



(51) International Patent Classification:  
**G06F 11/10** (2006.01)

(21) International Application Number:  
PCT/US2010/044695

(22) International Filing Date:  
6 August 2010 (06.08.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
12/539,407 11 August 2009 (11.08.2009) US

(71) Applicant (for all designated States except US): **SAN-DISK CORPORATION** [US/US]; 601 Mccarthy Boulevard, Milpitas, CA 95035 (US).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **SELINGER, Robert, D.** [US/US]; 7215 Gold Creek Court, San Jose, CA 95120 (US).

(74) Agent: **HETZ, Joseph, F.**; Brinks Hofer Gilson & Lione, P.O.box 10087, Chicago, IL 60610 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: CONTROLLER AND METHOD FOR DETECTING A TRANSMISSION ERROR OVER A NAND INTERFACE USING ERROR DETECTION CODE

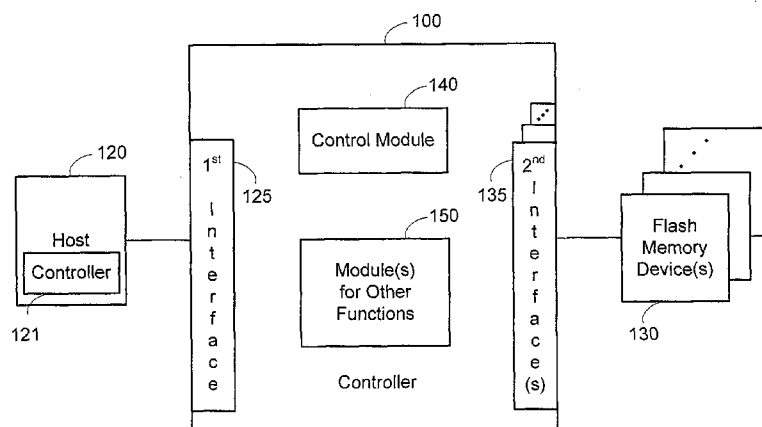


FIG. 1

(57) Abstract: The embodiments described herein provide a controller and method for detecting a transmission error over a NAND interface using error detection code. In one embodiment, a controller receives a write command, data, and an error detection code associated with the data from a host through a first NAND interface of the controller using a NAND interface protocol. The controller uses the error detection code to detect if a transmission error occurred. In another embodiment, a controller generates an error detection code based on data read from a flash memory device and provides the data and error detection code to a host through a first NAND interface of the controller, so the host can detect if a transmission error occurred.

## **Controller and Method for Detecting a Transmission Error Over a NAND Interface Using Error Detection Code**

### **Background**

[0001] NAND flash memory devices are commonly used to store data by a host, such as a personal computer. In many architectures, a NAND controller is used to facilitate communication between a host and a NAND flash memory device. In some controller architectures, a NAND controller interacts with a NAND flash memory device using a NAND interface and interacts with a host using a standard, non-NAND interface, such as USB or SATA. In such systems, the host can generate an error correction code (ECC) to protect against both transmission errors as well as storage errors. Alternatively, the controller can generate ECC, and the host can generate an error detection code (EDC) to protect the data from transmission errors that may occur over the non-NAND interface between the host and the controller. “NAND Flash Memory Controller Exporting a NAND Interface,” U.S. patent application no. 11/326,336 (published as U.S. Patent Publication No. US 2007/0074093), which is hereby incorporated by reference, discloses a controller that exports a NAND interface to the host. In this way, the controller exports to the host the same type of interface that is exported to the host by a standard NAND flash memory device. This controller can also be used to generate ECC to protect data to be stored in the NAND flash memory device or to provide additional protection to data already protected by ECC generated by the host.

### **Summary**

[0002] The present invention is defined by the claims, and nothing in this section should be taken as a limitation on those claims.

[0003] By way of introduction, the embodiments described below provide a controller and method for detecting a transmission error over a NAND interface using error detection code. In one embodiment, a controller receives a write command, data, and an error detection code associated with the data from a host through a first NAND interface of the controller using a NAND interface protocol. The controller uses the error detection code to detect if a transmission error occurred. In another embodiment, a controller generates an error detection code based on data read from a flash memory

device and provides the data and error detection code to a host through a first NAND interface of the controller, so the host can detect if a transmission error occurred.

[0004] Other embodiments are disclosed, and each of the embodiments can be used alone or together in combination. The embodiments will now be described with reference to the attached drawings.

## **Brief Description of the Drawings**

[0005] Figure 1 is a block diagram of a system of an embodiment comprising a controller, a host, and one or more flash memory devices.

[0006] Figures 2A, 2B, and 2C are block diagrams illustrating different arrangements of a controller and flash memory device(s) of an embodiment.

[0007] Figure 3 is a block diagram of an exemplary controller of an embodiment.

[0008] Figure 4 is a block diagram of a controller of an embodiment for writing data to and reading data from flash memory device(s).

[0009] Figure 5 is a flow chart of a method for writing data in a flash memory device using a controller of an embodiment.

[0010] Figure 6 is a flow chart of a method for reading data from a flash memory device using a controller of an embodiment.

[0011] Figure 7 illustrates a controller arrangement of an embodiment configured for providing read status and spare block management control.

[0012] Figures 8A, 8B, 8C, and 8D are examples of data message formats that may be generated by the controller of Figure 7.

[0013] Figure 9 is an embodiment of data fields available for use in the data message format of Figure 8C.

[0014] Figure 10 is a flow chart of a method of an embodiment for providing status information to a host using the controller of Figure 7.

[0015] Figure 11 is a flow chart illustrating one embodiment of managing spare blocks using the controller of Figure 7.

[0016] Figures 12A and 12B are illustrations of good, bad, and spare block areas within an exemplary flash memory device.

[0017] Figures 13A-13D are block diagrams of exemplary controllers of an embodiment.

## **Detailed Description of the Presently Preferred Embodiments**

### **[0018] Introduction**

[0019] The following embodiments are directed to flash memory controllers and methods for use therewith. In one embodiment, a controller and method are provided for interfacing between a host controller in a host and a flash memory device. In another embodiment, a controller and method for detecting a transmission error over a NAND interface using error detection code are disclosed. In yet another embodiment, a controller and method for providing read status and spare block management information are disclosed. It should be noted that any of these embodiments can be used alone or in various combinations. Before turning to these and other embodiments, a general overview of exemplary controller architectures and a discussion of NAND interfaces and NAND interface protocols are provided.

### **[0020] Exemplary Controller Architectures**

[0021] Turning now to the drawings, Figure 1 is a system of an embodiment in which a controller 100 is in communication with a host 120 (having a host controller 121) through a first interface 125 and is in communication with one or more flash memory device(s) 130 through one or more second interface(s) 135. (The number of second interface(s) 135 can match the number of flash memory device(s) 130, or the number of second interface(s) 135 can be greater than or less than the number of flash memory device(s) 130 (e.g., a single second interface 135 can support multiple flash memory device(s)).) As used herein, the phrase “in communication with” means directly in communication with or indirectly in communication with through one or more components, which may or may not be shown or described herein.

[0022] A “host” is any entity that is capable of accessing the one or more flash memory device(s) 130 through the controller 100, either directly or indirectly through one or more components named or unnamed herein. A host can take any suitable form, such as, but not limited to, a personal computer, a mobile phone, a game device, a

personal digital assistant (PDA), an email/text messaging device, a digital camera, a digital media (e.g., MP3) player, a GPS navigation device, a personal navigation system (PND), a mobile Internet device (MID), and a TV system. Depending on the application, the host 120 can take the form of a hardware device, a software application, or a combination of hardware and software.

**[0023]** “Flash memory device(s)” refer to device(s) containing a plurality of flash memory cells and any necessary control circuitry for storing data within the flash memory cells. In one embodiment, the flash memory cells are NAND memory cells, although other memory technologies, such as passive element arrays, including one-time programmable memory elements and/or rewritable memory elements, can be used. (It should be noted that, in these embodiments, a non-NAND-type flash memory device can still use a NAND interface and/or NAND commands and protocols.) One example of a passive element array is a three-dimensional memory array. As used herein, a three-dimensional memory array refers to a memory array comprising a plurality of layers of memory cells stacked vertically above one another above a single silicon substrate. In this way, a three-dimensional memory array is a monolithic integrated circuit structure, rather than a plurality of integrated circuit devices packaged or die-bonded in close proximity to one another. Although a three-dimensional memory array is preferred, the memory array can instead take the form of a two-dimensional (planar) array. The following patent documents, which are hereby incorporated by reference, describe suitable configurations for three-dimensional memory arrays, in which the three-dimensional memory array is configured as a plurality of levels, with word lines and/or bit lines shared between levels: U.S. Patent Nos. 6,034,882; 6,185,122; 6,420,215; 6,631,085; and 7,081,377. Also, the flash memory device(s) 130 can be a single memory die or multiple memory dies. Accordingly, the phrase “a flash memory device” used in the claims can refer to only one flash memory device or more than one flash memory device.

**[0024]** As shown in Figure 1, the controller 100 also comprises a control module 140 for controlling the operation of the controller 100 and performing a memory operation based on a command (e.g., read, write, erase, etc.) and an address received from the host 120. As used herein, a “module” can include hardware, software, firmware, or any

combination thereof. Examples of forms that a “module” can take include, but are not limited to, one or more of a microprocessor or processor and a computer-readable medium that stores computer-readable program code (e.g., software or firmware) executable by the (micro)processor, logic gates, switches, an application specific integrated circuit (ASIC), a programmable logic controller, and an embedded microcontroller, for example. (The following sections provide examples of the various forms a “module” can take.) As shown in Figure 1, the controller 100 can include one or more additional modules 150 for providing other functionality, including, but not limited to, data scrambling, column replacement, handling write aborts and/or program failures (via safe zones), read scrubbing, wear leveling, bad block and/or spare block management, error correction code (ECC) functionality, error detection code (EDC) functionality, status functionality, encryption functionality, error recovery, and address mapping (e.g., mapping of logical to physical blocks). The following sections provide more details on these functions, as well as additional examples of other functions.

**[0025]** While the controller 100 and flash memory device(s) 130 are shown as two separate boxes in Figure 1, it should be understood that the controller 100 and flash memory device(s) 130 can be arranged in any suitable manner. Figures 2A, 2B, and 2C are block diagrams illustrating different arrangements of the controller and flash memory device(s). In Figure 2A, the controller 200 and the flash memory device(s) 230 are packaged in different packages 260, 270. In this embodiment, an inter-die interface can interface between the controller 200 and the flash memory device(s) 230. As used herein, an “inter-die interface” (e.g., an inter-die NAND interface) is operative to interface between two distinct units of electronic circuitry residing on distinct dies (e.g., to provide the necessary physical and logical infrastructure for the distinct units of electronic circuitry to communicate with each other, for example, using one or more specific protocols). Thus, the inter-die interface includes the necessary physical elements (e.g., pads, output, input drivers, etc.) for interfacing between the two distinct units of electronic circuitry residing on separate dies.

**[0026]** In Figure 2B, the controller 200 and the flash memory device(s) 230 both reside within a common multi-chip package 280. In this embodiment, an inter-die interface can interface between the controller 200 and the flash memory device(s) 230 fabricated on

two distinct dies that are packaged in the common multi-chip package 280. In Figure 2C, the controller 200 and the flash memory device(s) 230 are integrated on a same die 290. As another alternative, the controller 200 and/or flash memory device(s) 230 can be fabricated on two distinct dies, where one or both of these dies has no package at all. For example, in many applications, due to a need to conserve space, memory dies are mounted on circuit boards with no packaging at all.

[0027] It should be noted that in each of these arrangements, the controller 200 is physically located separately from the host. This allows the controller 200 and flash memory device(s) 230 to be considered a separate circuitry unit, which can be used in a wide variety of hosts.

[0028] As noted above with reference to Figure 1, the controller 100 communicates with the host 120 using a first interface 125 and communicates with the flash memory device(s) 130 using second interface(s) 135. In general, the first and second interfaces 125, 135 can take any suitable form. However, in a presently preferred embodiment, which will be described below in conjunction with Figure 3, the first and second interfaces 125, 135 are both NAND interfaces that use NAND interface protocols. Before turning to Figure 3, the following section provides a general discussion of NAND interfaces and NAND interface protocols.

[0029] **NAND Interfaces and NAND Interface Protocols**

[0030] A NAND interface protocol is used to coordinate commands and data transfers between a NAND flash device and a host using, for example, data lines and control signals, such as ALE (Address Latch Enable), CLE (Command Latch Enable), and WE# (Write Enable). Even though the term “NAND interface protocol” has not, to date, been formally standardized by a standardization body, the manufacturers of NAND flash devices all follow very similar protocols for supporting the basic subset of NAND flash functionality. This is done so that customers using NAND devices within their electronic products could use NAND devices from any manufacturer without having to tailor their hardware or software for operating with the devices of a specific vendor. It is noted that even NAND vendors that provide extra functionality beyond this basic subset of functionality ensure that the basic functionality is provided in order to provide compatibility with the protocol used by the other vendors, at least to some extent.

**[0031]** A given device (e.g., a controller, a flash memory device, a host, etc.) is said to comprise, include, or have a “NAND interface” if the given device includes elements (e.g., hardware, software, firmware, or any combination thereof) necessary for supporting the NAND interface protocol (e.g., for interacting with another device using a NAND interface protocol). (As used herein, the term “interface(s)” can refer to a single interface or multiple interfaces. Accordingly, the term “interface” in the claims can refer to only one interface or more than one interface.) In this application, the term “NAND Interface protocol” (or “NAND interface” in short) refers to an interface protocol between an initiating device and a responding device that, in general, follows the protocol between a host and a NAND flash device for the basic read, write, and erase operations, even if it is not fully compatible with all timing parameters, not fully compatible with respect to other commands supported by NAND devices, or contains additional commands not supported by NAND devices. One suitable example of a NAND interface protocol is an interface protocol that uses sequences of transferred bytes equivalent in functionality to the sequences of bytes used when interfacing with a Toshiba TC58NVG1S3B NAND device (or a Toshiba TC58NVG2D4B NAND device) for reading (opcode 00H), writing (opcode 80H), and erasing (opcode 60H), and also uses control signals equivalent in functionality to the CLE, ALE, CE, WE, and RE signals of the above NAND device.

**[0032]** It is noted that a NAND interface protocol is not symmetric in that the host – not the flash device – initiates the interaction over a NAND interface. Further, an interface (e.g., a NAND interface or an interface associated with another protocol) of a given device (e.g., a controller) may be a “host-side interface” (e.g., the given device is adapted to interact with a host using the host-side interface), or the interface of the given device may be a “flash memory device-side interface” (e.g., the given device is adapted to interact with a flash memory device using the flash memory device-side interface). The terms “flash memory device-side interface,” “flash device-side interface,” and “flash-side interface” are used interchangeably herein.

**[0033]** These terms (i.e., “host-side interface” and “flash device-side interface”) should not be confused with the terms “host-type interface” and “flash-type interface,” which are terminology used herein to differentiate between the two sides of a NAND interface protocol, as this protocol is not symmetric. Furthermore, because it is the host that



initiates the interaction, we note that a given device is said to have a “host-type interface” if the device includes the necessary hardware and/or software for implementing the host side of the NAND interface protocol (i.e., for presenting a NAND host and initiating the NAND protocol interaction). Similarly, because the flash device does not initiate the interaction, we note that a given device is said to have a “flash-type interface” if the device includes the necessary hardware and/or software for implementing the flash side of the NAND protocol (i.e., for presenting a NAND flash device).

[0034] Typically, “host-type interfaces” (i.e., those which play the role of the host) are “flash device-side interfaces” (i.e., they interact with flash devices or with hardware emulating a flash device) while “flash device-type interfaces” (i.e., those which play the role of the flash device) are typically “host-side interfaces” (i.e., they interact with hosts or with hardware emulating a host).

[0035] Because of the complexities of NAND devices, a “NAND controller” can be used for controlling the use of a NAND device in an electronic system. It is possible to operate and use a NAND device directly by a host with no intervening NAND controller; however, such architecture suffers from many disadvantages. First, the host has to individually manipulate each one of the NAND device’s control signals (e.g., CLE or ALE), which is cumbersome and time-consuming for the host. Second, the support of error correction code (ECC) puts a burden on the host. For at least these reasons, “no controller” architectures are usually relatively slow and inefficient.

[0036] In some conventional controller architectures, a NAND controller interacts with a flash memory device using a NAND interface and interacts with a host using a standard, non-NAND interface, such as USB or SATA. That is, in these conventional controller architectures, the NAND controller does not export a NAND interface to the host. Indeed, this is reasonable to expect, as a host processor that does not have built-in NAND support and requires an external controller for that purpose typically does not have a NAND interface and cannot directly connect to a device exporting a NAND interface and, therefore, has no use of a controller with a host-side NAND interface. On the other hand, a host processor that has built-in NAND support typically also includes a built-in NAND controller and can connect directly to a NAND device, and, therefore, has no need for an external NAND controller.

[0037] “NAND Flash Memory Controller Exporting a NAND Interface,” U.S. patent application no. 11/326,336 (published as U.S. Patent Publication No. US 2007/0074093), which is hereby incorporated by reference, discloses a new type of NAND controller, characterized by the fact that the interface it exports to the host side is a NAND interface. In this way, the NAND controller exports to the host the same type of interface that is exported by a standard NAND flash memory device. The controller also preferably has a NAND interface on the flash memory device side as well, where the controller plays the role of a host towards the NAND flash memory device and plays the role of a NAND device towards the host.

[0038] **Exemplary NAND Flash Memory Controller Exporting a NAND Interface**

[0039] Returning to the drawings, Figure 3 is a block diagram of an exemplary controller 300 of an embodiment. As shown in Figure 3, the controller 300 includes a control module 340 for controlling the operation of the controller 300 and, optionally, one or more additional modules 350 for providing other functions. Examples of other functions include, but are not limited to, data scrambling, column replacement, handling write aborts and/or program failures (via safe zones), read scrubbing, wear leveling, bad block and/or spare block management, error correction code (ECC) functionality, error detection code (EDC) functionality, status functionality, encryption functionality, error recovery, and address mapping (e.g., mapping of logical to physical blocks). The following paragraphs describe some of these functions, and sections later in this document describe others of these functions.

[0040] “Data scrambling” or “scrambling” is an invertible transformation of an input bit sequence to an output bit sequence, such that each bit of the output bit sequence is a function of several bits of the input bit sequence and of an auxiliary bit sequence. The data stored in a flash memory device may be scrambled in order to reduce data pattern-dependent sensitivities, disturbance effects, or errors by creating more randomized data patterns. More information about data scrambling can be found in the following patent documents: U.S. patent application nos. 11/808,906, 12/209,697, 12/251,820, 12/165,141, and 11/876,789, as well as PCT application no. PCT/US08/88625.

[0041] “Column replacement” refers to various implementations of mapping or replacing entirely bad columns, portions of columns, or even individual cells. Suitable

types of column replacement techniques can be found in U.S. Patent Nos. 7,379,330 and 7,447,066.

**[0042]** There are several potential problems in writing to flash memory devices where logically or physically adjacent data may be corrupted outside of the location where the data is attempted to be written. One example is when a write to one area (e.g., a cell, page, or block) of memory fails, and the contents of some surrounding memory may be corrupted. This is referred to as a “program failure” or “program disturb.” A similar effect known as “write abort” is when a write (or program) operation is terminated prematurely, for example when power is removed unexpectedly. In both cases, there are algorithms which may be used to pro-actively copy data from a “risk zone” to a “safe zone” to handle write aborts and program failures, as described in U.S. Patent No. 6,988,175.

**[0043]** “Read scrubbing” or, more generally, “scrubbing” refers to the techniques of refreshing and correcting data stored in a flash memory device to compensate for disturbs. A scrub operation entails reading data in areas that may have received exposure to potentially disturbing signals and performing some corrective action if this data is determined to have been disturbed. Read scrubbing is further described in U.S. Patent Nos. 7,012,835, 7,224,607, and 7,477,547.

**[0044]** Flash memory devices may be written unevenly, and “wear leveling” refers to techniques that attempt to even out the number of times memory cells are written over their lifetime. Exemplary wear leveling techniques are described in U.S. Patent Nos. 6,230,233 and 6,594,183.

