AN1267
APPLICATION NOTE

Advanced Features of the M50FW040 Firmware Hub

CONTENTS

INTRODUCTION

The new STMicroelectronics M50FW040 Firmware Hub Flash Memory is a 4 Mbit device with additional features that are designed to add flexibility for PC platform designers, while lowering the overall system cost. This technical brief describes the additional features of the M50FW040.

The M50FW040 Advanced Features are:

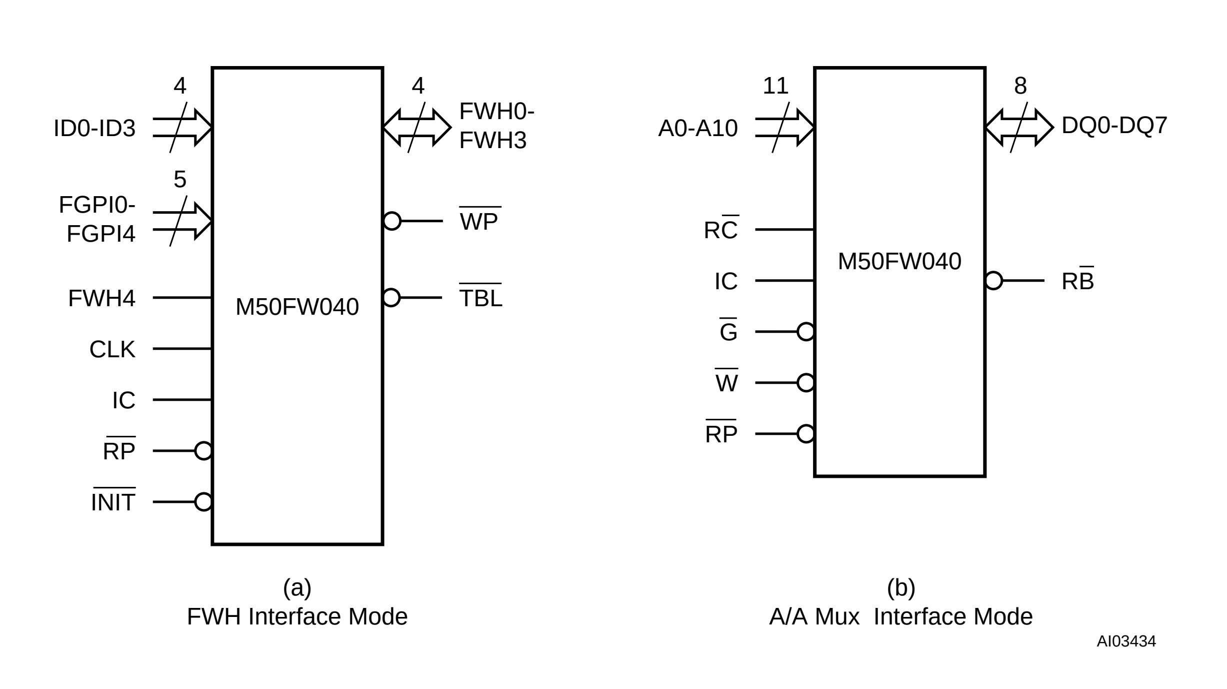
- Two Interface Modes:
  - A/A Mux Interface Mode for bulk programming
  - FWH Interface Mode for in-system use
- Hardware Write Protect Pins for Block Protection
- Register Based Block Locking
- 5 General Purpose Input Pins
- Capability to cascade multiple devices using Identification Inputs

The Logic Diagram of the STMicroelectronics M50FW040 is shown in Figure 1; the memory block addresses are shown in Table 1.

Table 1. M50FW040 Memory Block Addresses

Block Number	Block Size (Kbytes)	Address Range	Block Type
7	64	70000h-7FFFFh	Top Block
6	64	60000h-6FFFFh	Main Block
5	64	50000h-5FFFFh	Main Block
4	64	40000h-4FFFFh	Main Block
3	64	30000h-3FFFFh	Main Block
2	64	20000h-2FFFFh	Main Block
1	64	10000h-1FFFFh	Main Block
0	64	00000h-0FFFFh	Main Block

Figure 1. M50FW040 Logic Diagram



A/A MUX INTERFACE MODE

A/A Mux Interface mode of operation is designed to be compatible with existing flash programming equipment for production line programming. It provides a method for component distributors and motherboard manufacturers to pre-program the Flash before and during the motherboard build process. The A/A Mux mode is not designed to be the primary interface during normal use in PC systems. Normal operations should use the FWH Interface mode of operation. A/A Mux Interface mode is selected by driving the Interface Configuration pin, IC, high. The Interface Configuration pin must be driven during reset or prior to power-up and must not be changed during operation.

