SST89E/V516RDx and SST89E/V58RDx Security Features

Application Note
August 2008

1.0 INTRODUCTION

The SST89E/V58RDx / SST89E/V516RDx offer advanced security features that can protect against software piracy and code corruption resulting from accidental erasing and programming to the internal flash memory locations. Through proper usage of the security features and In-Application Programming (IAP) commands, it is possible to attain protection of code, while allowing the flexibility of authorized code updates. There are two different types of security locks in the SST89E/V58RDx / SST89E/V516RDx security system: hard lock and SoftLock. These two security lock types can be enabled on the two internal flash blocks in one of six combinations. The following is a general description of each security lock type and the six possible security lock options.

2.0 HARD LOCK

When a block is hard locked, the following security measures are put in place:

1. MOVC commands executed from program code residing in an unlocked (external memory is always considered unlocked) or soft locked flash block is not allowed to access a target address in a hard locked flash block. This protects against software piracy by making the code in the hard locked block inaccessible to less secure code.
2. All external host mode and IAP commands (except for Chip-Erase and Prog-SBx) are disabled for the hard locked flash block.
3. EA# is sampled and latched on reset which prevents it from being switched during the middle of code execution and jumping to external code.

3.0 SOFTLOCK

SoftLock allows the flash contents to be read and altered under a secure environment. This lock option allows the user to update program code in the soft locked flash block by executing IAP commands from the other flash block. A flash block that is soft locked will have the following security measures in place:

1. MOVC commands executed from program code residing in an unlocked (external memory is always considered unlocked) flash block are not allowed to access a target address in a soft locked flash block. This protects against software piracy by making the code in the soft locked block inaccessible to less secure code.
2. IAP commands (except Chip-Erase and Prog-SBx) issued from an unlocked flash block (external memory is always considered unlocked) are disabled.
3. IAP commands issued from a soft locked flash block to a flash block of the same security level or lower are enabled. Thus, IAP commands issued from a hard locked flash block to a soft locked flash block are also enabled.
4. EA# is sampled and latched on reset which prevents it from being switched during the middle of code execution and jumping to external code.

4.0 SECURITY LOCK GUIDELINES

4.1 Programming the Security Lock Bits

There are six general ideas to remember when programming the security lock bits:

1. Security in the SST89E/V58RDx / SST89E/V516RDx is controlled by the three security lock bits SB1, SB2, and SB3.
2. The three bits can be programmed through external host mode or IAP using the Prog-SB1, Prog-SB2, and Prog-SB3 commands. The security bits can always be programmed regardless of the current security level.
3. Once one of the security lock bits has been programmed, it cannot be unprogrammed except by an external host mode or IAP Chip-Erase command that will unprogram all three security lock bits.
4. The status of the security lock bits can be checked at any time by looking at the three bits located in the special function register SFST[7:5].
5. There are eight possible combinations of the security lock bits. Security level 3 has two security options that contain two combinations each. This leaves a total number of six different security lock options. (See Table 9-2)
6. The six security lock options are grouped into 4 different security levels. The four security levels and the six individual security lock options are described below and summarized in Table 7-1, Table 7-2, Table 9-1, and Table 9-2.

4.2 IAP Command Interactions

IAP commands interact with the security lock functions as follows:

1. IAP commands executed from a higher security level can always access flash blocks of a lower security level (hard lock to SoftLock or unlock and SoftLock to unlock).
2. IAP commands executed from a SoftLock or unlock security level may access the other flash block if it is the same security level (SoftLock to SoftLock, and unlock to unlock).
3. IAP security commands are always enabled regardless of security level if executed from Block 1 or external memory.
4. IAP Chip-Erase is always enabled from external memory regardless of security level.

5.0 SECURITY LEVEL 1 - NO SECURITY

Security level 1 exists when all three security lock bits are unprogrammed. This is the default security state after a Chip-Erase command has been executed either through external host mode or IAP. In this state, the Security-Status bits (SFST[7:5]) will read 000b. In security level 1, all security features are disabled for both internal flash blocks and both are unlocked. The MOVC command and all external host mode and IAP commands are enabled on both blocks.

