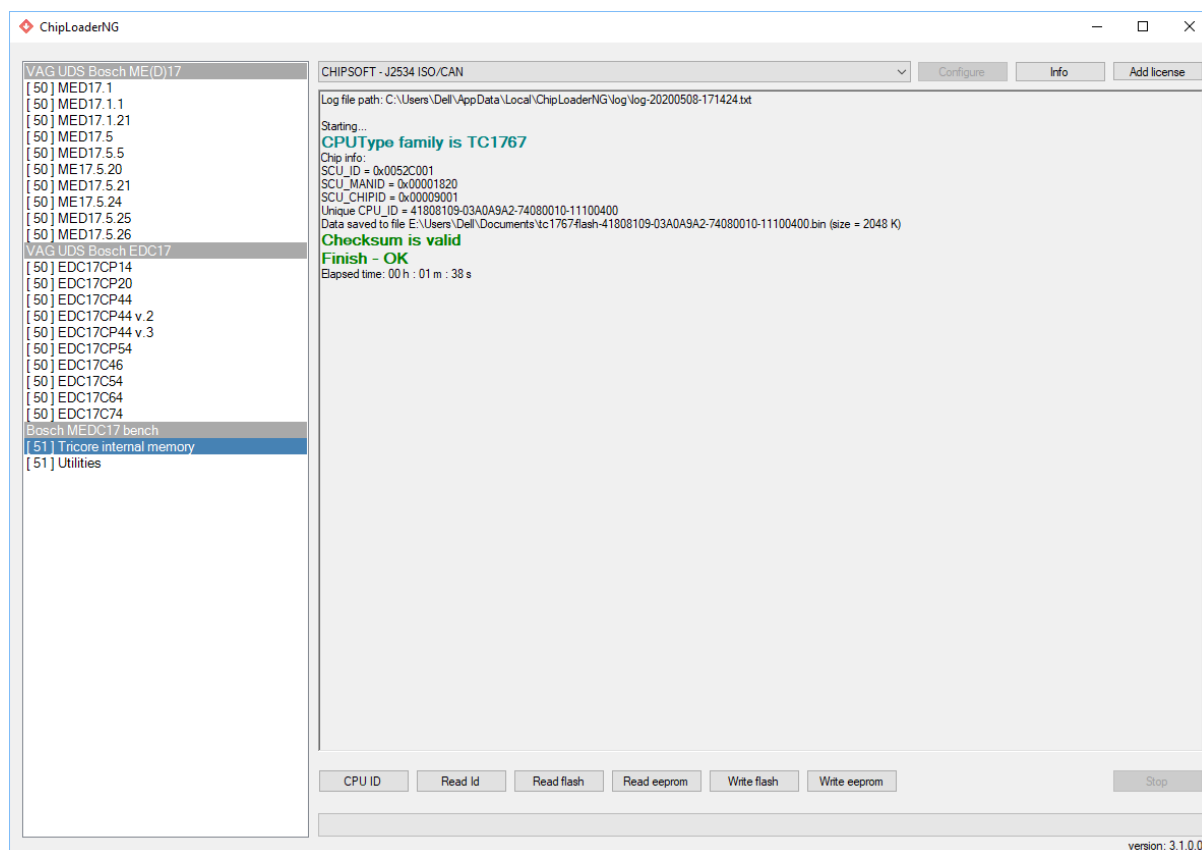
Операция **Read Id** служит для вывода подробной информации о процессоре ЭБУ:

1. Уникального номера процессора
2. Значение определенных регистров
3. Карты секторов процессора с указанием его характеристик
4. Версии используемого TPROT

Если подключенный ЭБУ будет иметь высокую версию TPROT и не поддерживается программой, то будет выведено соответствующее сообщение.



Чтение Flash / EEPROM памяти



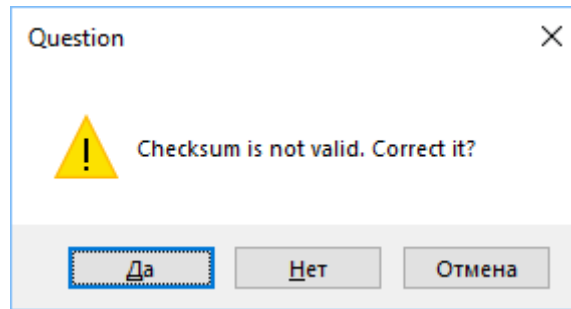
Операция **Read flash**, **Read eeprom** осуществляет чтение полного дампа памяти внутренней памяти процессора. Для сохраняемого файла с дампом памяти в качестве имени файла используется тип процессора, тип памяти и уникальный серийный номер процессора.

