Read a secure MC9S08GT32A ?

Options

01-04-2014 11:09 AM • 678 Views

andrewstancliff
Contributor I

Does anyone out there know of a way to read the contents of a secured mc9s08 using the USBDM interface? I bought both the multilink and cyclone pro and then found the USBDM beat these into the ground for a fraction of the price.

i Am not wanting to reverse engineer or anything dubious just tweak a couple of settings.

i Have seen software for reading and writing to the same family of mcu for cars that are secure using software like UPA-USB and ULTRAPROG with other interfaces so I live in hope someone somewhere can point me in the right direction.

Thanks in advance

Andrew

Labels: General

Tags:

usbdm

2 Replies

01-05-2014 08:55 PM • 337 Views

ZhangJennie
NXP TechSupport

It is possible to do so but only if the code is designed to perform such action from the beginning. The way to do it is to use the backdoor key access which is a way to write an 8-byte key into the MCU to un-secure the device. The problem here is that this is also a software routine that should be implemented in the MCU so, if your customer doesn't have this in their code, they'd need to add it and then read the MCU contents in the future.

The way to use such feature is to write the 8-byte key from address 0xffb0 to 0xffb7 and secure the device by writing the NVOPT register with a value of 0xFC for example. To unsecure it, you have to set the KEYEN bit in the FCNF register, then write the 8-byte key and then clear the same bit. If the key is the right one, the MCU will be unsecured until next reset so you could read the memory contents using a Hot-Sync with the debugger for example.

For your reference, I attached a code that is un-securing an S08QD; it is not the exact same device you are using but the routine is exactly the same. In my case, I'm directly writing the contents of the Backdoor key but the ideal scenario would be to receive such key through a serial or any other external interface to ensure that only the authorized persons have access to the MCU. Once the code un-secures the device, PTA0 is being changed from 1 to 0 to indicate that the part is not secure anymore; I hope you find this example useful.

Backdoor Key.zip

01-06-2014 12:20 AM • 337 Views

kef2
Senior Contributor IV

ZhangJennie,

did you verify your code is working? I think that it is like on S12, where setting KEYEN bit makes flash memory not readable, so to make backdoor unsecure routine working, you need to place or copy it to RAM.