TECHNICAL ARTICLE

FIRMWARE HUB (FWH): NEW GENERATION STORAGE FOR BIOS

James Lee
STMicroelectronics Inc.
Lexington, MA, USA

Sandro D'Angelo
STMicroelectronics
Catania, Italy

The traditional PC motherboard uses a chip-set containing two controllers, called the *North Bridge* and the *South Bridge.* Intel replaces these with the *Hub*. In the *Hub Architecture* the two controllers are connected to each other via a new Interlink dedicated bus. This is a high-speed bus that has twice the bandwidth of the PCI bus that works at 266 MBytes per second and resembles the new point-to-point channel. The new Intel PC platforms incorporate three primary components:

- the Memory Control Hub (MCH),
- the I/O Control Hub (ICH),
- the Firmware Hub (FWH).

They use the *Intel Hub Protocol* that allows a greater flow of information from the I/O controller to the memory controller.

What is the Firmware Hub?

The Firmware Hub (FWH) is a flash memory device for BIOS storage, based on Intel's Low Pin Count (LCP) Interface Specification. It eliminates a redundant nonvolatile memory component and is a fundamental part of the new generation PC motherboards. It is the key to future security and manageability of infrastructures for the PC platform.

Firmware Hub Functional Description

The memory of the FWH is constructed in a uniformed matrix array of 64 KByte blocks to allow each block to be erased and reprogrammed without affecting other blocks. For functional flexibility the FWH can be operated with two different interfaces:

- the Firmware Hub Interface (FWH) for embedded operation
- the Address/Address Multiplexed Interface (A/A Mux) for programming operation during manufacturing.

They are selected by the setting of the Interface Configuration (IC) pin at V_{IL} for FWH Interface mode and V_{IH} for A/A Mux Interface mode.