После окончания процесса чтения flash памяти программа проверяет корректность контрольных сумм в считанном дампе памяти и выводит соответствующее сообщение.

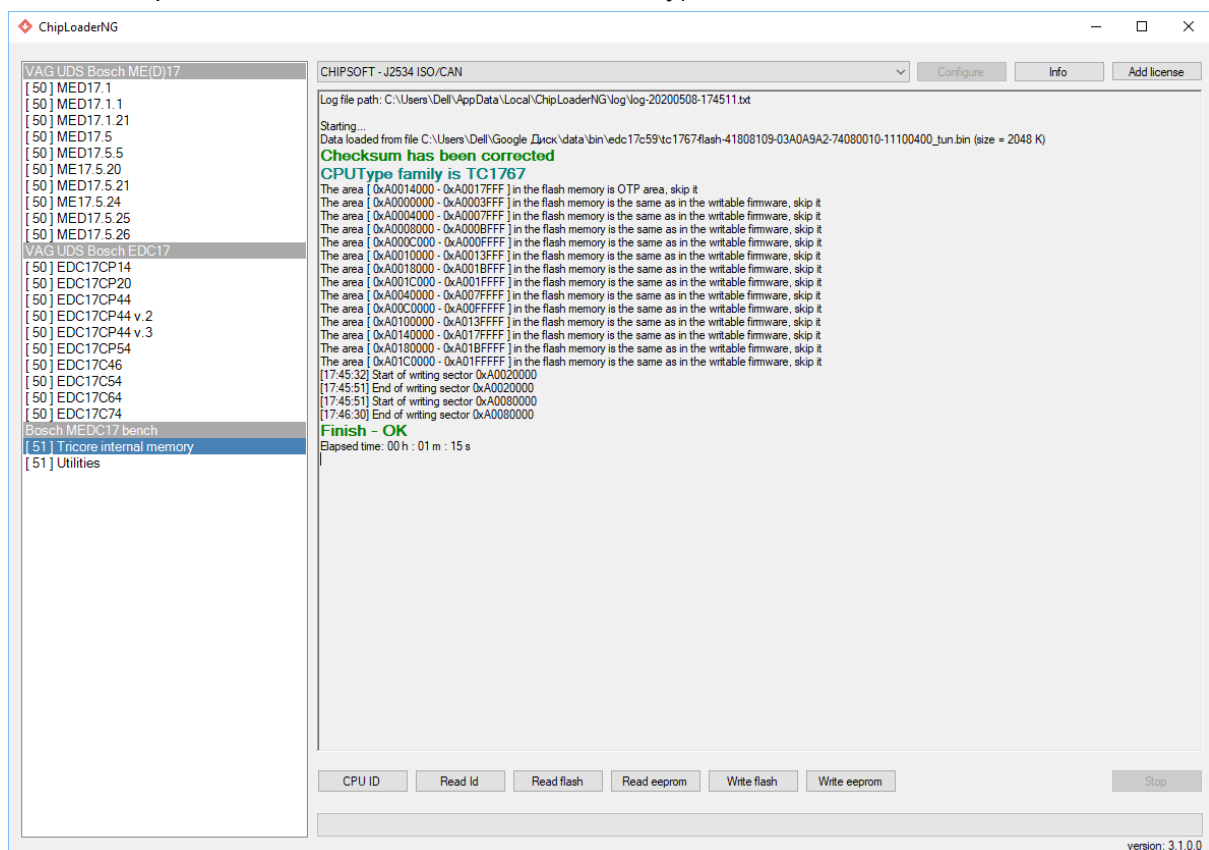
Запись Flash памяти

Операция **Write flash** осуществляет запись всех доступных для записи секторов, исключая OTP сектора (однократно программируемые сектора памяти). Используется интеллектуальный алгоритм записи, при котором перезаписываются только те сектора, которые отличаются от имеющихся во flash памяти. Это позволяет как ускорить процесс записи, так и сделать его более безопасным при обрыве связи с ЭБУ при записи.

