Reed Electronics Group

MICROPROCESSOR REPORT

www.MPRonline.com

THE INSIDER'S GUIDE TO MICROPROCESSOR HARDWARE

FREESCALE SECURES POWERQUICC

New PowerQuicc II Pro and PowerQuicc III Add Security Engines

By Tom R. Halfhill {5/10/04-02}

Freescale Semiconductor—the newborn spinoff from Motorola—has introduced a new PowerQuicc II Pro family of communications processors and two new members of the PowerQuicc III family. In all, there are eight new PowerQuicc chips. The most significant improvements over existing PowerQuicc processors are higher-performance CPU cores, faster memory systems, enhanced network interfaces, and integrated security engines for encrypting and decrypting data packets.

The integrated security engines are optional, so customers can still choose to use external security coprocessors or software-based security—or to not implement packet security at all, as export-control regulations sometimes require. Although the new processors aren't the first PowerQuicc chips to integrate security hardware, their security engines are more advanced than those in existing PowerQuicc chips.

In addition, the new PowerQuicc processors will deliver greater overall performance, thanks to faster DDR memory systems and enhanced PowerPC cores running at higher clock frequencies. Clock rates will get an even bigger boost when production moves from the current 0.13-micron fabrication process to the next-generation 90nm process, probably in late 2005 or early 2006.

All eight new PowerQuicc chips are scheduled to begin sampling later this year. Production quantities of the PowerQuicc III chips should be available in 4Q04, and production of PowerQuicc II Pro chips will follow in 1H05.

New Six-Chip PowerQuicc II Pro Family

The new PowerQuicc II Pro processors supplement the existing PowerQuicc I, II, and III families. The first six Pro chips are based on the new PowerPC e300 CPU core, an improved version of the PowerPC 603e core found in the PowerQuicc II and other processors. It has several enhancements, including larger caches, higher potential clock frequencies, and architectural extensions for embedded processing. The e300 is one of three new PowerPC cores that Freescale has announced for its PowerQuicc line. (See sidebar, "New PowerPC Cores Promise Higher Performance.")

A faster memory system will also contribute to better performance. Instead of the SDR SDRAM controller on the PowerQuicc II, new Pro chips have DDR SDRAM controllers. External bus frequencies can range from 133MHz to 167MHz, yielding effective DDR speeds of 266–333MHz. Core-to-bus frequency ratios can range from 1:1 to 5:1 in half steps. Four of the six new Pro chips have 32/64-bit memory buses, and the other two have 32-bit buses.

Three of the Pro chips have an integrated security engine, and three do not. The MPC8349E, '47E, and '43E all have security—"E" stands for "encryption"—and are otherwise identical to their E-less counterparts: the MPC8349, '47, and '43. Although security engines are a hot feature in network processors, some customers prefer to use a security coprocessor from a different vendor or their own proprietary security hardware. Then, too, some applications require no packet security or can tolerate the lower performance of software-based encryption.

Some existing PowerQuicc chips incorporate Freescale's SEC 1.0 security engine, which was adapted from Motorola's S1 series of standalone security coprocessors. Pro chips have a more advanced engine: SEC 2.0. It uses less CPU and bus

Price & Availability

Freescale Semiconductor says initial samples of PowerQuicc II Pro chips will be available in 4Q04, followed by general sampling in 1Q05 and production in 2Q05. Prices for MPC834x/E chips purchased in 10,000-unit quantities range from about $20 to about $50, depending on clock speed. Quantity prices for MPC8541/E chips range from about $72 to $102, depending on clock speed. Initial samples of the PowerQuicc III MPC8541/E are available now, and general sampling will begin in 3Q04, followed by production in 4Q04.

bandwidth, and it's more flexible in addressing new security protocols, such as the Advanced Encryption Standard (AES). Freescale says the SEC 2.0 engine is software compatible with drivers for Motorola's existing MPC184 and MPC185 security coprocessors, although programmers must make minor modifications to take advantage of new features.

SEC 2.0 has a hardware random-number generator and five execution units: a public-key unit, DES unit, AES unit, ARC4 unit, and message digest unit. The public-key unit supports RSA Laboratories' Diffie-Hellman key-agreement protocol with keys up to 2,048 bits long, plus elliptical-curve cryptography with programmable field sizes up to 511 bits. The DES unit supports single DES, triple DES (3DES), two- or three-key algorithms, and the electronic-codebook (ECB) and cipher-block chaining (CBC) modes.

