AN1120
APPLICATION NOTE

EEPROM-Based Application Specific Memories

Although the bulk of memory devices shipped today are standard commodity products, there is a rapidly growing market for Application Specific Memories (ASMs). These are devices that are specifically optimized for particular applications. These include both custom devices, and standard products that are designed to perform a specific function.

The general concept of ASM is applicable to any type of memory, but the greatest activity today involves devices that include non-volatile memories, such as Flash, OTP or EEPROM.

The concept of ASM is not new, but recent advances in technology, manufacturing efficiency and design re-use have made it possible to develop and produce ASMs at previously unobtainable levels of price-to-performance, and with very short design times. This is opening up a huge range of innovative potential applications that were not previously feasible on technical, economic or time-to-market grounds.

One of the first Application Specific Memory devices was the phonecard chip, which ST began manufacturing over 20 years ago. Today's phonecard chips are considerably more sophisticated, but still retain the same basic requirements: they are non-volatile memories with extremely special protection features, and they must be produced at extremely low cost. Many applications need devices with the same characteristics, with the result that the techniques developed to meet the economic and technical demands of the phonecard market can be successfully applied to other areas.

The two main benefits of ASM technology are cost reduction through the use of fewer packages, and the protection of stored data or intellectual property. Reducing component count can be achieved either by mounting different memory chips in a single package or by implementing different memory functions on the same chip. A wide range of protection functions is available, including:

- read and write control mechanisms, both hardware and software
- OTP (one-time programmable) areas
- logic functions
- transport codes, anti-tearing functions, issuer keys, and other sophisticated mechanisms developed for the smartcard and phonecard markets.

Application Note *AN1292* illustrates the general structure of an ASM, and the variety of building blocks that are available. Typically, the core of the ASM is an EEPROM array. EEPROM is ideal for ASMs because of its byte-level programmability, its high write-cycle endurance and – increasingly important – its ability to operate at low voltage, and with very low operating and standby currents. The EEPROM can also be complemented by other types of memory, such as EPROM (for OTP functions) and Flash memory (for large scale program code storage).

The wide choice of building blocks allows the customer to choose the optimum trade-off between the security mechanisms employed and the cost of the ASM. This is essential because many ASM applications are extremely cost-sensitive, and the target device costs can be as low as tens of cents in very high volumes.

The following examples illustrate some of the ways in which ASM technology is currently being applied to improve security, to enhance functionality and to lower costs in all of the major equipment segments, including the computer, telecommunications, consumer and automotive markets.

DIMM CARDS IDENTIFIER (SPD)

To illustrate how effective the ASM concept is, consider the M34C02. This has been developed for a highly specific market that is more conventionally handled as part of the standard applications market.

JEDEC defines a standard for DRAM in Dual In-line Memory Modules (DIMM). Part of this includes the Serial Presence Detect (SPD) function, which used by the PC during system configuration, and is mandatory for all new 168-pin and 200-pin DIMMs for PCs and workstations and will also be used in DIMMs for new PC VGA cards. This function allows the identification of the parameters that specify the DIMM (DRAM type, speed, organization, manufacturer, etc.).

The M34C02, is a serial EEPROM that is specifically designed to implement this non-volatile parameter storage, in such as way as to enhance the reliability of the Serial Presence Detect (SPD) function in DIMM. The M34C02 stores the DIMM configuration data, which can be read through the SMBus.

The M34C02 offers a superior solution to the standard 2 Kbit I^2C serial EEPROM. Because the SPD data is critical to the reliability of the system, the EEPROM needs to be immune to both accidental data corruption and tampering by the user. Standard EEPROMs offer good security against accidental data corruption but can obviously provide no protection against tampering as they are designed to support repeated erase/program cycles. This problem is solved with the M34C02 by making one half of the memory array permanently lockable. This means that after programming the SPD data in the DIMM, the manufacturer can issue an irreversible command to write-protect this area, still leaving the other half of the memory array free for scratch-pad use.