Перед началом записи программа проверяет корректность записываемого дампа памяти и также проверяет корректность контрольных сумм. Если контрольные суммы будут некорректны, программа предложит их исправить:



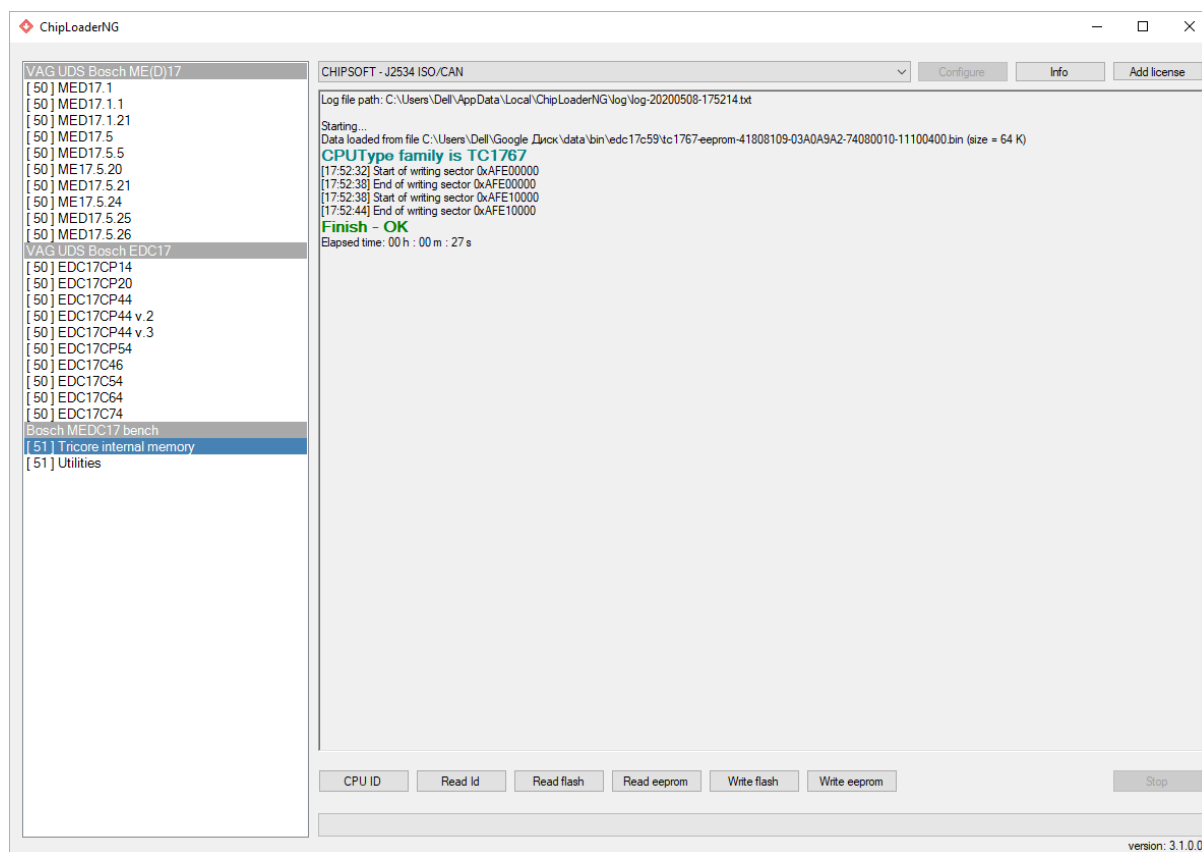
Программа при записи выводит полную информацию по всем записанным секторам (какие сектора были пропущены, как OTP области и какие сектора были пропущены, т.к. их содержимое эквивалентно записываемому).



Т.к. используется интеллектуальный метод записи, то в некоторых случаях время записи может быть меньше времени чтения.

Запись EEPROM памяти

Операция **Write eeprom** осуществляет запись внутренней EEPROM памяти процессора. В данном случае, интеллектуальный алгоритм записи не используется, в отличие от записи flash памяти.