FWH INTERFACE MODE

FWH Interface mode is used for normal operation and for access to the advanced features in the M50FW040. This mode is selected by driving the Interface Configuration pin, IC, low. The Interface Configuration pin has an internal pull-down resistor, so this pin can be left unconnected to select FWH Interface mode. The Interface Configuration pin must be set during reset or prior to power-up and must not be changed during operation. The advanced features detailed in the following sections are only accessible in FWH Interface mode.

Hardware Write Protection

There are two pins that provide write protect capabilities, Top Block Lock and Write Protect. These pins are designed to provide a hardware write protect mechanism directly to the Flash core. If the state of either of these pins changes during a program, erase, or suspend command, the M50FW040 block protection does not change until after completion of the command in progress.

The Top Block Lock pin, $\overline{TBL}$, controls write access to the top most block of the Flash array. When held low, Top Block Lock prevents program or block erase operations on the top 64 Kbytes block where critical code can be stored. Motherboard designers can use the Top Block for local PC boot code and remote program load information, which are normally not modified after manufacturing.

The Write Protect pin, $\overline{WP}$, provides the same function as Top Block Lock but affects all remaining blocks. It can be used in conjunction with Top Block Lock to write protect the entire Flash array. These pins override the function of the software Lock Registers, which are discussed in the Register Based Locking section that follows. There is no default status register to detect the state of these pins, however motherboard designers can use the General Purpose Input pins, FGPI0-FGPI4, report their state. This is shown in detail in the General Purpose Input Pins section of this application note.

Register Based Locking

Access to the Flash array is additionally controlled by a Lock Register for each 64 Kbytes block. The M50FW040 register configuration map is shown in Table 2. Each block has its own Lock Register. The default value for all Lock Registers at power up or after reset is 01h (write locked). Three bits within each register control access to the blocks: the Read Lock bit, the Write Lock bit and the Lock Down bit. The independent access for each block provides flexibility for system designers to control access to specific regions of the Flash array. This can be useful for backup copies of critical program code and confidential data that is to be stored away from user access.

The significance of the three bits in the Lock Registers is:

Read Lock. The block is protected from read access when set.

Write Lock. The block is protected from write access when set.

Lock Down. Lock Down prevents further set or clear operations to the Lock Register bits when set. Lock Down can only be set by software, it cannot be cleared by software once set. The bit is cleared after power cycle or reset operations.

Table 2. M50FW040 Lock Register Configuration Map

Memory Address	Register Name	Default Value	Access
FFBF0002h	70000h-7FFFFh (Top Block) Lock Register	01h	R/W
FFBE0002h	60000h-6FFFFh Lock Register	01h	R/W
FFBD0002h	50000h-5FFFFh Lock Register	01h	R/W
FFBC0002h	40000h-4FFFFh Lock Register	01h	R/W
FFBB0002h	30000h-3FFFFh Lock Register	01h	R/W
FFBA0002h	20000h-2FFFFh Lock Register	01h	R/W
FFB90002h	10000h-1FFFFh Lock Register	01h	R/W
FFB80002h	00000h-0FFFFh Lock Register	01h	R/W

The Write Lock bit is sampled at the beginning of the operation and must be set to the desired protection state prior to starting a program or erase operation. The state of the bit should not be changed until the end of the operation. If the state of the Write Lock bit is changed during program or erase suspend, the change will not take effect until the end of the suspended operation. Individual bit settings are shown in Table 3, Lock Register Truth Table.