Of course, an ASM specifically designed for one application may still be useful in others. For example, the concept of software-lockable EEPROM has wider applications than DIMMs, and the M34C02 has given rise to a range of devices offering this facility.

ACR SERIAL BUS EEPROM FOR PC MOTHERBOARDS

The M34A02 EEPROM is a dedicated chip for the Advanced Communication Riser market. It is designed for plug and play cards that connect to the PC motherboard SMBus structure. The M34A02 stores the ACR configuration data, which can be read through the SMBus. In addition, the M34A02 memory architecture offers the flexibility required to define both variable size enumeration areas and defined size vendor areas.

The ACR configuration data includes the parameters describing the configuration of modem, Ethernet, phoneline, wireless networking, xDSL and audio functions available on the ACR card.

The M34A02 EEPROM device contains a two-wire SMBus serial interface that uses a bi-directional data line and one clock line. It is powered by a single 2.7 V to 3.6 V supply voltage, and has a hard-ware write-control. The device is programmed by the ACR Card Issuer, and the application retrieves card configuration data in read mode using the standard 100 kHz SMBus bus protocol. The serial bus pin-out is also standard.

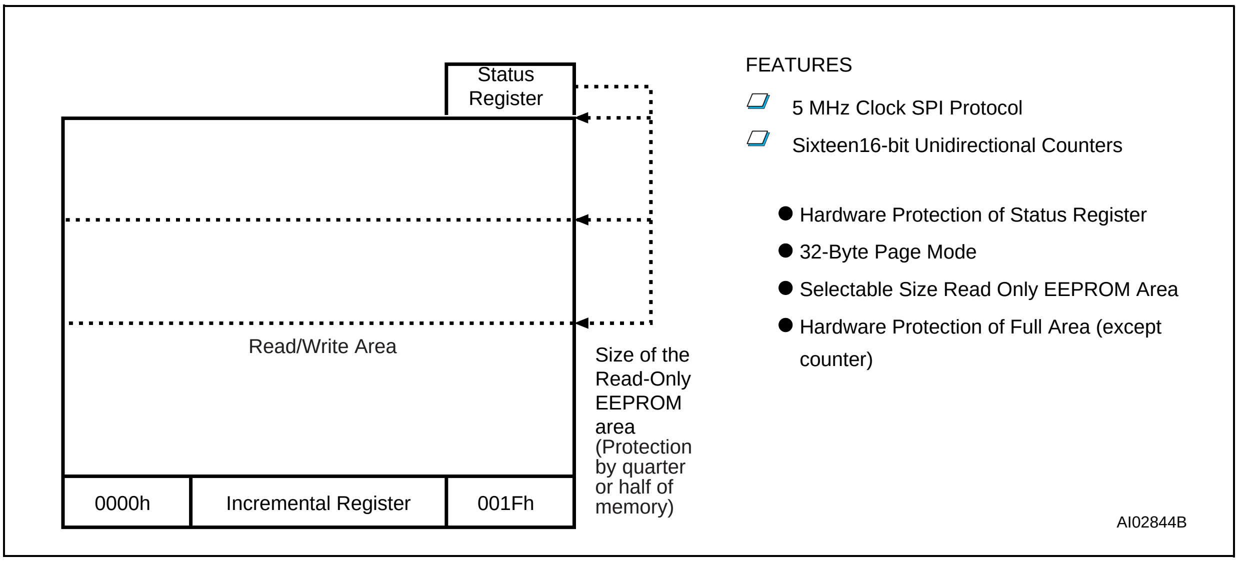
Among the M34A02 performance figures are more than one million erase/write cycles and data retention of more than 40 years. It fulfills all the ACR requirements contained in the new industry-wide standard for advanced PC communication riser cards established by the ACR SIG (Advanced Communication Riser Association Special Interest Group) of which STMicroelectronics is an adopted member.

Other features of the device include up to 16 byte page write, together with random and sequential read modes, automatic address incrementing and enhanced ESD/latch-up behavior. These devices come in plastic small outline (SO8) or thin shrink small outline (TSSOP8) packages.