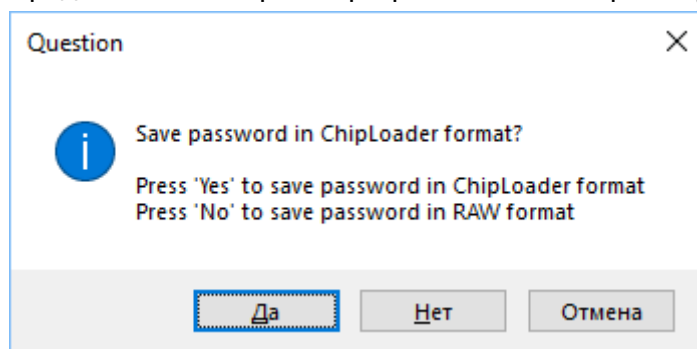
Извлечение пароля из прошивки

Операция **Extract PWD** осуществляет извлечение пароля доступа к процессору Tricore из бинарного файла (для тех бинарных файлов, где пароль хранится в них).

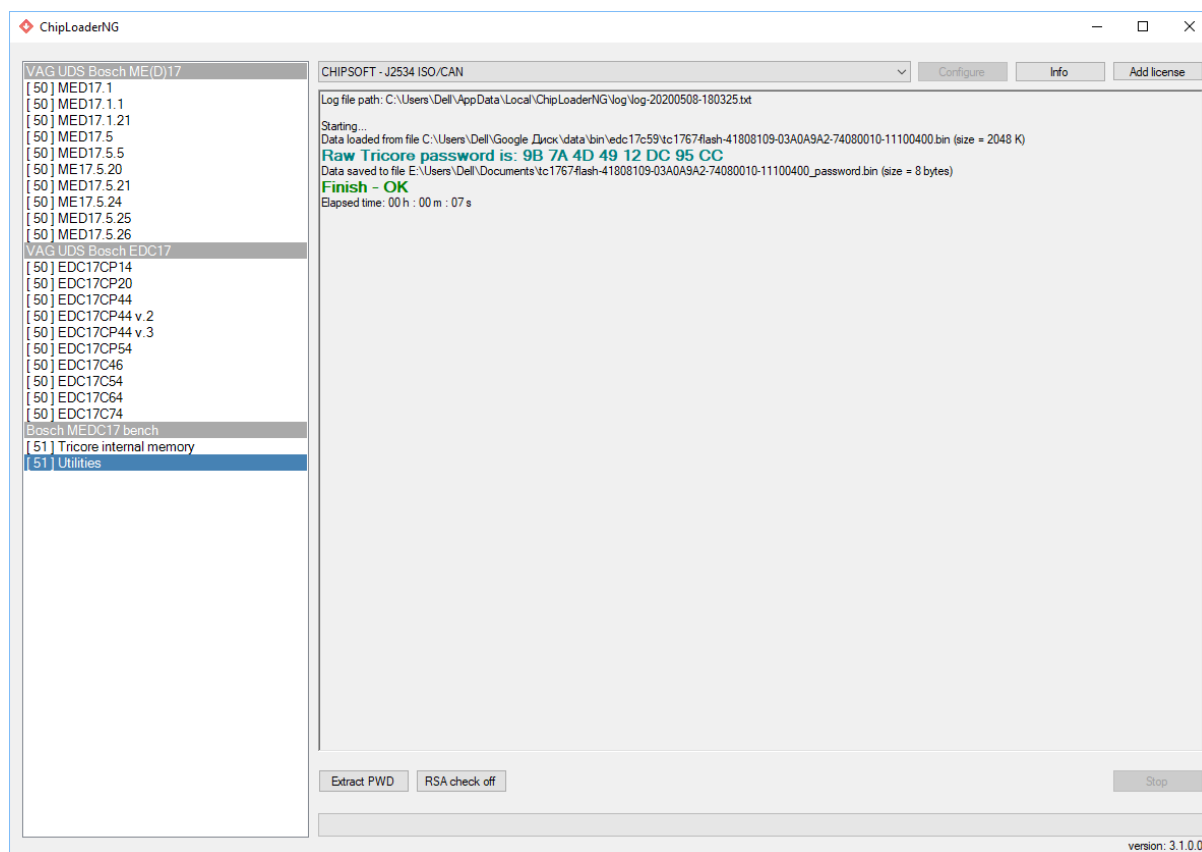
Извлеченный пароль можно получить в следующих представлениях:

1. Текстовое представление
2. В виде файла в формате ChipLoader
3. В виде файла в RAW формате

