AN_65XX_005 NOVEMBER 2010

71M65XX Precautions for Setting ECK_DIS and SECURE Bits

This document describes hardware and firmware precautions that have to be taken when setting the *ECK_DIS* bit in I/O RAM and/or when setting the *SECURE* bit in the SFR area of the 71M651X and 71M652X Energy Meter chip family.

In addition, methods are described for erasing and reprogramming the flash in cases where the *ECK_DIS* bit and/or the *SECURE* bit are set.

Background on *ECK_DIS*

The *ECK_DIS* bit in I/O RAM can be used to switch off the emulator clock that normally appears at the E_TCLK pin. The E_TCLK pin is multiplexed with a LCD segment function in the 71M652X family, and pulling the ICE_E pin up to 3.3V will switch the multiplexed pins to their emulator function. However, with *ECK_DIS* = 1, no clock will appear at the E_TCLK pin, preventing emulators and programming devices to connect to the device.

This means that parts that have to be re-programmed should have the *ECK_DIS* bit reset to 0.

Background on *SECURE*

A program that sets the *SECURE* bit in the SFR area will render the part secure, hiding the code image from potential intruders. While the *ECK_DIS* bit can be set and reset under MPU program control, the *SECURE* bit can only be set by the MPU, not reset. Once the *SECURE* bit is set, additional steps will be required if the part must be erased and re-programmed,

When enabled, the security feature limits the ICE to global flash erase operations only. All other ICE operations are blocked. This guarantees the security of the program code in MPU and CE. Security is enabled by MPU code that is executed in a 32 cycle preboot interval before the primary boot sequence begins. Once security is enabled, the only way to disable it is to perform a global erase of the flash, followed by a chip reset.

The first 32 cycles of the MPU boot code are called the preboot phase because during this phase the ICE is disabled. Usually, the first few instructions in the assembler file “startup.A51” are executed right after reset and thus will be located in the preboot phase. This is where the programmer may place the following code:

```
STARTUP1:
                CLR     0xA8^7      ; Disable interrupts
                MOV     0B2h,#40h   ; Set security bit.
                MOV     0E8h,#0FFh  ; Refresh WDT.
```

The second instruction sets bit 6 (*SECURE*) in the *FLSHCTRL* register (SFR 0xB2). The ICE is only enabled after completion of the preboot phase, and it is only then permitted to take control of the MPU.

SECURE is reset whenever the chip is reset until it is potentially set in the preboot phase. The following conditions apply when *SECURE* is set:

- The ICE is limited to bulk flash erase only.
- Page zero of flash memory, the preferred location for the user’s preboot code, may not be page-erased by either MPU or ICE. Page zero may only be erased with global flash erase.
- Write operations to page zero, whether by MPU or ICE are inhibited.

For the reasons listed above, the *SECURE* bit is to be used with caution! Inadvertently setting this bit will inhibit access to the part via the ICE interface, unless a reset can be forced.

Precautions to be Taken in Hardware Design

This section details hardware design rules that, when followed, ensure safe recovery from situations where the *ECK_DIS* bit and/or the *SECURE* bit are set.

To recover a part from situations where the *SECURE* bit and/or *ECK_DIS* bit are set early in the code execution, a reset of the part is necessary. This is easy to achieve for demo or prototyping boards that have a dedicated reset button. Usually, the ADM51 emulator is fast enough to take control of the E_RST pin and can halt the MPU right after reset or power-up. The TFP-1 is not as fast as the ADM51 emulator and may not be sufficient to recover the part. Again, the newer TFP-2 programmer will be fast enough and will also provide an output that can control the ICE_E pin of the 652X chips, when this pin is brought out to the emulator connector (see Figure 3).

The reprogramming process may not be as straight-forward for production boards because these may have the RESET or RESETZ pin shorted to either GND or V3P3D in order to achieve high tolerance to EFT events (electrical fast transients). In that case, cycling the power to the board achieves the required reset, if the chip is a 71M651X or if it is a 71M652X without a battery attached. A 71M652X chip will not reset if it is supported by a battery, it will merely change from mission to brownout mode and back to mission mode. If the battery can be manually disconnected, the required reset will occur, but this operation is cumbersome and does not lend itself to mass production (automated programming). It is far better to use the ICE_E pin of the 652X chip to generate a watchdog reset (the TERIDIAN TFP-2 programmer will support this mode of operation). The TFP-2 will be able to control the ICE_E pin, taking it low to initiate a reset caused by a watchdog time-out. The reset is important also, because the CE must be halted before any operations can be initiated that affect the flash memory.

