Freescale Semiconductor

Engineering Bulletin

Unexpected Interaction Between the HCS08 Backdoor Key Sequence and Stop Mode

1   Problem Description

If KEYACC is set to 1 in a secure device to start the backdoor unlock sequence, and the device enters stop mode before the unlock sequence is completed, then security will be disengaged when the MCU wakes up from stop using an interrupt. If reset is used to wake up from stop, KEYACC is cleared and the MCU will remain secure. If the backdoor access feature is not enabled (nonvolatile KEYEN bit = 0), this unexpected operation cannot arise.

There is no known reason a user would enter stop mode after a backdoor unlock sequence has started but has not been completed. This stop instruction must be executed from within the (secure) user code and is not an occurrence that can be forced by actions external to the MCU. RAM is considered a secure resource when security is enabled, so a potential pirate cannot introduce code to force the MCU into stop mode.

2   Workaround

Avoid the conditions that lead to the unexpected security-unlock condition. You could choose to not allow the backdoor access mechanism by clearing the nonvolatile KEYEN bit in NVOPT. If you plan to use the backdoor access mechanism, and your application also uses stop mode, you could choose to use reset instead of an interrupt to wake the MCU from stop. If you plan to use the backdoor access mechanism, and your application also uses stop mode with the possibility of an interrupt wakeup, then do not allow entry into stop during a backdoor access operation. Backdoor access is a rare operation so there should be no need to enter stop mode during the unlocking sequence.

3   Mask Sets Affected

- MC9S08AW60 — 0L16X, 0M75B, 1M75B, 3M75B, 5M75B

- PC9S08GT16A — 2M70C

- MC9S08JR12 — 0L95Y

- PC9S08LC60 — 0M78B

- MC9S08QG8/4 — 0M77B, 1M77B, 2M77B, 3M77B

- MC9S08RT16 — 0M14A