ORANGE5

Read and Write though CAN of Renesas processors based Toyota and Subaru SRS by programmer Orange-5

Contents:

Read and Write though CAN of Renesas processors based Toyota and Subaru SRS by programmer Orange-5

The use of certain Renesas processors with internal EEPROM in some SRS has led to increased complications when erasing crash data in them. Up till now the main course of action required specialized programmers targeted only at doing these MCUs. Erasing of the EEPROM and the crash data within is impossible unless the Flash memory is erased first, but in the end in order to restore the block in working condition with no errors the erased flash has to be written back. This whole process of obtaining the FLASH area of the MCU, erasing it requires expensive flash programmers and in general requires the chip to be unsoldered/soldered which if not done properly may damage irreversibly the chip and as a whole makes clearing of crash data in these blocks both time and money consuming process.

Researching this type of SRS blocks revealed yet another way to work with them, namely work through the CAN bus. Work was conducted on Toyota SRS and Subaru SRS blocks.

In the following section of the document the different operational modes used in the software will be reviewed and as example will be used SRS Toyota:

Work Mode (CAN) – This is the mode in which the SRS block operates while in a car. It is also possible to connect to the block while it is unplugged. In this mode it is possible to read, compare and erase the Flash area.

Reading the model number of the block is also available. If the flash is erased in this mode, then the block "freezes" and after several manipulations (described in the later chapters of this document) it will become accessible in *Boot-Mode*.

Boot-Mode(CAN) – In this mode everything accessible and any kind of manipulation of the block is possible. It is all up to the knowledge and need to add a particular code in the block. In this software project the available operations are Read/Erase/Write Flash, Read ID of the block from the EEPROM area, Blank Check and erase EEPROM. After writing a correct Flash dump file (which is to be obtained and saved from the block in *Work-Mode*, or replaced with a dump from another block) and a restart the block goes back to *Work-Mode*.

Boot-Mode (Tx-Rx) –Advanced function that erases completely both Flash and EEPROM areas, after which write correct dump and read in order to compare and verify the operation are available. This function is to be used on SRS blocks which are stuck with corrupt or incomplete Flash data.

Work with SRS blocks in all modes is implemented in a software package for programmer Orange-5 with CAN adapter. For Boot-Mode (Tx-Rx) additional adapters are not required. The version of the Orange-5 software required for work with this module is 1.31 or higher. Because work with these blocks in both modes differs, there are separate HPX programs for each Mode.

The software module for programmer Orange-5 contains two main parts. One is a *.cfg file which has to be placed in the root directory of Orange-5 base software (where orange.exe is located) and a folder with the HPX files and Info files that has to be placed within subfolder HPL.

This software package enables work with different types of MCUs that have 256KB and 512KB Flash.

Work-Mode (CAN)

In order to connect to the SRS while it is unplugged from the car you can be guided by the following photo*
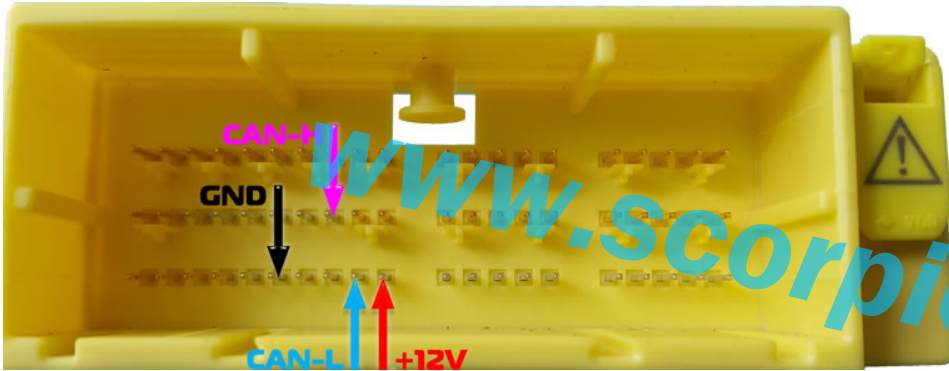
  In order to work with the block while it is in a car, an adapter cable from Orange-5 CAN adapter to the OBD connector will be required. K-Line and BATT lines are currently not used and required for work with this software, but they might be used in future for other types of blocks.