**[0045]** In general, flash memory devices are manufactured with an excess number of blocks (greater than the defined minimum capacity). Either during factory testing or during use of the device, certain blocks may be discovered as “bad” or “defective,” meaning that they are unable to correctly store data and need to be replaced. Similarly, there may be an excess of “good” blocks (greater than the defined minimum capacity) which may be used as “spares” until another block fails or becomes defective. Keeping track of these extra blocks is known as bad block management and spare block management, respectively. More information about bad block and spare block management can be found in U.S. Patent No. 7,171,536.

**[0046]** As mentioned above, additional information about these different functional modules and how they are used in exemplary controller architectures is provided later in this document.

**[0047]** Returning to the drawings, as also shown in Figure 3, the controller 300 includes one or more flash memory device-side NAND interface(s) 335 for interfacing with one or more NAND flash device(s) 330 (e.g., 1-8 memory dies). Furthermore, it is noted that the flash memory device-side NAND interface 335 is also a host-type NAND interface (i.e., that it is adapted to initiate the interaction over the NAND interface and to present a host to a NAND flash device(s) 330). The controller 300 also includes a host side NAND interface 325 for interfacing to a host 320 (having a host controller 321) that supports a NAND interface protocol. This host side NAND interface 325 is also a flash memory-type NAND interface (e.g., the controller 300 is adapted to present to the host 320 a NAND flash memory storage device). Examples of NAND interfaces include, but are not limited to, Open NAND Flash Interface (ONFI), toggle mode (TM), and a high-performance flash memory interface, such as the one described in U.S. Patent No. 7,366,029, which is hereby incorporated by reference. The controller 300 may optionally include one or more additional host-side interfaces, for interfacing the controller 300 to hosts using non-NAND interfaces, such as SD, USB, SATA, or MMC interfaces. Also, the interfaces 325, 335 can use the same or different NAND interface protocols.

**[0048]** It should be noted that the controller 300 and flash memory device(s) 330 can be used in any desired system environment. For example, in one implementation, a product manufactured with one or more controller 300/flash memory device(s) 330 units is used in a solid-state drive (SSD). As another example, the controller 300 can be used in OEM designs that use a Southbridge controller to interface to flash memory devices.

**[0049]** There are several advantages of using a NAND flash memory controller that exports a NAND interface to a host. To appreciate these advantages, first consider the realities of current controller architectures. Today, there are two types of NAND interfaces: a “raw” interface and a “managed” interface. With a raw interface, the basic memory is exposed with primitive commands like read, program, and erase, and the external controller is expected to provide memory management functions, such as ECC, defect management, and flash translation. With a managed interface, through some

higher level interface, logical items such as sectors/pages/blocks or files are managed, and the controller manages memory management functions.

[0050] However, the set of firmware required to “manage” the NAND can be divided into two categories. The first category is generic flash software that mostly manages the host interface, objects (and read/modify/write sequences), and caching. This is referred to as the “host management” layer. The second category is flash-specific management functionality that does, for example, the ECC, data scrambling, and specific error recovery and error prevention techniques like pro-active read scrubbing and copying lower-page blocks to prevent data loss due to write aborts, power failures, and write errors. This is referred to as the “device management” layer.

[0051] The first category of software is relatively constant and may be provided by various companies, including OS vendors, chipset and controller vendors, and embedded device vendors. In general, let’s assume there are M specific systems/Os/ASICs that may want to use flash in their designs. The second set is potentially proprietary to individual companies and even specific to certain memory designs and generations. In general, let’s assume there are N different memory specific design points. Today, this is an all-or-nothing approach to flash management – either buy raw NAND or managed NAND. This also means that a solution must incorporate one of the M system and host management environments with one of the N memory device management environments. In general, this means that either (1) a flash vendor with the second kind of knowledge must provide all layers of a solution, including ASIC controller and host interface software, and do M different designs for the M different host opportunities, or (2) any independent ASIC and firmware company has little opportunity to customize their solutions to specific memory designs without doing N different designs, or (3) two companies have to work together, potentially exposing valuable trade secrets and IP and/or implement different solutions for each memory design. This can also produce a time-to-market delay if M different host solutions have to be modified to accept any new memory design or vice versa.

[0052] By using a NAND flash memory controller that exports a NAND interface to a host, a new logical interface is provided that uses existing physical NAND interfaces and commands, such as legacy asynchronous, ONFI, or TM, to create a new logical interface

above raw or physical NAND and below logical or managed NAND, create “virtual” raw NAND memory with no ECC required in the host controller, and disable host ECC (since 0 ECC is required from the host to protect the NAND memory). This new logical interface also can provide, for example, data scrambling, scrubbing, disturbs, safe zone handling, wear leveling, and bad block management (to only expose the good blocks) “beneath” this interface level.

**[0053]** This different logical interface provides several advantages over standard flash interfaces or managed NAND interfaces, including ONFI Block Abstraction (BA) or Toshiba LBA. For example, separation of the memory-specific functions that may vary from memory type and generation (e.g., NAND vs. 3D (or NOR) and 5Xnm vs. 4Xnm vs. 3Xnm) allows for different amounts of ECC, vendor-unique and memory-unique schemes for error prevention and correction schemes, such as handling disturbs and safe zones, and allows vendor-unique algorithms to remain “secret” within the controller and firmware. Additionally, there is greater commonality between technology (and vendors) at this logical interface level, which enables quicker time to market. Further, this allows much closer to 1:1 command operation, meaning improved and more-predictable performance versus managed NAND or other higher level interfaces.

**[0054]** There are additional advantages associated with this controller architecture. For example, it allows for independent development, test, and evolution of memory technology from the host and other parts of the system. It can also allow for easier and faster deployment of next generation memories, since changes to support those memories are more localized. Further, it allows memory manufactures to protect secret algorithms used to manage the raw flash. Also, page management can be integrated with the file system and/or other logical mapping. Thus, combined with standard external interfaces (electrical and command sets), this architecture makes it easier to design in raw flash that is more transparent from generation to generation.

**[0055]** There is at least one other secondary benefit from the use of this architecture – the controller 300 only presents a single electrical load on the external interface and drives the raw flash internal to the MCP. This allows for potentially greater system capacity without increasing the number of flash channels, higher speed external interfaces

(since fewer loads), and higher-speed internal interfaces to the raw flash devices (since very tightly-controlled internal design (substrate connection) is possible).

**[0056]** Another advantage associated with the controller of this embodiment is that it can be used to provide a “split bus” architecture through the use of different host and memory buses, potentially at different speeds (i.e., the bus between the host and the controller can be different from the bus between the controller and the flash memory device(s)). (As used herein, a “bus” is an electrical connection of multiple devices (e.g., chips or dies) that have the same interface. For example, a point-to-point connection is a bus between two devices, but most interface standards support having multiple devices connected to the same electrical bus.) This architecture is especially desired in solid-state drives (SSDs) that can potentially have hundreds of flash memory devices. In conventional SSD architectures, the current solution is to package N normal flash memory devices in a multi-chip package (MCP), but this still creates N loads on a bus, creating N times the capacitance and inductance. The more loads on a bus, the slower it operates. For example, one current architecture can support a 80 MHz operation with 1-4 devices but can support only a 40 MHz operation with 8-16 devices. This is the opposite of what is desired – higher speeds if more devices are used. Furthermore, more devices imply the need for greater physical separation between the host and the memory MCPs. For example, if 16 packages were used, they will be spread over a relatively large physical distance (e.g., several inches) in an arbitrary topology (e.g., a bus or star-shaped (or arbitrary stub) topology). This also reduces the potential performance of any electrical interface. So, to obtain, for example, 300 MHz of transfers (ignoring bus widths), either four fast buses or eight slow buses can be used. But, the fast buses could only support four flash memory devices each, or 16 total devices, which is not enough for most SSDs today. If the buses run faster, the number of interface connections (pins and analog interfaces) can be reduced, as well as potentially the amount of registers and logic in the host.

**[0057]** Because the controller 300 in this embodiment splits the interconnection between the host and the raw flash memory device(s) into a separate host side interface and a flash side interface with a buffer in between, the host bus has fewer loads and can run two to four times faster. Further, since the memory bus is internal to the MCP, it can

have lower power, higher speed, and lower voltage because of the short distance and finite loads involved. Further, the two buses can run at different frequencies and different widths (e.g., one side could use an 8-bit bus, and the other side can use a 16-bit bus).

**[0058]** While some architectures may insert standard transceivers to decouple these buses, the controller 300 of this embodiment can use buffering and can run these interfaces at different speeds. This allows the controller 300 to also match two different speed buses, for example, a flash side interface bus running at 140MB/sec and an ONFI bus that runs at either 132 or 166 MB/sec. A conventional bus transceiver design would have to pick the lower of the two buses and run at 132 MB/sec in this example, while the controller 300 of this embodiment can achieve 140 MB/sec by running the ONFI bus at 166 MB/sec and essentially have idle periods. Accordingly, the controller 300 of this embodiment provides higher performance at potentially lower cost and/or lower power and interface flexibility between different products (e.g., different speed and width host and memory buses, fewer loads on the host in a typical system (which enables faster operation and aggregation of the memory bus bandwidth to the host interface), and different interfaces on the host and memory side with interface translation).

**[0059]** As mentioned above, a single controller can also have multiple flash side interface(s) 335 to the flash memory device(s), which also enables further parallelism between raw flash memory devices and transfers into the controller, which allows the flash side interface to run slower (as well as faster) than the host side interface 325. A single controller can also have multiple host side interfaces that may be connected to different host controller interfaces to allow for greater parallelism in accessing the flash memory device(s), to share the controller, or to better match the speed of the flash side interface (which could be faster than the host side interface for the reasons described above).

**[0060]** Another advantage of importing a NAND interface to a host relates to the use of a distributed controller architecture. Today, flash memory devices are typically implemented with a single level of controller. In large solid-state drives (SSDs), there may be tens or even hundreds of flash devices. In high-performance devices, it may be desirable to have parallel operations going on in as many of these flash devices as possible, which may be power constrained. There are interface specs today at 600



MB/sec, and these are still increasing. To reach this level of performance requires very fast controllers, memories, and ECC modules. Today, high performance controllers are built with either one or a small number of ECC modules and one or two microprocessors to handle memory device management. Since some of the functions are very localized to the memory devices themselves, such as ECC, with the controller 300 of this embodiment, a two-tiered network of devices can be utilized. Specifically, the host 320 can manage the host interface and high-level mapping of logical contents, and one or more controllers 300 can manage one or more raw NAND flash memory devices to provide local management of memory device functions (e.g., ECC) and parallelism in the execution of these functions due to parallel execution of the controller 300 and the host 320 and parallel execution of multiple controllers 300 handling different operations in parallel on different memories 320. In contrast to conventional controllers in SSDs, which perform memory device management functions in one place, by splitting these functions into two layers, this architecture can take advantage of parallel performance in two ways (e.g., between host and slave, and between many slaves). This enables higher total performance levels (e.g., 600 MB/sec) without having to design a single ECC module or microprocessor that can handle that rate.

**[0061]** Yet another advantage of this architecture is that a higher-level abstraction of the raw memory can be developed, such that system developers do not need to know about error recovery or the low-level details of the memory, such as ECC and data scrambling, since the controller 300 can be used to perform those functions in addition to handling memory-specific functions such as read, erase, and program disturbs, and safe zones. This level of support is referred to herein as “corrected” flash,” which is logically in between raw flash and managed NAND. On the other hand, this architecture is not fully managed memory in the sense of page or block management at a logical level and may require the host to provide for logical-to-physical mapping of pages and blocks. However, the controller 300 can still present some flash memory management restrictions to the host and its firmware, such as: only full pages can be programmed, pages must be written in order within a block, and pages can only be written once before the entire block must be erased. Wear leveling of physical blocks to ensure that they are used approximately evenly can also be performed by the controller 300; however, the host 320

can be responsible for providing this function. Also, the controller 300 preferably presents the host 320 with full page read and write operations into pages and blocks of NAND. The characteristics of logical page size and block size will likely be the same as the underlying NAND (unless partial page operations are supported). The majority of the spare area in each physical page in the raw NAND will be used by the controller 300 for ECC and its metadata. The controller 300 can provide for a smaller number of spare bytes that the using system can utilize for metadata management.

**[0062] Embodiments Relating to Detecting a Transmission Error Over a NAND Interface**

**[0063]** With reference to Figure 3, transmission errors may occur as data is being sent from the host 320 to the controller 300 over a NAND interface bus to the host-side NAND interface 325. Since ECC is generated and checked within the controller 300, there is no ECC protecting the data transmitted over the host-side NAND interface 325. This problem and a proposed solution will now be discussed in conjunction with Figure 4.

**[0064]** Figure 4 is a block diagram of a controller 400 of an embodiment for writing data to and reading data from one or more flash memory device(s) 430. As shown in Figure 4, the controller 400 in this embodiment comprises a first NAND interface 425 configured to transfer data between the controller 400 and a host 420 (having a host controller 421) using a NAND interface protocol, as well as second NAND interface(s) 435 configured to transfer data between the controller 400 and one or more flash memory device(s) 430 using a NAND interface protocol. As discussed above, the NAND interface protocol used by each interface 425, 435 can be the same protocol or can be different protocols. As also discussed above, the controller 400 and the flash memory device(s) 430 can be packaged in different packages, can both reside within a common multi-chip package, or can be integrated on the same die. Also, in one embodiment, the host 420 performs logical-to-physical address mapping, so the host 420 provides the controller 400 with a physical address over the first NAND interface 425 along with a command to write or read to that physical address.

**[0065]** In this embodiment, the controller 400 comprises a control module 440 to control the operation of the controller 400, an error detection code (EDC) module 450

(e.g., an ECC encoder/decoder), and an error correction code (ECC) module 460 (e.g., an ECC encoder/decoder). The EDC module 450 is operative to generate an error detection code based on inputted data, and the ECC module 460 is operative to generate an error correction code based on inputted data. In this embodiment, the control module 440 is configured to correct errors using an ECC code (e.g., part of the control module 440 is an ECC correction engine). Data as used in this context can include the normal data page to be stored or retrieved as well as header, metadata, or spare fields used to store addresses, flags or data computed by either the host 420 or the controller 400. Whereas an error detection code allows at least one error to be detected but not corrected, an error correction code allows at least one error to be both detected and corrected. The number of errors that can be detected and/or corrected depends on the type of error detection code scheme and error correction code scheme that are used. Suitable types of error detection code schemes include, but are not limited to, a one or more byte checksum, a longitudinal redundancy check (LRC), a cyclic redundancy check (CRC), or an 8b/10b code. Suitable types of error correction code schemes include, but are not limited to, Hamming code and Reed-Solomon code.

**[0066]** Figures 5 and 6 are flow charts 500, 600 illustrating how the controller 400 in this embodiment is used in write and read operations, respectively. Turning first to the flow chart 500 in Figure 5, the controller 400 receives a write command, data, and an error detection code associated with the data from the host 420 over the first NAND interface 425 (act 510). (Because the host 420 is not necessarily aware of the fact that it is issuing the command to a controller, it may assume that it is interfacing with a standard NAND flash storage device of the type it is capable of handling.) The error detection code can be sent before, after, or mixed with data, and, in one embodiment, the error detection code is part of a header (e.g., 8-16 spare bytes) of a data packet that contains the data. As discussed above, the error detection code allows at least one error in the data to be detected but not corrected. Next, the EDC module 450 generates an error detection code based on the data, and the control module 440 compares the generated error detection code with the error detection code received from the host 420 (act 520). Based on this comparison, the control module 440 determines whether the generated error detection code matches the error detection code received from the host 420 (act 530). If

the generated error detection code does not match the error detection code received from the host 420, the control module 440 sends a signal to the host 420 indicating that an error occurred in transmission of the data from the host 420 to the controller 400 (act 540). The host 420 can then resend the data to the controller 400. However, if the generated error detection code matches the error detection code received from the host 420, the write process continues with the ECC module 460 generating an error correction code based on the data (act 550). As discussed above, the error correction code allows at least one error in the data to be both detected and corrected. The control module 440 then stores the data and the error correction code in the flash memory device(s) 430 over the second NAND interface 435. Again, the command is issued according to the NAND interface protocol, including command bytes, address bytes, header bytes, and data bytes that contain both the host's data bytes and the corresponding ECC bits generated by the ECC module 460. In this way, the flash memory device(s) 430 are not necessarily even aware that they are receiving information indirectly via the controller 400 and not directly from the host 420.

**[0067]** Turning now in Figure 6, flow chart 600 illustrates how the controller 400 is used in a read operation. As shown in Figure 6, the controller 400 receives a read command from the host 420 (act 610). The controller 400 then reads data and an error correction code associated with the data from the flash memory device(s) 430 (act 620). As mentioned above, the error correction code allows at least one error in the data to be both detected and corrected. Next, the ECC module 460 generates an error correction code based on the data, and the control module 440 (e.g., using an ECC correction engine) compares the generated error correction code with the error correction code received from the flash memory device(s) 430 (act 630). Based on that comparison, the control module 440 determines whether the generated error correction code matches the error correction code received from the flash memory device(s) 430 (act 640). If the generated error correction code does not match the error correction code received from the flash memory device(s) 430, the control module 440 attempts to correct the error(s) in the data (act 650). (As discussed above, depending on the ECC scheme used, the control module 440 may be able to correct one or more than one detected error or the control module may use other means to attempt to correct the error.) If the correction does not

succeed, a signal can be sent to the host 420 indicating that a storage error occurred. However, if the generated error correction code matches the error correction code received from the flash memory device(s) 430, the read process continues with the EDC module 450 generating an error detection code based on the data (act 660). As discussed above, the error detection code allows at least one error in the data to be detected but not corrected. The control module 440 then sends the data and the error detection code to the host 420 (act 670). The host 420 would then generate its own error detection code based on the data and optional header and compare it to the error detection code received from the controller 420. If the codes do not match, the host 420 would know that a transmission error occurred and can send a signal to the controller 400 to resend the data.

[0068] As can be seen from these flow charts 500, 600, this embodiment protects against transmission errors that may occur as data is being sent between the host 420 and the controller 400 over the first NAND interface 425. In some controller architectures, in a write operation, the host generates ECC and sends the ECC and data to the controller, which stores both the ECC and data in the flash memory device. Similarly, in a read operation, the controller retrieves the data and the ECC from the flash memory device and sends the data and the ECC to the host. In these architectures, ECC is not only used to protect against memory device errors, but it is also used to protect against interface transmission errors between the host and the controller. However, in this embodiment, it is the controller 400 – not the host 420 – that generates ECC to store with data in the flash memory device(s) 430. By having the host 420 generate EDC and having the controller 400 check the EDC on writes and by having the controller 400 generate EDC and having the host 420 check the EDC on reads, this embodiment provide protection against transmission errors over the first NAND interface 425 even though the host 420 does not generate ECC for storage, as in conventional controller architecture. Further, while the process of having the host generate EDC and having the controller check the EDC and then generate ECC is used in some prior controller architectures that provide a non-NAND interface to the host (e.g., USB), this embodiment can be used in controller architectures, such as shown in Figure 3 and 4, where the host and the controller communicate over a NAND interface using a NAND protocol. Further, some existing host interface protocols (especially serial ones such as SATA, SAS, FC, and PCIe)

provide for some kind of CRC per packet that can be used to detect transmission errors, and this information could be passed thru the host 420 and appended to the data packet and used for a similar purpose. However, data transfers over the external host interface (such as SATA) may have a different transfer length than the pages sent over the first NAND interface 425 to the controller 400, and appropriate adjustments may need to be made.

[0069] In the above, the EDC computed by the host 420 and by the EDC module 450 could also be a simpler form of ECC than that used by the ECC module 450. For example, the ECC used over the first NAND interface 425 only needs to detect or correct transmission errors, while the ECC used over the second NAND interface 435 preferably is used to detect and correct NAND storage errors, which may require a longer or more complicated ECC.