Тип необходимого представления пароля программа сама запросит у пользователя:



Текстовое представление пароля будет выведено на экран:

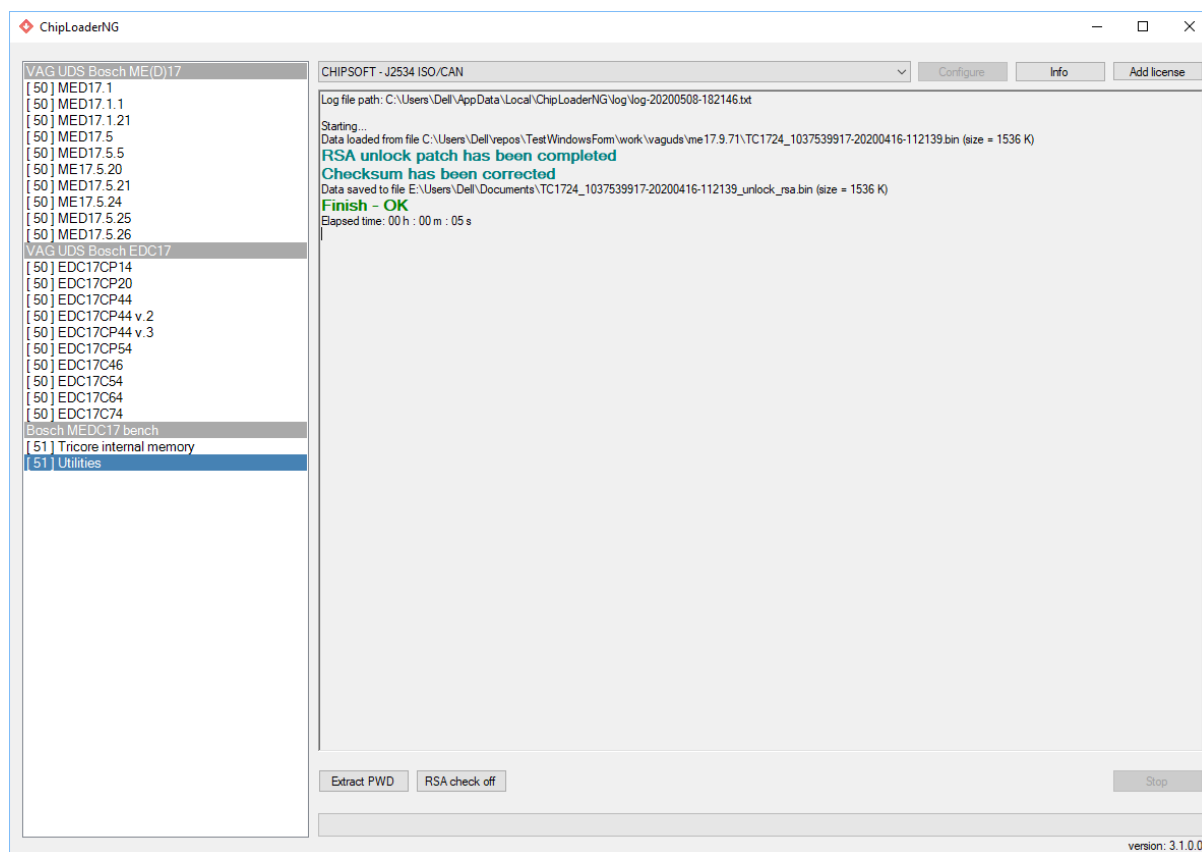


В файле прошивки пароли сохраняются только для тех ЭБУ, которые используют алгоритм защиты версии TPROT 8 и выше. Версию используемого TPROT можно посмотреть, выполнив [операцию Read Id](#).