| Orange-5 Адаптер CAN K-Line Разъем DB9	
Name	**Pin**
GND	1
GND	2
CAN High	3
K Line (ISO 9141-2)	4
CAN Low	5
Battery Power (+12V Vbat	9
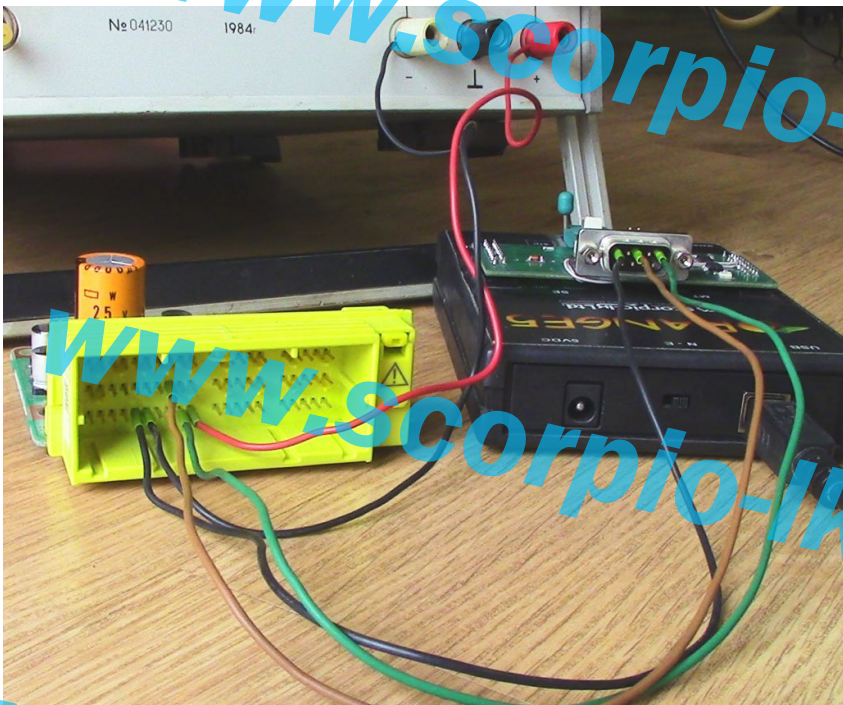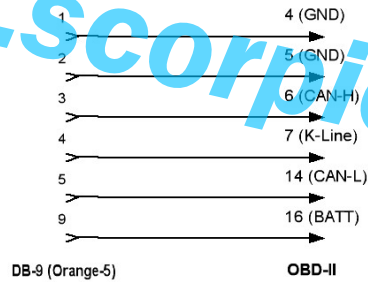
Example connection of SRS block to Orange-5. GND (black wire), CAN-H (brown wire), CAN-L (green wire). Power is supplied to the SRS block.
No additional power has to be supplied to the programmer!
Jumper «CAN Term» is placed.

*In Chapter "Variants SRS", different variants of the SRS blocks are presented. In this example is used Variant 1
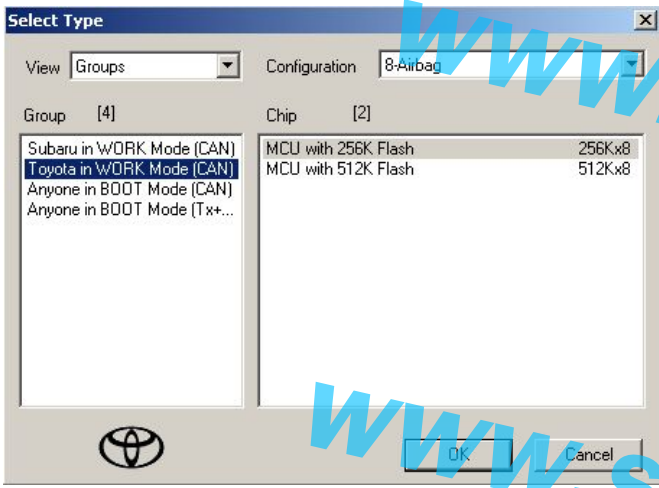
After start of Orange-5 software Mode is selected depending on the Flash size of the MCU found in the SRS block.