**[0070] Embodiments Relating to Providing Read Status and Spare Block Management Information in a Flash Memory System**

[0071] Returning to the drawings, Figure 7 is an illustration of a controller 700 of an embodiment that includes a control module 740, an error correction code (ECC) module 750, a status module 760, and a spare block management module 770. The controller 700 may be in communication with a host 720 (having a host controller 721) and flash memory device(s) 730 via first and second interfaces 725, 735, respectively. The first and second interfaces 725, 735 can take any suitable form, and, in one embodiment, are NAND interfaces, as described above in connection with Figure 3. However, other, non-NAND-type interfaces can be used, such as, but not limited to, USB and SATA.

Additionally, the controller 700 may be placed in any of the physical arrangements discussed above, for example on a separate die that is packaged in a memory system that also contains one or more flash memory dies, independently packaged from the host and the flash memory, and so on.

[0072] The control module 740 may be configured for controlling the operation of the controller 700 and performing a memory operation based on a command (e.g., read, write, erase, etc.) and address received from the host 720. An ECC module 750 is used in the process of determining if an error, such as a read or write error, has occurred in handling data retrieved from or sent to blocks of memory in the flash memory. The

controller 700 may be configured to apply any of a number of error correction code (ECC) algorithms to detect read errors and to correct for certain detected errors within the capability of the particular error correction code algorithm. The controller 700 handles application of error correction coding such that the host 720 receives data over the first interface 725 processed according to the error correction algorithm rather than having to do error correction at the host. (Alternatively, the ECC module 750 can be replaced with an error handling module that could use other error recovery techniques in addition to or instead of ECC. In such alternative, the controller 700 would still correct the data, so that the data sent over the first interface 725 does not require further error processing by the host 720 (e.g., calculating a single error code or re-reading with a voltage shift).) Conversely, during write operations, the controller 700 handles error encoding data and transfers the ECC code and data over the second interface 735 for storage on the flash memory device(s) 730.

**[0073]** The status module 760 cooperates with the ECC module 750 to provide the host 720 with data relevant to the status of particular operations on the flash memory device(s) 730. For example, the status module 760 may review error analysis activity in the controller 700 and prepare status information on read error information based on whether a read error has been detected, has been corrected, or is uncorrectable. Because of the host, controller, and flash memory arrangement, where the host 720 will typically not be handling the error analysis or correction of data as it is retrieved from the flash memory device(s) 730, the host 720 will have no details of the status of a read operation. The status module 760 allows for this information to be tracked and presented to the host 720 so that the host 720 may make any desired adjustments in how or where data is sent or requested to memory. The host 720 may also use this status to trigger some other proactive or preventative operation, such as wear leveling, data relocation, or read scrubbing.

**[0074]** The status module 760 may present status information to the host 720 in one of several formats. In situations where the status module is preparing read status information for transmission to the host 720, the read status may be appended to retrieved data from the flash memory, as indicated in Figures 8A and 8C. (It should be noted that the fields shown in these figures can come in any order.) Figure 8A illustrates a data

transfer format 800 where data retrieved from the flash memory, after processing for error analysis by the controller 700, is placed in a message having a header 802, a data payload section 804, and a status bit 806, which can be padded to two or more bytes (accordingly, “bit” as used in the claims, can refer to a single bit or to one or more bits, such as one or more bytes). This status bit 806 may be a binary success or failure indication for use by the host 720. The status bit 806 would not necessarily differentiate between the type or extent of read error, but would provide a flag to the host 720 alerting it that some form of error had been encountered. Alternatively, the status bit may be a single field for carrying an encoded value associated with an error message in a look-up table maintained in the host 720 or by the controller 700. Figure 8B is similar to Figure 8A but the status bit 806’ is included as part of the header 802’ which would normally be filled in by the controller 700 on reads, and there is no separate status bit field.

**[0075]** Alternatively, as seen in Figure 8C, the data transfer format 808 may include a header 810, data payload section 812, and a status section 814 having one or more bits arranged in multiple fields 816 in the status section 814. In the arrangement of Figure 8C, more detailed information on status may be transferred regarding read errors and will be available for the host 720. In one implementation of the status message, only read error information may be provided to the host 720. In other implementations, the status information may be arranged to convey one or more of read, write, and erase error information detected by the control module 740 and formatted by the status module 760 of the controller 700. In yet other embodiments, fields 816 of the status section 814 may also, or alternatively, present data relating to spare block management. Details on spare block management activities engaged in or reported on by the spare block management module 770 of the controller 700 are provided in the following section. The multiple field embodiment of Figure 8C provides a mechanism for combinations of errors associated with a memory operation to be reported. Figure 8D is similar to Figure 8C but the status field 814’ is part of the header 810’ and may similarly be composed of multiple fields 816’.

**[0076]** In another embodiment, the result or success/failure of a read could be indicated in the status register or extended status register in one of the reserved or vendor unique fields. However, beyond polling for busy status, host controllers today may not



necessarily look for read errors in the status or extended status registers. Program and erase errors are reported over the second interface 735 in response to program or erase commands (this is standard error reporting from a raw NAND device), and this information could be returned to the host. The usual response to such an error is to allocate a new block, copy any current valid data pages from the block with errors, and have any metadata indicate that this is now the valid block and then mark the existing block that has errors as bad. In one embodiment, the controller can indicate the program or erase failures and leave it to the host controller to perform the above copying and metadata management. In another embodiment, the controller can perform these operations and manage the bad block within the controller. In this case, it could be totally transparent to the host controller that an error occurred or the controller could indicate that it took this corrective action (for example, the host could log this like a soft error had occurred). So, in summary, these bits could indicate that an error occurred that the host must manage, that an error occurred that the controller managed (and the host is merely informed), or that the error could be handled by the controller and hidden from the host.

**[0077]** The alternative ways of signaling an error, such as the single status bit 806 or 806', the status section 814 or 814' with multiple fields 816 or 816', or via bits in the status or extended status register, will collectively be referred to as an "error signal." In another embodiment, in addition to one or more of these error signals, the controller 700 may be configured to store detailed status information in a known location in combination with usage of one or more of the error signals. For example, the status module 760 of the controller 700 may store detailed status information (e.g., read status data) in a predetermined location on the flash memory device(s) 730 or in the controller 700 that the host may access in response to receiving one or more of the error signals. Thus, the status bit or field may not convey any more information than a flag indicating that more information is available to the host if the host wants additional details on the status (e.g. a read error). Also, the additional status information flagged by the bit or field may be stored in a location tracked by the controller 700 that the host may access by sending a general command to the controller 700 to retrieve the status information, rather than the host needing to know the location and retrieving the status information.

**[0078]** If the single bit appended status message format of Figure 8A is used, where the bit is representative of the bare assertion of success or failure of error correction, the bit may be implemented as part of a vendor-specific bit in an extended read format for an available interface protocol, such as ONFI 2.0 available from the Open NAND Flash Interface Working Group. Multiple bit status information, or single or multiple bit information formats, that alerts the host 720 to more detailed information at a location that the status module causes to be stored, may also be used as described above.

**[0079]** Figure 9 shows one possible arrangement of status fields 900 that may be placed in locations 806, 806', 814, 814' in the embodiments of Figures 8A-8D or stored in the controller 700 or flash memory device(s) 730 in the embodiments where the host 720 may request further information after notification of status availability or retrieve the information from the controller 700. The status fields 900 may include a field 902 indicating success or failure of a read operation, a field 904 providing information as to whether a correction such as ECC correction was performed, and a field 906 flagging whether there was a "hard" ECC failure (i.e., where data was lost). In addition to read status information, the status fields 900 may also include one or more fields 908 representing whether a program or erase error was detected by the controller 700. Status information relating to spare block management, as discussed further below, may also be included, such as a field 910 requesting a block copy and remapping, a field 912 asking a host to return a new spare block, and a field 914 indicating to the host 720 that there has been an attempted operation on a defective block in the flash memory device(s) 730. One or more additional fields 916 may be arranged to handle other status information that may be necessary for a particular application. For example, such a field 916 can indicate the number of soft errors (i.e., errors corrected by the ECC).

**[0080]** Figure 10 illustrates a flow chart 1000 of a method of an embodiment operable on the controller 700 for providing read status information to the host 720. The controller 700 first receives a read command from the host 720 (act 1002). In order to read the data, the controller 700 issues a read command to the flash memory device(s) 730 (act 1004), and the flash memory device(s) 730 return a page of data along with error correction code to the controller 700 over the second interface 735 (act 1006). The ECC module 760 of the controller 700 conducts an error analysis on the retrieved data (act 1008). The error

analysis or handling may be an error correction code algorithm or other error correction mechanism. If an ECC algorithm is used, the controller 700 computes the ECC bytes on the retrieved data from the flash memory device(s) 730 and compares the computed ECC bytes with those previously stored and retrieved with the data. If the computed ECC bytes and the retrieved ECC bytes do not match, the controller 700 identifies an error (act 1010). If the difference between the computed ECC and stored ECC is correctable by the controller 700, then the controller 700 will fully correct the data before transfer over the first interface 725 and will identify the error as a “soft” or correctable error.

Alternatively, if the error is severe enough that the ECC algorithm or other error recovery procedures cannot compensate for the error, the controller 700 will identify a hard error that signals a data loss has occurred. The corrected data read from flash memory device(s) 730 is then sent over the first interface 725 to the host 720 with the status information appended in a data message format such as one of the data message formats 800, 800', 808, 808' discussed above (act 1012).

**[0081]** With reference to the method of providing a read status error, an embodiment in which is illustrated in Figure 10, the read status error may be calculated and provided only at the end of each page of information read and analyzed by the controller 700 so that streaming of multiple pages is not interrupted, and it is explicit as to which pages may contain errors. Additionally, in another embodiment, it is contemplated that the controller 700 may read data from the flash memory device(s) 730 and compute the ECC as the data comes in and before a complete page of flash memory has been processed. For example, if the page size is 8 kilobytes (KB), the controller 700 may calculate ECC in 2 KB segments, with each comprising less than a page, so that after each portion of the page is done, the ECC can be checked or corrected for that information representing that part of the page. After one or more 2 KB segments have been transferred from flash memory device(s) 730 to the controller 700, the controller 700 may simultaneously start transferring the error-corrected data over the first interface 725 before the last of the data has transferred for that page from flash memory to the controller.

**[0082] Good, Bad, and Spare Block Management Embodiments**

**[0083]** Referring again to Figure 9, as mentioned above, the status fields 900 may include information relating to spare block management, for example fields 910-914,

useful for handling spare blocks needed to manage bad (defective) blocks that may develop over the useful life of the flash memory. As shown in Figure 7, a spare block management module 770 may be included in the controller 700 to operate in one of several ways. Depending on the particular spare block management mode adopted, one or more fields of information, such as the example fields 910-914 may be utilized.

**[0084]** In general, flash memory devices are manufactured with an excess number of blocks (greater than the defined minimum capacity). Either during factory testing or during use of the device, certain blocks may be discovered as “bad” or “defective,” meaning that they are unable to correctly store data and need to be replaced. Similarly, there may be an excess of “good” blocks (greater than the defined minimum capacity) which may be used as “spares” until another block fails or becomes defective. Keeping track of these extra blocks is known as bad block management and spare block management, respectively. These concepts will be described in more detail in the following paragraphs, which refer to the blocks of an example flash memory device 1200 shown in Figures 12A and 12B.

**[0085]** Figure 12A shows a physical view of the blocks of a device that is designed and fabricated with an example of 1,000 total blocks of memory. In this diagram, the blocks are shown in physical order, and each white block 1210 represents an independent block in the flash memory device (only a few of the 1,000 blocks are shown). Each black block 1220 represents a block that is defective at the time of manufacturing (which are randomly distributed in this example). Figure 12B shows an abstract view of the same part 1200, where the various good and bad blocks are shown grouped together (and not in physical order). An example vendor data sheet for a part such as 1200 may indicate that it can be relied upon to have at least 900 good blocks at its end of life, as shown in 1230. For our specific exemplary flash memory device 1200, there are 950 good (white) blocks (not all shown) and 50 bad (black) blocks (not all shown). The 50 bad blocks (at time of manufacturing or initial testing) are shown logically grouped together as 1260.

**[0086]** Continuing in our example, the data sheet may also specify that no more than 10 blocks may fail during its specified lifetime, so these are shown as the “minimum spares” 1240. Thus, the device 1200 must have a minimum of 910 good blocks at the time of manufacturing (or the factory would not ship such a device since it would not

comply with the data sheet). The other 40 good (white) blocks (the difference between the 950 good blocks and the 910 guaranteed good blocks) are considered “extra spare” blocks and are shown as 1240. The number of extra spares cannot necessarily be relied upon and could theoretically vary between 90 (if there are no bad blocks, although this is very rare) and 0 (implying 90 bad blocks, which would just meet the data sheet requirements). Collectively, the minimum spares and extra spares may also be referred to as the “spare blocks.”

**[0087]** Typically, a host would handle spare block management directly with raw flash memory. For example, a standard host may have its own controller that scans all blocks in a flash memory to look for a specific signature to determine which blocks are useable blocks and which blocks are unusable, also referred to as defective or “bad” blocks. Thus, if a flash memory, such as flash memory device(s) 730 described above and as shown in detail in 1200, is manufactured as having 1,000 blocks of memory, the host controller would typically analyze all 1,000 blocks and identify the good and bad blocks. The typical host controller may then use all or a subset of the 940 good blocks (in this example) and reserve 10 blocks as spare blocks for use in replacing currently-usable blocks when the currently-usable blocks go bad. It can also use any extra spare (good) blocks it finds (e.g., 40 in this example). Utilizing a controller 700 with a spare block management module 770 as described in Figure 7, different aspects of spare block management typically handled by a host may be taken over by the spare block management module 770 of the controller 700.

**[0088]** In one implementation, the spare block management module 770 may be selectively configured to operate in one of three spare block management operation modes: (1) an unmanaged mode wherein the controller 700 provides no management of spare blocks and the host 720 scans blocks for defects on its own; (2) a fully-managed spare block management mode where the controller 700 provides the host 720 with only N good logical blocks, where N is a data sheet parameter and readable in a parameter page available on flash memory; and (3) a split-spare block management mode where the host may use the extra spare blocks but the controller 700 may request a host to release some of these extra blocks for use by the controller 700 when the controller’s spare block supply falls below a desired level.

**[0089]** Although the controller 700 may be initialized by the host 720 while still at a manufacturing facility assembling separate host 720, controller 700, and flash memory device(s) 730, or even pre-initialized for use by a specific original equipment manufacturer (OEM), the spare block management module 770 in the controller 700 may be reconfigurable to change the spare block management mode after a different spare block management mode has been selected.

**[0090]** With reference to the flow chart 1100 of Figure 11, upon initialization of the spare block management module in the controller 700, either upon original initialization at an OEM or upon resetting a previously-selected mode, the controller 700 receives a selection command identifying a desired mode of operation (act 1102). If the selection command indicates that the unmanaged spare block management mode has been chosen (act 1104), the spare block management module 770 permits the host 720 to directly scan the flash memory device(s) 730 to identify useable and bad blocks (act 1106). In the unmanaged mode, the controller 700 is also prevented from managing spare block usage. Instead, when the spare block management module 770 identifies an error indicative of a bad block (such as an uncorrectable ECC failure (field 906) or a program or erase failure (field 908)), the controller 700 can also inform the host 720 that that particular block needs copying and remapping using an appropriate status field, such as field 910 (Figure 9). (Field 908 could also be two fields – one for program fail and another for erase fail, or they could be combined in one field.)

**[0091]** Although spare block management may be entirely left up to the host 720 in the unmanaged spare block management mode, the controller 700 may still scan for a few spare blocks and keep those invisible to the host 720 to use for error recovery. In other words, using the example in Figure 12 of a flash memory having a maximum of a 1,000 blocks, the data sheets could show a minimum guaranteed number of blocks as 900 and a maximum guaranteed number of blocks as 990. If the true number of good blocks in our specific part is 950, the host 720 would only find 940 good blocks if the controller 700 hid 10 blocks for its own use prior to the host 720 scanning for good blocks. The controller 700 may hide good blocks from the host 720 by falsely indicating that the hidden blocks are bad blocks, since the controller 700 knows which blocks it is hiding. For example, if the controller 700 decides to hide block X, then when the host reads

block X, it can return arbitrary data along with a defective block flag. Likewise, on any erase or program requests from the host to block X, the controller can signal an erase or program error.

**[0092]** With respect to the second mode of spare block management (act 1108), in the fully-managed mode, the spare block management module 780 performs all scanning of blocks in the flash memory device(s) 730 to identify good blocks and provides only N good blocks to the host controller, where N is a data sheet parameter readable in the parameter page of flash memory of a guaranteed number of usable blocks (acts 1110, 1112). The controller 700 then only allows host operation on the N good blocks. The controller 700 keeps any extra good blocks as spares that it may use for error handling (act 1114). Referring again to the hypothetical flash memory having 1,000 blocks described in Figure 12 above, N may be 900, where the controller 700 would keep all of the extra 50 useable blocks as spares, and the host 720 has no access to these spares until they are brought into use by the spare block management module 780 in response to a currently-good block going bad.

**[0093]** The third spare block management mode noted above, split management, permits cooperation between the controller 700 and the host 720 as to the use of the extra blocks 1250 (i.e., those above the guaranteed number on the data sheet less any blocks originally reserved as spares). These extra spare blocks can be made available to the host 720 for optimizing host operations. In one embodiment of the split management technique, if the spare block management is initialized with a command for split block management (act 1116), the spare block management module 770 of the controller 700 scans the flash memory device(s) 730 to find good and bad blocks and reserves a few of the good blocks as spare blocks, for example five, for error recovery (act 1118). The controller 700 may discover all the good blocks and only “show” the good blocks to the host.

**[0094]** For example, the controller 700 may read the parameter page of the flash memory device(s) 730 and determine how many remaining good blocks there are in the specific flash memory. The product data sheet for the class of flash memory devices may report the minimum and maximum number of possible good blocks (e.g., 900-990). So, referring again to the example above of a hypothetical flash memory having 1,000

possible blocks where 950 blocks are scanned by the spare block management module 770 and found actually useable, if the controller 700 retains 5 of these good blocks as spare blocks, it would report 945 good blocks to the host 720 (act 1120). Thus, the host 720 would not know that 5 other good blocks exist. The controller 700 may remap the good blocks to a compact logical address range (e.g., addresses of good blocks are sequentially remapped as-is 0-N) with the bad blocks removed (act 1122). If the host 720 attempts a read, program, or erase operation on addresses greater than N, the controller 700 will report an error. Using the data fields 900 of Figure 9 as an example, this error may be reported by the spare block management module 770 appending data in field 914 so that the host 720 believes it is addressing a defective block when it tries to go outside the controller prescribed range.

**[0095]** In an alternative embodiment of the split management mode, the spare block management module 780 may, instead of scanning all the blocks in flash memory device(s) 730, simply scan and reserve only a set of good blocks to keep as spare blocks for its own and allow the host 720 to scan all the blocks to determine which are good and which are defective. In this alternative implementation of the split management mode, when the host 720 attempts to perform a read, program, or erase operation to one of the blocks that the spare block management module 770 had identified as spare blocks, the controller 700 would either indicate a defect in the block or record an error. For example, the controller 700 may insert a defect flag in the appropriate bytes used to mark defective blocks, or it may populate a field in the read status such as the “attempted operation on a defective block” field 914 in Figure 9. The host 720 would then use all other usable blocks, including those beyond the number guaranteed in the parameter page, for its purposes.

**[0096]** Regardless of which version of the split block management technique is employed, the host 720 would typically be able to use any extra spare blocks above the minimum for its own benefit, for example to improve performance or endurance, both of which the host 720 could not rely on more than the minimum number of blocks. So, in this example, the host would have 45 extra blocks it could use (950 total useable, minus 5 reserved, vs. 900 guaranteed minimum on data sheet).



**[0097]** With split management mode, when the controller 700 encounters an error that requires a spare block, such as a program or erase error, the spare block management module 770 uses one of its spares to replace the newly-discovered defective block. In this example, the spare would be one of the five blocks reserved as identified above. After using the spare block, the spare block management module 780 would have less than the minimum number of spare blocks (i.e., 5) that it typically maintains and would notify the host 720 that it needs another spare block (act 1124). The notification provided to the host 720 from the spare block management module 780 of the controller 700 may be via a field in the status value returned with retrieved data. For example, in Figure 9, a flag may be conveyed in field 912 requesting return of an extra block for use as a spare. In this example, the host 720 would need to return one of the 45 extra blocks that it was previously able to use but that exceeded the minimum number it was guaranteed as having access to. The host 720 can indicate to the controller 700 which block is being returned for use as a spare by writing information to a dedicated address or offset with a Set Feature command or by using a vendor-unique command with the block address as its address field.