Table 3. Lock Register Truth Table

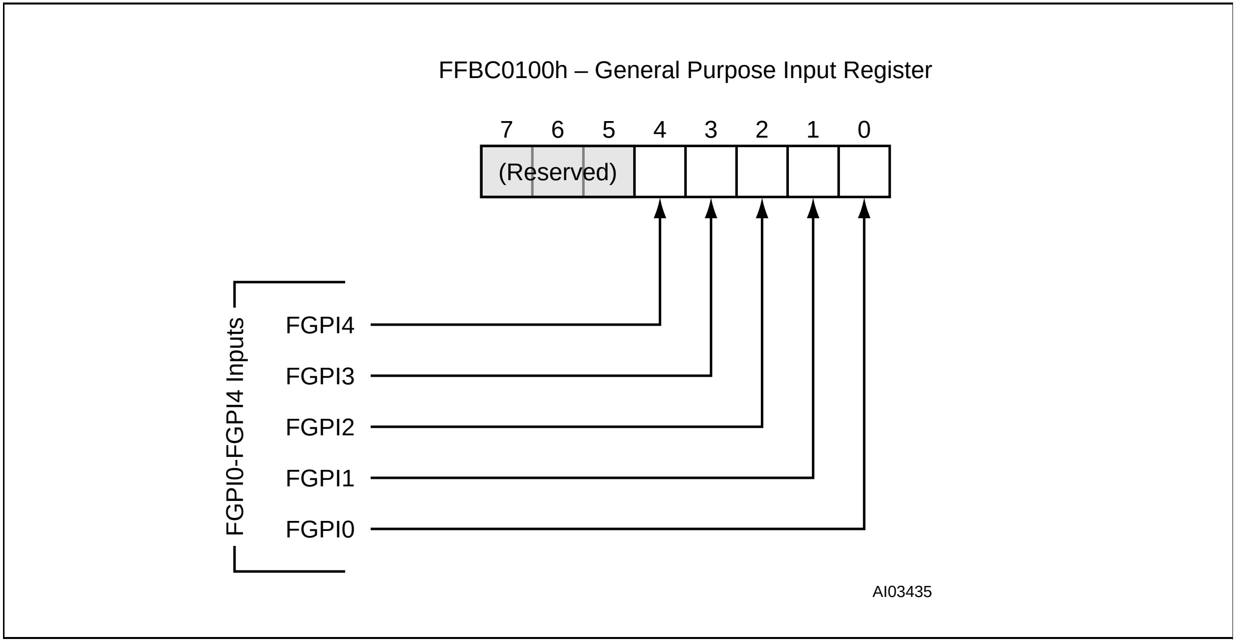
Reserved Bits DQ7-DQ3	Read Lock DQ2	Lock Down DQ1	Write Lock DQ0	Hex Value	Resulting Block State
00000	0	0	0	00h	Full R/W Access
	0	0	1	01h	Write Locked (default)
	0	1	0	02h	Locked Open
	0	1	1	03h	Write Locked Down
	1	0	0	04h	Read Locked
	1	0	1	05h	Read and Write Locked
	1	1	0	06h	Read Locked Down
	1	1	1	07h	Read and Write Locked Down

Note that the hardware write protection pins (Top Block Lock and Write Protect) take precedence over the software locking registers. When Top Block Lock or Write Protect is active, no write access is allowed to the Flash array regardless of the state of the Lock Register.

General Purpose Input Pins

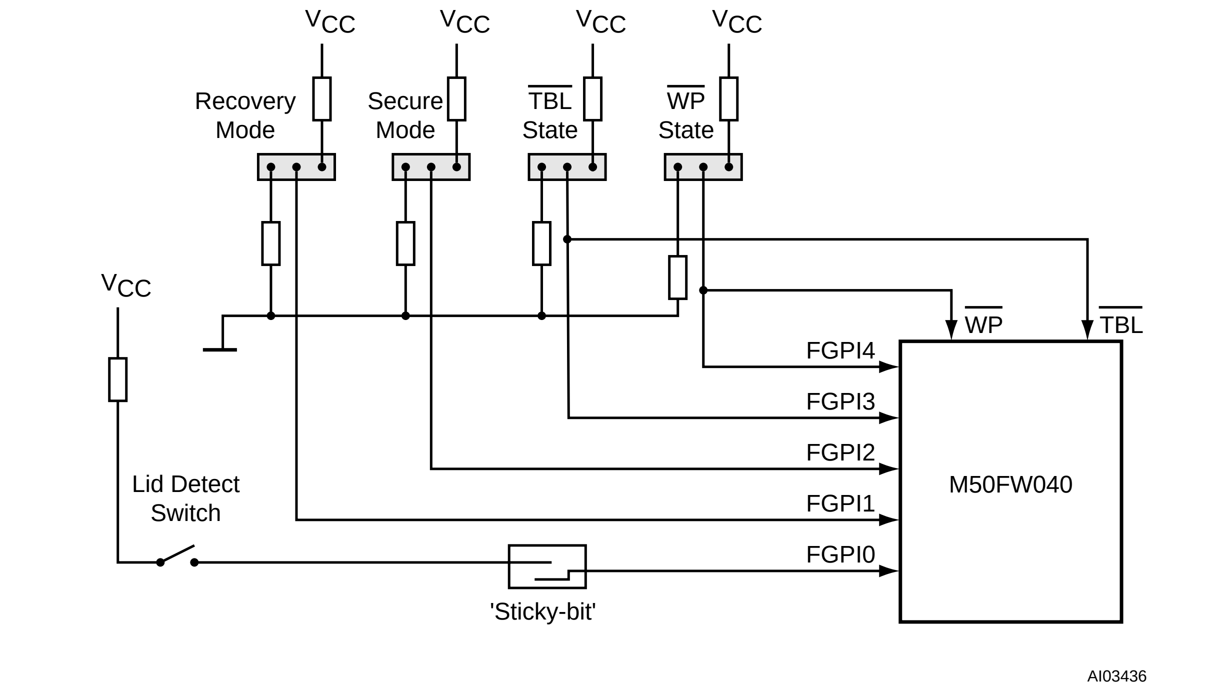
The M50FW040 provides 5 General Purpose Input pins which are mapped internally to a register as shown in Figure 2. This is a pass-through register, meaning that the five input pins are mapped internally to the register. The register can be read during boot to determine on board device status.