Figure 1. Firmware Hub Interface Configuration

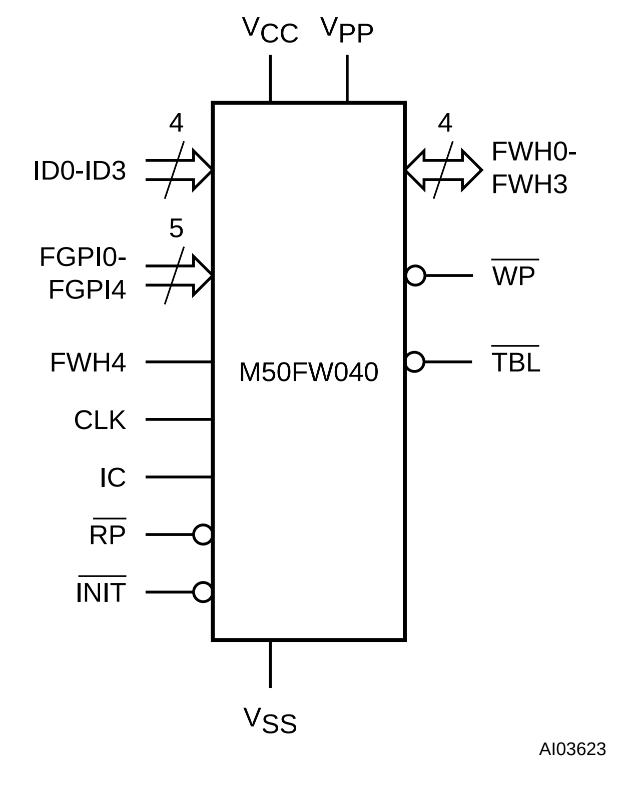


Figure 2. Firmware Hub Read Protocol

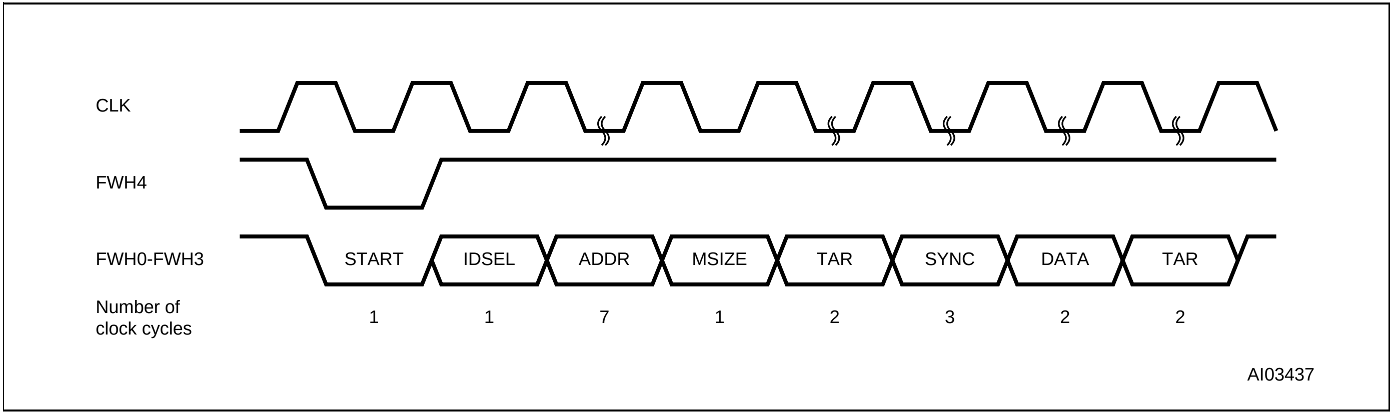
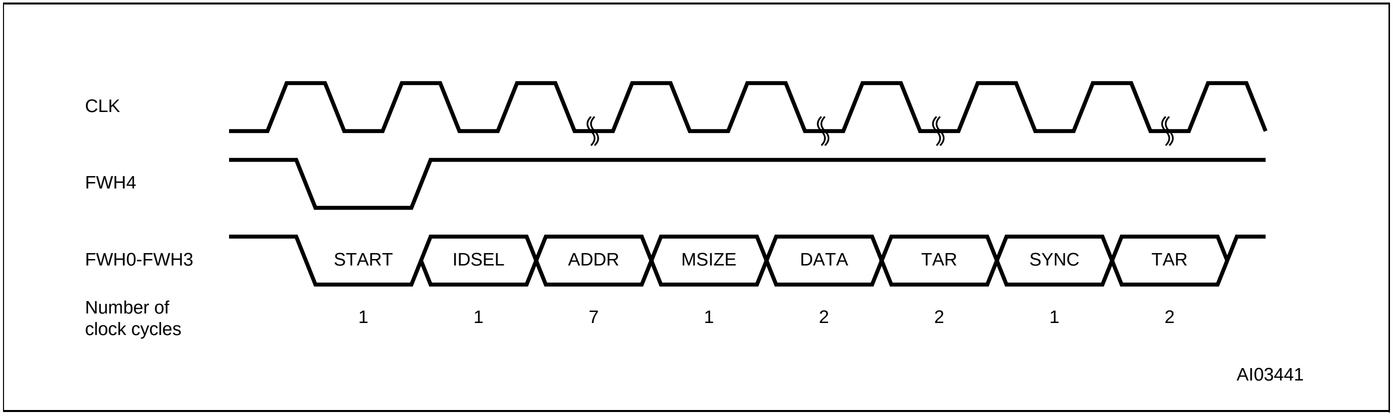