**[0098]** In the split management mode, the extra blocks above the minimum guaranteed by the data sheet for a class memory would be “split” between extras that the host 720 may use but may be recalled as spares later on and spares that are reserved immediately for the controller 700. This differs from the unmanaged mode where the controller 700 cannot ask for any extra blocks back and has a fixed number of spare blocks that it may use and from the fully-managed mode where all extra blocks are used by the controller 700 and unavailable to the host 720. The flexibility of having full or partial (split) controller-managed mode of spare block management can provide an advantage over typical host management or spare block information by reducing the needed complexity for a host controller.

**[0099]** While specific examples of read status have been described in the examples of Figures 7-9, the status module may be used to determine and communicate write (also referred to as “program”) or erase errors from controller to host as well using the normal error status bit. In addition, the controller could also optionally use a reserved or vendor-unique field in the error status to indicate that extra status is available. Upon receiving

any of these error indicators (read status error, normal write or erase error, or extra status available field), the host could read this extra status information, an example of which is shown in Figure 9. Bits 2, 3, or 4 in the existing status register fields in ONFI 2.0 could be used to signal the extra status. Additionally, although status information and spare block management are shown as part of the same message format, the controller may be configured to only provide one of status information or spare block management information in other embodiments.

**[00100]** An improved independent controller for use with a flash memory has been described that may handle error analysis and error correction, manage communications relating to spare blocks for error recovery in one of several modes in cooperation with a host, and provides status information regarding read commands or write and erase errors in a message field accessing by the host. The method and controller disclosed herein permit for activity by a controller separate from a host that may allow a host controller to have a more simplified design and permit for customized architecture of a discrete controller that may be used with a host in a flash memory while providing a host with information related to the activities of the controller such that various levels of controller and host cooperation and optimization may be achieved.

**[00101]      Exemplary NAND Flash Memory Controller Embodiment**

**[00102]** This section discusses an exemplary controller architecture and provides more details on some of the various functional modules discussed above. As noted above, a “module” can be implemented in any suitable manner, such as with hardware, software/firmware, or a combination thereof, and the functionality of a “module” can be performed by a single component or distributed among several components in the controller.

**[00103]** Returning now to the drawings, Figure 13A is a diagram of a presently preferred implementation of the NAND controller 300 of Figure 3. It should be understood that any of the components shown in these drawings can be implemented as hardware, software/firmware, or a combination thereof. In this implementation, the first NAND Interface 325 in Figure 3 is implemented by the Host Interface Module (“HIM”) 3010. The HIM 3010 is a collection of logic that supports the “host side interface” as a “flash device-type interface.” The HIM 3010 comprises a first-in-first-out (“FIFO”)

module 3080, a control unit 3090, a cyclic redundancy check (“CRC”) module 3100 (although another type of error detection code (“EDC”) module can be used), a command register 3110, an address register 3120, and a host direct memory access (“HDMA”) unit 3130. In this embodiment, the HIM 3010 takes the form of an ONFI HIM. As will be discussed in more detail below, some HIMs receive a high-level request from a host controller for a relatively-large amount of data that spans several pages, and the NAND controller determines what actions are needed to satisfy the request. In contrast, an ONFI HIM receives several smaller-sized requests (e.g., for individual pages) from a host controller, so the ONFI HIM is required to simultaneously handle multiple (e.g., eight) read and write requests.

**[00104]** Returning to Figure 13A, the second NAND Interface 335 of Figure 3 is implemented here by a Flash Interface Module (“FIM”) 3020. In a current embodiment, the FIM 3020 is implemented as a collection of logic and a low-level programmable sequencer that creates the “device side interface” as a “host-type interface.” In this embodiment, the FIM 3020 comprises a command register 3140, an address register 3150, an ECC encode module 3160, an ECC decode module 3170, a data scrambler 3180, and a data descrambler 3190.

**[00105]** Internal to the NAND controller 300 is a processor 3040, which has local ROM, code RAM, and data RAM. A central bus 3030 connects the processor 3040, the HIM 3010, the FIM 3020, and the other modules described below and is used to transfer data between the different modules shown. This bi-directional bus 3030 may be either an electrical bus with actual connections to each internal component or an Advanced High-Speed Bus (“AHB”) used in conjunction with an ARC microprocessor, which logically connects the various modules using an interconnect matrix. The central bus 3030 can transmit data, control signals, or both. The NAND controller 300 also comprises a buffer RAM (“BRAM”) 3050 that is used to temporarily store pages of data that are either being read or written, and an ECC correction engine 3060 for correcting errors. The NAND controller 300 further comprises an encryption module 3070 for performing encryption/decryption functions.

**[00106]** The NAND controller 300 can further comprise a column replacement module, which is implemented here by either the FIM sequencer, firmware in the

processor 3040, or preferably in a small amount of logic and a table located in the FIM 3020. The column replacement module allows the flash memory device(s) 330 (Figure 3) to contain information on bad column locations. The bad column address information is contained in the flash memory device(s) 330 and is scanned by firmware prior to any read or write operation. After firmware scans the flash memory device(s) 330, it builds a bad column address table with the bad column location to be used by the column replacement module. On flash write operations, the column replacement module inserts the data (0xFFFF) for the address that is detected in a bad column address table. On flash read operations, data from the bad column address will be discarded.

**[00107]** With the components of the NAND controller 300 now generally described, exemplary write and read operations of the NAND controller 300 will now be presented. Turning first to a write operation, the FIFO 3080 in the HIM 3010 acts as a buffer for an incoming write command, address, and data from a host controller and synchronizes those elements to the system card domain. The CRC module 3100 checks the incoming information to determine if any transmission errors are present. (The CRC module 3100 is an example of the EDC module discussed above.) The CRC module generates or checks an error detection code to check for transmission errors as part of an end-to-end data protection scheme. If no errors are detected, the control unit 3090 decodes the command received from the FIFO 3080 and stores it in the command register 3110, and also stores the address in the address register 3120. The data received from the host controller is sent through the HDMA AHB interface 3130 to the BRAM 3050 via the central bus 3030. The control unit 3090 sends an interrupt to the processor 3040, in response to which the processor 3040 reads the command from the command register 3080 and the address register 3120 and, based on the command, sets up the data path in the FIM 3020 and stores the command in the FIM's command register 3140. The processor 3040 also translates the address from the NAND interface 325 into an internal NAND address and stores it in the FIM's address register 3150. If logical-to-physical address conversion is to be performed, the processor 3040 can use a mapping table to create the correct physical address. The processor 3040 can also perform one or more additional functions described below. The processor 3040 then sets up a data transfer from the BRAM 3050 to the FIM 3020.

**[00108]** The FIM 3020 takes the value from the address register 3150 and formats it in accordance with the standard of the NAND interface 335. The data stored in the BRAM 3050 is sent to the encryption module 3070 for encryption and is then sent through the data scrambler 3180. The data scrambler 3180 scrambles the data and outputs the data to the FIM's ECC encoder 3160, which generates the ECC parity bits to be stored with the data. The data and ECC bits are then transferred over the second NAND interface with the write command to the flash memory device(s) for storage. As an example of an additional function that may occur during writes, if protection for write aborts or program failures is enabled and if the write request is to an upper page address, the processor 3040 can send a read command to the flash memory device(s) over the second NAND interface for the corresponding lower page and then send a program command to have it copied into a safe zone (a spare scratchpad area) by writing it back to another location in the flash memory device(s) 330. If an error occurs in writing the upper page, the lower page can still be read back from the safe zone and the error corrected. (This is an example of the module discussed above for handling write aborts and/or program failures via safe zones.)

**[00109]** Turning now to a read operation, the HIM 3010 receives a read command from a host controller, and the processor 3040 reads the command and logical address. If logical-to-physical address conversion is to be performed, the firmware in the processor 3040 could use a mapping table to create the correct physical address. (This is an example of the address mapping module discussed above.) The firmware then sends the physical address over the second NAND interface 335 to the flash memory device(s) 330. After the read access, the data is transferred over the NAND interface, decoded and used to generate the syndrome data for error correction, descrambled by the data descrambler 3190, and then sent over the central bus 3030 to the BRAM 3050. The ECC correction engine 3060 is used to correct any errors that can be corrected using the ECC on the data that is stored in the BRAM 3050. Since the ECC may be computed and stored in portions of a physical page, the processor 3040 can be interrupted as each portion of the page is received or corrected, or once when all of the data is transferred. The encryption module 3070 then performs a decryption operation on the data. The timing described above is flexible since the first NAND interface 325 and the second

NAND interface 335 may operate at different speeds, and the firmware can transfer the data using either store-and-forward techniques or speed-match buffering. When the data is sent back to the host controller, it is sent through the HIM 3010, and the transmission CRC is sent back to the host over the first NAND interface 325 to check for transmission error.

**[00110]** As mentioned above, in addition to handling commands sent from the host controller, the processor 3040 may perform one or more additional functions asynchronously or independent of any specific command sent by the host. For example, if the ECC correction engine 3060 detects a correctable soft error, the ECC correction engine 3060 can correct the soft error and also interrupt the processor 3040 to log the page location so that the corresponding block could be read scrubbed at a later point in time. Other exemplary background tasks that can be performed by the processor 3040 are wear leveling and mapping of bad blocks and spare blocks, as described below.

**[00111]** Turning again to the drawings, Figure 13B is a block diagram showing a more detailed view of a NAND controller of an embodiment. As with the controller shown in Figure 13A, the controller in this embodiment contains an ONFI HIM 3200 and a FIM 3260 that communicate through a central bus (here, an Advanced Microcontroller Bus Architecture (“AMBA”) High-performance Bus (“AHB”) multi-layer matrix bus 3270 for the data path and an advanced peripheral bus (“APB”) 3330 for the command path). The ONFI HIM 3200 and the FIM 3260 can be associated with any of the processors. For example, the ONFI HIM 3200 can be associated with an ARC600 microprocessor 3280 (with a built-in cache 3285) that runs ARC code stored in a MRAM 3290. In general, the ARC600 3280 is used to service interrupts from the ONFI HIM 3200 and manages the data path setup and transfers information to the flash control RISC 3250. The flash control RISC 3250 is the microprocessor that can be used with the FIM 3260 and, in general, handles the function of setting up the FIM 3260 by generating micro-control codes to various components in the FIM 3260. More particularly, the flash control RISC 3250 sets up the flash direct memory access (“FDMA”) module 3440 in the FIM 3260, which communicates with the AHB bus 3270 and generates the AHB bus protocol commands to read data from the DRAM 3220. The flash control RISC 3250

also sets up the EDC module 3450, which contains the ECC encoder and decoder. The MRAM 3240 stores code used to run the flash control RISC 3250.

**[00112]** The NAND controller in this embodiment also contains a ROM 3210 that stores instruction code to get the controller running upon boot-up. Additional components of the NAND controller include a DRAM 3220, an ECC correction engine 3230, an encrypt module 3300, an APB bridge 3310, an interrupt controller 3320, and a clock/reset management module 3340.

**[00113]** The encryption module 3300 enciphers and decipheres 128 bit blocks of data using either a 128, 192, or 256 bit key according to the Advanced Encryption Standard (AES). For write operations, after data is received from the host and sent to the BRAM 3050 (Figure 13A) by the ONFI HIM, the ARC600 processor 3280 creates a control block with defined parameters of the encipher operations. The encryption module 3300 then performs the encipher operations and stores the resulting data to BRAM 3050 and interrupts the ARC600 processor 3280 to indicate that the data is ready. For read operations, after the ECC engine completes error correction in the BRAM 3050, the ARC600 processor 3280 creates a control block with defined parameters of the decipher operations. The encryption module 3300 then performs the decipher operations and stores the resulting data to the BRAM 3050 and interrupts the ARC600 processor 3280 to indicate data is ready.

**[00114]** Turning now to the ONFI HIM 3220 and the FIM 3260 in more detail, the ONFI HIM 3220 comprises an ONFI interface 3350 that operates either in an asynchronous mode or a source synchronous mode, which is part of the ONFI standard. (Asynchronous (or “async”) mode is when data is latched with the WE# signal for writes and the RE# signal for reads. Source synchronous (or “source (src) sync”) is when the strobe (DQS) is forwarded with the data to indicate when the data should be latched.) The ONFI HIM 3200 also contains a command FIFO 3360, a data FIFO 3370, a data controller 3380, a register configuration module 3400, a host direct memory access (“HDMA”) module 3380, and a CRC module 3415, which function as described above in conjunction with Figure 13A. The ONFI HIM 3200 further contains an APB interface 3390 and an AHB port 3420 for communicating with the APB bus 3330 and the AHB bus 3270, respectively. The FIM 3260 comprises an EDC module 3450 that includes an EDC

encoder and an EDC decoder, a flash protocol sequencer (“FPS”) 3430, which generates commands to the NAND bus based on micro-control codes provided by the flash control RISC 3250 or the ARC600 microprocessor 3280, an FDMA 3440, a data scrambler/de-scrambler 3470 and a NAND interface 3460.

**[00115]** The scrambler/descrambler 3470 performs a transformation of data during both flash write transfers (scrambling) and flash read transfers (de-scrambling). The data stored in the flash memory device(s) 330 may be scrambled in order to reduce data pattern-dependent sensitivities, disturbance effects, or errors by creating more randomized data patterns. By scrambling the data in a shifting pattern across pages in the memory device(s) 330, the reliability of the memory can be improved significantly. The scrambler/descrambler 3470 processes data on-the-fly and is configured by either the ARC600 processor 3280 or the Flash Control RISC 3250 using register accesses. ECC check bit generation is performed after scrambling. ECC error detection is performed prior to de-scrambling, but correction is performed after descrambling.

**[00116]** The NAND controller in this embodiment processes write and read operations generally as described above with respect to Figure 13A. For example, for a write operation, the command FIFO 3360 and the data FIFO 3370 store an incoming write command and data, and the CRC module 3415 checks the incoming information to determine if any transmission errors are present. If no errors are detected, the data controller 3380 decodes the command received from the command FIFO 3360 and stores it in a command register in the register configuration module 3400. The address received from the host controller is stored in the address register in the register configuration module 3400. The data received from the host controller is sent through the HDMA 3410 to the DRAM 3220. The data controller 3380 then sends an interrupt to the ARC600 3280 or the Flash Control RISC 3250, which reads the command from the command register, reads the address from the address register, and passes control to the flash control RISC 3250 to set up the FIM 3260 to start reading the data from DRAM 322 and perform ECC and data scrambling operations, the result of which is sent to the flash memory device(s) 330 for storage. The ARC600 microprocessor 3280 and/or the FIM 3260 can perform additional operations. For example, the FIM 3260 can perform column replacement, and the following operations can be performed using the ARC600



microprocessor 3280 together with the FIM 360: bad block and spare block management, safe zones, read scrubbing, and wear leveling. These operations are described in more detail below.

**[00117]** For a read operation, the ONFI HIM 3200 sends an interrupt to the ARC600 microprocessor 3280 when a read command is received. The ARC600 microprocessor 3280 then passes the command and address information to the flash control RISC 3250, which sets up the FPS 3430 to generate a read command to the NAND flash memory device(s) 330. Once the data is ready to be read from the NAND flash memory device(s) 330, the FPS 3430 starts sending read commands to the NAND bus. The read data goes through the NAND interface unit 3460 to the data descrambler 3470 and then through the EDC module 3450, which generates the syndrome bits for ECC correction. The data and syndrome bits are then passed through the FDMA 3440 and stored in the DRAM 3220. The flash control RISC 3250 then sets up the ECC correction engine 3230 to correct any errors. The encrypt module 3300 can decrypt the data at this time. The ARC600 microprocessor 3280 then receives an interrupt and programs the register configuration module 3400 in the ONFI HIM 3200 to state that the data is ready to be read from the DRAM 3220. Based on this information, the ONFI HIM 3200 reads the data from the DRAM 3220 and stores it in the data FIFO 3370. The ONFI HIM 3200 then sends a ready signal to the host controller to signal that the data is ready to be read.

**[00118]** As mentioned above, unlike other HIMs, an ONFI HIM receives several smaller-sized requests (e.g., for individual pages) from a host controller, so the ONFI HIM is required to simultaneously handle multiple (e.g., eight) read and write requests. In this way, there is more bi-directional communication between the ONFI HIM and the host controller than with other HIMs. Along with this increased frequency in communication comes more parallel processing to handle the multiple read and write requests.

**[00119]** Figures 13C and 13D illustrate the logical operations of an ONFI HIM for read and write operations, respectively. Turning first to Figure 13C, the ONFI HIM 3480 of this embodiment receives a read command from a host controller through an ONFI bus 3490. The ONFI HIM 3480 can operate in an asynch or a source synch mode and

communicates the read command to a command FIFO 3540 via signal multiplexors 3500, 3530. (The ONFI HIM 3480 can be used in an async mode and source sync mode using the Async and ONFI source sync components 3510, 3520, respectively.) The ONFI HIM 3480 also stores the address received from the host controller in a logical unit number ("LUN") address FIFO 3550. (The NAND controller in this embodiment supports multiple logical units, which are treated as independent entities that are addressable by LUN addresses.) The command and address are read from the FIFOs 3540, 3550 into a command and data controller 3560, which synchronizes these items. The command and data controller 3560 then sends an interrupt to the system register controller 3570, which generates an interrupt to the ARC600 microcontroller. The ARC600 microcontroller then reads the LUN address from the register in the system register controller 3570, and the process of reading data from the flash memory device(s) is as described above. When all the read data is written to the DRAM, the ARC600 microprocessor programs the status register in the system register controller 3570 to inform the ONFI HIM 3480 that the data is ready to be read. The ONFI HIM 3480 then reads the data through the HDMA 3580 using the read request control unit 3585. The read data is stored in the read data FIFO 3590, which is partitioned for each LUN 3595. Once that is done, a ready indicator is stored in the status register, and the data is streamed to the host controller.

**[00120]** Turning now to Figure 13D, in a write operation, a write command is received from a host controller through an ONFI 3410 bus. The ONFI HIM 3400 communicates the write command to a command FIFO 3460 via signal multiplexors 3420, 3450. (The ONFI HIM 3400 can be used in an async mode and source sync mode using the Async and ONFI source sync components 3430, 3440, respectively.) The ONFI HIM 3400 also stores the address received from the host controller in a logical unit number ("LUN") address FIFO 3470. The data received from the host controller is stored in a write data FIFO 3520. The command and address are read from the FIFOs 3460, 3470 into a command and data controller 3480, which synchronizes these items. The command and data controller 3480 then sends an interrupt to the system register controller 3490, which generates an interrupt to the ARC600 microcontroller. The ARC600 microcontroller then reads the LUN address from the register in the system register controller 3490, and the process of setting-up the controller from a write

operation is as described above. The HDMA 3530 has an AHB port 3540 in communication with the AHB bus 3550 and sends the data to the DRAM. The CRC module 3545 checks for transmission errors in the data. Once the data has been stored in the flash memory device(s) 330 and the flash memory device(s) 330 indicate ready and the status of program operation is successful or fail, a ready indicator is stored in the status register in the system register controller 3490, indicating that the ONFI HIM 3400 is ready for another command from the host controller.

**[00121]** Returning to Figure 13A, the NAND controller 300 can also handle program failures and erase failures. As the NAND flash memory device(s) 330 attached to the flash interface module 3020 (hereafter FIM) are programmed, the NAND memory device(s) 330 report the success or failure of the program operation to the NAND controller 300 (or optionally to the ONFI Host through the host interface module 3010 (hereafter HIM)). The NAND memory device(s) 330 may experience some number of program failures over the expected life of the memory due to defects in the NAND cells or due to the limited endurance the NAND cells have with regard to erase and program cycles.