TAMPER-PROOF COUNTING

There are many applications where it is necessary to keep an incorruptible count of the number of times a particular event has occurred. Many photocopiers, for example, keep a count of the number of copies made, and this information is often used to calculate rental or service charges or to investigate warranty claims. For example, if the number of copies recorded is significantly greater than the number of copies expected from a toner cartridge, this could indicate that the user has refilled the cartridge (perhaps with an inferior toner) and this could, in turn, affect the warranty. Clearly, the end user should not be able to modify the data stored in the photocopier's non-volatile memory.

Figure 1. M35080 block diagram


Status Register
Read/Write Area
0000h
Incremental Register
001Fh
Size of the Read-Only EEPROM area (Protection by quarter or half of memory)
FEATURES
5 MHz Clock SPI Protocol
Sixteen16-bit Unidirectional Counters
Hardware Protection of Status Register
32-Byte Page Mode
Selectable Size Read Only EEPROM Area
Hardware Protection of Full Area (except counter)
AI02844B

An application where tamper-proof counting is even more important is in the car odometer. The value of a used car is greatly affected by its total mileage, and so the illegal practice of "turning back the clock" is as old as the used-car market. The M35080 was developed as a solution to this problem. As shown in Figure 1, the M35080 is derived from the M95080, an 8 Kbit EEPROM with an SPI interface. The main difference is the addition of comparators and control logic to govern the write operations in the first 32 bytes of the EEPROM array. This allows the write operation to proceed in this area only if the new value for each 16-bit word is greater than the data already stored there. As a result, the first 32 bytes of the EEPROM array emulate an array of 16 unidirectional 16-bit counters.

The particularly demanding requirements of this application would not have been met by the typical EEPROM endurance of 100K erase/write cycles and ten year data retention (both of which would have been too low). The M35080, therefore, is built with ST's high endurance double polysilicon CMOS technology. For the M35080, one million erase/write cycles and a 40-year data retention are guaranteed over a temperature range of –40 °C to +85 °C, ensuring that the odometer will function correctly throughout the lifetime of the car.

