intel®

AB-57

APPLICATION
BRIEF

Intel's Flash Memory Boot Block Architecture for Safe Firmware Updates

PETER HAZEN
MEMORY COMPONENTS DIVISION

December 1995

Order Number: 292130-001

Information in this document is provided in connection with Intel products. Intel assumes no liability whatsoever, including infringement of any patent or copyright, for sale and use of Intel products except as provided in Intel's Terms and Conditions of Sale for such products.

Intel retains the right to make changes to these specifications at any time, without notice. Microcomputer Products may have minor variations to this specification known as errata.

*Other brands and names are the property of their respective owners.

†Since publication of documents referenced in this document, registration of the Pentium, OverDrive and iCOMP trademarks has been issued to Intel Corporation.

Contact your local Intel sales office or your distributor to obtain the latest specifications before placing your product order.

Copies of documents which have an ordering number and are referenced in this document, or other Intel literature, may be obtained from:

Intel Corporation
P.O. Box 7641
Mt. Prospect, IL 60056-7641

or call 1-800-879-4683

In highly competitive environments where time-to-market pressures must be balanced with product functionality, quality and reliability, system designers and manufacturers gain advantage with Intel's boot block flash memory for updateable firmware. Flash memory enables system firmware updates, allowing manufacturers to cost-effectively enhance product features, fix product bugs and keep up with changing standards *after* their product is sold.

Intel's boot block flash memory is the architecture of choice for providing *safe* firmware updates for a wide range of applications that includes cellular phones, modems, medical instrumentation, printers, PC BIOS and many more. Flash memory solutions should be evaluated based on a checklist of key criteria for updateable firmware. With multiple supply sources, a full family of boot block products provides the key features required for updateable firmware.

SAFE FIRMWARE UPDATES

A fundamental tradeoff that comes with the ability to update firmware in the system is the possibility of losing firmware during the update process. Because flash memory must first be erased before it can be reprogrammed, the system could be rendered inoperable if something disrupts the firmware update process before reprogramming is complete. For example, if a power glitch occurs, if the communication link providing the updated code is lost, or if an asynchronous reset occurs, firmware can be lost. Without the firmware, the system won't operate.

Intel's boot block architecture enables system recovery even if the firmware upgrade is disrupted. The hardware protected boot block guarantees that code stored in the boot block cannot be erased in the system. The boot block is designed to store key kernel code that initiates the system and, if necessary, starts a recovery routine to restore firmware. Although firmware updates may be infrequent and the likelihood of disrupting the firmware update process remote, the consequences are extreme. The alternative to using a hardware protected boot block flash memory is to risk losing your firmware with no chance of recovery. If firmware is completely lost, the product must be disassembled and the memory replaced, a consequence that can be very costly to both the end-user and manufacturer.

CHOOSING THE OPTIMAL FLASH MEMORY ARCHITECTURE

Today's system designer and manufacturer are faced with a number of options when choosing a flash memory solution for updateable firmware. Intel optimizes different flash memory architectures to meet the specific requirements of different applications. Figure 1 shows two primary application vectors and Intel's associated solutions.

First Generation Flash Memories

First generation bulk-erase flash memory products, used for both firmware storage and high density storage, are characterized by bulk erase operation (the entire memory is erased at one time), and non-automated program and erase algorithms. First generation prod-

Key Benefits of Updateable Firmware

Firmware is the dedicated software stored in a system's nonvolatile memory (memory contents are retained even after power is removed). Flash memory's nonvolatility and ability to be updated in-system, provide ideal characteristics for firmware storage.

Before the advent of flash memory, designers relied on ROM or EPROM memory technologies, neither of which provided an ideal solution. Both technologies are nonvolatile but neither can be updated without removing the component from the system, which is both expensive and inconvenient.

With flash memory and the ability to update firmware in-system, manufacturers enhance product features, fix product bugs and keep up with changing standards by providing firmware updates either directly to the end-user or through a convenient service center. Manufacturers also download test code to flash memory during production and then update their system with the latest application code for just-in-time delivery. For example, manufacturers download different language codes to flash memory on their universal platform, just prior to shipping their product. Flash memory allows manufacturers to differentiate their products and provide valuable services in a highly competitive environment.

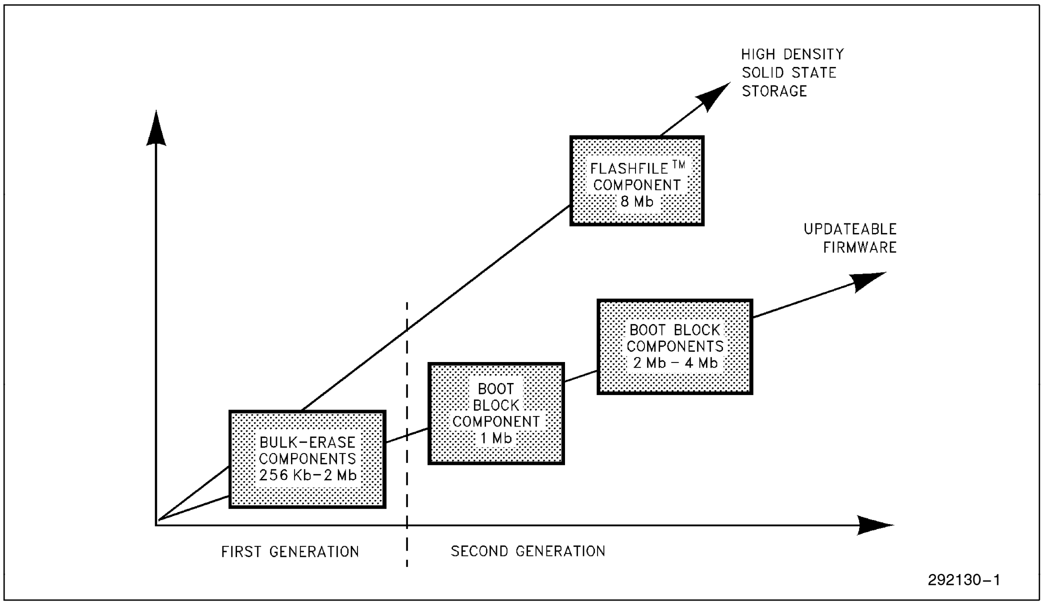


Figure 1. Intel Manufactures Optimized Architectures for Specific Application Vectors

ucts add in-system update capability to traditional embedded systems which typically use ROM/EPROM for kernel code storage and EEPROM or SRAM for parameter data storage.