**[00122]** The NAND memory device(s) 330 will return a FAIL status to the controller 300 when the program page operation does not complete successfully. The controller processor 3040 (Figure 13A) or flash protocol sequencer 3430 (Figure 13B) verifies the success or failure of each program page operation. Generally, the failure of any single program page operation will cause the processor 3040 (or optionally the ONFI Host) to regard the entire NAND block (which may contain multiple pages) to be defective. The defective block will be retired from use. Typically, the controller 300 will copy the data that was not successfully programmed and any data in preceding pages in the defective block to another replacement block (a spare block). The controller 300 may read preceding pages into the BRAM 3050 using the FIM 3020, the data de-scrambler 3190, and the ECC decoder 3170 and applying ECC correction as needed. The data is then written to the replacement block using the FIM 3020 in the normal fashion.

**[00123]** One aspect of program failures is that a failure programming one page may corrupt data in another page that was previously programmed. Typically, this would be possible with MLC NAND memory which is organized physically with upper and

lower logical pages sharing a word-line within the memory array. A typical usage would be to program data into a lower page and subsequent data into the upper page. One method to prevent the loss of data in the lower page when a program failure occurs when programming the upper page on the word-line is to read the lower page data prior to programming the upper page. The lower page data could be read into the controller BRAM 3050 and could additionally be programmed into a scratch pad area in the non-volatile flash memory device(s) 330, sometimes called a “safe zone.” The data thus retained in the BRAM 3050 or safe zone would then be protected from loss due to a programming failure and would be available to be copied to the replacement block, particularly in cases where the data was corrupted in the lower page of the NAND memory device(s) 330 and could no longer be read successfully.

**[00124]** It is possible that some NAND failure modes could similarly corrupt data in other areas of the memory array, such as on adjacent word lines. This method of reading other potentially vulnerable data into the controller BRAM 3050, and/or saving the data into a scratch pad or safe zone area could also be used to protect data in these circumstances.

**[00125]** As the NAND flash memory device(s) 330 attached to the FIM 3020 are erased, the NAND memory device(s) 330 report the success or failure of the block erase operation to the NAND controller 300 (or optionally to the ONFI Host through the HIM 3010). The NAND memory device(s) 330 will return a FAIL status to the controller 300 when the erase operation does not successfully complete. The controller processor 3040 or circuits in the flash protocol sequencer 3430 verifies the success or failure of each erase operation. Generally, the failure of any erase operation will cause the processor 3040 (or ONFI Host) to regard the entire NAND block to be defective. The defective block will be retired from use and a spare block used in its place.

**[00126]** The NAND controller 300 can also handle program disturbs, erase disturbs, and read disturbs within the flash memory device.

**[00127]** The internal NAND programming operations could possibly effect, or disturb, other areas of the memory array, causing errors when attempting to read those other areas. One method to prevent failures from program disturb is to perform reads or “read scrubbing” operations on potentially vulnerable areas in conjunction with

programming operations, in order to detect disturb effects before they become uncorrectable or unrecoverable errors. Once a disturb condition is detected (by high soft error rates during the read scrubbing operation), the controller processor 3040 (or the external ONFI host) can copy the data to another area in the flash memory device(s) 330.

**[00128]** The internal NAND erase operations could possibly effect, or disturb other areas of the memory array, causing errors when attempting to read those other areas. One method to prevent failures from erase disturb is to perform reads or “read scrubbing” operations on potentially vulnerable areas in conjunction with erase operations, in order to detect disturb effects before they become uncorrectable or unrecoverable errors. Once a disturb condition is detected, the controller processor 3040 (or the external ONFI host) can copy the data to another area in the flash memory device(s) 330.

**[00129]** The internal NAND read operations could possibly effect, or disturb other areas of the memory array, causing errors when attempting to read those other areas. The disturb effects can sometimes accumulate over many read operations. One method to prevent failures from program disturb is to perform reads or “read scrubbing” operations on potentially vulnerable areas in conjunction with read operations, in order to detect disturb effects before they become uncorrectable or unrecoverable errors. Once a disturb condition is detected, the controller processor 3040 (or the external ONFI host) can copy the data to another area in the flash memory device(s) 330.

**[00130]** Referring now to Figure 13A, the NAND controller 300 handles read errors in the following manner. Typically, the data that is programmed into the NAND memory device(s) 330 through the FIM 3020 has an error detection or error correction code appended and stored with the data in the NAND array. The controller 300 uses the ECC encoder 3160 for this function. When such data is read from the flash array to the BRAM 3050, the ECC decoder 3170 re-generates the ECC code from the data and compares it to the ECC code that was appended to the data when programmed into the flash. If the data is identical to the data that was written, the ECC circuits indicate that there is no data error present. If some difference in the read data is detected, and the difference is small enough to be within the capability of the ECC to correct, the read data (typically contained in the BRAM 3050) is “corrected” or modified to restore it to the original value by the ECC correction engine 3060, as controlled by the processor 3040.

If the data errors exceed the ECC correction capability, an “uncorrectable” read error occurs. Typically, an uncorrectable read error would result in an error status being returned to the Host interface when read.

**[00131]** One method to prevent uncorrectable read errors, or to recover when an error is detected, is for the controller 300 (or the external ONFI host) to retry the read operation. The retry may use shifted margin levels or other mechanisms to decrease the errors within the data, perhaps eliminating the errors or reducing the number of errors to a level that is within the ECC correction capability.

**[00132]** Optionally, when a read error is recovered, or if the amount of ECC correction needed to recover the data meets or exceeds some threshold, the data could be re-written to the same or to another block in order to restore the data to an error-free or improved condition. The original data location may optionally be considered as defective, in which case it could be marked as defective and retired from use.

**[00133]** Referring again to Figure 13A, the NAND controller 300 can also handle write aborts. Write aborts are the unexpected loss of power to the controller 300 and NAND memory device(s) 330 while a program or erase operation is in progress. The loss of power can result in incomplete programming or erase conditions in the NAND memory device(s) 330 that could result in uncorrectable read errors. In some cases, such as with MLC NAND, other pages that share a word line (i.e., a lower page) could be corrupted by an aborted program operation on the upper page of a word line, much like the program failure condition described above.

**[00134]** There are several methods to reduce or eliminate write abort errors, or minimize their impact. One method is to use a low voltage detection circuit to notify the processor 3040 that the power has been interrupted. The processor 3040 can then allow current program or erase operations to finish but not allow new operations to start. Ideally, the current operations would have enough time with sufficient power to complete.

**[00135]** An alternative method, perhaps used in conjunction with the low voltage detection method, is to add capacitance or a battery (or some alternative power supply source) to the power supply circuits to extend the power available to complete program or erase operations.

[00136] Another method is to provide a scratch pad “safe zone” similar to that described above. Any “old” data that exists in lower pages that may be vulnerable during an upper page program could be read and saved in the safe zone before the upper page program is started. That would provide protection for previously-programmed data in case of a power loss event. In some implementations, it may be acceptable to not be able to read data that was corrupted in a write abort situation, but other possibly un-related older data must be protected.

[00137] Another method is to search for potential write abort errors when the controller is powered on. If an error is found that can be determined (or assumed) to be a result of a write abort, the error data may be discarded. In this situation, the controller 300 effectively reverts back to previous data, and the interrupted operation is as if it did not happen.

[00138] Referring again to Figure 13A, the NAND controller 300 can also conduct wear leveling on the memory. Wear leveling is a method to increase overall product endurance and lifetime by more evenly distributing block usage amongst all physical blocks than would otherwise occur as a result of normal flash management algorithms. This is done by forcing “cold” blocks to the spare blocks pool, which will in turn be used for host data updates, and, at the same time, moving the data from “cold” blocks, which are not updated by the host, to a “hot” block. This swap will result in mixing up “hot” and “cold” blocks. The swap can be done either randomly or cyclically, choosing blocks for the swap, or choosing them on the basis of a hot count (number of program-erase cycles) analysis. The swap can be done periodically, say in every 100 block cycles, typically calibrated by a system parameter to balance between overall system performance and evening of block usage to balance wear and performance overhead.

[00139] An example high level sequence is:

1. Schedule wear leveling operation
2. Identify “hot” and “cold” blocks by either hot count analysis or on random or cyclic basis.
3. Copy data from the selected “cold” block to the selected “hot” free block in the free block pool.

4. Release the “cold” block to the free block pool. As a result, the free block pool is populated by a cold block instead of hot one.

**[00140]** Some operations can be skipped, like analysis-based blocks selection. The wear level operation itself can also be skipped if block wear distribution is detected as even.

**[00141]** The wear level operations and hot count management are performed in firmware by the processor 3040, such that the host controller 121 (Figure 3) will not be aware of these housekeeping flash block level operations

**[00142]** Referring to Figure 13A, the controller 300 can also implement read scrubbing on the flash memory device(s) 330 upon detection of a read disturb. Read operations to one area of the NAND memory array within the flash memory device(s) 330 may affect or disturb other areas of the memory array, causing cells to shift from one state to another, and ultimately causing bit errors when attempting to read data previously stored to those other areas. The disturb effects can accumulate over many read operations, eventually leading to a number of bit errors that may exceed the data correction capabilities of the system. The errors that exceed the system correction capabilities are referred to as uncorrectable errors. One method to prevent failures from program disturbs is to perform reads or “scrubbing” operations on potentially vulnerable areas, in order to detect disturb effects before they become uncorrectable or unrecoverable errors. Once a disturb condition is detected, typically by detecting that there are a number of bits in error on the data read, the processor 3040 can move the data to another area in the memory generally by copying the data to another area of the NAND memory array in order to “refresh” it.

**[00143]** Read scrub copy is usually triggered by correctable ECC error discovered by the ECC correction engine 3060 (Figure 13A), either in blocks read during the course of a host read operation, an internal system read operation, or by a scheduled read scrub scan. System read operations are those needed by the flash storage system to read firmware, parameters, or mapping information stored in the NAND flash. Read scrub scan is a read of all data in a block to determine whether any data contained therein has been disturbed. Blocks are selected for a read scrub scan typically when they have been partially read during the course of a host read or system read operation, but may also be



selected using other criteria, such as randomly, or via deterministic sequencing through the blocks of memory. Because a read scrub scan operation takes time and affects data throughput of the system, the system may select blocks for read scrub scan only periodically or infrequently, by use of a random selection, a counter, or other mechanisms. The frequency of scheduling may be calibrated to balance between the system performance needs, and the frequency require to detect disturbed data before it becomes uncorrectable. Upon detection of a correctable error that has some number of bits in error above a pre-defined threshold, the read scrub copy is scheduled for the block.

**[00144]** Read scrub copy is a method by which data is read from the disturbed block and written to another block, after correction of all data which has correctable ECC error. The original block can then be returned to the common free block pool and eventually erased and written with other data. Read scrub scan and read scrub copy scheduling will be done in the NAND controller 300 in firmware by the processor 3040, such that the host controller 121 will not be aware of these housekeeping flash block level operations.

**[00145]** **Conclusion**

**[00146]** It is intended that the foregoing detailed description be understood as an illustration of selected forms that the invention can take and not as a definition of the invention. It is only the following claims, including all equivalents that are intended to define the scope of this invention. Also, some of the following claims may state that a component is operative to perform a certain function or configured for a certain task. It should be noted that these are not restrictive limitations. It should also be noted that the acts recited in the claims can be performed in any order — not necessarily in the order in which they are recited.

What is claimed is:

1. A method for writing data in a flash memory device using a controller interfacing between a host and the flash memory device, the method comprising:

performing in a controller in communication with a host and a flash memory device:

receiving a write command, data, and an error detection code associated with the data from the host through a first NAND interface of the controller using a NAND interface protocol, wherein the error detection code allows at least one error in the data to be detected but not corrected;

generating an error detection code based on the data and comparing the generated error detection code with the error detection code received from the host;

if the generated error detection code does not match the error detection code received from the host, sending a signal to the host through the first NAND interface indicating that an error occurred in transmission of the data from the host to the controller; and

if the generated error detection code matches the error detection code received from the host:

generating an error correction code based on the data, wherein the error correction code allows at least one error in the data to be both detected and corrected; and

storing the data and the error correction code in the flash memory device through a second NAND interface of the controller using a NAND interface protocol.

2. The method of Claim 1, wherein the error detection code received from the host is part of a header of a data packet that contains the data.
3. The method of Claim 2, wherein the error detection code covers the header and the data.
4. The method of Claim 1, wherein the error detection code is selected from the group consisting of: a one or more byte checksum, a longitudinal redundancy check (LRC), and a cyclic redundancy check (CRC).
5. The method of Claim 1, wherein the NAND interface protocol used by the first NAND interface is the same as the NAND interface protocol used by the second NAND interface.
6. The method of Claim 1, wherein the NAND interface protocol used by the first NAND interface is different from the NAND interface protocol used by the second NAND interface.

7. The method of Claim 1, wherein the controller and the flash memory device both reside within a common multi-chip package.
8. The method of Claim 7, wherein the controller presents a single electrical load on the first NAND interface and flash memory device internal to the multi-chip package.
9. The method of Claim 1, wherein the controller and the flash memory device are packaged in different packages.
10. The method of Claim 1, wherein the controller and the flash memory device are integrated on a same die.
11. A method for reading data from a flash memory device using a controller interfacing between a host and the flash memory device, the method comprising:
  - performing in a controller in communication with a host and a flash memory device:
    - receiving a read command from the host through a first NAND interface of the controller using a NAND interface protocol;
    - reading data and an error correction code associated with the data from the flash memory device through a second NAND interface of the controller using a NAND interface protocol, wherein the error correction code allows at least one error in the data to be both detected and corrected;

generating an error correction code based on the data and comparing the generated error correction code with the error correction code received from the flash memory device;

if the generated error correction code does not match the error correction code received from the flash memory device, attempting to correct an error in the data; and

if the generated error correction code matches the error correction code received from the flash memory device:

generating an error detection code based on the data, wherein the error detection code allows at least one error in the data to be detected but not corrected; and

sending the data and the error detection code to the host through the first NAND interface.

12. The method of Claim 11, wherein the error detection code is part of a header of a data packet that contains the data.

13. The method of Claim 12, wherein the error detection code covers the header and the data.

14. The method of Claim 11, wherein the error detection code is selected from the group consisting of: a one or more byte checksum, a longitudinal redundancy check (LRC), and a cyclic redundancy check (CRC).

15. The method of Claim 11, wherein the NAND interface protocol used by the first NAND interface is the same as the NAND interface protocol used by the second NAND interface.

16. The method of Claim 11, wherein the NAND interface protocol used by the first NAND interface is different from the NAND interface protocol used by the second NAND interface.

17. The method of Claim 11, wherein the controller and the flash memory device both reside within a common multi-chip package.

18. The method of Claim 17, wherein the controller presents a single electrical load on the first NAND interface and flash memory device internal to the multi-chip package.

19. The method of Claim 11, wherein the controller and the flash memory device are packaged in different packages.

20. The method of Claim 11, wherein the controller and the flash memory device are integrated on a same die.

21. A controller for interfacing between a host and a flash memory device, the controller comprising:

a first NAND interface configured to transfer data between the controller and a host using a NAND interface protocol;

a second NAND interface configured to transfer data between the controller and a flash memory device using a NAND interface protocol;

an error detection code module operative to generate an error detection code, wherein the error detection code allows at least one error to be detected but not corrected;

an error correction code module operative to generate an error correction code, wherein the error correction code allows at least one error to be both detected and corrected; and

a control module operative to perform the following in response to receiving a write command, data, and an error detection code associated with the data from the host through the first NAND interface:

compare an error detection code generated by the error detection code module based on the data with the error detection code received from the host;

if the generated error detection code does not match the error detection code received from the host, send a signal to the host through the first NAND interface indicating that an error occurred in transmission of the data from the host to the controller; and

if the generated error detection code matches the error detection code received from the host, store the data and an error correction code generated by the error correction code module based on the data in the flash memory device through the second NAND interface.

22. The controller of Claim 21, wherein the control module is further operative to perform the following in response to receiving a read command from the host through the first NAND interface:

read data and an error correction code associated with the data from the flash memory device through the second NAND interface;

compare an error correction code generated by the error correction code module based on the read data with the error correction code received from the flash memory device;

if the generated error correction code does not match the error correction code received from the flash memory device, attempt to correct an error in the data; and

if the generated error correction code matches the error correction code received from the flash memory device, send the data and an error detection code generated by the error detection code module based on the data to the host through the first NAND interface.

23. The controller of Claim 21, wherein the error detection code received from the host is part of a header of a data packet that contains the data.

24. The controller of Claim 23, wherein the error detection code covers the header and the data.



25. The controller of Claim 21, wherein the error detection code is selected from the group consisting of: a one or more byte checksum, a longitudinal redundancy check (LRC), and a cyclic redundancy check (CRC).
26. The controller of Claim 21, wherein the NAND interface protocol used by the first NAND interface is the same as the NAND interface protocol used by the second NAND interface.
27. The controller of Claim 21, wherein the NAND interface protocol used by the first NAND interface is different from the NAND interface protocol used by the second NAND interface.
28. The controller of Claim 21, wherein the controller and the flash memory device both reside within a common multi-chip package.
29. The controller of Claim 28, wherein the controller presents a single electrical load on the first NAND interface and flash memory device internal to the multi-chip package.
30. The controller of Claim 21, wherein the controller and the flash memory device are packaged in different packages.
31. The controller of Claim 21, wherein the controller and the flash memory device are integrated on a same die.