6.0 SECURITY LEVEL 2 SOFTLOCK/SOFTLOCK CODE CORRUPTION PREVENTION

Security level 2 can only be reached from security level 1 by programming security bit SB1 through either external host mode or IAP Prog-SB1 and leaving the other two bits unprogrammed.

In security level 2, SoftLock/SoftLock:

1. Both flash blocks are soft locked.
2. The Security-Status bits (SFST[7:5]) will read 100b.
3. External host mode and IAP Byte-Verify commands are allowed. IAP commands are allowed as long as they reside within Block 1 or Block 0[1].
4. MOVC commands are disabled from external memory to any of the flash blocks, but can be executed by either Block 0 or Block 1 on itself or any of the flash blocks and external memory.

The following code segment will put the SST89E/V58RDx / SST89E/V516RDx in security level 2 (100b) from security level 1 (000b) using an IAP command with interrupt:

```
ORL     SFCF, #40H      ; enable IAP commands
MOV     SFDT, #0AAH     ; program security bit setup
MOV     SFCM, #8FH      ; issue Prog-SB1 IAP
                        ; command
                        ; interrupt INT1# occurrence
                        ; indicates completion
```

7.0 SECURITY LEVEL 3 CODE CORRUPTION AND SOFTWARE PIRACY PREVENTION WITH CONTROLLED CODE UPDATE

Security level 3 includes three of the six security lock options. In each of these three security types, MOVC commands from external memory are disabled and EA# is sampled and latched on reset which prevents someone from switching it during the middle of code execution and jumping to external code. Each one will be described separately.

7.1 Level 3 SoftLock/SoftLock

This security type can only be reached from security level 1 by programming security bit SB2 through either external host mode or IAP Prog-SB2 and leaving the other two bits unprogrammed.

In security level 3, SoftLock/SoftLock:

1. Both flash blocks are soft locked.
2. The Security-Status bits (SFST[7:5]) will read 010b.
3. All external host mode commands (except Chip-Erase and Prog-SBx) are disabled.
4. All IAP commands (except IAP Chip-Erase) executed from either Block 0 or Block 1 are enabled.
5. MOVC commands are disabled from external memory to any of the flash blocks, but can be executed by either Block 0 or Block 1 on itself or any of the flash blocks and external memory.

1. All IAP commands except IAP security commands and IAP Chip-Erase. IAP security commands can only be executed from Block 1 and external memory, but not Block 0. IAP Chip-Erase can only be executed from external memory.

The code residing in the internal flash blocks is protected from software piracy because it is inaccessible from external sources. The code in both blocks can still be updated in a controlled environment. Code executing in Block 1 can update the code in Block 0 and vice versa. Thus, the user can design a method to perform field updates without exposing the code residing in the internal flash blocks. However, since the code in either block can be altered via IAP, it is possible that the code performing those IAP commands could become corrupt, which would in turn corrupt the other block.

The following code segment will put the SST89E/V58RDx / SST89E/V516RDx in security level 3, SoftLock/SoftLock, (010b) from security level 1 (000b) using an IAP command with interrupt:

```
ORL     SFCF,#40H       ; enable IAP commands
MOV     SFDT, #0AAH     ; program security bit setup
MOV     SFCM, #83H      ; issue Prog-SB2 IAP command
                        ; interrupt INT1# occurrence
                        ; indicates completion
```

7.2 Level 3 Hard Lock/SoftLock

This security lock option can be reached from security levels 1, 2, or 3. Refer to Table 7-1 for combinations.

In security level 3, hard lock/SoftLock:

1. Block 1 is hard locked and Block 0 is soft locked.
2. The Security-Status bits (SFST[7:5]) will read 001b or 110b.
3. All external host mode commands (except Chip-Erase and Prog-SBx) are disabled.
4. Only Block 1 can IAP to Block 0. IAP Chip-Erase can be executed from external memory to either of the flash blocks.
5. MOVC commands from Block 0 to Block 1 are disabled, but are enabled from Block 1 to Block 0.

Since the code in Block 1 is hard locked, it is protected from code corruption because it cannot be altered. The code residing in Block 1 and Block 0 is completely protected from software piracy because it cannot be accessed externally. However, the user can still perform code updates on Block 0 by using IAP commands executed from the secure Block 1. This security state is more secure than the SoftLock/SoftLock state because the code that updates Block 0 resides in Block 1 which is hard locked and therefore protected from corruption.