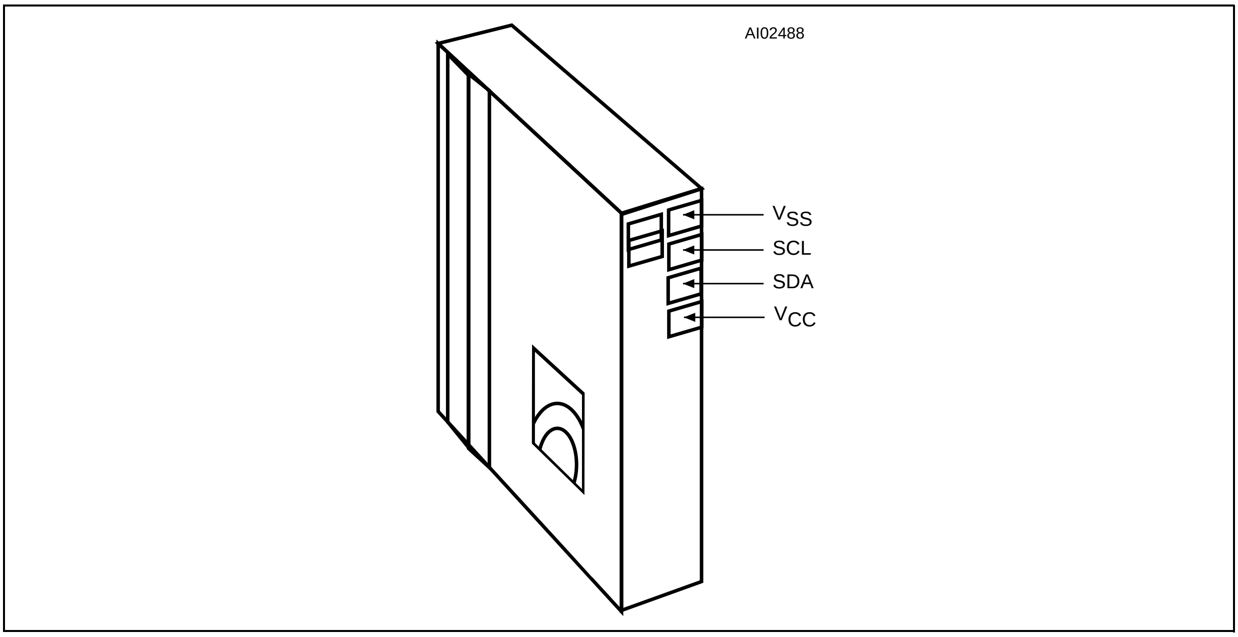
EMBEDDING ASMS IN OBJECTS

In the examples considered so far, the ASM is incorporated into equipment subsystems, but there is also currently an enormous interest in embedding ASMs in objects. Often, the reason is to enhance the functionality of the object, or to provide protection against cloning, misuse or similar undesirable activities.

A simple example of how ASMs can enhance the functionality of equipment is provided by the “smart” digital video cassette recorder (DV Standard). In a standard VCR, users often need to find a particular part of the tape, such as the beginnings and ends of the recordings that have been strung together on a single cassette tape. This can often involve frustrating and time-consuming winding and rewinding. Storing this information in a non-volatile memory in the VCR would make the equipment more user-friendly (allowing the machine to position the tape quickly at the required location) but would become invalid if the cassette were changed.

The functionality of the VCR can be considerably enhanced by incorporating the memory in the cassette rather than in the equipment. Because each cassette then carries its own data, cassettes can be removed and the subsequently reloaded into the same machine or into a different machine, without losing any of the stored information.

Figure 2. Memory-in-Cassette Module



If the object does not normally contain a PCB, a means must be found for incorporating the ASM so that it is electrically accessible, and in the form that can be engineered for minimum cost and space. For example, for the DV application, ST has developed memory modules that consist of a small PCB, on which an EEPROM memory is mounted, and a Transil device to protect the memory against voltage transients (encountered when the module is brought into electrical contact with the VCR).

The modules are electrically compatible with standard I^2C EEPROMs, such as the M24xxx series. The PCB provides four contact pads for the V_{CC}, ground, serial clock and serial data lines (as shown in Figure 2). Consequently, these modules are equally applicable to a wide range of other applications, and are currently shipping in large volumes.

SMART CONSUMABLES

One of the most interesting classes of ASM applications involves embedding non volatile memories (NVM) in replacement parts or consumables. The motivation for doing this could be:

- for technical reasons, to ensure that only replacement parts meeting particular specifications are accepted by the equipment. For example, in an inkjet printer, the use of inks that do not exactly match the physical and chemical properties, for which the head was designed, may cause physical damage to the print head.
- or for commercial reasons. For example, if an equipment manufacturer can be sure of being the sole supplier of the equipment’s consumables, it would have the option of shifting some of its profit margin to the consumables, thereby reducing the purchase price to give it a competitive marketing edge.

ASMs can provide an effective solution in either case. By embedding a low-cost ASM in the replacement part, the equipment can be made to identify and authenticate the part, to determine whether or not it is officially approved and to take an appropriate action. One of the major advantages of this approach is that information stored in a memory chip is subject to the same copyright and trademark laws as information published on paper. This means that while there may be no legal impediment to producing clone parts that are electrically and mechanically compatible with the official parts, the clone manufacturer will not be able to duplicate the entire contents of the ASM without breaking laws that protect intellectual property.

In terms of the specific implementation, each “smart consumable” application has its own set of economic and engineering parameters. Sometimes these are compatible with “standard” ASMs such as the MIC modules, in which case the customer can use an off-the-shelf solution. In other cases, the best solution may be a custom device developed in partnership with ST’s ASM Business Unit, which brings together the technical and marketing resources needed to develop solutions rapidly to problems that involve the combination of non-volatile memory blocks and any other functions. As an example, the odometer application described earlier took just six months to implement fully, from the first customer enquiry to the start of volume production.