Figure 2. M50FW040 General Purpose Input Register Bit Assignments



A simple example of a motherboard implementation is shown in Figure 3. The 5 General Purpose Input pins, FGPI0-FGPI4 are connected to various mother board functions to determine status during pre-boot of the Operating System.

Figure 3. Example Usage of the General Purpose Input pins FGPI0-FGPI4



In this example, the General Purpose Input pin assignments are as follows:

FGPI0, Lid Detect Switch. The input is connected to a sticky latch which is set when the system unit top cover has been opened. Upon power-up, the FGPI register is read to determine if a transition has occurred. Removal of the system unit cover can be a security breach, thus the implementation provides another level of secure access.

FGPI1, Recovery mode. A jumper on the motherboard could be moved by a user or administrator to clear the contents of NVRAM, and boot the system using the critical code stored in the top block. This is sometimes necessary if the BIOS image gets corrupted - for example after a power outage during a write operation.

FGPI2, Secure Mode. By placing the jumper in a desired position, the system passwords can be bypassed. This is useful for a system administrator to access a system when a user has lost or forgotten a password.

FGPI3, Top Block Lock Status. Used to monitor the status of the Top Block Lock pin, $\overline{\text{TBL}}$.

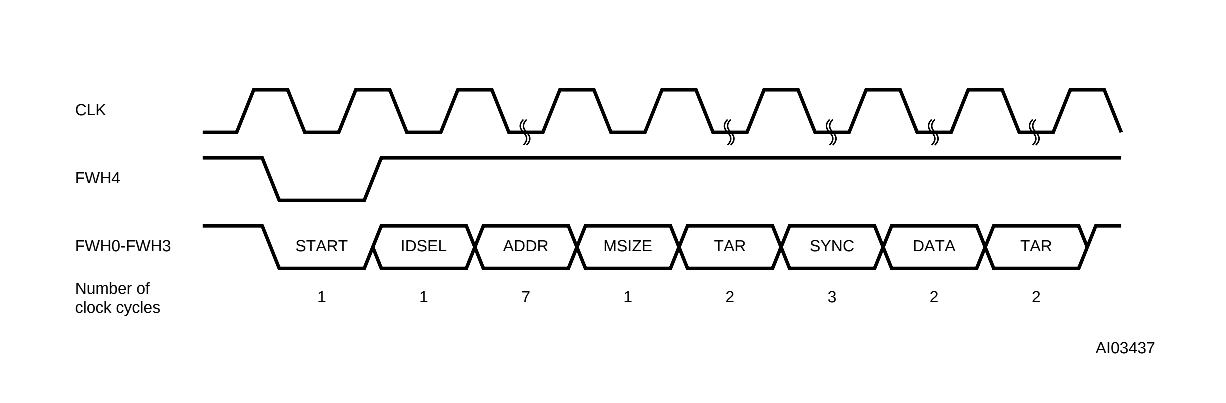
FGPI4, Write Protect Status. Used to monitor the status of the Write Protect pin.

Identification Inputs

The Identification Input pins, ID0-ID3, are used to map the M50FW040 into the system memory map. It is possible to connect up to 16 devices, but this may be limited due to bus loading and BIOS support. Multiple devices can be useful in certain instances, for example if more General Purpose Inputs are required or, possibly, when more Flash Memory is required but a higher density device is not available.

The appropriate device is selected and responds when the ID Select, IDSEL, field in the FWH cycle on the Low Pin Count, LPC, bus is compared to the hardware strapping on each devices ID pins.