The following code segment will show one way to put the SST89E/V58RDx / SST89E/V516RDx in security level 3 hard lock/SoftLock (001b) from security level 1 unlock/unlock (000b) using an IAP command with interrupt:

```
ORL     SFCF, #40H      ; enable IAP commands
MOV     SFDT,#0AAH      ; program security bit setup
MOV     SFCM, #85H      ; #85H = "001" (Prog-SB3 IAP
                        ; command)
                        ; interrupt INT1# occurrence
                        ; indicates completion
```

The following example will put the SST89E/V58RDx / SST89E/V516RDx in security level 3 hard lock/SoftLock (110b) from security level 2 SoftLock/SoftLock (100b).

```
MOV     SFCF, #40H      ; enable IAP commands
MOV     SFDT, #0AAH     ; program security bit setup
MOV     SFCM, #83H      ; #83H = "110" (Prog-SB2 IAP
                        ; command)
                        ; interrupt INT1# occurrence
                        ; indicates completion
```

The following example will put the SST89E/V58RDx / SST89E/V516RDx in security level 3 hard lock/SoftLock (110b) from security level 3 SoftLock/SoftLock (010b).

```
MOV     SFCF, #40H      ; enable IAP commands
MOV     SFDT, #0AAH     ; program security bit setup
MOV     SFCM, #8FH      ; #8FH = "110" (Prog-SB1 IAP
                        ; command)
                        ; interrupt INT1# occurrence
                        ; indicates completion
```

7.3 Level 3 Hard Lock/Hard Lock

Level 3 hard lock/hard lock security level can be reached from security levels 1, 2, or 3. If the SST89E/V58RDx / SST89E/V516RDx's current security level in level 3 is 110b, then only security level 4, hard lock/hard lock, can be reached. Table 7-2 shows the combinations for going from security levels 1, 2, or 3.

In security level 3, hard lock/hard lock:

1. Both flash blocks are hard locked.
2. The Security-Status bits (SFST[7:5]) will read 011b or 101b.
3. All external host mode and IAP commands (except Chip-Erase and Prog-SBx) are disabled.
4. MOVC commands are disabled from external memory to any of the flash blocks, but can be executed by either Block 0 or Block 1 on itself or any of the flash blocks and external memory.

Application Note

In this mode, both blocks are protected from software piracy and code corruption because all Program and Erase commands (except Chip-Erase and Prog-SBx) are disabled.

The following code segment will put the SST89E/V58RDx / SST89E/V516RDx in security level 3 hard lock/hard lock (101b) from security level 2 SoftLock/SoftLock (100b) using an IAP command with interrupt:

```
ORL     SFCF, #40H      ; enable IAP commands
MOV     SFDT, #0AAH     ; program security bit setup
MOV     SFCM, #85H      ; issue Prog-SB3 IAP command
                        ; interrupt INT1# occurrence
                        ; indicates completion
```

The following code segment will put the SST89E/V58RDx / SST89E/V516RDx in security level 3 hard lock/hard lock (011b) from security level 3 SoftLock/SoftLock (010b) using an IAP command with interrupt:

```
ORL     SFCF, #40H      ; enable IAP commands
MOV     SFDT, #0AAH     ; program security bit setup
MOV     SFCM, #85H      ; #85H = "001"
                        ; (Prog-SB3 IAP command)
                        ; interrupt INT1# occurrence
                        ; indicates completion
```

The following code segment will show one way to put the SST89E/V58RDx / SST89E/V516RDx in security level 3 hard lock/hard lock (011b) from security level 3 hard lock/ SoftLock using an IAP command with interrupt if SFST[7:5] is 001b:

```
ORL     SFCF, #40H      ; enable IAP commands
MOV     SFDT, #0AAH     ; program security bit setup
MOV     SFCM, #83H      ; issue Prog-SB2 IAP command
                        ; interrupt INT1# occurrence
                        ; indicates completion
```

