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

Although the concept of ASM is not new, 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.

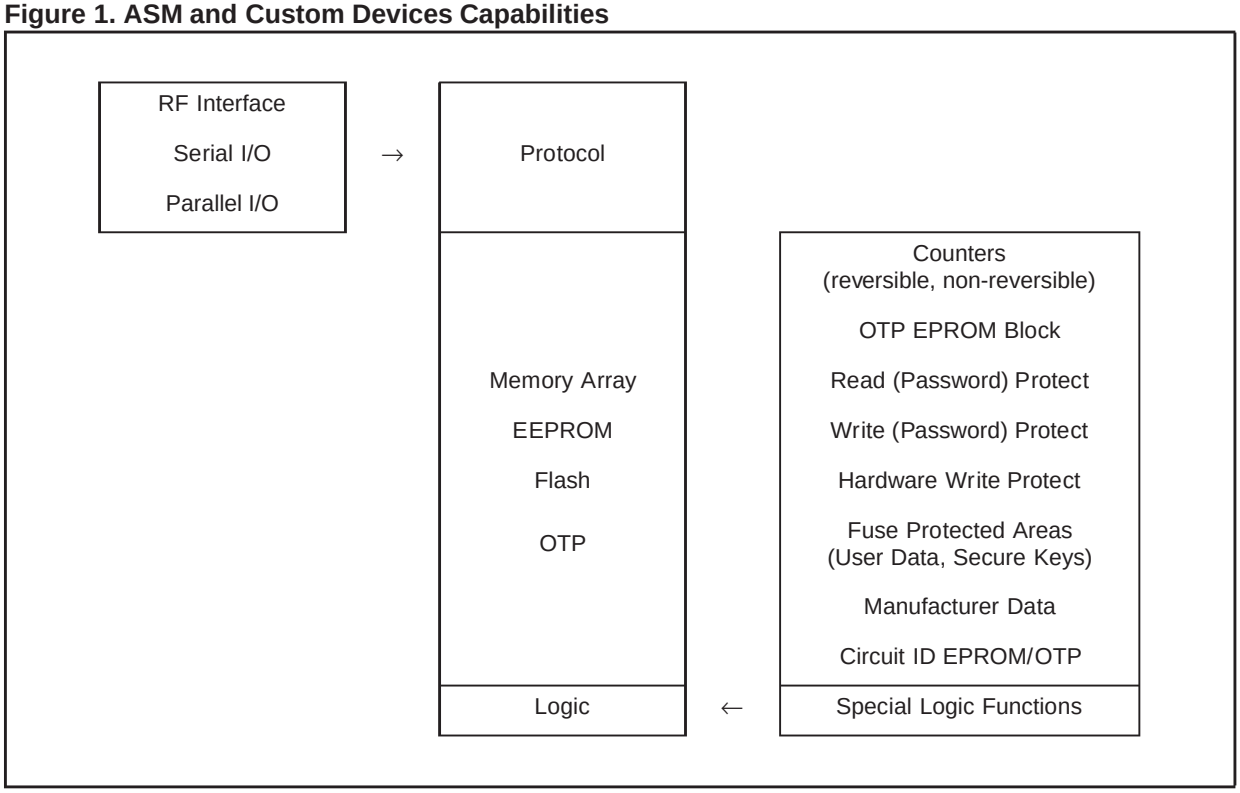
One of the first application specific memory devices was the phonecard chip, which ST began manufacturing over 20 years ago. Today's phonecard chips are considerably more sophisticated, but still retain the same basic requirements: they are non-volatile memories with special protection features, and they must be produced at extremely low cost. Many ASM 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.

Figure 1 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 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).

Figure 1. ASM and Custom Devices Capabilities



The full range of I/O protocols is available for ASM devices, including parallel access, 2-line serial bus access, 3-line serial bus access, and RF contactless interface schemes (not only loyalty cards, transport tickets, and contactless phonecards, but also in many different electronic tagging applications).

The versatility of ASM is a result of its great array of optional supporting features, as shown on the right hand side of Figure 1. Many of these are already widely used in smartcard chips but they are equally applicable to non-volatile memories designed to be embedded in any other type of objects. This 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.