If incorrect size is selected, for example 512KB instead of 256KB, an error will be displayed, after which the SRS block will not respond to commands and in order to continue work you will have to restart power supply of the block and proceed with Read after selecting the proper work variant of the software. In case of working in a care turn it on and off.

Functions available in Work-Mode:
- Read Flash
- Compare dump and Flash
- Read SRS Number
- Erase Flash.
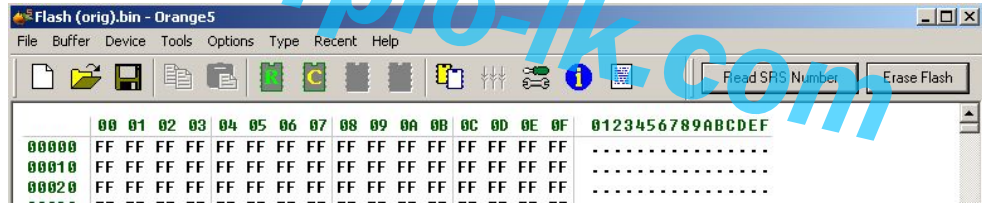
When turned on the SRS number can be read.

If you already have available a dump Flash file from same block, you can skip the read process. If not continue with reading the Flash by pressing the button R (Read). Time required to read Flash is roughly 12 minutes for 256KB and 25-30 minutes for 512KB.
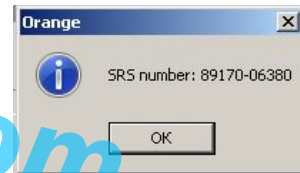
Work with the EEPROM, reading it, or erasing its errors is impossible in Work-Mode. In order to access the EEPROM it is required to make the block enter Boot-Mode. This is achieved by erasing the Flash.

When button "Erase Flash" is pressed block 0 of the Flash memory (the starting 4 KB) will be erased.

While this operation renders the block unworkable in car, it allows connecting to it in Boot-Mode.

Boot-Mode (CAN)

Boot-mode is available when the Flash is completely or partially erased. Except this condition several operations have to be performed on the block: Unsolder the 0-resistor of the processor Reset line (otherwise it interferes with the work of the Watch Dog Timer), then solder on the processor Reset line an additional resistor with a nominal value in the range of 10kOm 0 47kOm (lifting Reset to +5V).
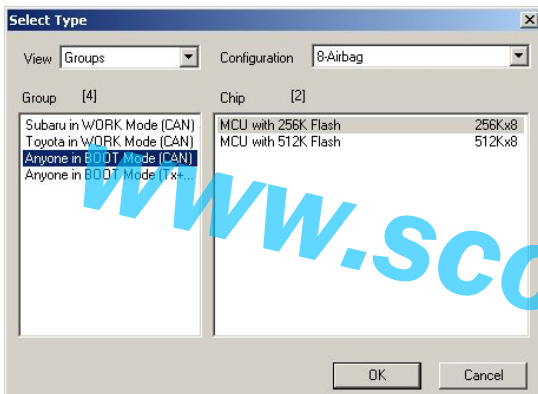

0-resistor, which is to be removed*.
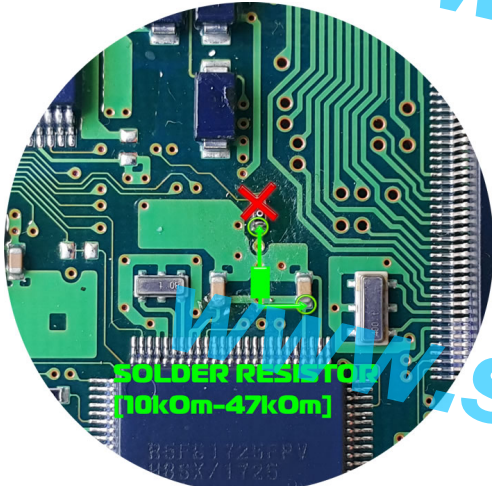
Additional resistor which is to be soldered*.