TABLE 7-1: SECURITY LEVEL 3 HARD LOCK/SOFTLOCK COMBINATIONS

Device	Current Security Level (Block 1 / Block 0)	Current SFST[7:5]	New Security Level (Block 1 / Block 0)	New SFST[7:5] value
SST89E/V58RDx SST89E/V516RDx	1 (Unlock/Unlock)	000b	3 (Hard Lock/SoftLock)	001b/110b
	2 (SoftLock/SoftLock)	100b		110b
	3 (SoftLock/SoftLock)	010b		110b

T7-1.0 2040

TABLE 7-2: SECURITY LEVEL 3 HARD LOCK/HARD LOCK COMBINATIONS

Device	Current Security Level (Block 1 / Block 0)	Current SFST[7:5]	New Security Level (Block 1 / Block 0)	New SFST[7:5] value
SST89E/V58RDx SST89E/V516RDx	1 (Unlock/Unlock)	000b	3 (Hard Lock/Hard Lock)	011b/101b
	2 (SoftLock/SoftLock)	100b		101b
	3 (SoftLock/SoftLock)	010b		011b
	3 (Hard Lock/SoftLock)	001b		011b/101b

T7-2.0 2040

8.0 SECURITY LEVEL 4 - HARD LOCK/ HARD LOCK MAXIMUM SECURITY

Level 4 can be reached from any of the other security configurations by simply programming all of the unprogrammed security bits SB1, SB2, and SB3 through either external host mode or IAP.

In security level 4, hard lock/hard lock:

1. Both flash blocks are hard locked.
2. The Security-Status bits (SFST[7:5]) will read 111b.
3. All external host mode commands (except Chip-Erase) are disabled.
4. All IAP commands are disabled.
5. MOVC commands are disabled from external memory to any of the flash blocks, but can be executed by either Block 0 or Block 1 on itself or any of the flash blocks and external memory.
6. Execution of external code is disabled regardless of EA#. The only exception to this is if the code jumps to code space that doesn't exist in either internal block (8000H to DFFFH for SST89E/V58RDx). In this case, external code will be executed (even if it doesn't exist!).

In this security state, internal code is protected from both corruption and software piracy since erase and program commands are disabled on both flash blocks and internal code is externally inaccessible. Additionally, the microcontroller can only be used to start the user code residing in its internal flash memory.

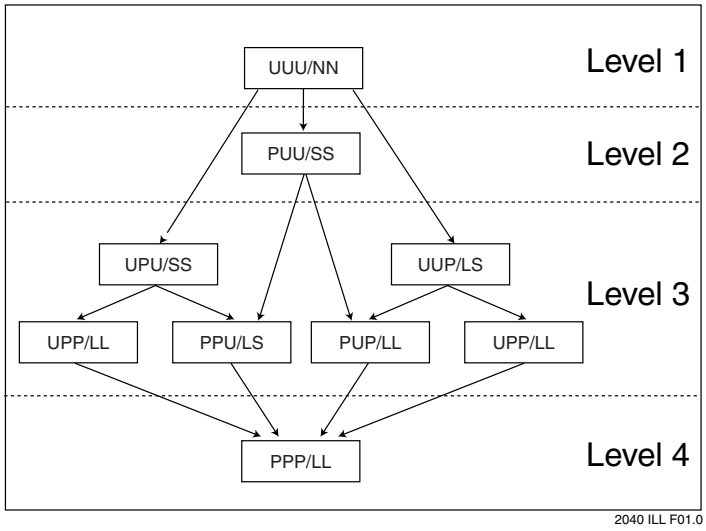
The following code segment will put the SST89E/V58RDx / SST89E/V516RDx in security level 4 (111b) from security level 1 (000b) using IAP commands with interrupts:

```
ORL     SFCF, #40H      ; enable IAP commands
MOV     SFDT, #0AAH     ; program security bit setup
MOV     SFCM, #8FH      ; issue Prog-SB1 IAP command
                        ; interrupt INT1# occurrence
                        ; indicates completion

MOV     SFDT, #0AAH     ; program security bit setup
MOV     SFCM, #83H      ; issue Prog-SB2 IAP command
                        ; interrupt INT1# occurrence
                        ; indicates completion

MOV     SFDT, #0AAH     ; program security bit setup
MOV     SFCM, #85H      ; issue Prog-SB3 IAP command
                        ; interrupt INT1# occurrence
                        ; indicate completion
```