Boot Block Architecture Integrates ROM, EEPROM/SRAM and Bulk Flash Functionality

Intel's second generation products include the boot block architecture for updateable firmware and the FlashFile™ architecture for high density storage.

The boot block architecture integrates ROM functionality with a hardware protected boot block, a requirement for safe firmware updates. The boot block is optimized to store the minimum code necessary to initialize the system, as well as recovery code, necessary to restore firmware if it is inadvertently lost during a firmware update. Two parameter blocks emulate EEPROM and battery-backed SRAM, and allow for parameter data storage. One or more main blocks store the majority of system firmware and allow for modular software development with each block being erased independently from other blocks. Figure 2 shows the resultant architecture for the 4-Mbit boot block product. Appendix A shows the memory maps for all products in the boot block family.

(Byte Addresses)

7FFFFH 7C000H	16 Kbyte Boot Block
7BFFFH 7A000H	8 Kbyte Parameter Block
79FFFH 78000H	8 Kbyte Parameter Block
77FFFH 60000H	96 Kbyte Main Block
5FFFFH 40000H	128 Kbyte Main Block
3FFFFH 20000H	128 Kbyte Main Block
1FFFFH 00000H	128 Kbyte Main Block

Figure 2. Intel's Boot Block Architecture (4-Mbit shown) Integrates ROM, EEPROM and Bulk Flash Functionality

High Density Applications

High density storage applications are best suited to a symmetrically blocked architecture as defined in Intel's FlashFile™ architecture, whereas with firmware applications, many symmetrical blocks become cumbersome to the programmer. While Intel delivers optimized architectures for specific applications, some "all-purpose" alternate architectures attempt to meet the needs of both application vectors with a symmetrically blocked architecture, only to fall short on both accounts.

Second Generation Products Provide Program and Erase Automation

Second generation products feature an on-chip state machine for controlling program and erase operations. This on-chip control simplifies the program and erase algorithms. Appendix B shows the simplified algorithms compared to the first generation algorithms. The on-chip state machine simplifies device interface, reduces device driver code size and improves performance by allowing the CPU to attend to other activities during program and erase operations. These features provide key benefits over first generation products. An application note, AP-380, "Upgrading System Designs from Bulk Erase to Boot Block Flash Memories" describes the necessary steps for upgrading to the boot block architecture.

EVALUATING FLASH MEMORY ALTERNATIVES FOR SAFE FIRMWARE UPDATES

Flash memory alternatives should be evaluated based on key criteria required by firmware update applications (see Figure 3: "Checklist for Choosing a Flash Memory Solution for Safe Firmware Updates"). Careful examination of alternatives reveals architectural tradeoffs. For example, flash memories with on-chip write and erase automation require reset capability as described later in this paper, however, some alternate architectures omit this feature to allow their product to fit into a package with less pins. Such tradeoffs can adversely affect the quality and reliability of the final system product.

Checklist for Choosing a Flash Memory for Safe Firmware Updates

☑ Does a complete family of products exist to meet your needs today and in the future?

☑ Is the flash memory architecture supported by high-volume suppliers?

☑ Does a hardware protected boot block exist for secure code storage and safe updates?

☑ Does a WE# pin exist for reliable in system updates?

☑ Does the solution provide adequate protection against unwanted writes during power transitions?

☑ Does the solution have write and erase automation?

☑ Can the flash memory be RESET whenever the CPU is reset?

☑ Does the solution provide for the lowest energy consumption?

☑ Is the product supported by PROM programmers?

Figure 3. Follow this Checklist when Evaluating a Flash Memory Architecture for Firmware Updates

A Full Family of Boot Block Flash Memory Products

Intel provides a full family of boot block products ranging from 1 to 4 Mbits in density. 2-Mbit and 4-Mbit products include user-selectable x8 and x16 modes of operation. The 8-bit 1-Mbit component is available in DIP, PLCC and TSOP packages, while the 2-Mbit and 4-Mbit components offer PSOP and TSOP packages.

Density	Boot Block Products	
	x8	x16
1-Mbit	28F001BX	—
2-Mbit	28F002BX	28F200BX
4-Mbit	28F004BX	28F400BX

Figure 4. Intel's Family of Boot Block Products

The 4-Mbit family offers a direct pinout upgrade replacement for the 2-Mbit boot block family. Migration from the 1-Mbit component to higher densities requires a change in package and pinout due to increased number of address pins along with the standard control pins required by firmware applications. Some alternate products may offer 2-Mbit and 4-Mbit densities in 32-lead packages, however only by sacrificing one or more of the standard control features provided by WE# and RP#, as described below. Appendix C shows the boot block family pinouts. This complete family of products provides an upgrade solution with all the features of the boot block architecture.

Highest Performance and 16-Bit Operation

With access times as fast as 60 ns on the 2-Mb and 4-Mb boot block products, these components are the highest-performance flash memories on the market at these densities. This performance and 16-bit operation delivers zero wait-state performance for a wide range of microprocessors and microcontrollers. 16-bit operation also reduces system chip-count and piece-part inventory as well as improving system reliability and power.

