TECHNICAL NOTE

ABSTRACT
This technical note provides additional information about the code security feature of the P89(L)V51RB2/RC2/RD2 microcontroller family from Philips Semiconductors.

Disclaimer
Described applications are for illustrative purposes only. Philips Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

MACC-05009

P89(L)V51Rx2 Code security

Author: Paul Seerden

2005 November 25

Philips Semiconductors

PHILIPS

SECURITY BIT

Bit location six of the Flash Status Register (FST.6) at SFR address B6h of the P89(L)V51Rx2 contains the Security Bit SB.

This bit is used to protect against software piracy and prevents the contents of the flash from being read by unauthorized parties. It also protects against code corruption resulting from accidental erasing and programming of the internal flash memory.

The following sections describe in more detail the level of protection against different internal and external ways of accessing the on-chip flash memory.

MOVC INSTRUCTIONS

With SB set only MOVC instructions executed from external program memory are disabled from fetching code bytes from internal memory (see table below)

Table 1: MOVC with SB set

Source Address	Target Address	MOVC allowed	
		V51RD2	V51RC2/RB2
Block 0	Block 0	Yes	Yes
	Block 1	Yes	Yes
	External	No	Yes
Block 1	Block 0	Yes	Yes
	Block 1	Yes	Yes
	External	No	Yes
External	Block 0/1	No	No
	External	Yes	Yes

IN APPLICATION PROGRAMMING

The Flash may be programmed or erased in the end-user application by calling low-level routines through a common entry point, this is called IAP.

With the Security Bit set, the user is still allowed to update program code using IAP commands. In other words: code in Block 1 may program Block 0 and vice versa.

The following IAP commands can still be operated on both blocks: Block-Erase, Sector-Erase, Byte-Program and Byte-Verify

PARALLEL PROGRAMMER

The Flash may also be programmed or erased using the parallel method by a commercially available programmer, which supports this device.

When the Security Bit is activated all parallel programming commands except for Chip-Erase are ignored (thus the device cannot be read and verified).

IN SYSTEM PROGRAMMING

In-System Programming (ISP) capability, is provided to allow the user code to be programmed in-circuit through the serial port (UART) controlled by internal firmware (provided by Philips), called the Bootloader.

With the Security Bit set, ISP reading, writing, or erasing of the user's code can still be performed. For that reason a Serial Number is implemented. Therefore, when a user requests to program the Security Bit, to be save he should also program a Serial Number into the device.

SERIAL NUMBER

The LV51 devices have the option of storing a 31-byte serial number along with the length of the serial number (for a total of 32 bytes) in a non-volatile memory space. When ISP mode is entered, the serial number length is evaluated to determine if the serial number is in use. If the length of the serial number is programmed to either 00H or FFH, the serial number is considered not in use. If the serial number is in use, reading, programming, or erasing of the user code memory or the serial number is blocked until the user transmits a 'verify serial number' command containing a serial number and length that matches the serial number and length previously stored in the device. The user can reset the serial number to all zeros and set the length to zero by sending the 'reset serial number' command. In addition, the 'reset serial number' command will also erase all user code.