9.0 SECURITY LOCK LEVELS, OPTIONS, AND ACCESS



Note: P = programmed (Cell logic state = 0), U = unprogrammed (Cell logic state = 1), N = not locked, L = hard locked, S = soft locked

FIGURE 9-1: SECURITY LOCK LEVELS

TABLE 9-1: SECURITY LOCK OPTIONS

Level	Security Lock Bits[1,2]				Security Status of:		Security Type
	SFST[7:5]	SB1	SB2	SB3	Block 1	Block 0	
1	000	U	U	U	Unlock	Unlock	No security features are enabled.
2	100	P	U	U	SoftLock	SoftLock	MOVC instructions executed from external program memory are disabled from fetching code bytes from internal memory, EA# is sampled and latched on Reset, and further programming of the flash is disabled.
3	010	U	P	U	SoftLock	SoftLock	Level 2 plus external host Byte-Verify disabled. Code in Block 1 may program Block 0 and vice versa.
	110 001	P U	P U	U P	Hard Lock	SoftLock	Level 2 plus external host Byte-Verify disabled. Code in Block 1 may program Block 0.
	011 101	U P	P U	P P	Hard Lock	Hard Lock	Level 2 plus external host Byte-Verify disabled, both blocks locked.
4	111	P	P	P	Hard Lock	Hard Lock	Same as Level 3 hard lock/hard lock, but MCU will start code execution from the internal memory regardless of EA#.

T9-1.0 2040

1. SFST[7:5] = Security Lock Decoding Bits (SB1, SB2, SB3).
2. P = Programmed (Cell logic state = 0);
   U = Unprogrammed (Cell logic state = 1).

TABLE 9-2: SECURITY LOCK ACCESS TABLE

Level	SFST[7:5]	Source Address[1]	Target Address[2]	Byte-Verify Allowed		MOVC Allowed	
				External Host[3]	IAP	516RDx	58RDx
4	111b (Hard Lock on both blocks)	Block 0/1	Block 0/1	N	N	Y	Y
			External	N/A	N/A	N	Y
		External	Block 0/1	N	N	N	N
			External	N/A	N/A	N	Y
3	011b/101b (Hard Lock on both blocks)	Block 0/1	Block 0/1	N	N	Y	Y
			External	N/A	N/A	N	Y
		External	Block 0/1	N	N	N	N
			External	N/A	N/A	Y	Y
	001b/110b (Block 0 = SoftLock, Block 1 = Hard Lock)	Block 0	Block 0	N	N	Y	Y
			Block 1	N	N	N	N
			External	N/A	N/A	N	Y
		Block 1	Block 0	N	Y	Y	Y
			Block 1	N	N	Y	Y
			External	N/A	N/A	N	Y
		External	Block 0/1	N	N	N	N
			External	N/A	N/A	Y	Y
	010b (SoftLock on both blocks)	Block 0	Block 0	N	N	Y	Y
			Block 1	N	Y	Y	Y
			External	N/A	N/A	N	Y
		Block 1	Block 0	N	Y	Y	Y
			Block 1	N	N	Y	Y
			External	N/A	N/A	N	Y
		External	Block 0/1	N	N	N	N
			External	N/A	N/A	Y	Y
2	100b (SoftLock on both blocks)	Block 0	Block 0	Y	N	Y	Y
			Block 1	Y	Y	Y	Y
			External	N/A	N/A	N	Y
		Block 1	Block 0	Y	Y	Y	Y
			Block 1	Y	N	Y	Y
			External	N/A	N/A	N	Y
		External	Block 0/1	Y	N	N	N
			External	N/A	N/A	Y	Y
1	000b (unlock)	Block 0	Block 0	Y	N	Y	Y
			Block 1	Y	Y	Y	Y
			External	N/A	N/A	N	Y
		Block 1	Block 0	Y	Y	Y	Y
			Block 1	Y	N	Y	Y
			External	N/A	N/A	N	Y
		External	Block 0/1	Y	Y	N	Y
			External	N/A	N/A	Y	Y

T9-2.0 2040

1. Location of MOVC or IAP instruction.
2. Target address is the location of the byte being read.
3. External host Byte-Verify access does not depend on a source address.