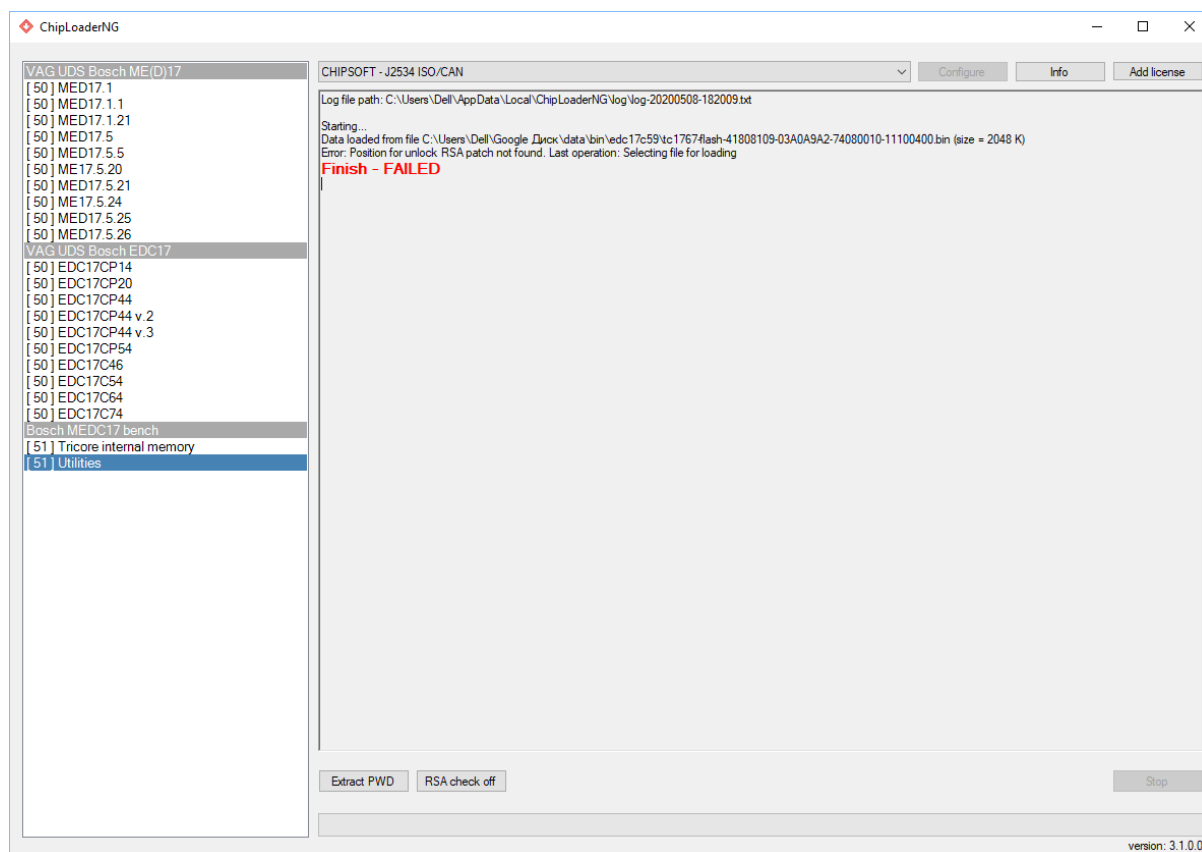
Отключение контроля цифровой подписи при записи диагностическим методом

Операция **RSA check off** вносит необходимые изменения в файл прошивки для того, чтобы в будущем была возможность записи в этот ЭБУ файлов прошивок с неверной цифровой подписью.

Результатом выполнения данной функции будет исправленный файл с уже пересчитанной контрольной суммой.