STANDARD ASMS

To illustrate how effective the concept is, consider the following ASMs. These have been developed for a highly specific market that is more conventionally handled as part of the standard applications market.

For example, standard ASMs have been developed for a number of applications, including Plug & Play monitors and DIMM memory modules that use the Serial Presence Detect (SPD) function.

Plug & Play peripherals contain an embedded non-volatile memory that holds information that allows the host PC to identify the peripheral. Once the PC has identified the peripheral, it can configure its subsystems and select appropriate software drivers. ST offers a range of EEPROMs (ST24xy21) specifically designed for use in Plug & Play monitors, where the standard access bus is the VESA Data Display Channel. The VESA specification requires the EEPROMs to have a standard I^2C interface augmented by an

additional VCLK input that is used to allow the PC to receive the display identification and operating parameter data.

The ST24xy21 devices are organized as 128 x 8-bits and are fully compatible with the VESA Data Display Channel (DDC) standards, communicating both in DDC1 (Transmit Only) and DDC2B (I^2C Bidirectional) modes. These devices allow a direct connection between the PC host and the monitor using the standard video cable and 15-pin VGA connector.

Although the ST24xy21 devices were developed from the first ST24LC21 1 Kbit EEPROM, they include specific enhancements, such as a Schmitt-Trigger input on the VCLK pin for better noise immunity, and a higher power-on reset value of 3 V. The range includes devices with a write control input, on pin 3, to improve data corruption rejection; and devices that offer full VESA 2.0 compatibility, including the error recovery mechanism that allows an automatic return to Transmit-Only mode in the event of invalid activity on the I^2C bus.

Another family of standard ASMs is illustrated by the M34C02, a serial EEPROM specifically designed to enhance the reliability of the Serial Presence Detect (SPD) function in DIMM DRAM modules. In the JEDEC SPD standard, the specifications of the DRAM module, including information such as DRAM type, speed, organization and manufacturer, is stored in an on-board non-volatile memory, and used by the PC during system configuration. SPD is mandatory for all new 168-pin and 200-pin DRAM modules for PCs and workstations and will also be used in DRAM Modules for new PC VGA cards.

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 the bottom 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 the first 128 bytes of the memory area, still leaving the upper half free for scratch-pad use.

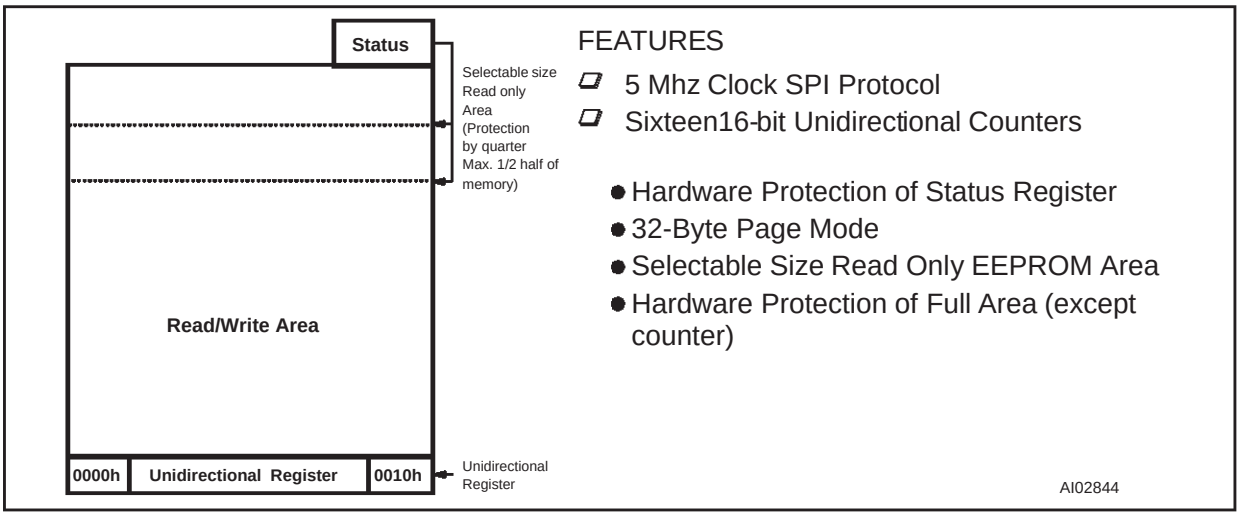
Of course, an ASM specifically designed for one application may still be useful in others. For example, the concept of software-lockable EEPROM has wider applications than DIMM modules and the M34C02 has given rise to a range of devices offering this facility, including the M34Wxx devices, in which the user can select the position (top or bottom of memory array) and size of the protected block.