32. The controller of Claim 21, wherein the control module comprises an ECC correction engine.

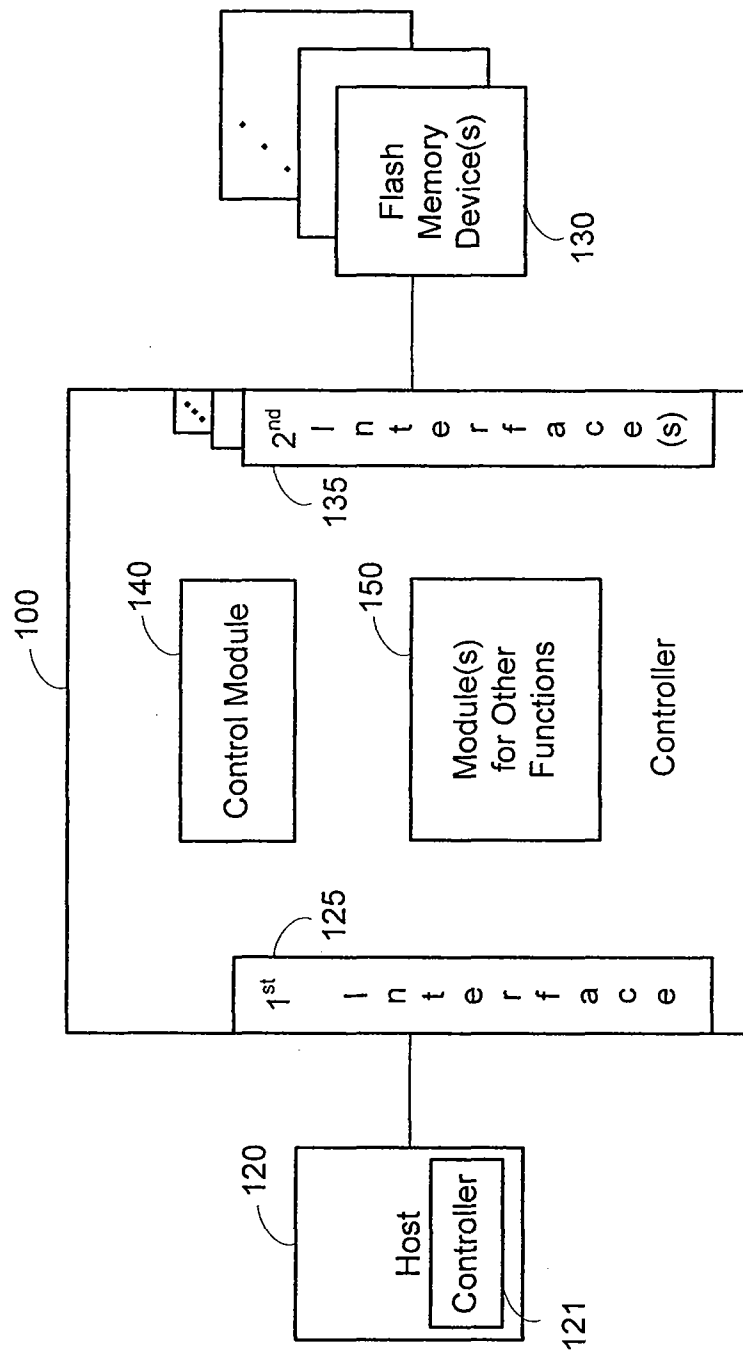


FIG. 1

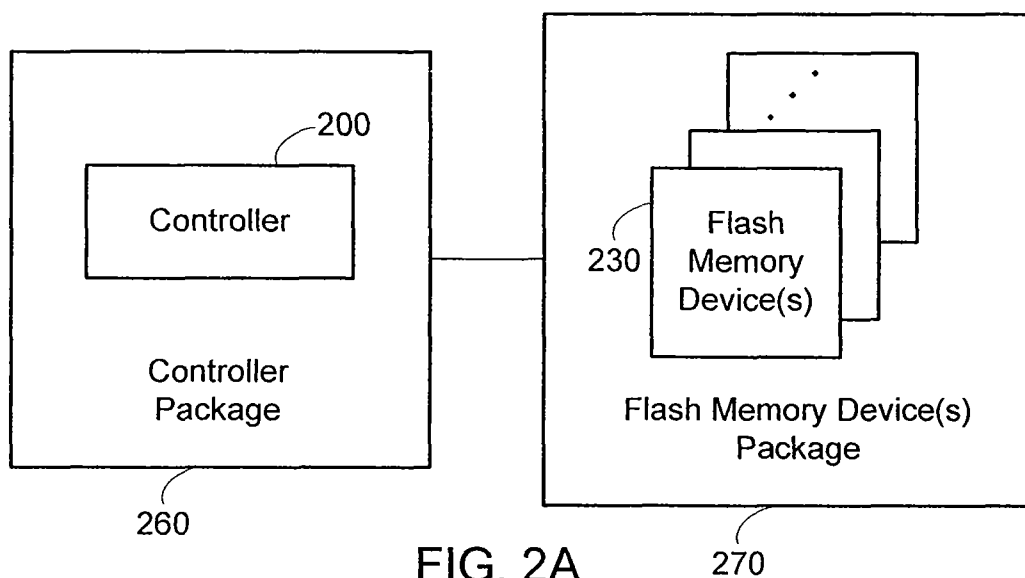


FIG. 2A

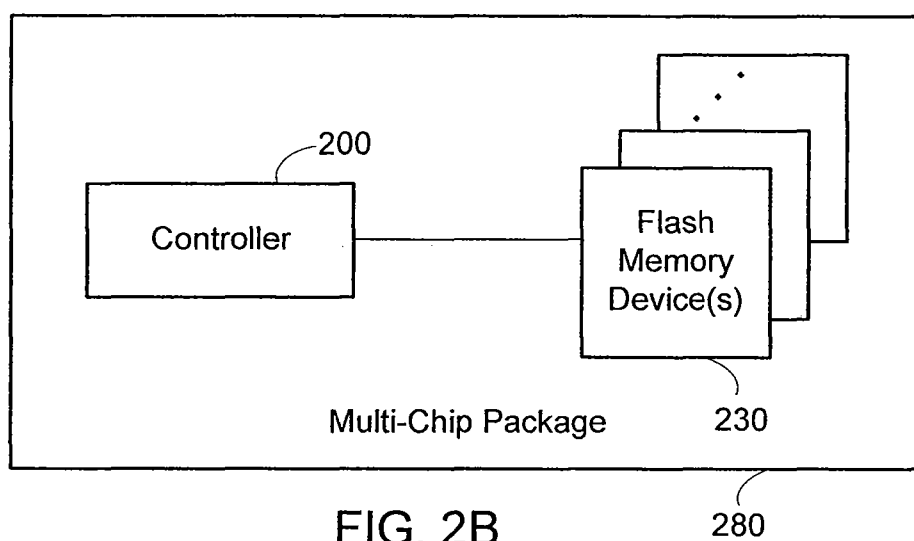


FIG. 2B

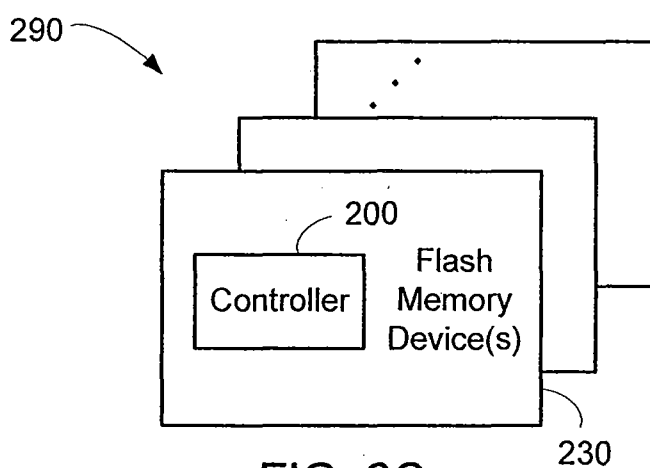


FIG. 2C

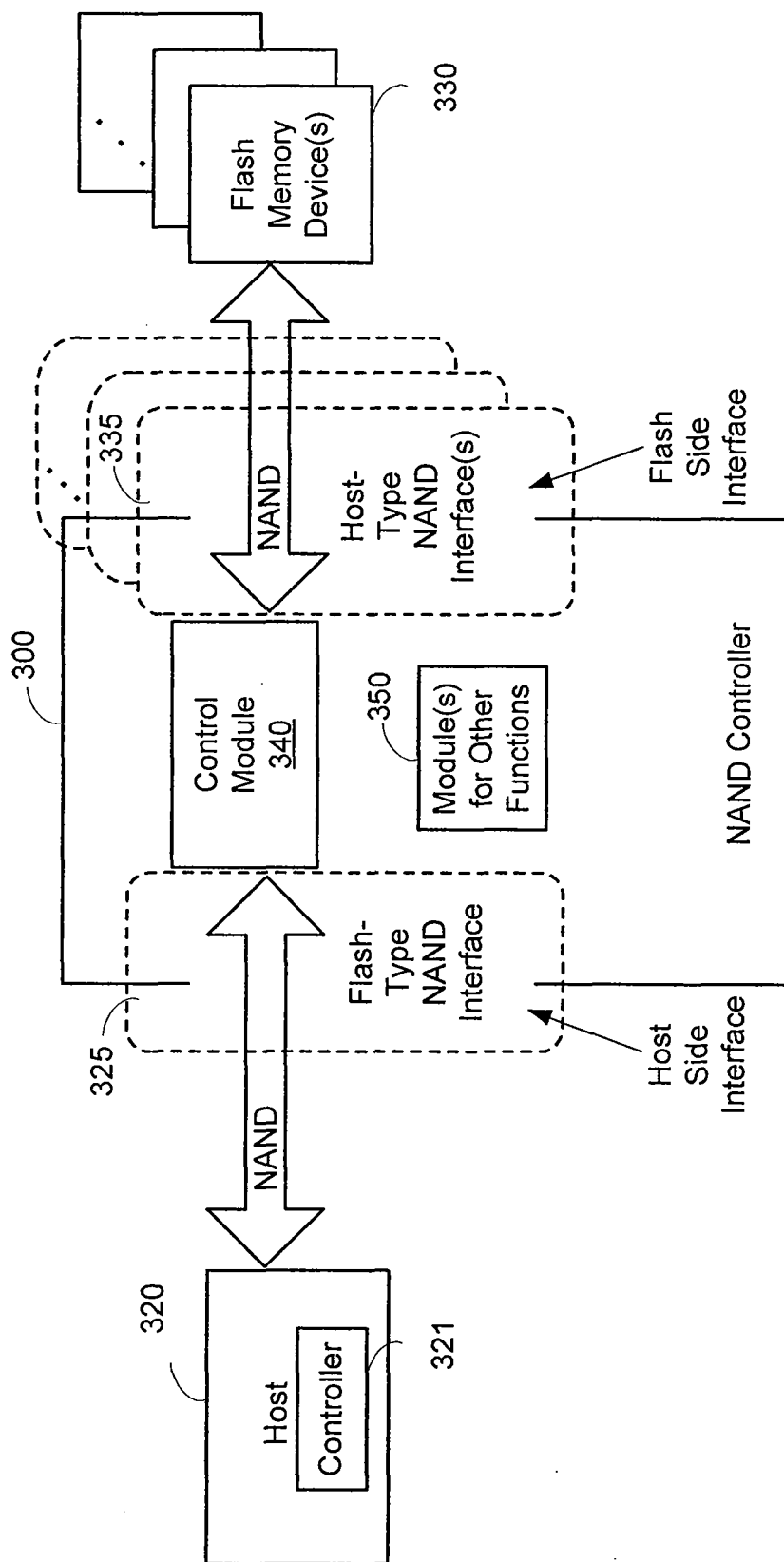


FIG. 3

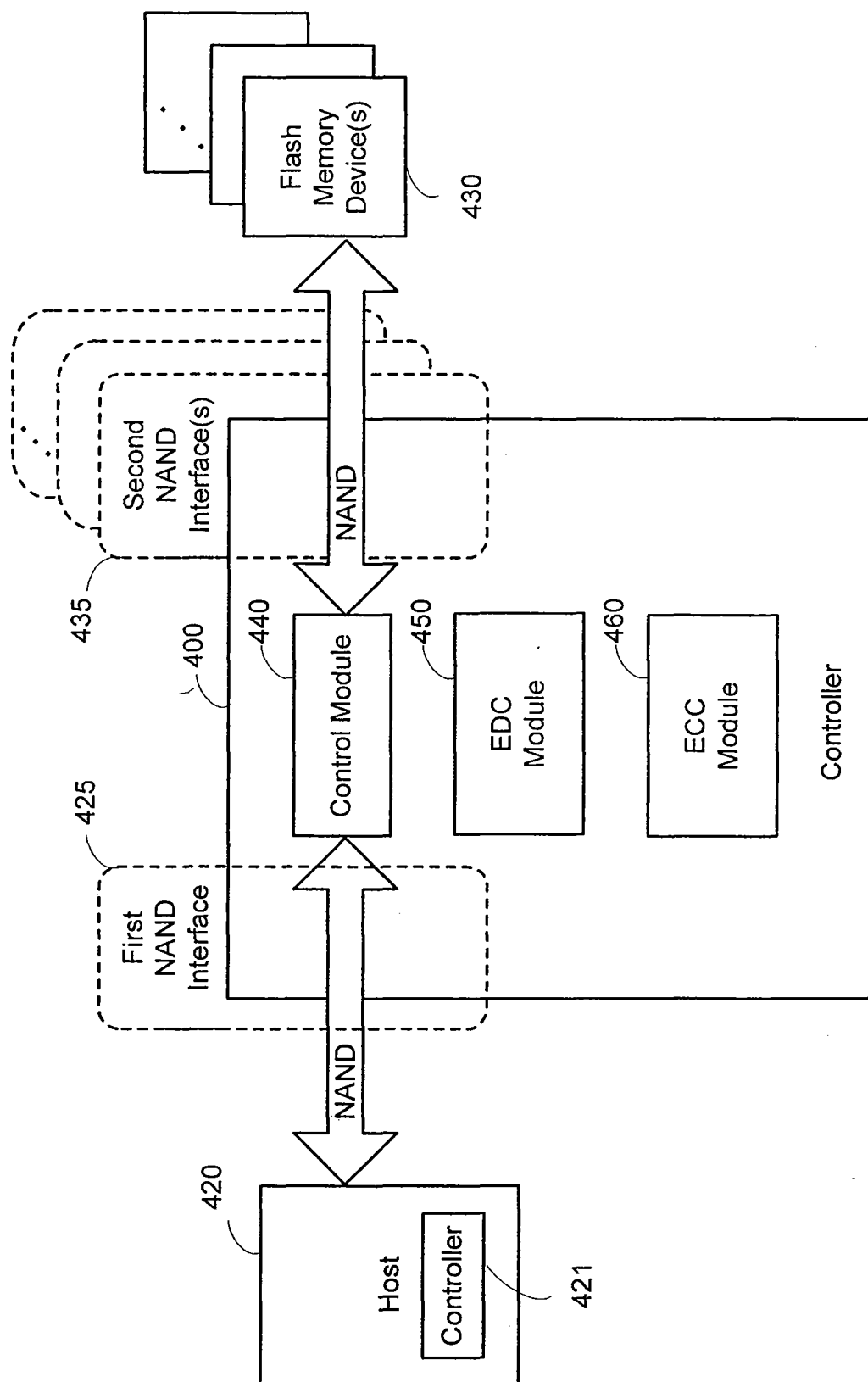


FIG. 4

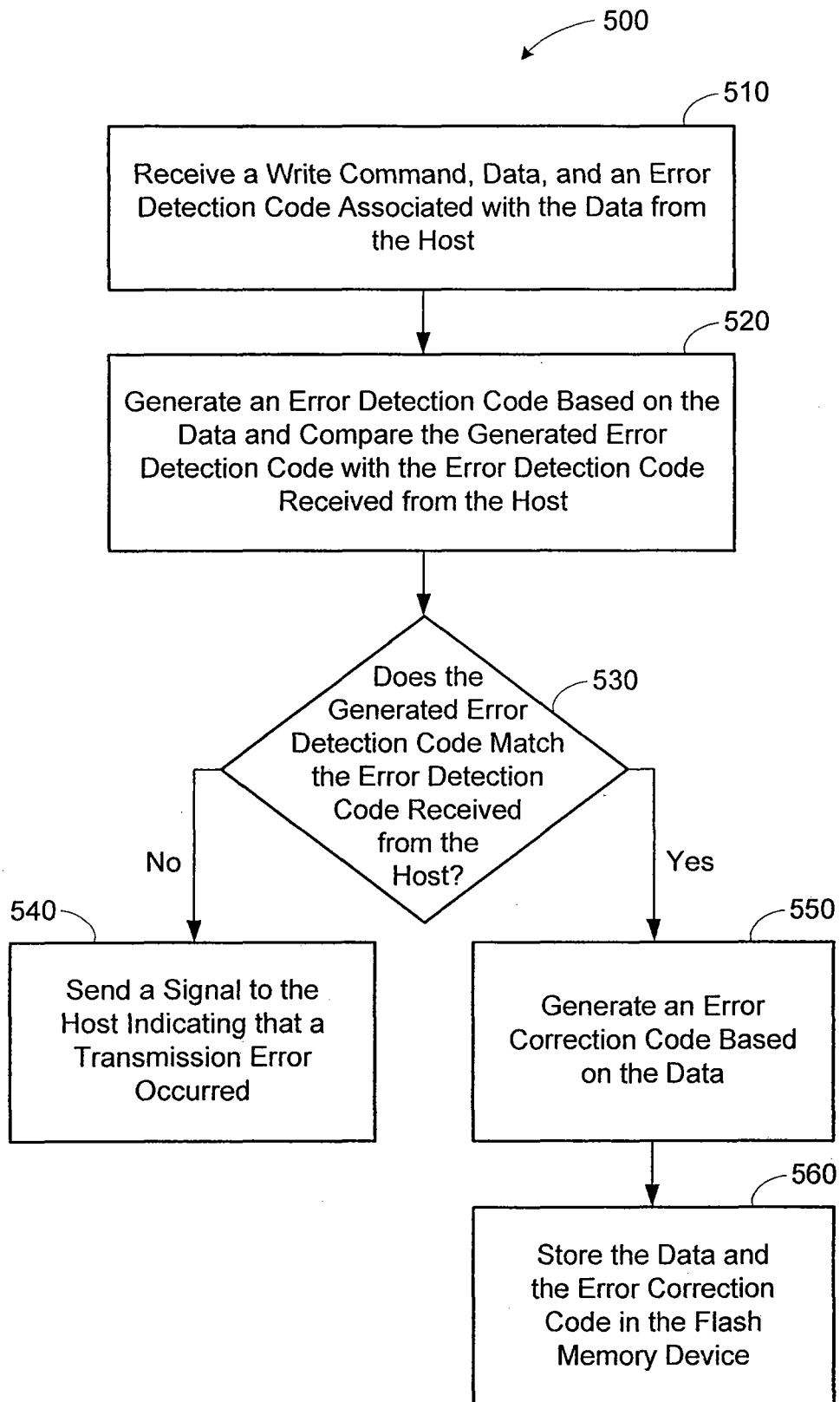


FIG. 5

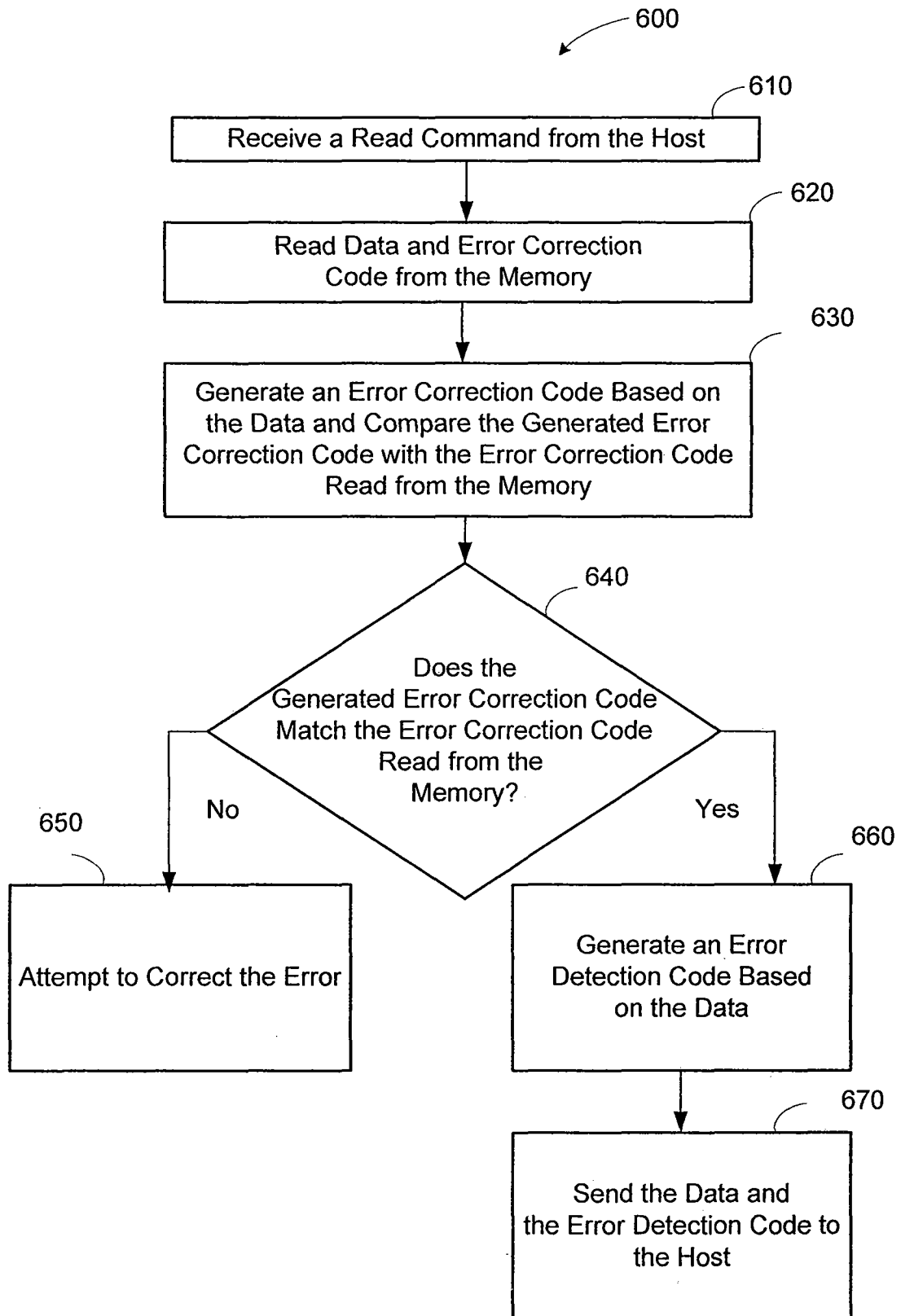


FIG. 6