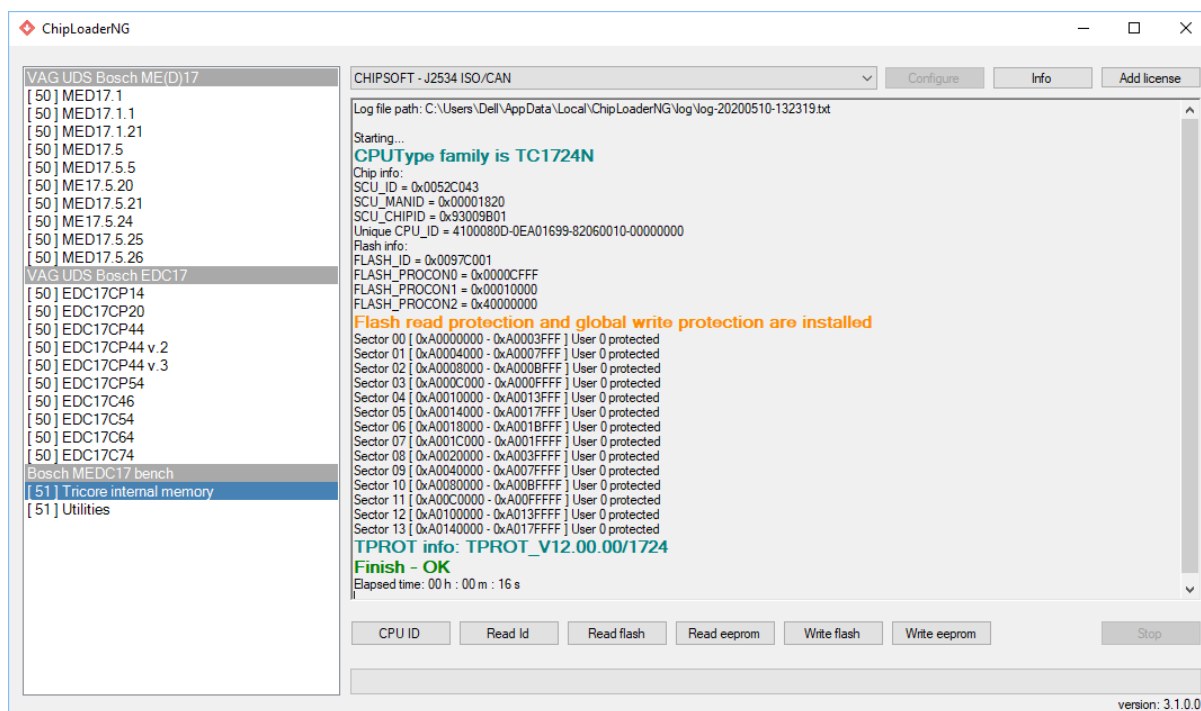
Обратите внимание! Не для всех прошивок доступна эта операция. Если операция недоступна для заданного файла прошивки, то будет выведено соответствующее сообщение.



Особенности работы с ЭБУ, использующий процессор без OTP областей во flash памяти

Некоторые ЭБУ могут иметь процессоры, которые не содержат OTP областей. При использовании TPROT 8 и выше это может стать проблемой при записи flash памяти от другого ЭБУ. Данный раздел описывает именно эту ситуацию.

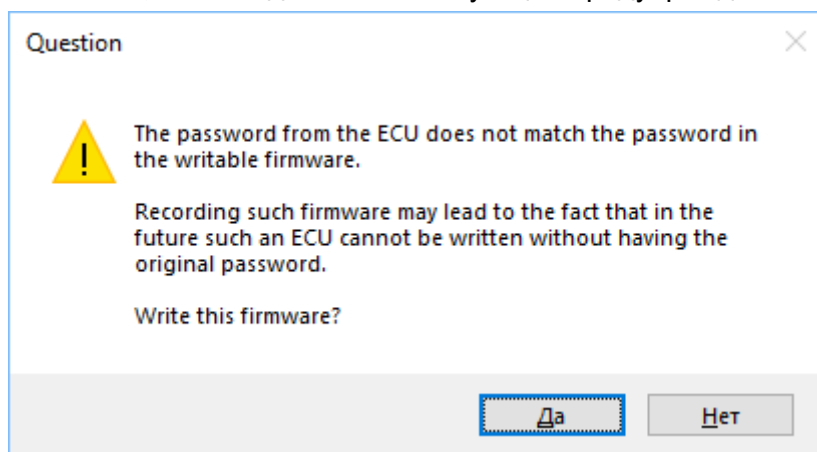
Наличие OTP областей и версию TPROT можно увидеть, выполнив [операцию Read Id](#). Типичным примером подобного ЭБУ есть Bosch ME17.9.71:



Проблемы могут возникнуть при перезаписи flash памяти ЭБУ прошивкой от другого подобного ЭБУ. Учитывая, что прошивка каждого ЭБУ сугубо индивидуальна, то отсутствие OTP областей приведет к тому, что при полной перезаписи flash памяти перезапишется и уникальная область, содержащая в том числе пароль доступа к данному экземпляру процессора Tricore. Таким образом, в будущем контроль над ЭБУ может быть утерян и это будет заключаться в том, что в ЭБУ невозможно будет перезаписать flash память.

