The Intel System Management Mode

By Simon C. Ellis, Intel Corp.

The System Management Mode (SMM) is the fifth operating mode of the Intel386™ architecture. SMM is a flexible architectural extension that allows new code to run completely transparently from any CPU mode (real, virtual, protected, or emulator) and any operating system or any application. The first implementation of this mode is in the i386 SL microprocessor and the 82360SL I/O subsystem, which use SMM for power management in portable PCs. However, the ability to add features independently of the operating system is a valuable capability beyond portable computers. Therefore SMM support will be implemented in all future x86 CPUs designed by Intel to allow vendors to add these differentiating features to their systems.

Intel established a transparent mode of operation that, in the area of power management, allows a computer to execute power-management code regardless of the software (past, present, and future versions) installed by the user. This operating mode enables vendors to build finely-tuned systems, providing the power management in a single driver that is part of the firmware. SMM, therefore, eliminates the need for multiple drivers for different operating systems or upgrades to support new releases of application software.

The significant investment in PC BIOS programs is amortized over multiple products because there is strict register, bit-level compatibility. Customers have been shipping products based on the i386 SL CPU during the last year and soon will be announcing follow-on products that rely on this bit-level compatibility to amortize their software investment. The customer can focus on new, exciting, value-added features in these products, and not have to keep re-inventing the underlying power-management capability.

Comparing SMMs

The concept of a special processor operating mode for system management was first introduced by Intel's 386SL. AMD then added a similar mode to its Am386DXL/SXL design, and Chips and Technologies incorporated a related set of features in its Super386.

In hopes of clarifying the differences between the three implementations, we invited each of the vendors to submit a short article explaining the advantages of their approach. Here are the three vendors' articles; in a future issue, we'll present our review of the strengths and weaknesses of each argument.

The Intel focus is on a *complete* power-management solution at the system level. Intel's SMM architectural extension is simple and flexible. It consists of a System Management Interrupt (SMI) in the i386 SL CPU and power-management resources in the 82360SL I/O subsystem (see Figure 1). The SMI is what provides the transparent operating environment for the system-management code.

SMM Features

The major features of the Intel SMI are as follows:

- SMCODE executes from a protected space. Code space may vary from 32 Kbytes to 4 Gbytes.
- CPU state is saved (at 03FE00h–03FFFFh) and the CPU jumps directly to 038000h.
- All PC memory and I/O space is directly accessible from SMM.
- SMM is exited through a new instruction, RSM (opcode 0FAAh). Two optional return functions are included: HALT restart and I/O restart.

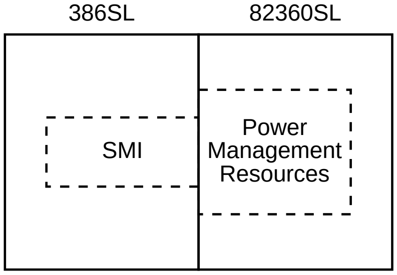

Figure 1. System management mode implementation.

The unique I/O restart feature is absolutely required for an efficient I/O trap function. For example, when a peripheral such as the hard disk is powered down, power-management code saves its state, removes power, and sets up the I/O trap. When the device is accessed, I/O restart is needed to ensure that the peripheral is reconfigured correctly prior to the re-execution of the last instruction. Without the I/O restart, if you try to back up the instruction pointer before resuming, it is impossible to determine by how many bytes it should be backed up. Even if you successfully recreate the physical address by manually going backward through paging and segmentation to reach the opcodes, which can take 200 lines of code, you cannot disassemble all the varieties of I/O cycles. With Intel's SMM, the I/O restart is handled automatically without the need for additional software.

Continued on page 19

with a system management mode.

SuperState V offers both hardware and software control. It traps on more conditions than Intel's or AMD's SMM, and SuperState V has no limit on the number of I/O addresses on which it can trap. SuperState can trap on hardware interrupts, software exceptions and interrupts, shutdown, and halt. The event capture ranges are specified through software parameters, rather than hardware signals, and while in the SuperState mode, access to normal user-mode memory is accomplished by using the simple GS prefix.

I/O events are faulted before execution rather than trapped afterwards, so there is no instruction retry and no complicated unwinding of the instruction stream, as required by Intel's SMM. A SuperState programmer simply powers up the device accessed by the trapped instruction and executes the faulted I/O instruction. Likewise, the system designer does not have to generate complicated signal sequences for each device that is powered-down to trap on I/O accesses to that device.

SuperState V provides several software features not found in Intel's or AMD's SMM. The new SCALL instruction allows privileged software to communicate with SuperState V code. The SuperVisor manages installation of multiple SuperState V applications and manages events. The SuperVisor's simple but robust programming interface (SPI) frees the programmer to simply use the SPI calls to manage events and resources, rather than coding from scratch. The SuperState V software advantage means faster development, greater functionality, and fewer problems. ♦

AMD SMM

Continued from page 17

separate address space. Power management is the obvious application. Other functions that system management modes support include network drivers, device drivers, file translation software, data security, and supervision.

AMD's system management solution provides the core functions while leaving room for flexibility and differentiation for the system designer. This allows the designer to choose the chip set that best fits the requirements. Thus, the system architecture, chip count, and power-management approaches are selected by the designer, rather than dictated by the silicon supplier, as is the case with the Intel approach. This flexibility is extended to the I/O trapping feature in the solution offered by AMD, as multiple event ranges can be implemented. This approach is superior to the one offered by CHIPS and Technologies which has fixed internal event ranges for I/O trapping. ♦

Intel SMM

Continued from page 16

The 82360SL peripheral unit contains the PC peripherals and most of the power-management resources. There are times when the latency of the SMI could corrupt the system integrity. In these cases, hardware is required to transparently delay the SMI until the time-critical event has completed. The 82360SL can generate an SMI interrupt from seven types of sources. The power-management resources are set up and controlled through many protected and visible I/O registers. The mapping and control of these power-management registers is now fixed, and all future SL products will have compatible mechanisms.

SMM Advantages

The i386 SL CPU is the lowest-risk solution for the newest generation of notebook computers, providing faster time-to-market for vendors and more robust, feature-rich systems for the end user. There are full-feature BIOS programs, controlling the Intel SMM power management, available from all the leading BIOS vendors. In addition, Intel provides a full-function in-circuit emulator, evaluation boards, and sample power-management code. The i386 SL microprocessor has been in production for the last year, and there are many proven notebook products already on the market. Intel is committed to future SL products and is currently developing the next generation. Only Intel provides the complete system solution by providing not only a special processor mode, but also a supporting peripheral chip, firmware, and development tools. ♦