After these manipulations the block can work in both Boot-(Flash erased) and Work-Mode (Flash written), but after completing job with the block it is advised to revert these operations before placing it back in a car.

Connecting to the SRS while it is unplugged from the car is showed is same as shown in Chapter Work-Mode. Start Orange-5 software and select Boot-mode.
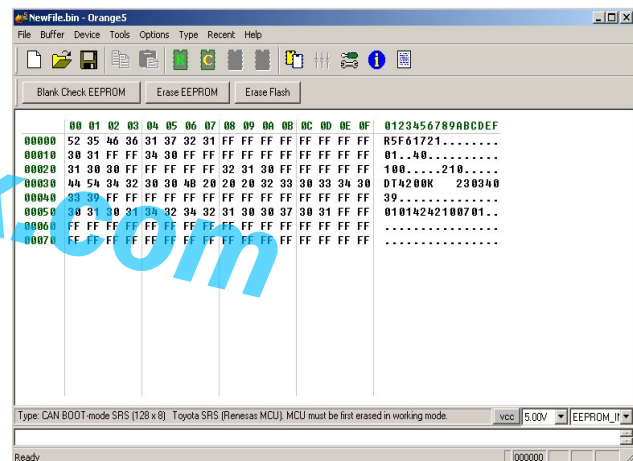
On the screenshot is shown EEPROM_INFO of after is was read. When area EEPROM_INFO is selected "Write" function is unavailable, because this area can only be read. In it there is interesting information, like the name of the MCU (R5F61721), its clock rate (40MHz), serial number of the block, etc….

*In Chapter "Variants SRS", different variants of the SRS blocks are presented. In this example is used Variant 1

Reading the Flash area is also available.

Since work is in Boot-Mode it means that Flash is completely or partially erased in which case reading it could be useful only after writing it back in order to verify that it was written correct.

Time to read 256KB Flash in this mode takes around 30 seconds.

The state of the EEPROM blocks can be checked by pressing button «Blank Check EEPROM». In the displayed window the clear blocks will be marked with a "tick":
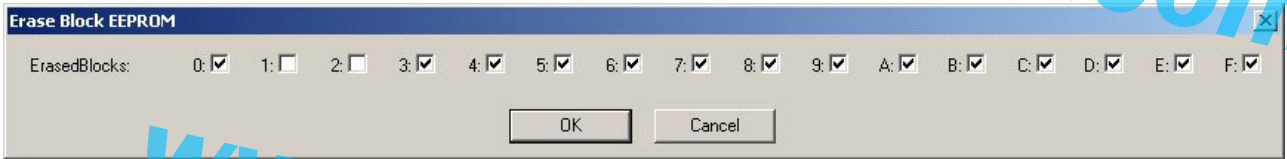
In order to clear the crash data (virginise the block) it is required to erase the EEPROM. This is done by pressing button «Erase EEPROM».Verification of this action can be done by pressing «Blank Check EEPROM» again.

Writing Flash area is possible after it was completely erased. In theory it would be possible to write only the 0 data block (first 4 KB), which is erased in Work-Mode, but there are possible variations. For example if a dump file from another block is to be written by filling the first 4KB the program will not work correct. Because of this pressing button «Erase Flash» in this mode completely erases the Flash are and the following command «Write Flash» writes the whole data area.

Next step in restoring the block to working condition is writing the Flash. Select FLASH data area, this will make the [W] (Write) button available. Open in Orange-5 software the original Flash dump file, which was read and saved in Work-Mode, then press Write. Time required to complete this operation is roughly 2 minutes but may vary. If after write the power supply was not interrupted or restarted it is possible to read the Flash area and verify that it was written correct. This is possible because the block will continue to be in Boot-Mode until its power is turned off, this means that operations of clear the EEPROM and writing the Flash can be done in any order, still we'd advise first to clear the EEPROM and then write the Flash.

If Write Flash was completed successfully, its contents were verified, EEPROM crash-data was cleared it is time to turn of the block, remove the additional resistor and place back the 0-resistor to its original position.

After all these operations the block is ready to be placed back in a car and used as intended.