Multiple Sources

Intel's flash memory manufacturing follows a multi-fab strategy where each product is manufactured at two different fabrication plants to ensure an uninterrupted high volume supply. Intel continues to make significant investments in flash memory manufacturing capacity, far outpacing the nearest competitor. In addition, a number of external suppliers have revealed plans to deliver products that follow the boot block architecture standard.

WE# for Reliable In-System Writes

Intel's flash memories feature two-line write control using WE# and CE#. Dedicated control signals provide the most reliable interface for in-system flash memory updates. WE# is typically driven directly from the CPU, providing dedicated control. Figure 5 shows Intel's standard read/write timing sequence.

Some alternate architectures do not provide WE#, instead providing an additional address pin for density upgrade in a given pinout and package. Often referred to as an "EPROM replacement pinout", this architectural tradeoff results in less reliable in-system writes.

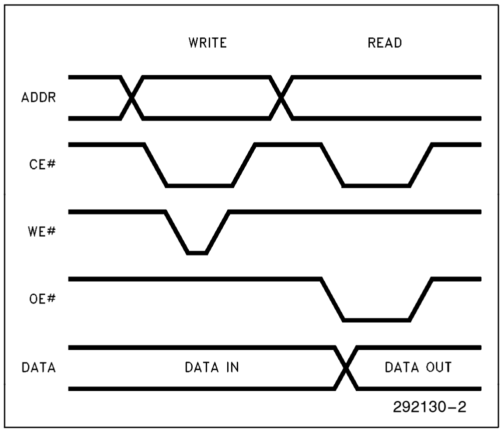


Figure 5. Intel's Two-Line Write Control is more Reliable than V_{PP} Power Supply Decoding

Without the WE# pin, the reads and writes are decoded using CE# and the high voltage V_{PP} power supply. When V_{PP} is at high voltage (12V), CE#-active (with OE#-inactive) initiates a write sequence. When V_{PP} is not at high voltage, CE#-active (with OE#-active) initiates a read operation.

Two reliability problems occur with this approach: 1) During writes, when V_{PP} is at high voltage, a glitch on CE# will initiate an unwanted write sequence. Glitches on CE# are not uncommon since CE# is often decoded from switching addresses, and 2) High capacitance on the V_{PP} power supply node degrades system performance.

Write Protection during Power Transitions

Flash memories lock out writes below a certain V_{CC} level defined by the V_{LKO} specification. A V_{CC}-monitoring circuit on the flash memory disables on-chip write circuitry whenever V_{CC} goes below this specified level, providing one level of protection against spurious writes during power transitions. However, complete protection is assured by holding the flash memory in reset mode during power transitions. The boot block architecture features Reset/Power-Down with RP# (formerly named PWD# and renamed for JEDEC standardization compatibility). When driven by the system POWERGOOD signal, RP# holds the flash memory in reset mode during power transitions, preventing all writes and erases, independent from all other device inputs.

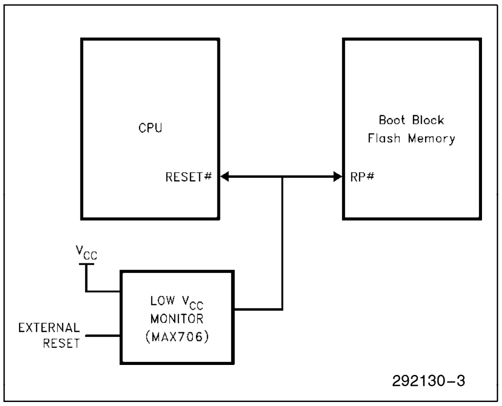


Figure 6. A Reset Feature is a Requirement for Updateable Firmware Applications

Reset

The boot block architecture simplifies program and erase operations by using on-chip state machines to control the complex write and erase algorithms. *Any flash memory with an on-chip state machine requires reset functionality,* as does any system peripheral with independent control capability. If a system reset occurs during a program or erase operation, the flash memory must be reset to the read mode so that the code stored in flash memory is accessible by the CPU after reset. If the memory is not reset, the flash memory will remain in the program or erase mode, resulting in the CPU reading invalid data from the flash memory. This results in an inoperable system. Imagine designing in peripheral controllers without the ability to reset them asynchronously. Flash memory automated or embedded algorithms are analogous to integrated memory controllers and therefore must have reset capability.

Intel features reset capability with its RP# pin. By connecting RP# to the system reset signal as shown in Figure 6, the flash memory is reset whenever the CPU is reset, and the memory is ready in read mode when the system comes out of reset.

3.3V Read and Other Low Power Features

The boot block products are optimized for 3.3V read operation, enabling the lowest energy consumption. In addition to low active and standby current levels, the 2-Mbit and 4-Mbit components also include an automatic power savings feature. With this feature, the flash memory automatically reduces its active current consumption to less than 1 mA, typically, during read mode when addresses and CE# are not toggled. This provides significant power savings by reducing DC current levels when used with system power management features such as clock stretching or when used in systems that access the flash memory much slower than its specified access time.

Extended Temperature Capability

Intel's boot block products are optimized over the extended temperature range of −40°C to +85°C, as required by many mobile and industrial applications. The 2-Mbit and 4-Mbit products are also available over the automotive temperature range (−40°C to +125°C).

A specially designed 44-lead PSOP (Plastic Small Outline Package) uses a copper lead frame for optimal solder joint reliability at extreme temperatures. This package is guaranteed at extended temperature ranges beyond 20 years.