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.

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 is a new ASM developed to provide an ideal solution to this problem. As shown in Figure 2, 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.

Figure 2. M35080 block diagram



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.

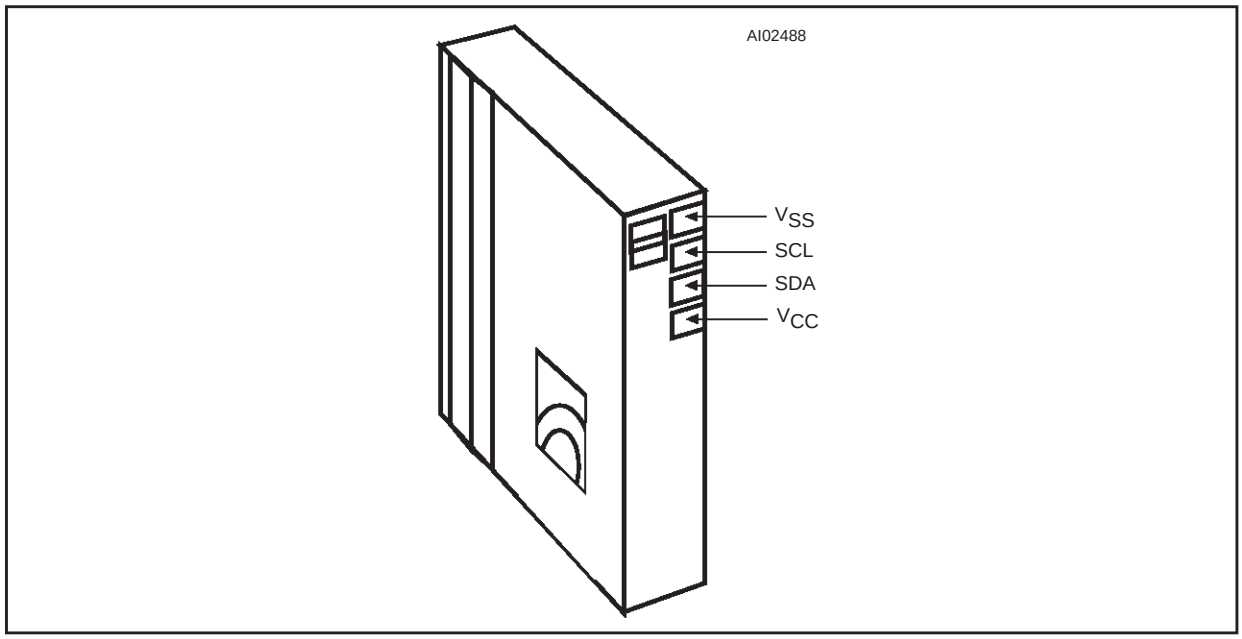
A simple example of how ASMs can enhance the functionality of equipment is provided by the "smart" digital video cassette recorder (digital VCR). In a standard VCR, users often need to find a particular part of the tape, such as the beginnings and ends of the recordings that have been strung together 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.

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 VCR 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 3). Consequently, these modules are equally applicable to a wide range of other applications, and are currently shipping in large volumes.

Figure 3. Memory-in-Cassette Module



SMART CONSUMABLES

One of the most interesting classes of ASM applications involves embedding non volatile (NV) memories 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, or in other ways. 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.

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.