NB!: If the block is turned on while unplugged from the car it will generate errors, which may or may not cause trouble when placed in a car, because of that after completing all operations of clearing the EEPROM crash-data and restoring the FLASH area don't turn the block on unless it is connected properly to a car.

Boot-Mode (Tx-Rx)

Boot-Mode (Tx-Rx) is used to write Flash dump in cases when connection through CAN gets no response from the MCU. Such state occurs when in the Flash are of the MCU is written corrupt data and/or the process of writing was interrupted. In this Mode when attempting to Read all data in the Flash and EEPROM will be completely erased. After erase is completed writing correct Flash dump becomes available. This mode is more time consuming than the others because there is significant amount of wires that have to be soldered to the SRS PCB and also difficulties may arise with SRS variants whose connect points are not yet covered.

MCU pinout. Used Pins are marked with red:
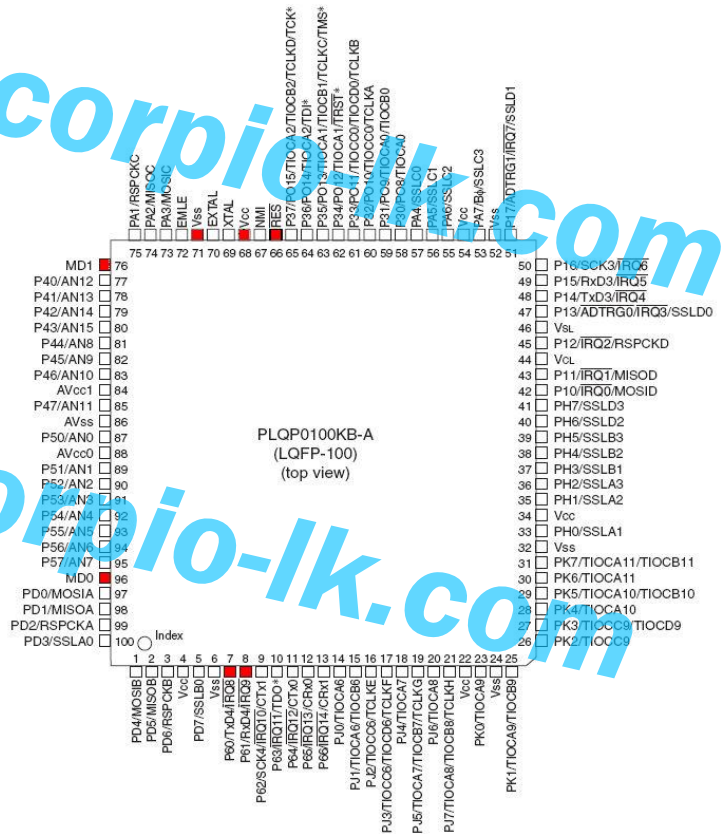
In order to allow the MCU to enter this mode, a jumper has to be placed on the board ("short" on the photo below). This jumper sets MD1 of the MCU to high logic level.

How these Pin points correlate to Orange-5 MT socket is shown in the following table:

| Orange-5	SRS
GND	GND
VCC	Vcc(+5v)
RXD	TxD
TXD	RxD
RST	Reset
PDX	MD0
	short MD1 – Vcc

Besides all these connections, the 0-resistor has to be removed as well , same as shown in the section *Boot-Mode (CAN)*. Additional resistor to Reset is not required, because in this Mode we use the programmer Orange-5's Reset.