Figure 3. Firmware Hub Write Protocol



Firmware Hub Interface

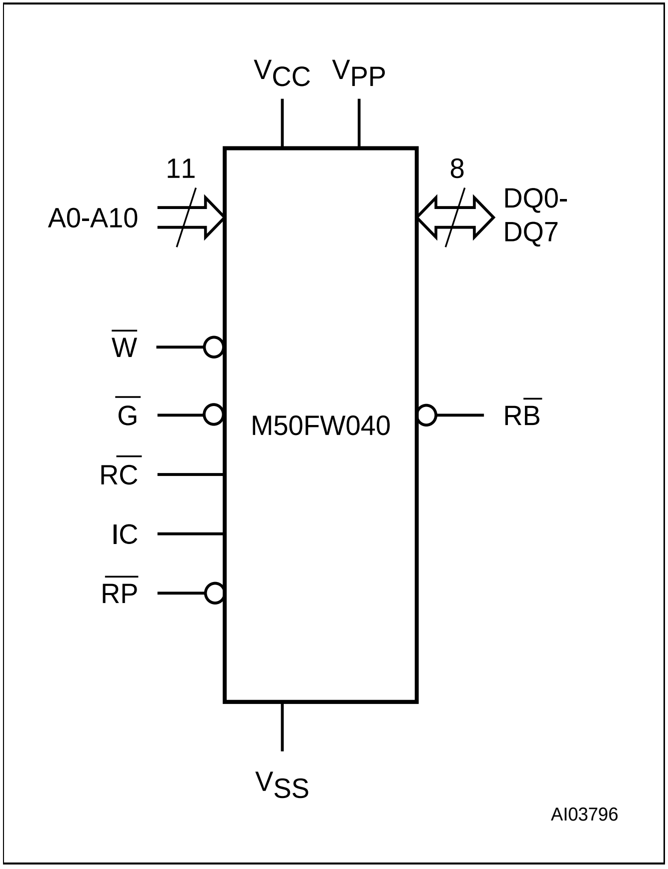
The FWH Interface features:

- a five Signal Communication Interface (FWH0-FWH4) to support the Read and Write operations,
- five General Purpose Inputs (FGPI0-FGPI4) for platform design flexibility,
- four Identification Inputs (ID0-ID3) to address up to 16 different memory devices,
- a Register Based Block Locking and a Hardware Block Protection for firmware security.

It has an Input Clock (CLK) synchronized with the 33MHz PCI clock and a 3.3V Input/Output bus. Figure 1 shows the pin description for FWH interface mode.

There are two different protection modes designed for the FWH interface. The hardware protection has the Top Block Lock (TBL) that prevents the Top Block from being changed, and the Write Protect (WP) that prevents all the other blocks from being changed.

Figure 4. Address/Address Multiplexed Interface Configuration



The software protection is a register based read and write protection in FWH interface mode. The registers can be altered to set the appropriate Locking to protect against piracy. Depending on the degree of protection required, the Lock Registers can set the memory in either Read Lock, Write Lock or Lock Down mode .

The Firmware Hub protocol is Intel proprietary and is based on the Low Pin Count Interface (LPC). Four Signal Communication pins (FWH0 – FWH3) together with an Input Communication Frame (FWH4) are used to determine the bus operation. A four bit Cycle Type (CYCLETYPE) defines whether it is Reading or Writing to the FWH.

The Device Select bits (IDSEL) indicate which FWH device is selected. The Memory Size Cycle (MSIZE) always gives 0000 (single byte transfer). The Turn Around bits (TAR), occupying two clock cycles, are driven by the host when it is turning control over to the peripheral and driven by the peripheral when it is turning control over to the host. Synchronize bits (SYNC) are required to bring the chip-sets into synchronization. Figure 2 shows the Firmware Hub Read Protocol and Figure 3 shows the Firmware Hub Write Protocol.

Address/Address Multiplexed Interface

The Address/Address Multiplexed Interface features:

- 11 Address Inputs for Row/Column addressing,
- 8 Data Inputs/Outputs for data bus operation,
- Output Enable for Read operation,
- Write Enable for Programming operation,
- Row/Column Address Select (RC*)* for Row or Column Address Latch
- Ready/Busy Output for verify operation.

Figure 4 shows the pin description for A/A Mux interface mode.