Figure 4. Example FWH Cycle showing IDSEL



The host controller has the ability to select which Firmware Hub array maps into each region of the system address space. In the existing host controller, the 4 Mbyte address map is broken into eight 512 Kbyte segments. Inside the host controller is a 32-bit register which contains the mapping information. Refer to the Intel 82801AA (ICH) and Intel 82801AB (ICH0) I/O Controller Hub data sheet for detailed information on the operation of the BIOS Select Register.

The BIOS Select Register is programmed by system BIOS. As an example of the mapping function, a system with eight 4 Mbit devices would program the register 01234567h. In this configuration, the top segment would be located in device 0 (always), the next 512 Kbytes segment would be located in device 1, and so on, as shown in Figure 5 and Table 4.

Figure 5. Example Usage of ID Select Signals

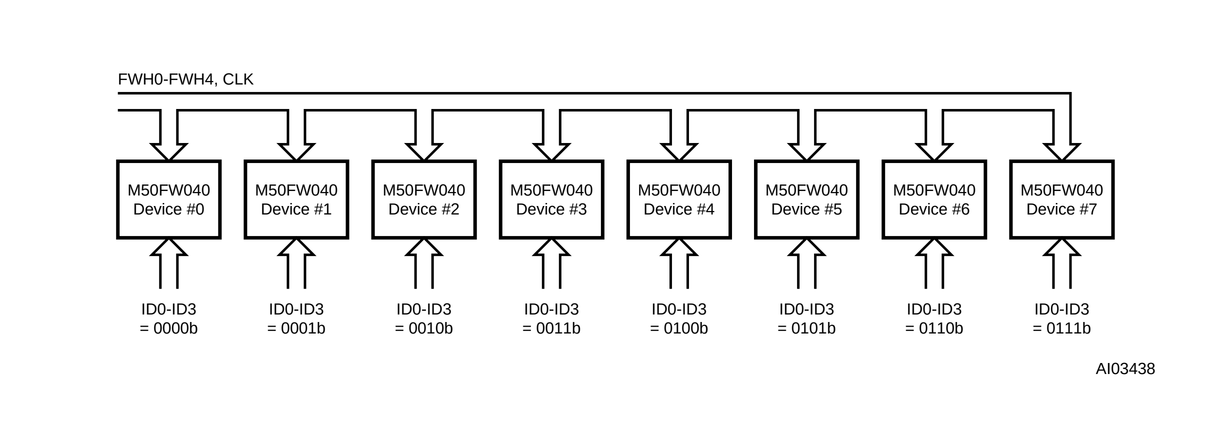


Table 4. Example System Memory Map

Device Number	Segment Size	Address Range
0	512 Kbytes	4 GB to 4GB – 0.5MB
1	512 Kbytes	4GB – 0.5MB to 4GB – 1MB
2	512 Kbytes	4GB – 1MB to 4GB – 1.5MB
3	512 Kbytes	4GB – 1.5MB to 4GB – 2MB
4	512 Kbytes	4GB – 2MB to 4GB – 2.5MB
5	512 Kbytes	4GB – 2.5MB to 4GB – 3MB
6	512 Kbytes	4GB – 3MB to 4GB – 3.5MB
7	512 Kbytes	4GB – 3.5MB to 4GB – 4MB
Main Memory Region		
0 to 16MB Compatibility Region		

CONCLUSION

The M50FW040 is a flexible Flash Memory with additional functions that can be useful to motherboard and system designers. The device is scalable, allowing multiple devices to connect together to expand the amount of Flash Memory available. Additional features like General Purpose Inputs add flexibility for system designers. The device also has several locking mechanisms to provide a secure path for system BIOS updates. All of these features make the M50FW040 a desirable device for future BIOS and resident OS implementations.

If you have any questions or suggestion concerning the matters raised in this document please send them to the following electronic mail address:

ask.memory@st.com (for general enquiries)

Please remember to include your name, company, location, telephone number and fax number.

Information furnished is believed to be accurate and reliable. However, STMicroelectronics assumes no responsibility for the consequences of use of such information nor for any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of STMicroelectronics. Specifications mentioned in this publication are subject to change without notice. This publication supersedes and replaces all information previously supplied. STMicroelectronics products are not authorized for use as critical components in life support devices or systems without express written approval of STMicroelectronics.

STMicroelectronics GROUP OF COMPANIES
Australia - Brazil - China - Finland - France - Germany - Hong Kong - India - Italy - Japan - Malaysia - Malta - Morocco -
Singapore - Spain - Sweden - Switzerland - United Kingdom - U.S.A.

http://www.st.com