Intel's Boot Block Architecture Provides the Optimal Flash Memory Solution for Safe Firmware Updates

By evaluating alternative memory solutions relative to a checklist of requirements for safe firmware updates, architectural tradeoffs and their impact on your application can be understood. Intel's boot block architecture provides the key features necessary for delivering safe firmware updates. Consult your Intel representative for upcoming opportunities with the boot block architecture and to receive additional information on product line extensions.

Appendices

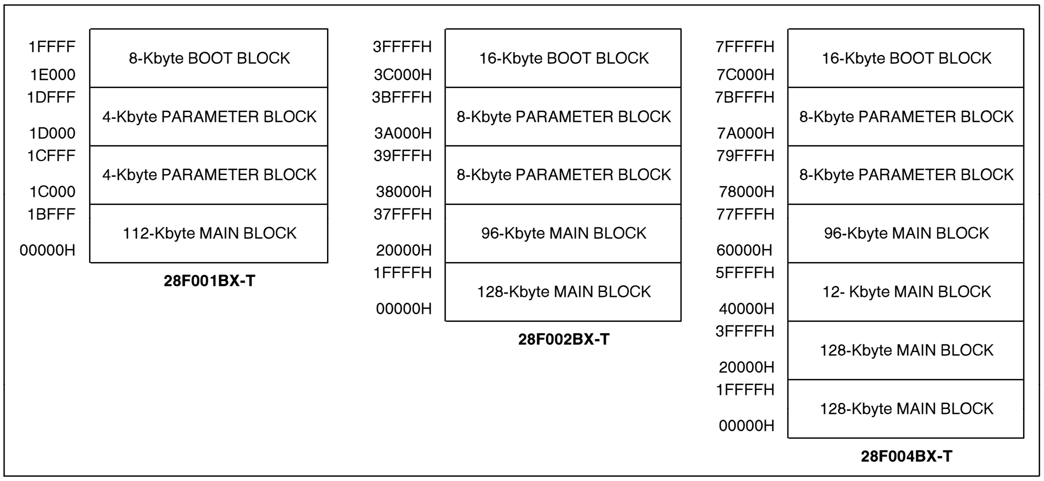
A. Boot Block Family Memory Maps

B. Boot Block Write and Erase Algorithms vs First Generation

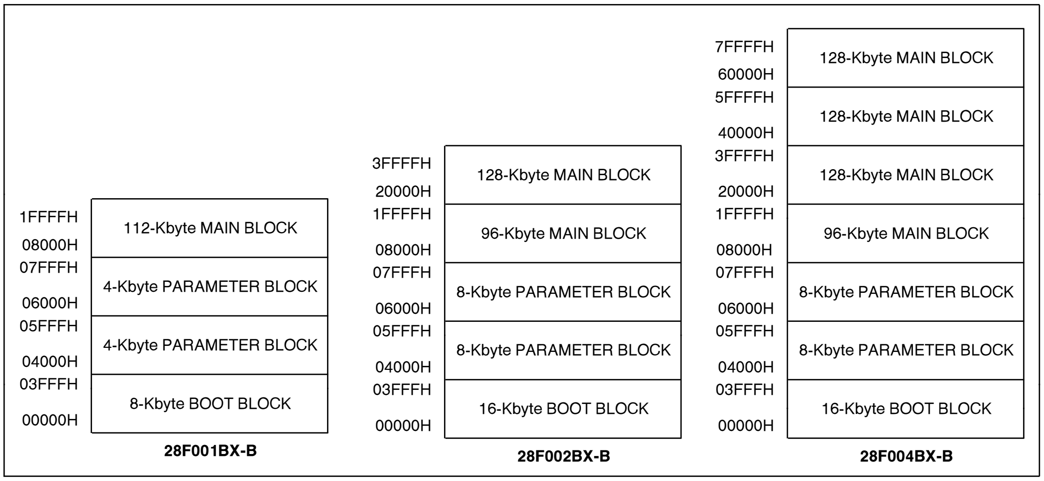
C. Boot Block Family Pinouts

D. Additional Tools/Information

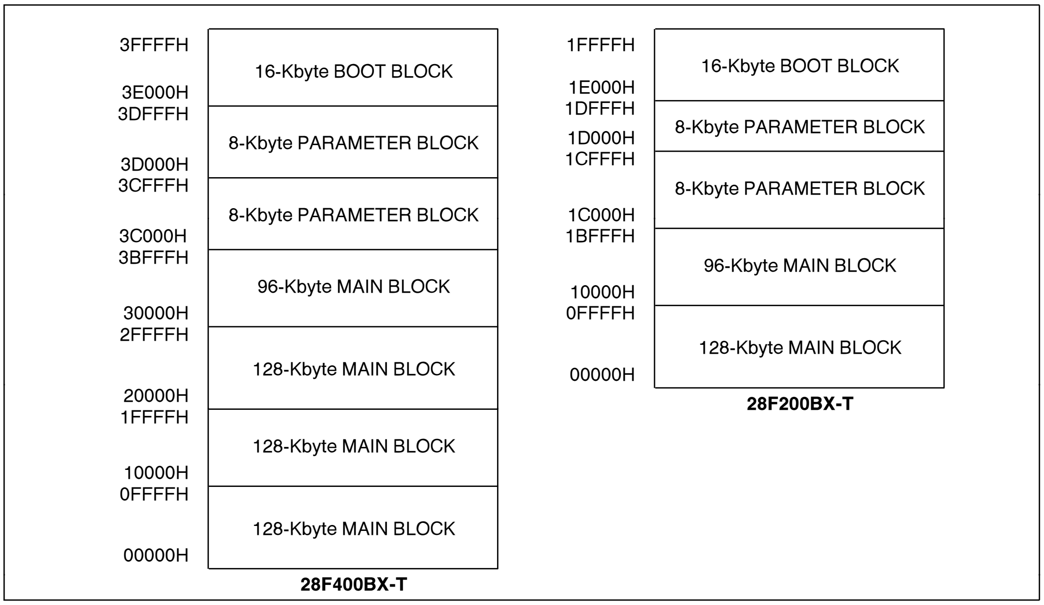
APPENDIX A
BOOT BLOCK FAMILY MEMORY MAPS