Here is what is required for a 71M651X–based hardware design:

1) **The hardware watchdog timer should be enabled (V1 < V3P3 – 400mV)**
2) **In order to program the chip on the PCB, there must be a way to disable the hardware watchdog timer. This can be done, for example, by providing a jumper that temporarily connects V1 directly to V3P3 (see Figure 1).**

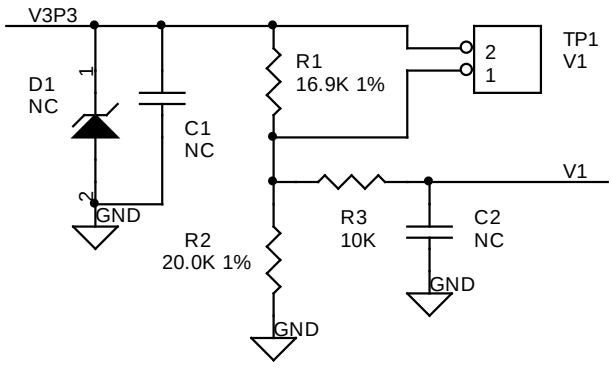

Figure 1: Circuit for V1

Below is a brief summary of the hardware precautions for the 71M652X chips:

1) **The hardware watchdog timer must be enabled (V1 < V3P3A - 400mV)**
2) **There must be a provision for a hardware reset, as shown in Figure 2, or for cycling power (including disruption of the battery power, if applicable).**
3) **To enable operation with the TFP-2, the ICE_E signal should be brought out to pin 2 of the programming connector, as shown in Figure 3.**
4) **The ICE_E signal should not be tied directly to GND but pulled down by a 1kΩ resistor, as shown in Figure 3, in order to enable the TFP-2 to pull it up.**

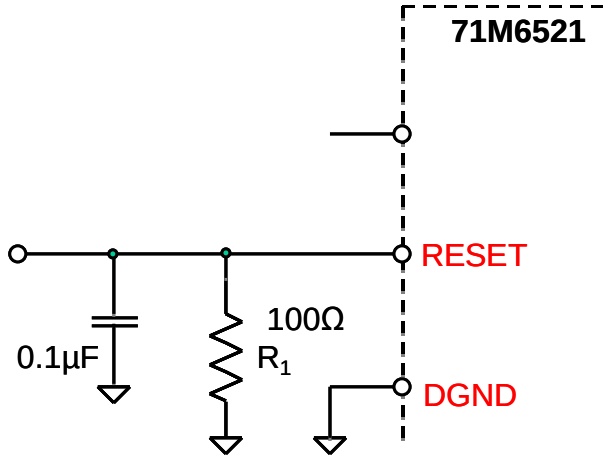

Figure 2: Reset Circuit for the 652X

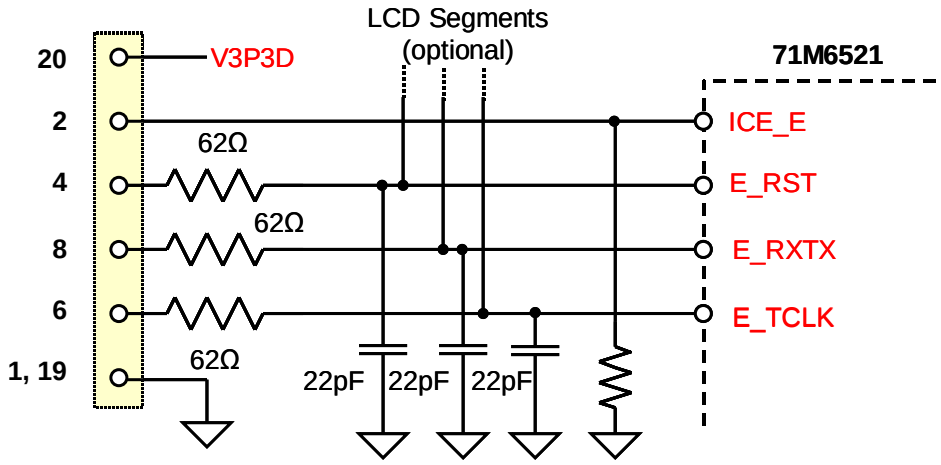

Figure 3: ICE Interface for the 652X

Precautions to be Taken in Firmware Design

With *ECK_DIS* = 1, no clock will appear at the E_TCLK pin, causing emulators and programming devices to malfunction. If the *ECK_DIS* is set to 1 early during code execution, recovery requires precise timing.

The ADM51 ICE and the TFP-2 can “break” into the 651X by quickly reacting to the E_RST signal.

Programming devices such as the TFP-1 may need the clock signal at the E_TCLK pin active for a longer time (at least one second) in order to handshake with the PC that they are connected to, before they can become active.

The following rule applies to 71M651X and 71M652X chips that will need to be re-programmed at some time during their life cycle:

If setting the *ECK_DIS* bit is necessary, *ECK_DIS* should be set late during program execution (1,000ms after reset) so that a programming device can erase and reprogram the chip.

Maxim Integrated Products, 120 San Gabriel Drive, Sunnyvale, CA 94086 408-737-7600