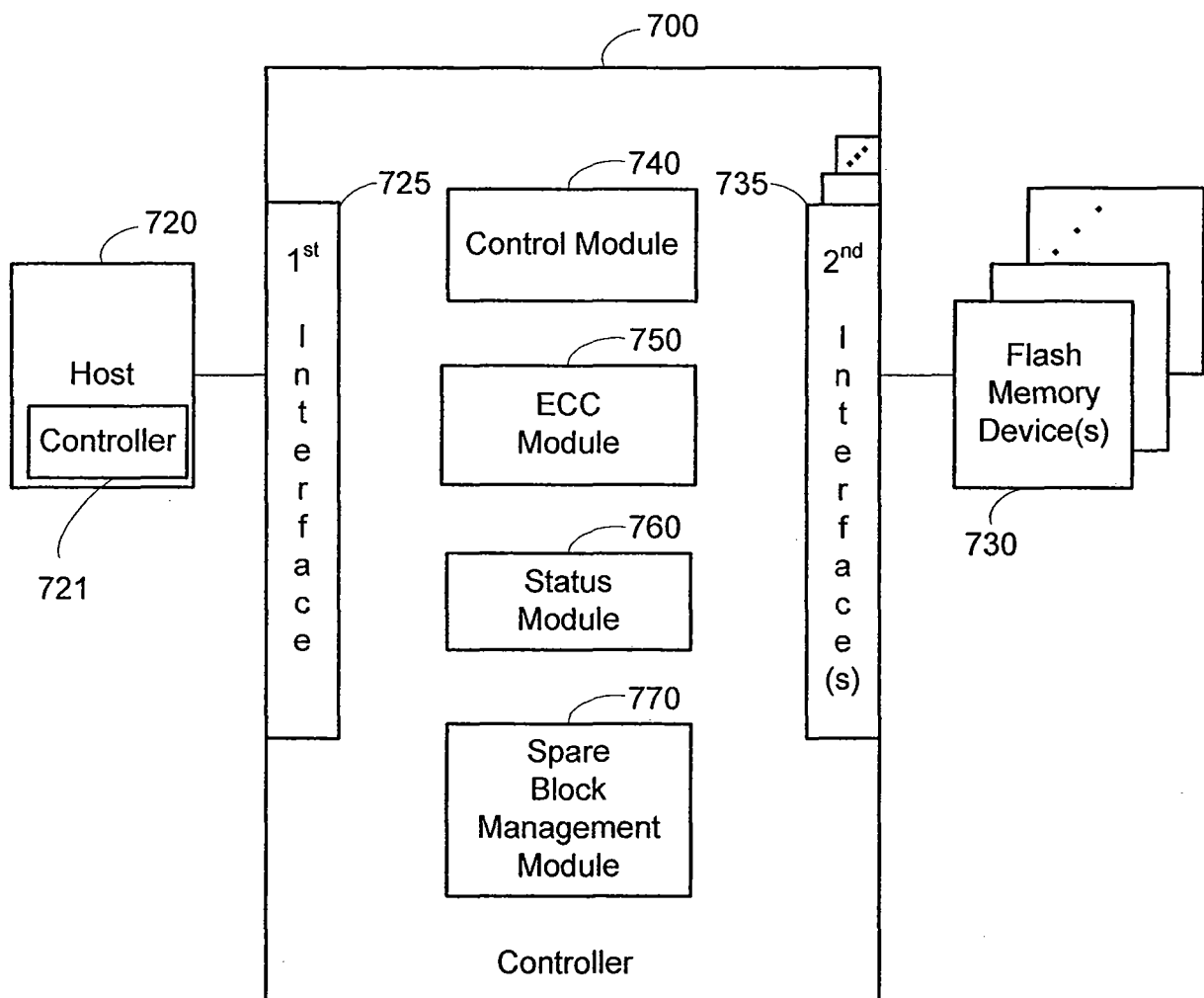


FIG. 7

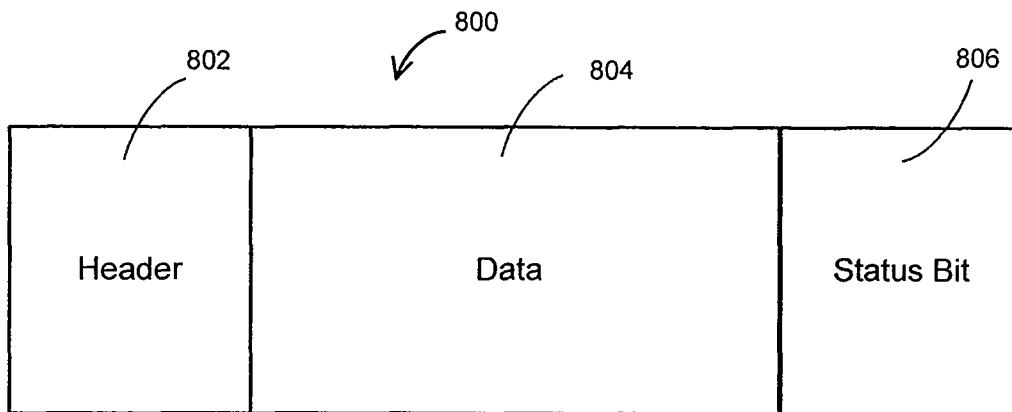


FIG. 8A

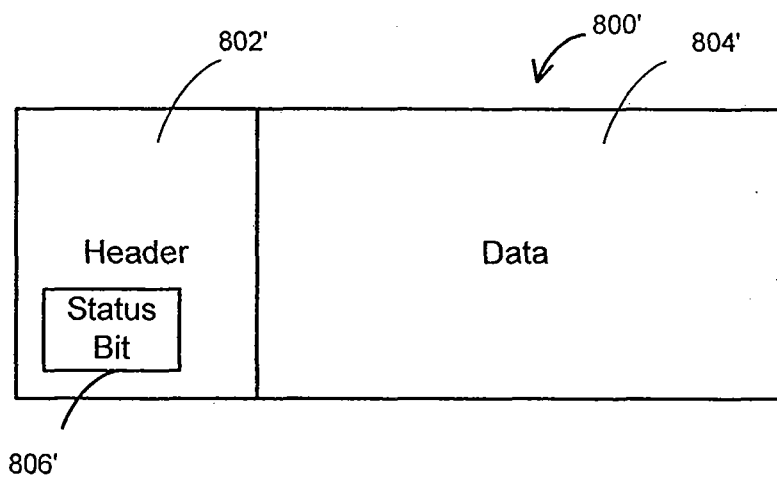


FIG. 8B

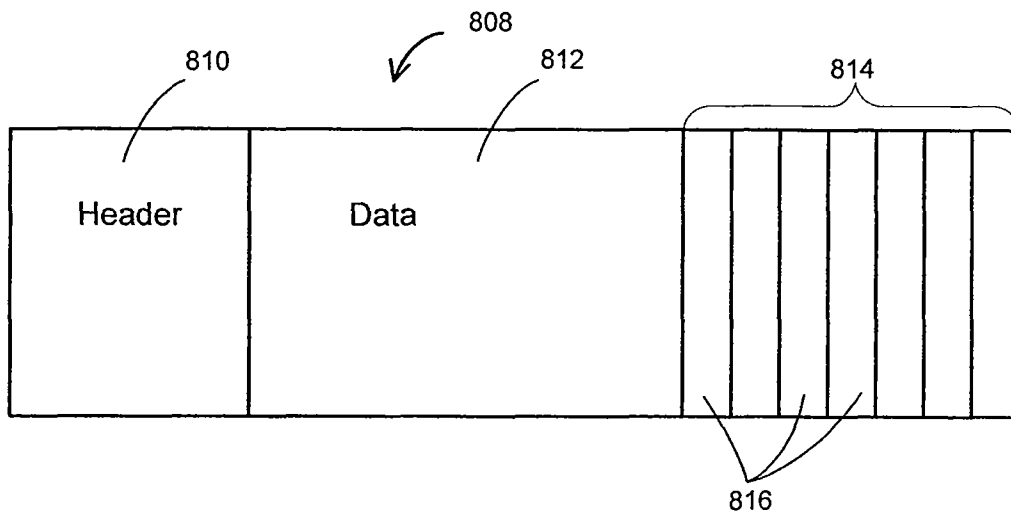


FIG. 8C

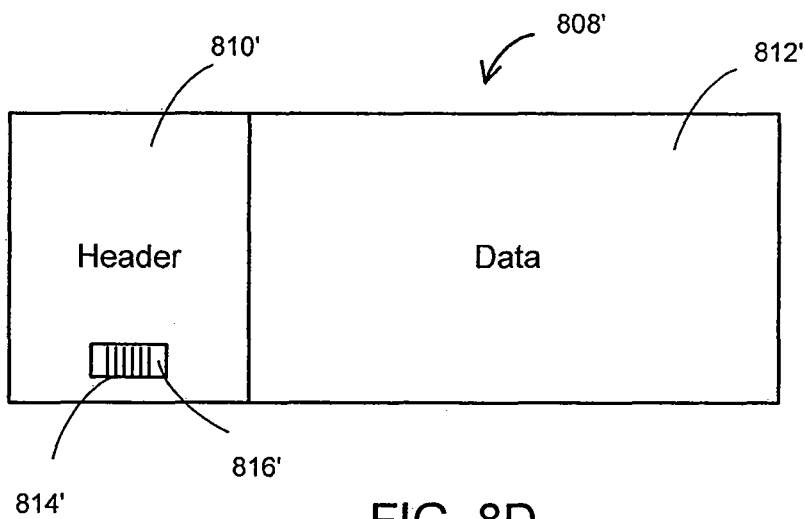
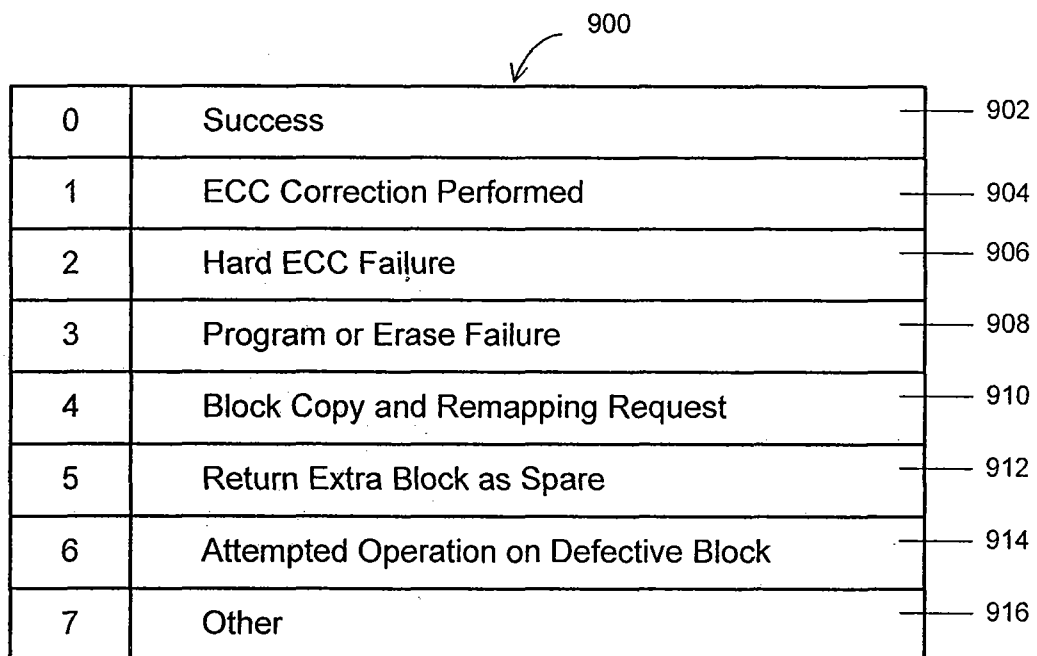


FIG. 8D



900

0	Success	902
1	ECC Correction Performed	904
2	Hard ECC Failure	906
3	Program or Erase Failure	908
4	Block Copy and Remapping Request	910
5	Return Extra Block as Spare	912
6	Attempted Operation on Defective Block	914
7	Other	916