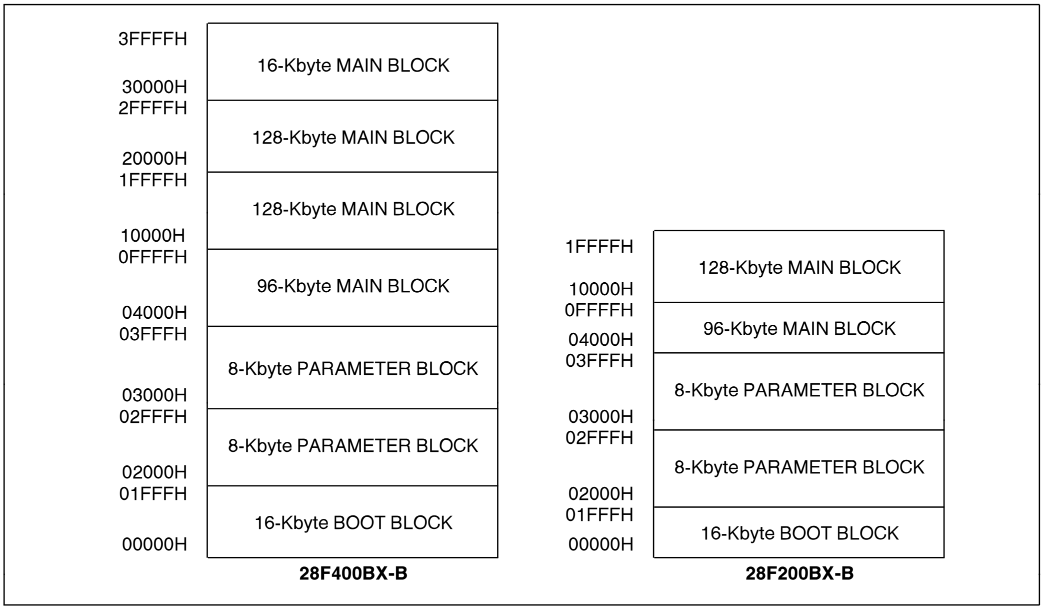
28F001BX-T, 28F002BX-T, 28F004BX-T Memory Maps