Figure 5. Address/Address Multiplexed Interface Read Protocol

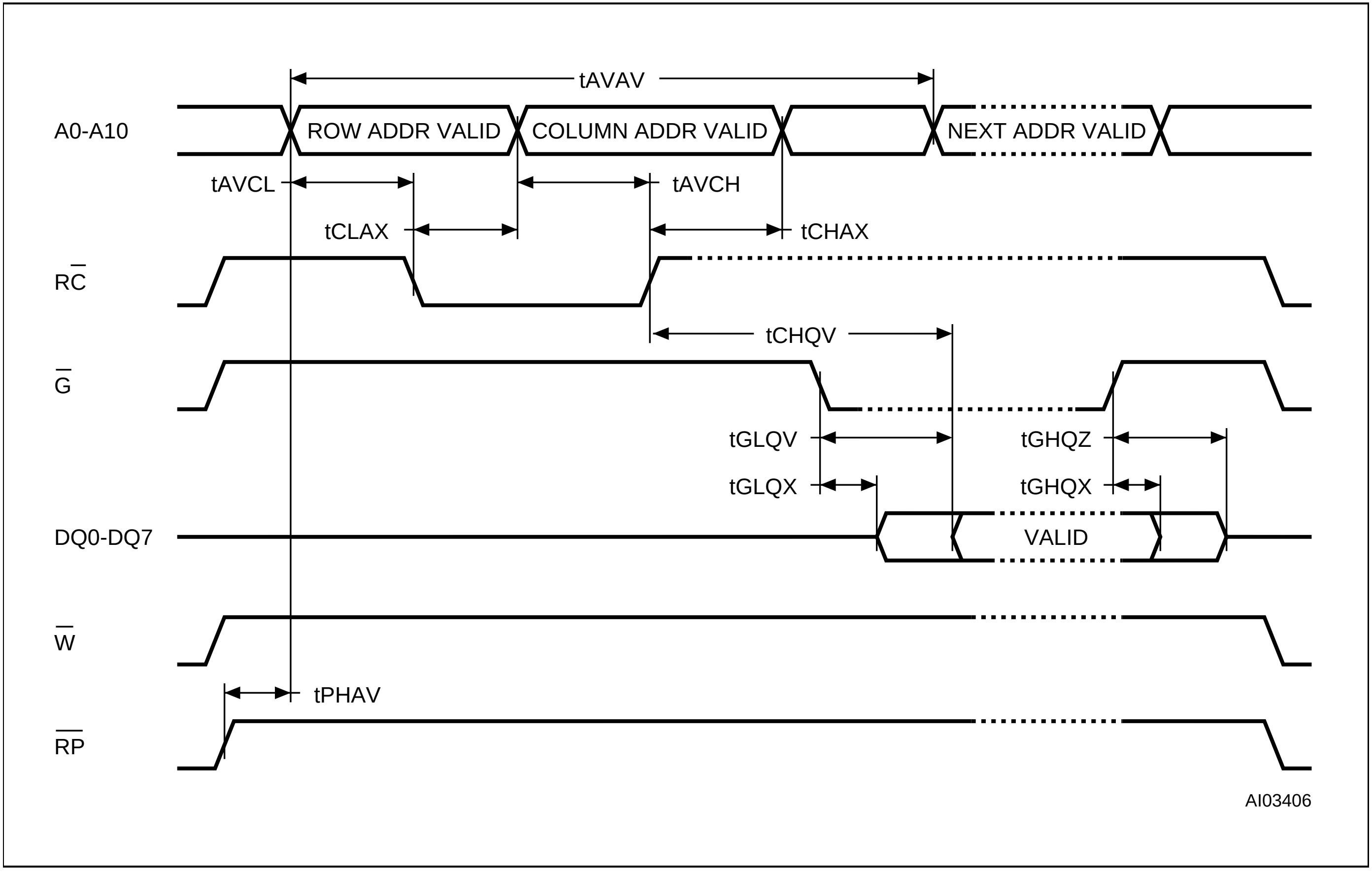
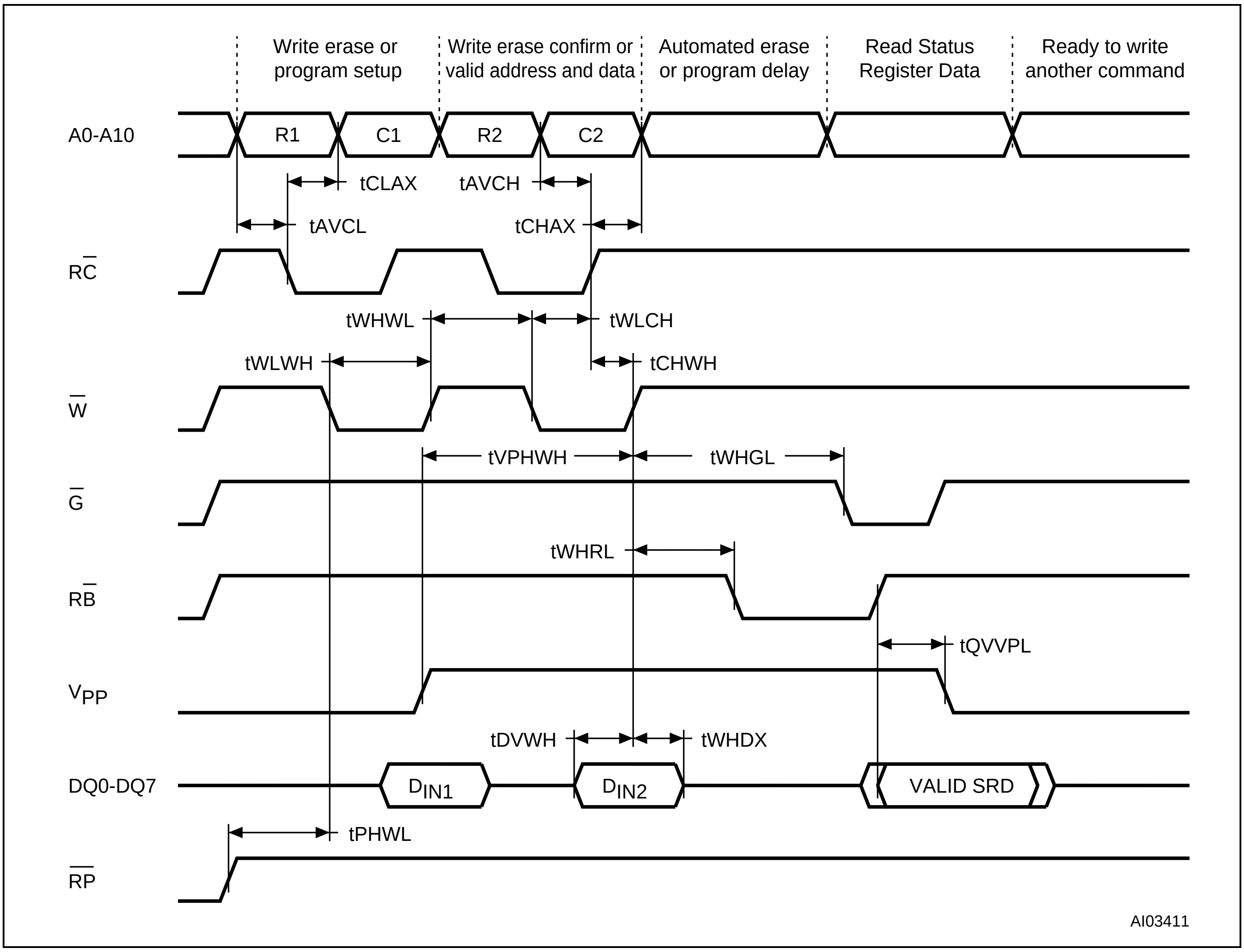