Example connection pins for SRS Toyota Camry:
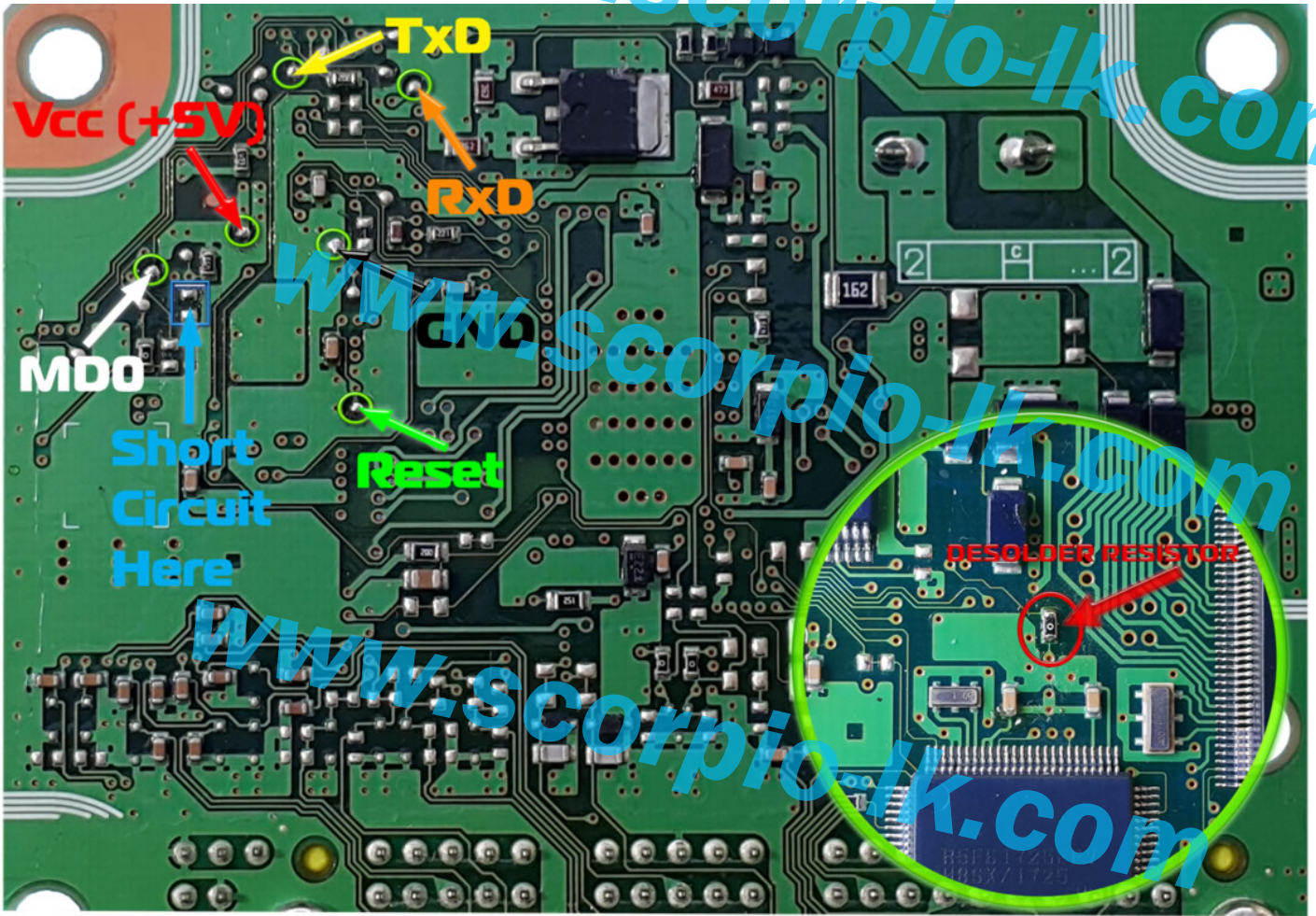
After preparing the block, we start Orange-5 and choose the corresponding software module, as shown in the right:
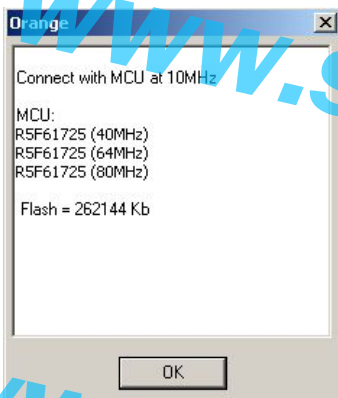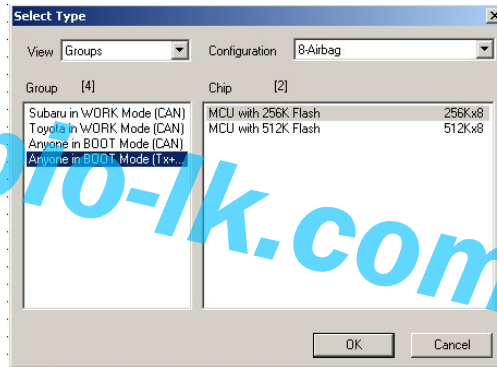
At first attempt to Read or Write connection with the MCU will be established and if successful an information window regarding the MCU

