SuperState: Beyond Hardware Solutions

By Gary Albitz, CHIPS and Technologies

Today, all three x86 microprocessor vendors support extended operating modes designed to add value to the ubiquitous PC. Intel and AMD offer the related (but, confusingly, somewhat different) System Management Mode, while CHIPS and Technologies has announced the SuperState™ System Management Architecture.

With support from all three x86 vendors, the SMM/SuperState system design style will become a major vehicle for system differentiation. The SuperState System Management Architecture meets this need for notebook, desktop, embedded, and server applications.

CHIPS supports two flavors of SuperState. SuperState R (real mode) is implemented in the PC/CHIP computer-on-a-chip. This article addresses SuperState V (virtual mode), supported by the recently announced Super38605 microprocessor.

SuperState V

SuperState V provides access to an alternative microprocessor “state” in which OEM-specific applications (such as interfacing pen-input signals or providing diagnostics) run transparently to the operating system and BIOS. The microprocessor enters the SuperState V mode through programmed external or internal hardware or software events.

In SuperState mode, OEM applications are executed via the CHIPS SuperVisor™ software kernel. The SuperVisor operates independently of “user” memory space and, when in this mode, controls microprocessor operations. SuperState V features fast entry and exit, optimal I/O handling, and maximum flexibility with hardware protection mechanisms. SuperState V is fully compatible with existing system and application software because SuperState V’s entry cleanly stops the operating environment and saves its state, which is later restored on exit.

SuperState V consists of both software and hardware facilities. The SuperVisor software facility interfaces the OEM SuperState application with the hardware and microcode. The SuperState V hardware facilities in the Super38605 consist of event capturing facilities, an external hardware interrupt, a separate physical address space, and instruction set extensions.

Event capturing allows dynamic selection of I/O port events or interrupt events to cause entry into SuperState V. The facility provides six event ranges, each of which can selectively capture from 1 to 128 consecutive ports or from 1 to 32 interrupt or exception vectors. No performance or response time degradation is experienced by the user.

The event capture facility can be operated to select events in either an inclusive or an exclusive mode. When in the inclusive mode, any match between one of the six ranges and the corresponding operation triggers SuperState V. When operating in the exclusive mode, SuperState V is entered only when an event does *not* match any of the programmed event ranges. Thus, the event capture facility can be operated much as a cache or TLB, providing unlimited capture capabilities with no impact on system response time.

The ANMI interrupt is an active-low, level-sensitive, non-maskable interrupt signal having the highest priority to trigger the Super386 into SuperState V mode. AADS is an active-low output signal that follows the ADS (bus cycle request) timing and requests a SuperState V memory access. This signal allows implementation of a separate hardware-protected SuperState V address space of up to 4 Gbytes. The Super38605 issues both the ADS and the AADS signals when in SuperState V.

Instruction Set Extensions

The Super386 has several new instructions to support SuperState V. The SCALL instruction is used to both emulate and initialize SuperState V at boot time, and to quickly enter SuperState V from a program.

SCALL saves a minimal set of registers, fetches a descriptor with the SuperState V address space base address, and then fetches and starts the SuperVisor from SuperState V address space. The SCALL instruction is enabled in user mode, but SCALL can only be invoked by a protected-mode application if the application has the same privilege level as the operating system. This protection mechanism is enforced in hardware by Super386 microcode.

Other SuperState V instructions only become enabled after entering SuperState V. The SRET instruction is used for normal return from SuperState V mode to user mode. The SRESUME instruction is used to return to user mode, but re-entry to SuperState V mode is disabled while executing the first user-mode instruction (used for processing I/O instructions).

SuperState Advantages

A major SuperState V advantage over its competitors is its fast entry time (9 bus accesses) and exit time (5 bus accesses), for a total entry/exit time of less than 150 clock cycles. This contrasts to AMD’s SMM, which requires over 1100 clock cycles, and Intel’s SMM, which uses about 1000 clock cycles, to enter and exit. The Super386 at 40 MHz is also the fastest microprocessor 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. ♦