Figure 6. Address/Address Multiplexed Interface Write Protocol


Write erase or program setup
Write erase confirm or valid address and data
Automated erase or program delay
Read Status Register Data
Ready to write another command
A0-A10
R1
C1
R2
C2
tCLAX
tAVCH
tAVCL
tCHAX
RC
tWHWL
tWLCH
tWLWH
tCHWH
W
tVPHWH
tWHGL
G
tWHRL
RB
tQVVPL
VPP
tDVWH
tWHDX
DQ0-DQ7
DIN1
DIN2
VALID SRD
tPHWL
RP
AI03411

The A/A Mux Interface bus operation is similar to a standard flash programming protocol with the exception that addressing is latched using the Row/Column Select inputs. The lower address signals (A0–A10) determine the Row Address bits and the higher address signals (A11-A18) determine the Column Address bits. Figure 5 shows the Address/Address Multiplexed Interface Read Protocol, and Figure 6 the Address/Address Multiplexed Interface Write Protocol.

Firmware Security

Intel plans to add new security and software functions to their chip-sets in a move that will boost the profile of its future processors for the multimedia and electronic markets. These are the key features of the FWH that is basically a flash with locks on its read and write capabilities that can be opened using a cryptographic protocol.

The hardware security functions include a cryptographic engine to authenticate ‘digital certificates’ which Intel or a third party could load in. The FWH could hold multiple certificates, each able to grant specific features and ensure a software program licensed to one user could not be copied and run on another machine. In addition, the certificates will act as unique serial numbers, identifying a given machine in any Internet or corporate network transaction.