28F001BX-B, 28F002BX-B, 28F004BX-B Memory Maps

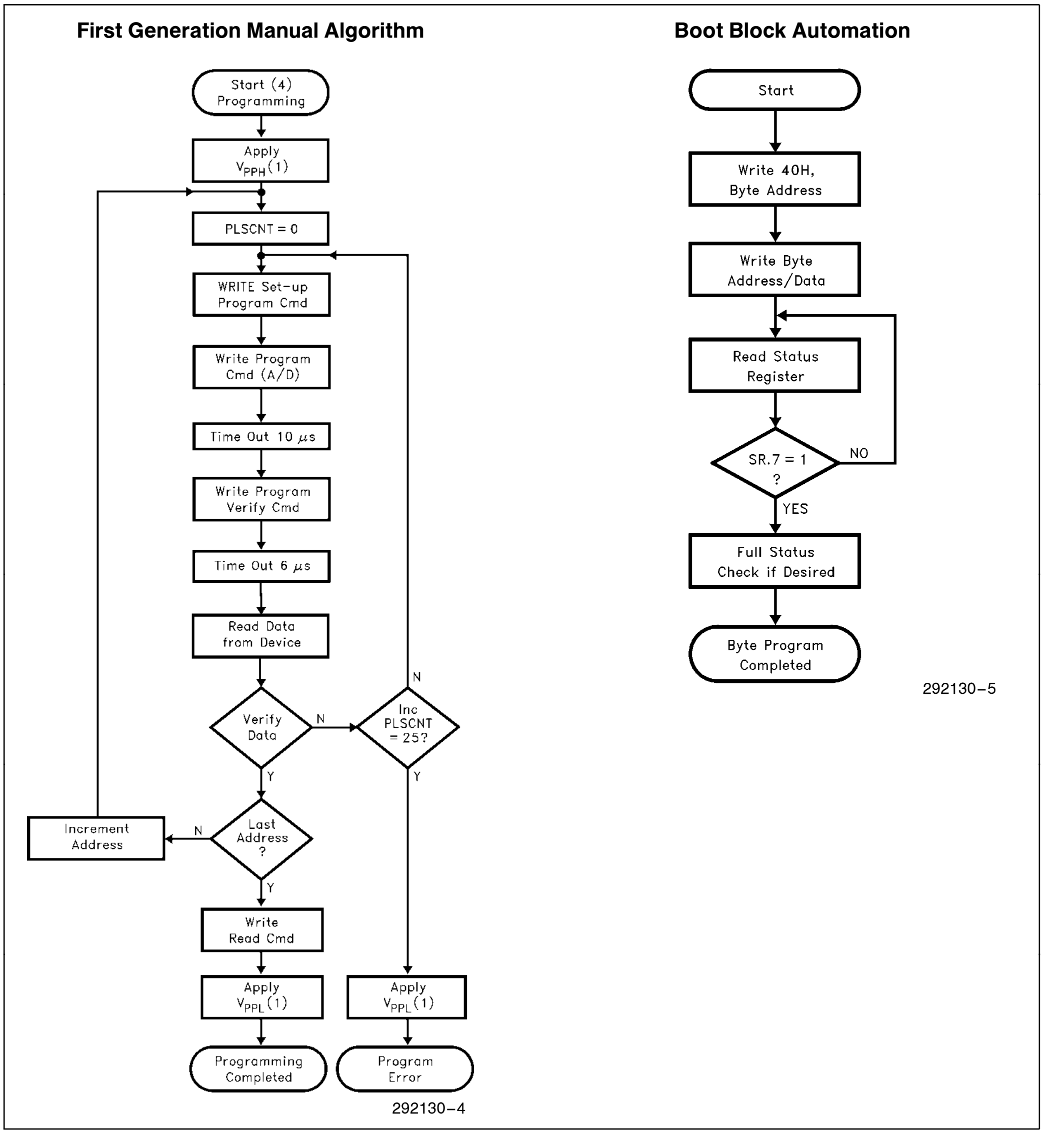


28F200BX-T, 28F400BX-T, Memory Maps



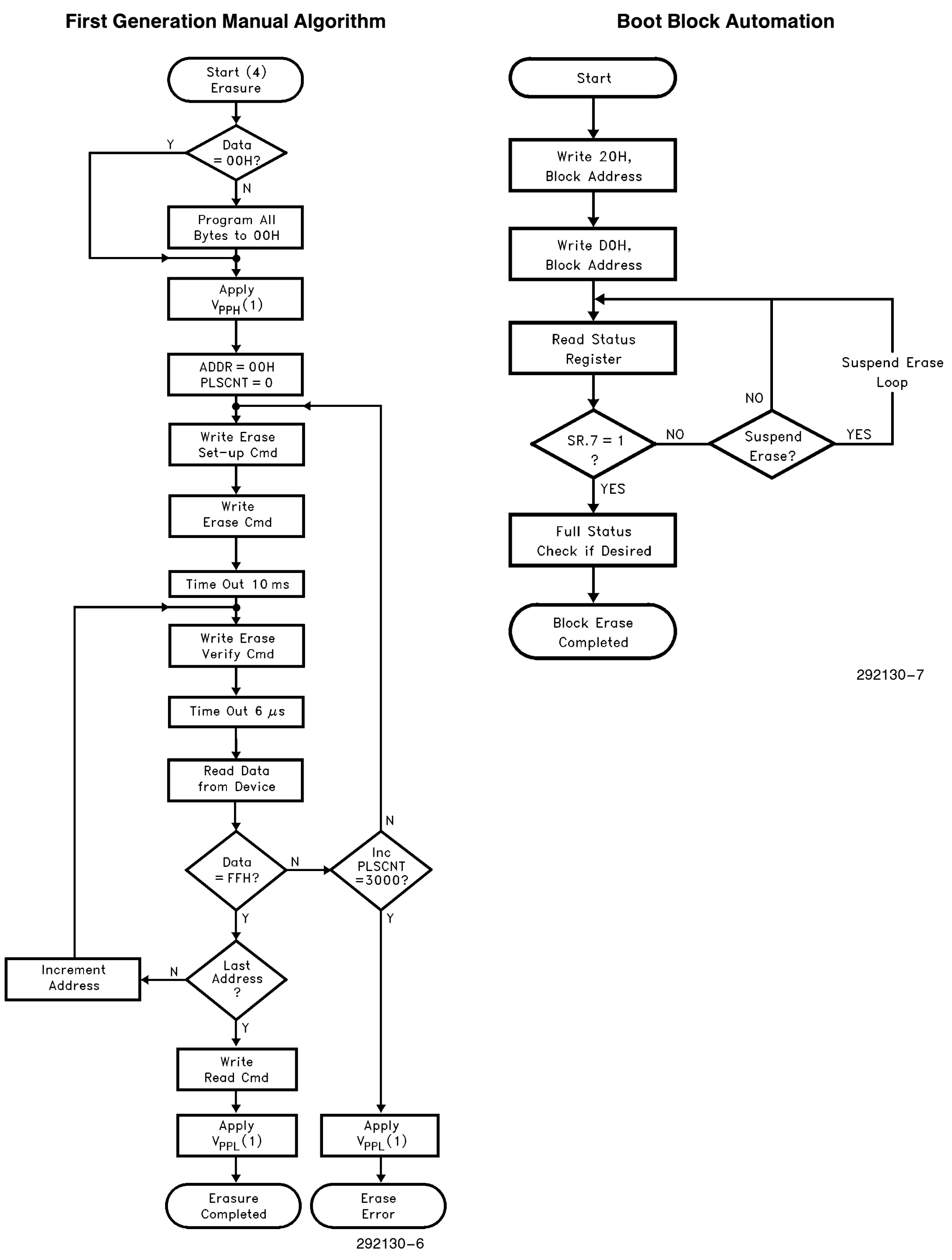
28F200BX-B, 28F400BX-B Memory Maps

APPENDIX B BOOT BLOCK WRITE AND ERASE ALGORITHMS VS FIRST GENERATION ALGORITHMS


First Generation Manual Algorithm

Boot Block Automation

Program Algorithms



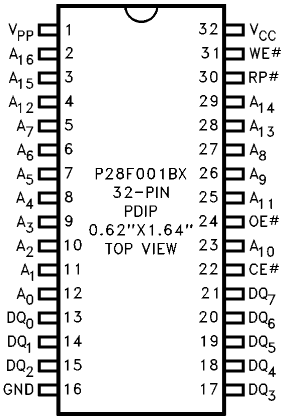
First Generation Manual Algorithm

Boot Block Automation