M34C00 384-BIT EEPROM IS INDUSTRY’S SMALLEST ELECTRICALLY WRITABLE TAG

The M34C00 is the industry’s smallest electrically writable tag (ee-tag) for storing serial numbers, factory and user settings, or other data needed for electronic circuit boards. It serves as a low-cost alternative to the M24C01 to help manufacturers trace their electronic products during and after manufacture, including after sales and during service.

The M34C00 is a 384-bit EEPROM organized as 48x8 bits and divided into three 128-bit blocks. The three memory blocks comprise non-erasable, standard EEPROM, and permanently write-protected blocks. Specifically, the memory’s bottom third (locations 00h to 0Fh), once written to, is irreversibly write-protected using software. The top third (locations 20h to 2Fh) works as non-erasable memory; that is, it comes with a 1 stored in each location, which the user can change to a 0. Once changed, however, no mechanism is available for returning the 0 to 1. The middle block operates like conventional EEPROM.

Access to the M34C00 is through an I^2C (two-wire serial) bus clocked at 400 kHz. The bi-directional bus carries clock and data bits, with the chip operating as a slave device as defined by the I^2C protocol. The interface and protocol also accommodate SMbus operation.

Other features of the M34C00 include a self-timed program cycle, 2.5 V to 5.5 V operation, and a power-on reset that prevents data from being corrupted by an unintended write operation while the supply voltage settles to its correct value.

The M34C00 is available in SO-8 and TSSOP-8 packages and operates over the industrial temperature range of –40°C to +85°C.

CONTACTLESS MEMORIES

The LRI512 and the SR176 are two contactless memory chips. The LRI512 is fully ISO/IEC15693-compliant and the SR176 is ISO/IEC14443 Type B-compliant. Both devices are EEPROM memories with on-board RF interfaces operating at the industry standard frequency of 13.56 MHz.

The SR176 is aimed at highly cost-sensitive short-range applications (0 m to 0.2 m operating distance), while the LRI512 targets “smart labels” and similar vicinity mode applications that operate between 0 m and 1 m from the reader.

The LRI512 is a 512-bit, write-lockable EEPROM that offers a 64-bit Unique Identification Device (UID) and an ISO compliant anticollision mechanism. Additionally the Electrical Article Surveillance (E.A.S.) feature provides anti-theft capability in point-of-sale applications such as shops and libraries.

Built using a highly reliable and mature CMOS technology with embedded EEPROM well-suited to address high volume, cost-driven markets, the LRI512 is organized as 16 blocks of 32 bits. Each memory block can be individually write-protected using a LOCK command that prevents any subsequent modification of the data. In addition, a 64-bit read-only UID block and an 8-bit Application Family Identifier code uniquely identify the device for the Anti-Collision mechanism.

With its 32-bit granularity and write-lock features, the LRI512 is particularly suitable for supply chain management applications, where the final user needs to be able to read data along the traceability chain and intermediate actors need to be sure that their data cannot be subsequently modified. The LRI512 is also perfectly suited for e-commerce and long range access control systems. It will be available in volume in various delivery formats, including thin unsawn wafer, sawn and bumped wafer, inlays with copper or aluminium antennas starting December 2001.

ST has also expanded its short range portfolio with the introduction of the R176, an ISO/IEC14443 TypeB chip that offers 176 bits of EEPROM plus a 64-bit unique identification number. The 176 user bits are organized as eleven 16-bit blocks, of which five can be write-protected. Target markets are cost-sensitive applications such as consumables, access control and low-value e-purses that do not need to be modified more than a few times.

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

apps.eeprom@st.com	(for application support)
ask.memory@st.com	(for general enquiries)

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

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

STMicroelectronics group of companies Australia - Brazil - Canada - China - Finland - France - Germany - Hong Kong -
India - Israel - Italy - Japan - Malaysia - Malta - Morocco - Singapore - Spain - Sweden - Switzerland - United Kingdom - United States.
www.st.com