Appendix 1

The Firmware Hub comes in two standard packages of 32 pins PLCC (as shown in Figure 7) and 40 pins TSOP (as shown in Figure 8).

References

1. Intel’s security plans raise fear from PC builders, Rick Boyd-Merritt & Mark Carroll, EDTN News, 15 Dec 1998.

Figure 7. PLCC Connections

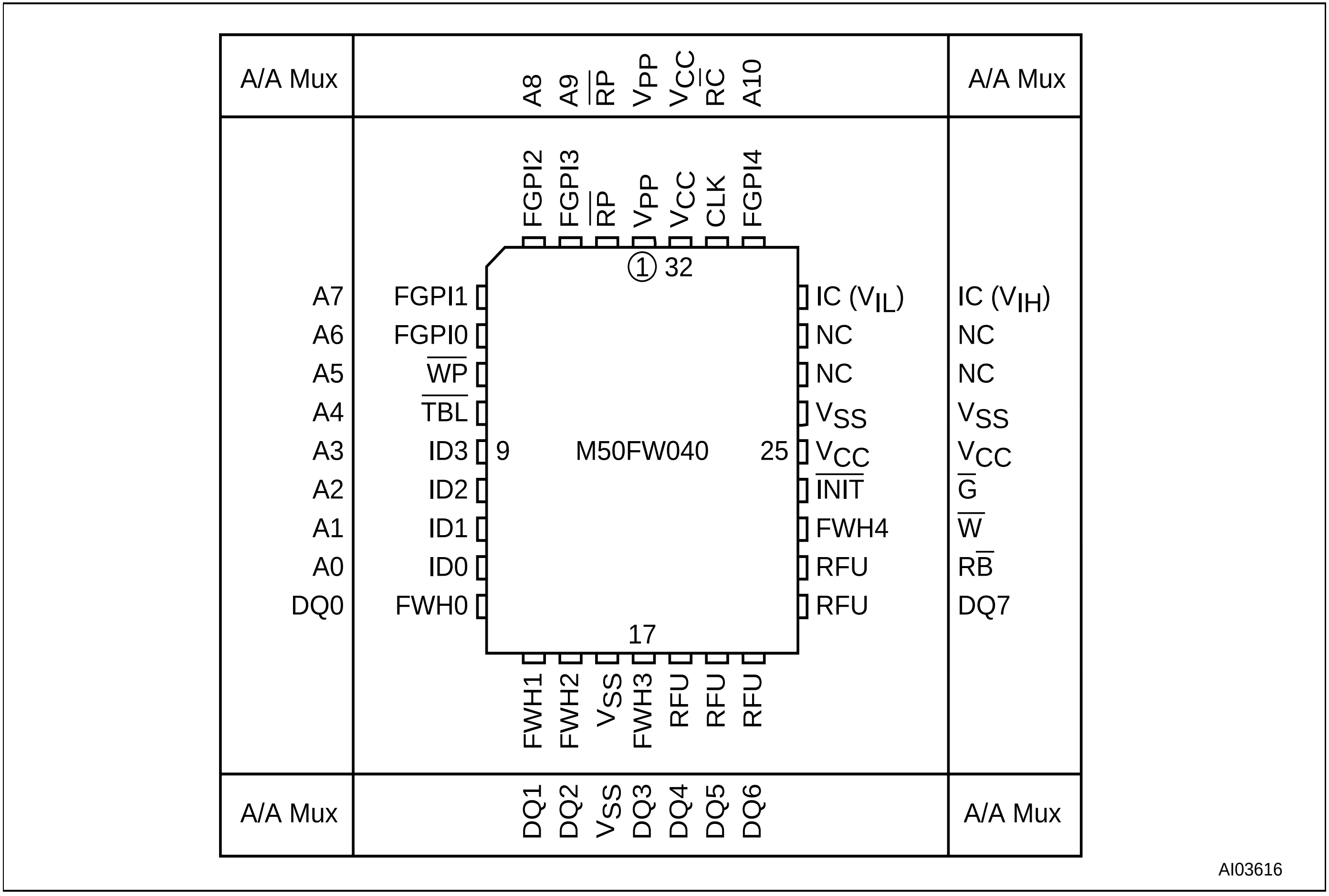
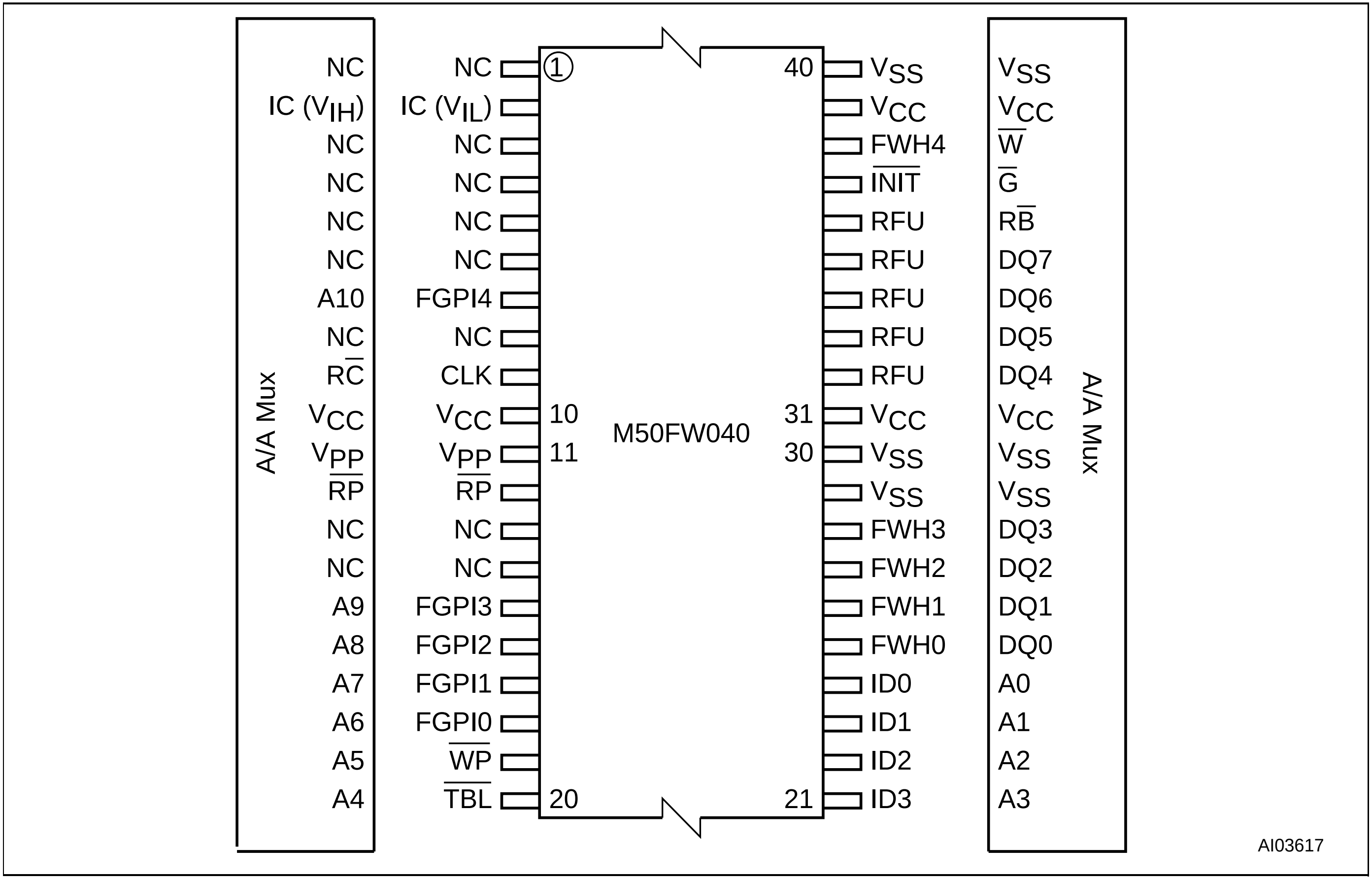


Figure 8. TSOP Connections



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