After pressing [OK] in the information window, a warning message will be displayed. It warns that the data in the MCU will be erased and asks for either confirmation or cancel of the operation:
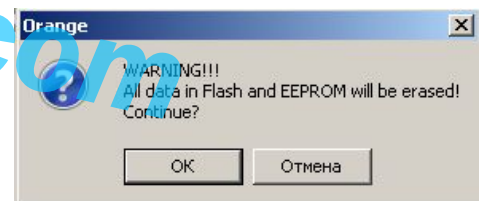
At this point the user may decide whether to proceed with [OK] or stop [Cancel]. If work proceeds then the Memory areas of the processor will erased. After this Flash will be available for Read/Write. A dump Flash file can then be opened in Orange-5 software and written. It takes 1-2 minutes to write 256KB Flash. After write it is possible to use command Compare in order to verify the data.

Recommended Operation Procedure

First step in the process is to determine the Model Number of the SRS block. This can be achieved directly in the car by utilising the *Work-Mode (CAN)* module of the software. After successful determination of the SRS Number the work may continue in two different directions. Choosing the right direction иc determined depending on the availability of previously read and saved Flash dump from same SRS Model.

I.   If a Flash dump is not available work continues in the car or unplugged by performing the following actions:

- Read the Flash area in Work-Mode (CAN) through the CAN adapter
- Save the read dump File
- Next continue with paragraph II.

II.   Flash dump for this model is available, next operations are performed on unplugged from car SRS:

- Desolder 0-resistor and place the additional resistor as shown in documentation
- In Work-Mode (CAN) erase the Flash
- Turn off the power supply to the SRS
- Open Type in Orange-5 software and select Boot-Mode (CAN)
- Turn on the power supply to the SRS
- Erase EEPROM;
- Erase Flash;
- Select in Orange-5 software Flash area.
- Load the previously saved in paragraph I. dump file
- Write Flash [Write];
- Perform a comparison of what was written by using [Compare] command
- If no errors were detected work is finished by removing the additional resistor and soldering back 0-resistor to its original spot. After this the SRS is ready to be placed back in a car.

In case during the course of work any errors occurred (wrong/non-compatible Flash dump was written, connection got interrupted, etc...) and as a result the block got stuck non responding to CAN requests in any Mode, then there is a procedure that allows Erase both Flash and EEPROM areas in an alternate Boot-Mode and then write correct dump. This procedure is described in chapter Boot-Mode (Tx - Rx).

Remarks

After all written above, we'd like to share some of our experience of a peculiar situation that occurred while researching these SRS modules. We stumbled upon a SRS module in which was written a Flash program from another SRS which had different Renesas MCU and a different frequency quartz. The SRS was working with this program in Work-Mode, but because the Timers and the CAN were designed for a different quartz, the we were failing to connect to it. In this case what helped was temporary replacing the quartz with one which frequency matched the one coded in the Flash program. After this we successfully connected to the block in Work-Mode, and managed to Erase the Flash. When this operation was completed we placed back the original quartz and continued work on the SRS block through the Boot-Mode with the methods described in the sections above. Except the above mentioned example, in cases when Flash is not responding by CAN controller, it is possible to use *Boot-Mode (Tx-Rx)*.

Variants SRS

Variant 1.

CAN-H

GND

CAN-L +12V

DESOLDER RESISTOR

SOLDER RESISTOR
[10kOm-47kOm]

Variant 2.

CAN-H

GND

CAN-L +12V

SOLDER RESISTOR
[10kOm - 47kOm]

DESOLDER RESISTOR

Variant 3.

DESOLDER RESISTOR

SOLDER RESISTOR
[10kOm - 47kOm]

CAN-H
GND
CAN-L +12V

Variant 4.

DESOLDER RESISTOR

SOLDER RESISTOR
[10kOm - 47kOm]

CAN-H
GND
CAN-L +12V

12