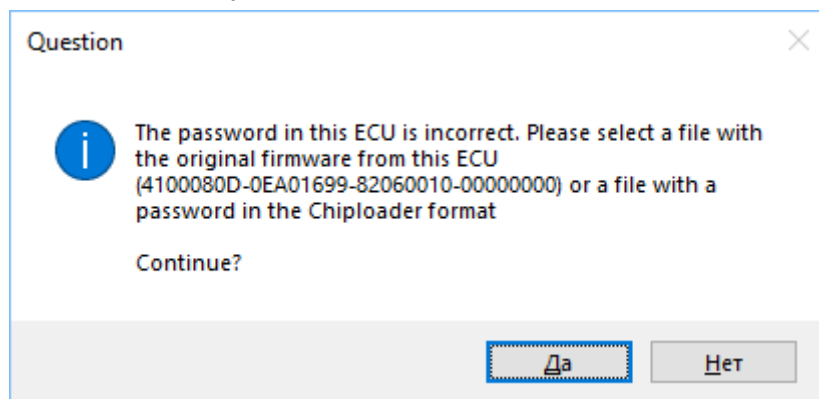
Имея оригинальный пароль от конкретного экземпляра процессора Tricore всегда можно восстановить полный контроль над ЭБУ. Т.к. оригинальная прошивка ЭБУ содержит этот пароль, то его можно восстановить из этой же прошивки. **Поэтому, всегда сохраняйте полный дамп flash и еепром памяти прежде чем что-то делать с ЭБУ.**

Если при записи загрузчик увидит, что пароль в текущей прошивке отличается от пароля в записываемой, он выведет соответствующее предупреждение.



“Да” нужно выбирать только в том случае, если перезаписью прошивки восстанавливается предыдущее состояние ЭБУ с корректным паролем. В противном случае нужно выбрать “Нет”, иначе контроль над ЭБУ в будущем будет утерян, но который можно будет восстановить при наличии либо оригинальной прошивки или ключа доступа к Tricore.

Если в процессе записи загрузчик увидит, что имеющийся во flash памяти пароль неверный, он предложит принудительно его задать.



Задать можно как сам пароль так и оригинальную прошивку от данного ЭБУ. При этом, в окне отображается уникальный идентификатор процессора, от которого нужен пароль. При чтении flash памяти загрузчик в название файла добавляет уникальный идентификатор процессора для облегчения поиска нужной прошивки.

Возможна ситуация, когда ЭБУ уже переписывался кем-то ранее, исходная оригинальная прошивка недоступна и уникальная область прошивки содержит пароль от другого ЭБУ. В этом случае контроль над ЭБУ утерян, перезаписать flash память или восстановить контроль над ЭБУ не получится.

Особенности некоторых ЭБУ при использовании CHIPSOFT GPT адаптера

Некоторые ЭБУ не содержат внутренней подтяжки пинов ЭБУ GPT1 и GPT2. Именно из-за этого может не устанавливаться связь с ЭБУ. Для проверки достаточно измерить напряжение на пине ЭБУ GPT1 и напряжение на пине GPT2, предварительно подав напряжение на ЭБУ. Если напряжение на одном из пинов менее 3.3В, то необходимо подтянуть этот пин к напряжению питания 3.3В через резистор 1К. На CHIPSOFT GPT адаптере есть 3 отдельных пина (boot pins to 3.3V). Для подтяжки достаточно соединить пин GPT1 или GPT2 с отдельным бут-пином на плате CHIPSOFT GPT адаптера.

Следует заметить, что количество ЭБУ, которые не имеют внутренней подтяжки GPT пинов очень мало.

Как показала практика, возможно доработать CHIPSOFT GPT адаптер, чтобы получить универсальное решение для работы с любыми ЭБУ. Для этого достаточно подтянуть пины GPT1, GPT2 на +12В через резистор 5К.

Возможные проблемы и способы их решения

Т.к. модуль использует алгоритм работы с ЭБУ по чтению и записи ранее заложенный в прошивке ЭБУ, то некорректная прошивка в ЭБУ может привести к тому, что данным модулем невозможно будет работать с ЭБУ. Это будет проявляться в том, что операции **CPU ID**, **Read Id** не будут выполняться и будут возвращать ошибку. В таком случае восстановить ЭБУ можно только модулем, который работает с процессором Tricore напрямую в бут режиме. В зависимости от версии используемого TPROT возможно понадобится пароль или оригинальная прошивка ЭБУ для его восстановления.