Erase Algorithms

APPENDIX C
BOOT BLOCK FAMILY PINOUTS

28F010
V_{PP}
A_{16}
A_{15}
A_{12}
A_7
A_6
A_5
A_4
A_3
A_2
A_1
A_0
DQ_0
DQ_1
DQ_2
GND

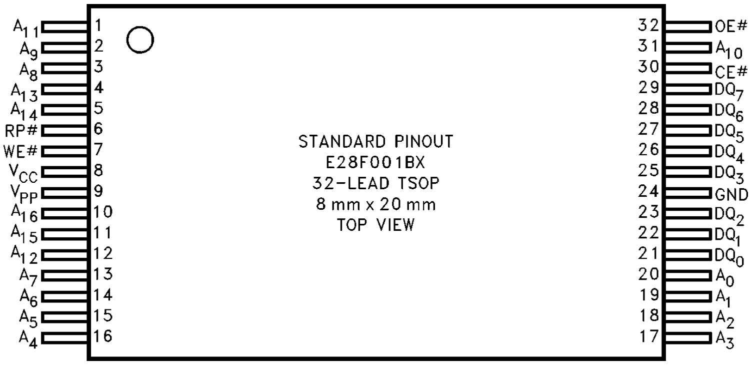


28F010
V_{CC}
WE#
NC
A_{14}
A_{13}
A_8
A_9
A_{11}
OE#
A_{10}
CE#
DQ_7
DQ_6
DQ_5
DQ_4
DQ_3

292130–8

28F001BX DIP Pin Configuration

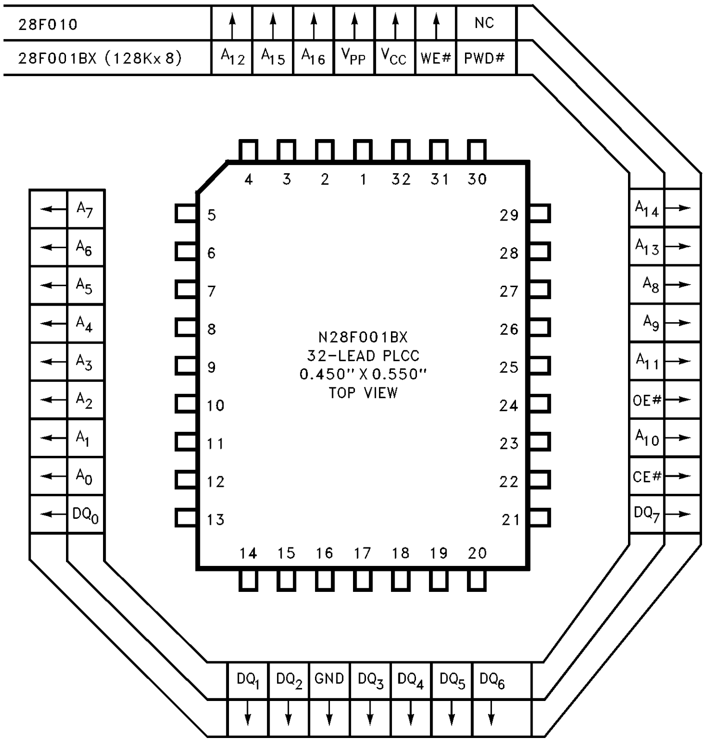
28F010
A_{11}
A_9
A_8
A_{13}
A_{14}
NC
WE#
V_{CC}
V_{PP}
A_{16}
A_{15}
A_{12}
A_7
A_6
A_5
A_4