FIG. 9

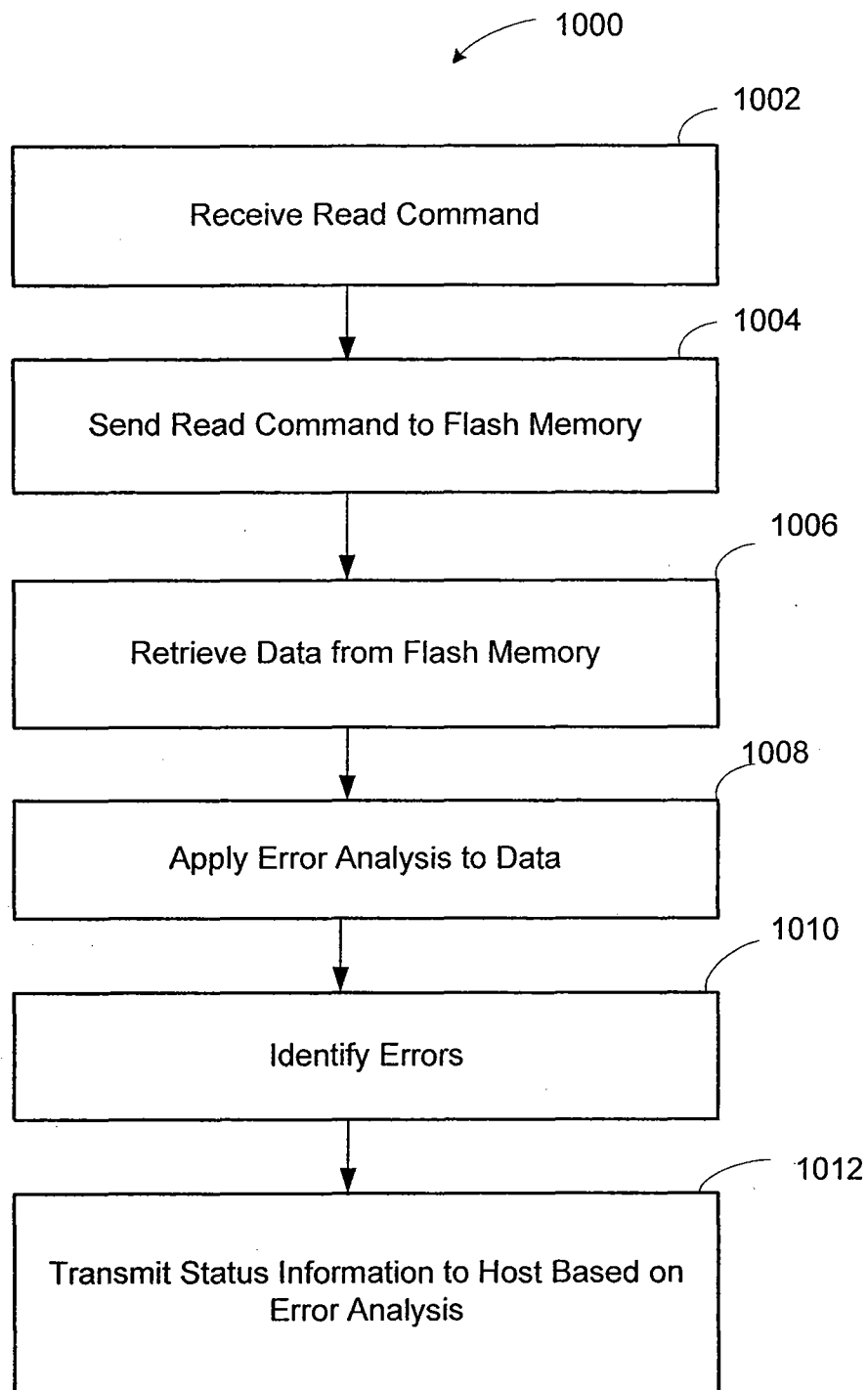


FIG. 10

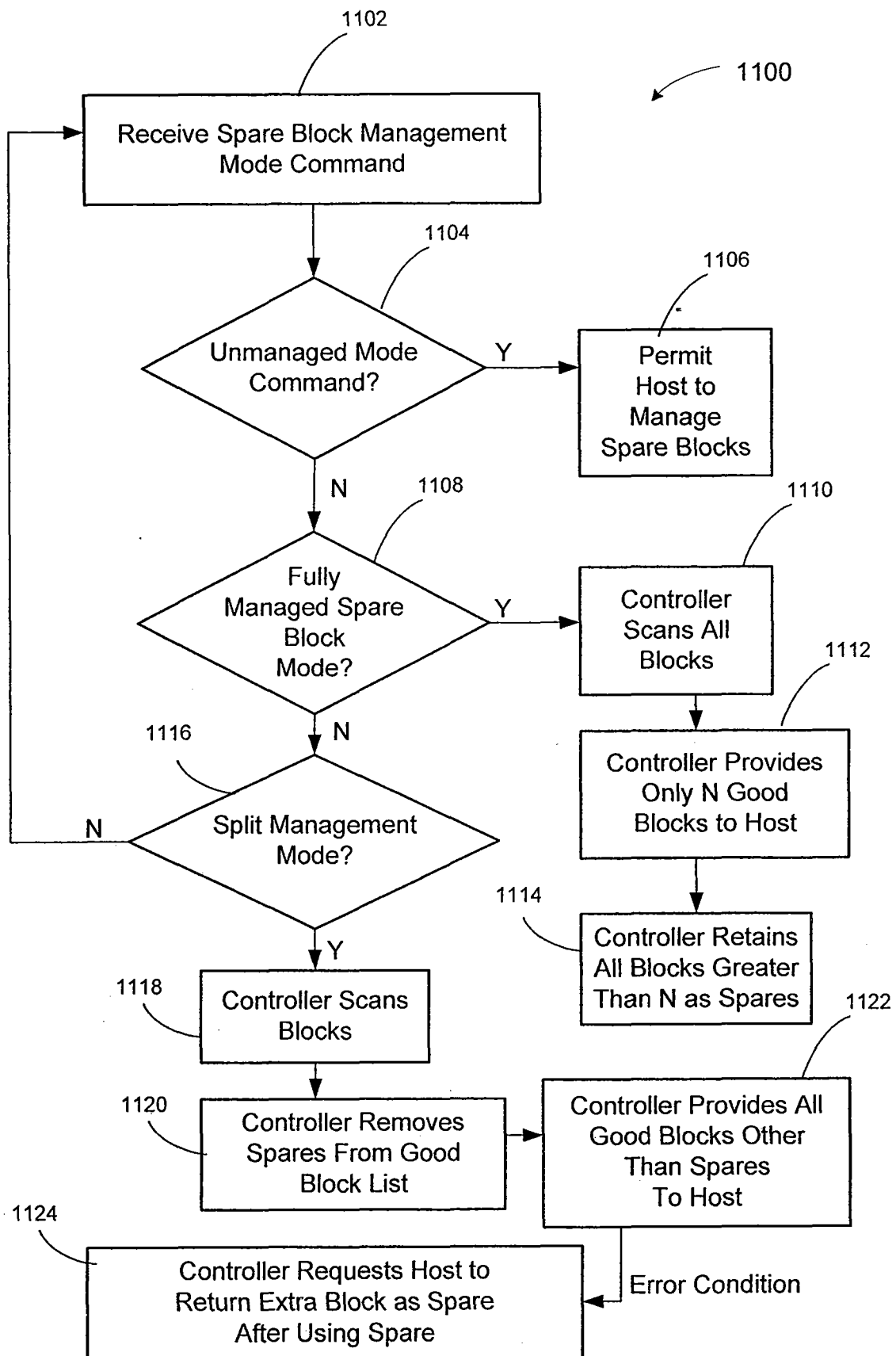


FIG. 11

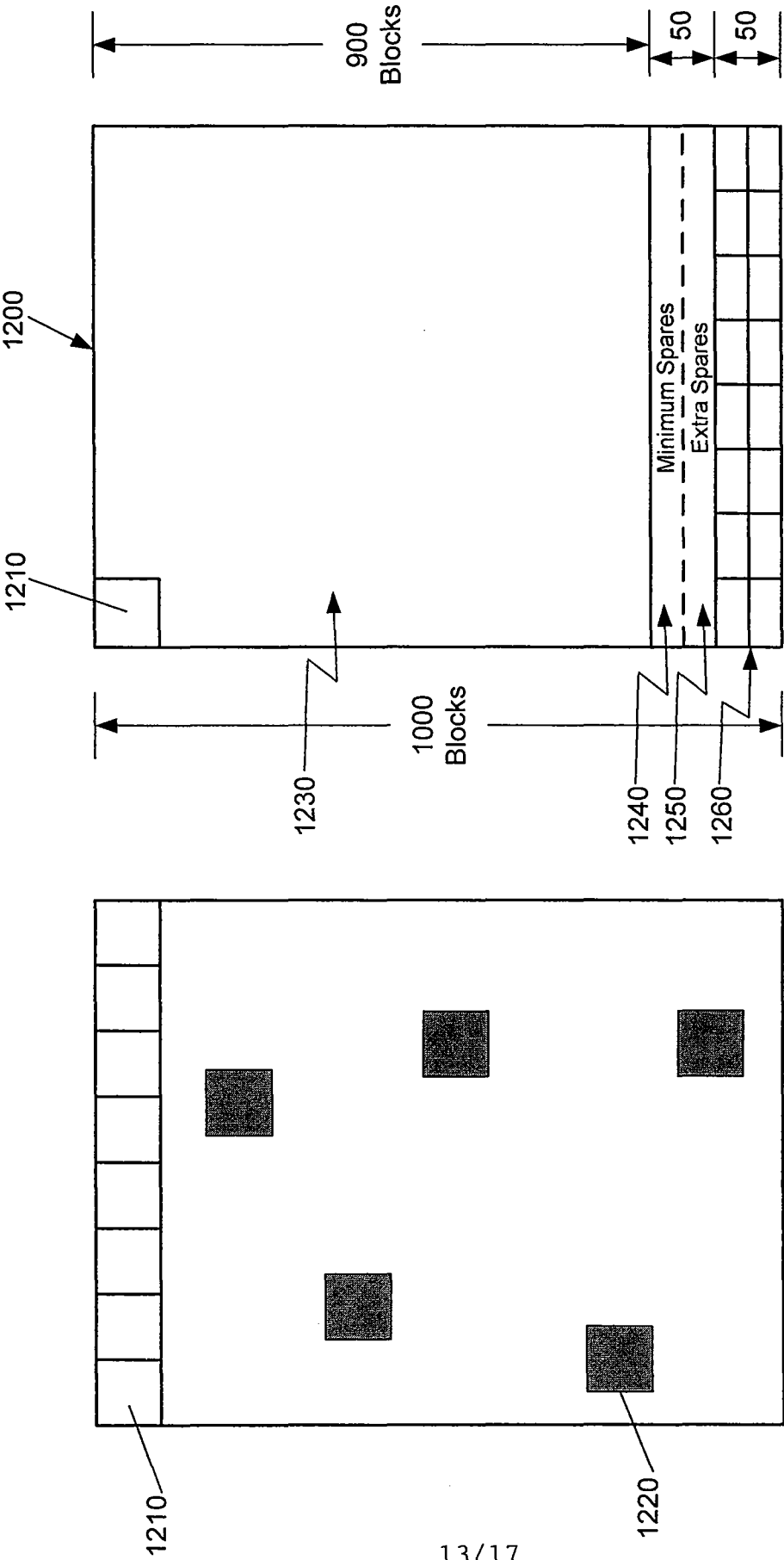


Figure 12B

Figure 12A

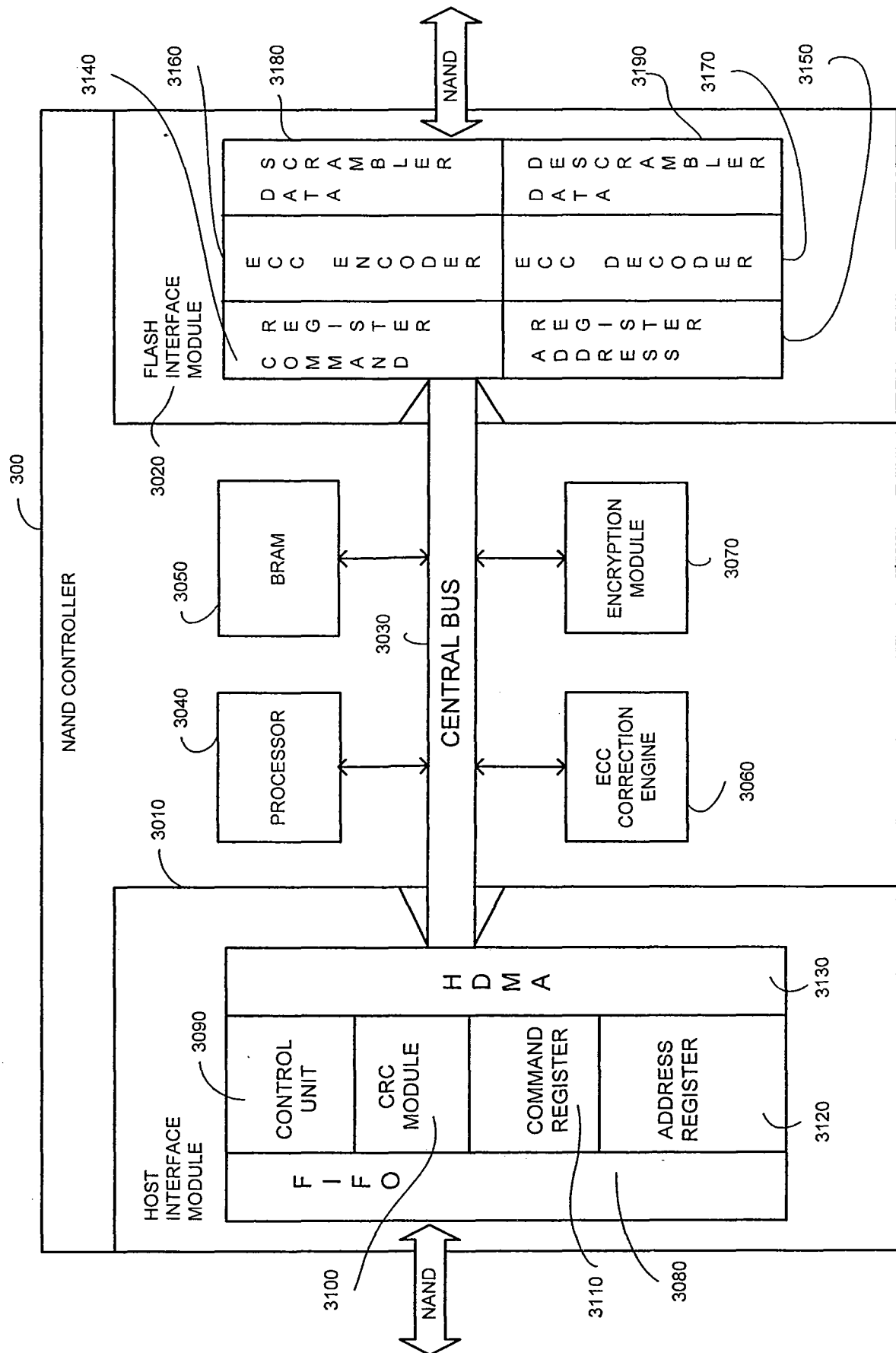


FIG. 13A



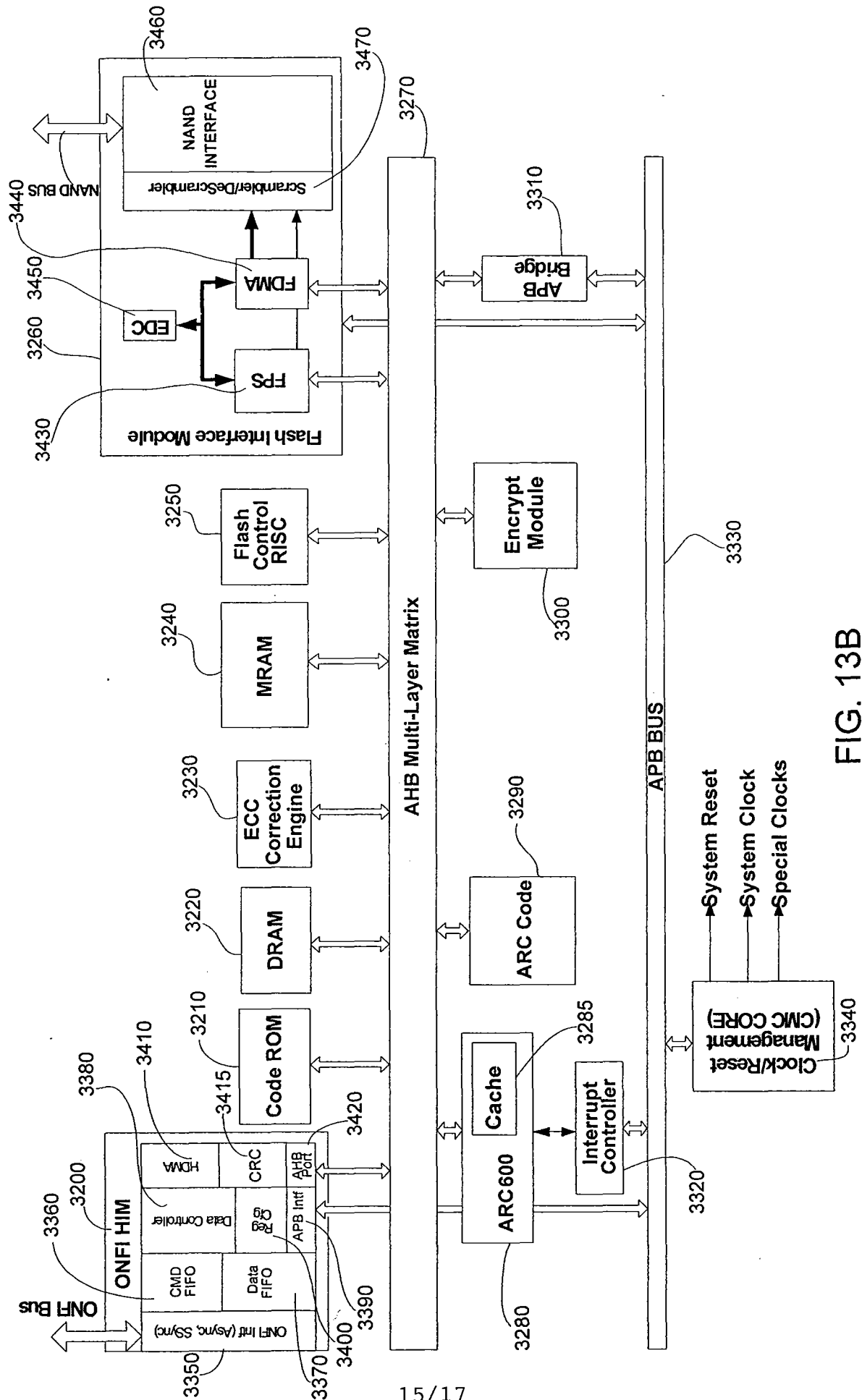
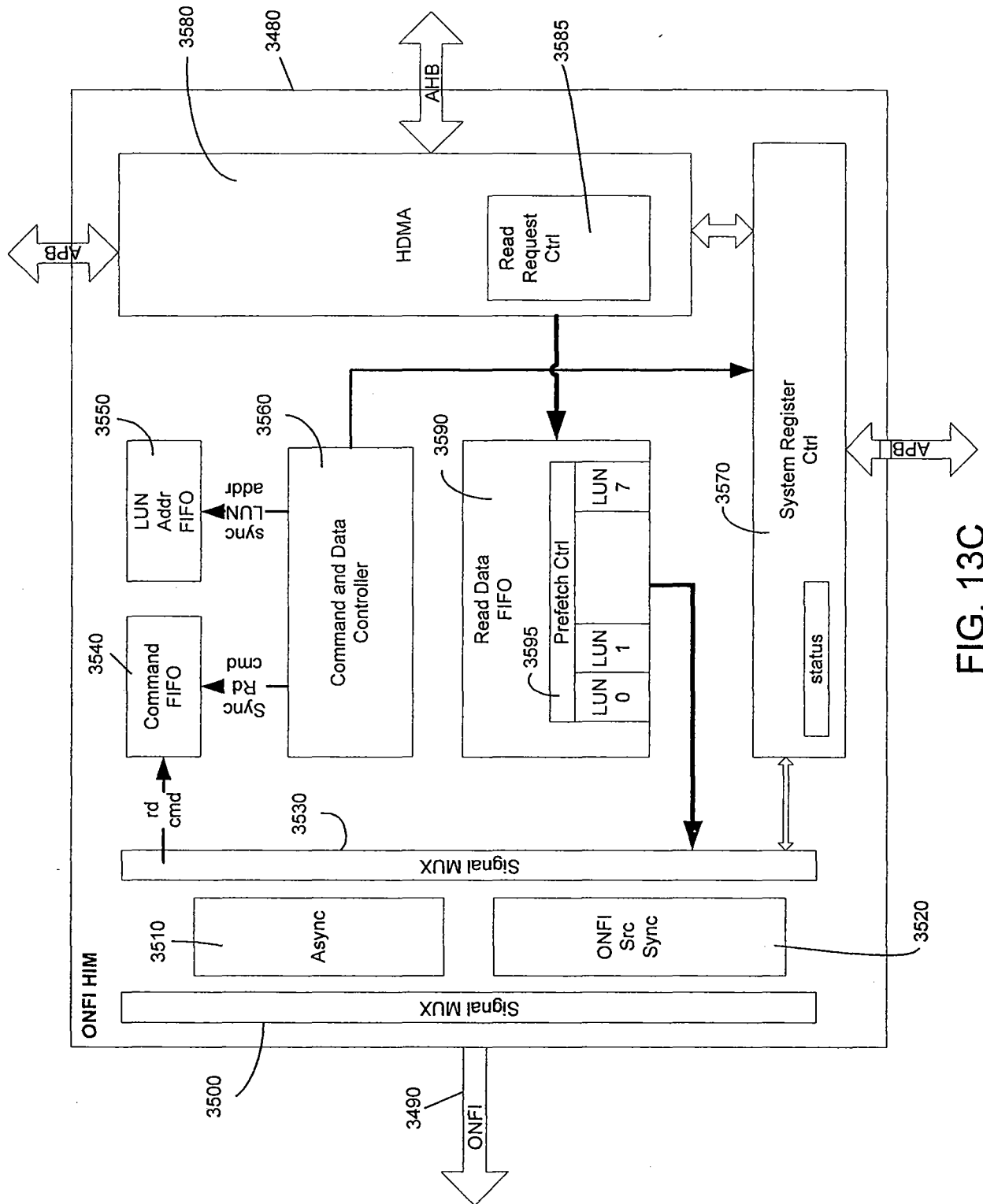


FIG. 13B



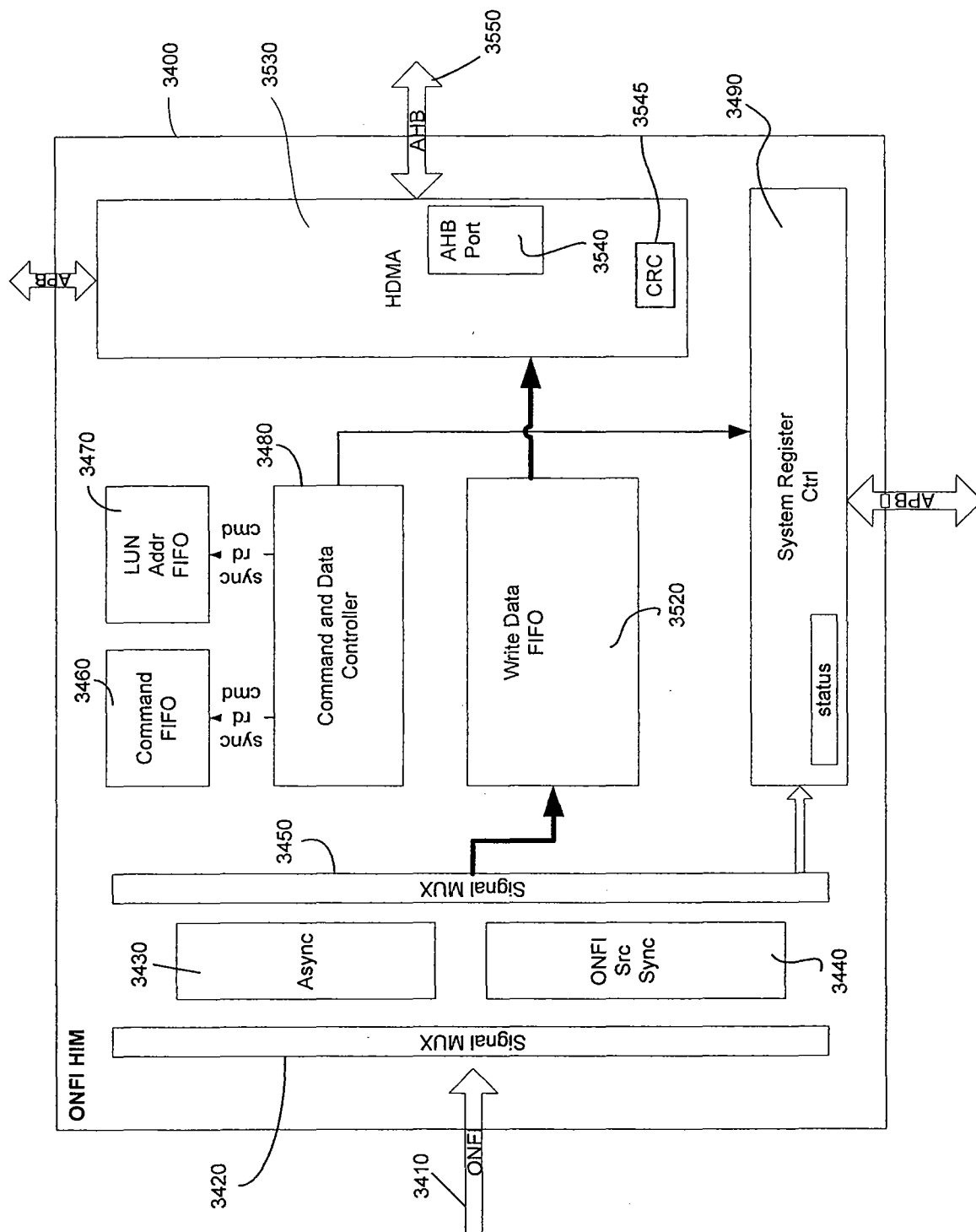


FIG. 13D

# INTERNATIONAL SEARCH REPORT

International application No  
PCT/US2010/044695

**A. CLASSIFICATION OF SUBJECT MATTER**  
INV. G06F11/10  
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)  
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EP0-Internal

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2007/220402 A1 (HAGI EIJI [JP] ET AL) 20 September 2007 (2007-09-20) page 2, paragraph 27 page 3, paragraph 31 - page 5, paragraph 50 page 6, paragraph 61 - paragraph 66 figures 1,3, 6	1-32
X	US 2005/185449 A1 (SHIOTA SHIGEMASA [JP] ET AL) 25 August 2005 (2005-08-25) page 4, paragraph 74 - page 6, paragraph 122; figures 1,2,3	1-32
A	WO 2007/034481 A2 (MSYSTEMS LTD [IL]; LASSER MENACHEM [IL]) 29 March 2007 (2007-03-29) the whole document	1-32

☐

Further documents are listed in the continuation of Box C.

☒

See patent family annex.

\* Special categories of cited documents:

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

9 November 2010

Date of mailing of the international search report

19/11/2010

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040,  
Fax: (+31-70) 340-3016

Authorized officer

Bauer, Regine

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2010/044695

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007220402 A1	20-09-2007	JP 2007183844 A	19-07-2007
US 2005185449 A1	25-08-2005	JP 2005234976 A	02-09-2005
WO 2007034481 A2	29-03-2007	EP 1929483 A2	11-06-2008
		EP 2110746 A1	21-10-2009
		JP 2009510560 T	12-03-2009
		KR 20080050433 A	05-06-2008
		KR 20100021497 A	24-02-2010
		US 2007074093 A1	29-03-2007
		US 2010049909 A1	25-02-2010