28F010
OE#
A_{10}
CE#
DQ_7
DQ_6
DQ_5
DQ_4
DQ_3
GND
DQ_2
DQ_1
DQ_0
A_0
A_1
A_2
A_3

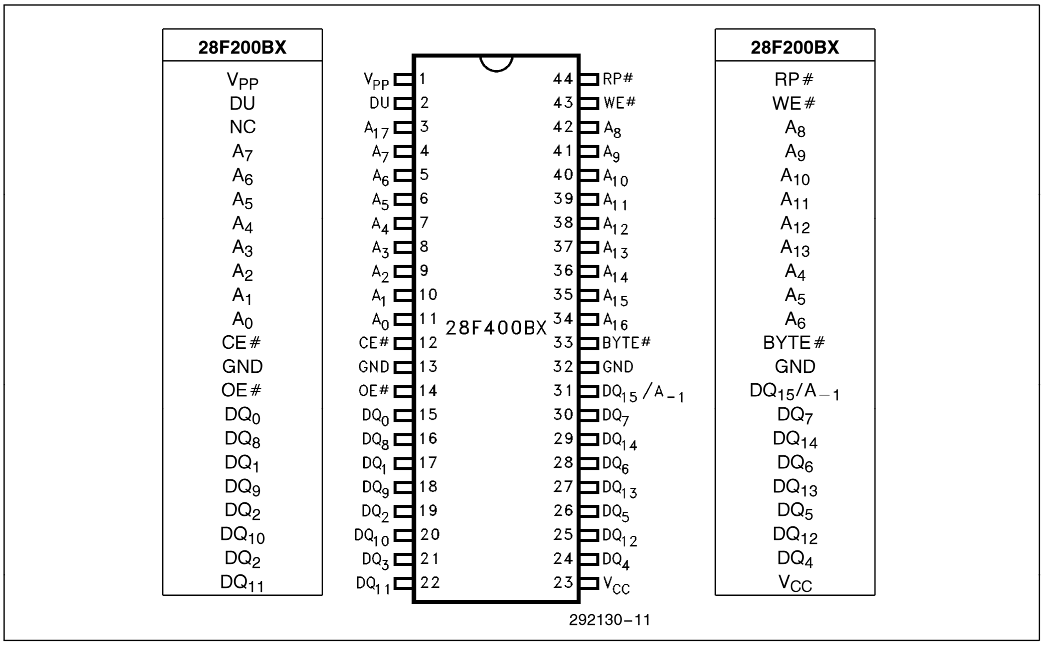
292130–9

28F001BX TSOP Lead Configuration

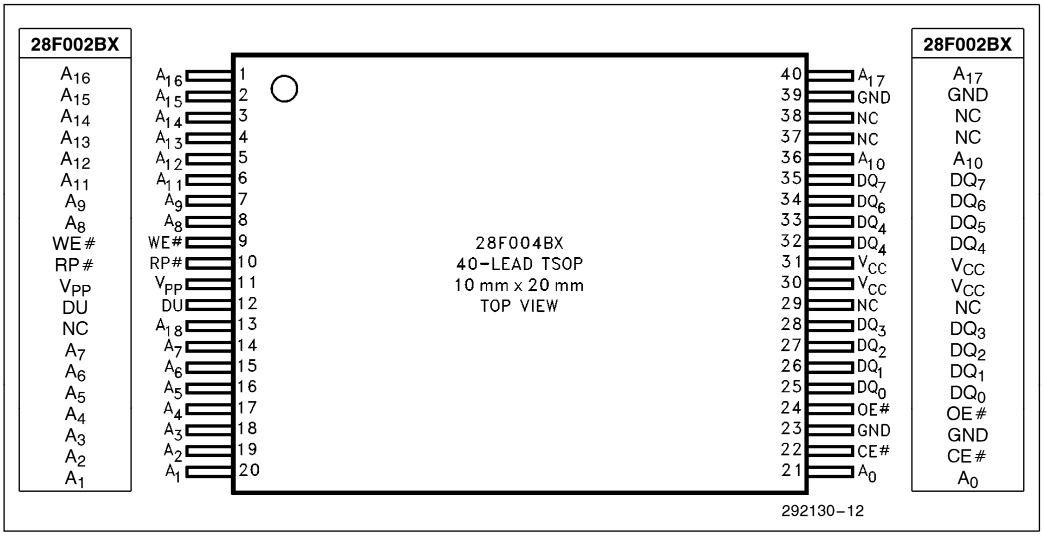


292130–10

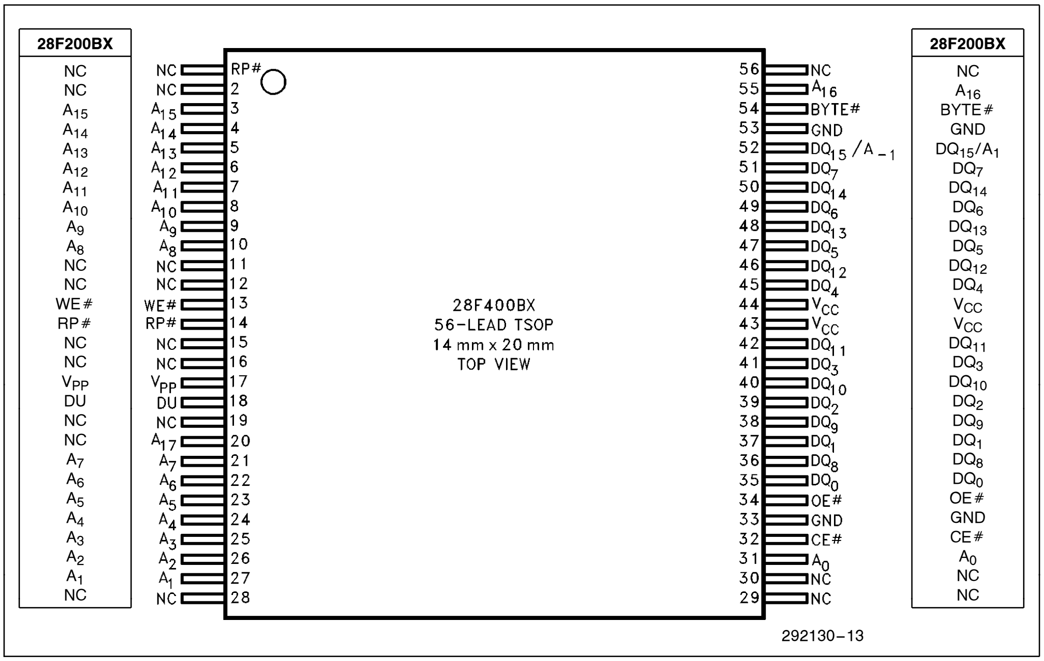
28F001BX PLCC Lead Configuration



28F200BX, 28F400BX PSOP Pin Configuration



28F002BX, 28F004BX TSOP Lead Configuration



28F200BX, 28F400BX TSOP Lead Configuration

APPENDIX D
ADDITIONAL TOOLS/INFORMATION

28F001BX-T/B: "1-Mbit CMOS Flash Memory" Data Sheet (order #290406)

28F200BX-T/B, 28F002BX-T/B: "2-Mbit Boot Block Flash Memory Family" Data Sheet (order #290448)

28F200BX-TL/BL, 28F002BX-TL/BL: "2-Mbit Low Power Boot Block Flash Memory Family (order #290451)

28F400BX-T/B, 28F004BX-T/B: "4-Mbit Boot Block Flash Memory Family" Data Sheet (order #290450)

28F400BX-TL/BL, 28F004BX-TL/BL: "4-Mbit Low Power Boot Block Flash Memory Family" (order #290451)

ER-28 "ETOX™ III Flash Memory Technology" Engineering Report (order #294012)

ER-26 "The Intel 28F001BX-T and 28F001BX-B Flash Memories" (order # 294010)

ER-29 "2/4-Mbit Boot Block Flash Memory Family" Engineering Report (order #294013)

AP-380 "Upgrading System Designs from Bulk Erase to Boot Block Flash Memories" (order #292129-001)