The AES unit supports key lengths of 128, 192, and 256 bits. Like the DES unit, it supports the ECB and CBC modes, as well as counter mode (CTR) and counter-with-CBC MAC (CCM) mode. The message digest unit supports 160-bit SHA-1, 256-bit SHA-2, 128-bit MD5, and a hashed message authentication code (HMAC) with all message-digest algorithms. The ARC4 cipher unit is compatible with RSA's Rivest Cipher 4 (RC4) symmetric stream cipher, which is part of the Secure Sockets Layer (SSL) built into virtually all web browsers. The hardware random-number generator complies with the National Institute of Standards and Technology (NIST) Common Criteria for Information Technology Security. It provides true random numbers for generating encryption keys and for padding messages, unlike software-based pseudorandom generators.

High-Speed On-Chip Peripherals and I/O

Freescale designed the PowerQuicc II Pro family for network routers, switches, line cards, hardware firewalls, virtual private network (VPN) gateways, wireless LANs, network-attached storage (NAS) subsystems, and other low-end to midrange communications products. The "E" chips in the family eliminate the need for a security coprocessor, and all Pro chips contain an impressive array of integrated peripherals and I/O interfaces to further reduce the system's chip count.

In addition to the DDR SDRAM controller already mentioned, Pro chips offer Gigabit Ethernet, Hi-Speed USB 2.0, and—with the MPC8349/E—dual-PCI capability. All these features set Pro chips apart from existing PowerQuicc II devices. As the block diagram in Figure 1 shows, all six Pro chips have two Gigabit Ethernet media-access controllers that also support the 10–100Mb/s modes and require only a PHY chip for a network connection. The USB 2.0 host/device controller supports the 480Mb/s Hi-Speed mode and On-the-Go (OTG) standard. The MPC8349/E has a 66MHz, 64-bit PCI interface that can operate as two 32-bit PCI interfaces, also at speeds up to 66MHz. The MPC-8347/E and MPC8343/E have only a single 66MHz, 32-bit PCI interface.

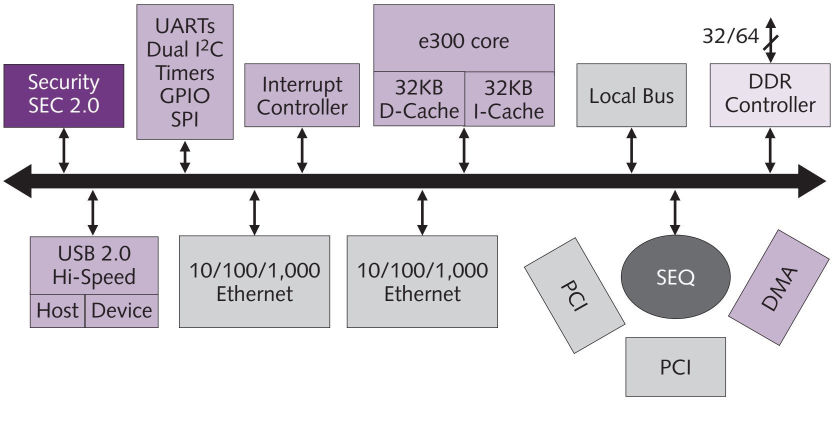

Figure 1. This block diagram of the PowerQuicc II Pro MPC8349E shows its PowerPC e300 CPU core, integrated SEC 2.0 security engine, on-chip peripherals, and I/O interfaces. Note especially the DDR SDRAM controller, dual Gigabit Ethernet controllers, and USB 2.0 Hi-Speed host/device controller. The PCI controllers can operate as two 32-bit interfaces or one 64-bit interface. The MPC8349 is identical except for the lack of a security engine. Other chips in the PowerQuicc II Pro family have a single 32-bit PCI interface, and the MPC8343/E has a narrower (32-bit) memory interface.

With six chips sporting the same basic design, the PowerQuicc II Pro family tries to offer enough variation to satisfy most customers. Even so, some customers may want a variation that Freescale didn't anticipate or whose expected sales volumes didn't justify developing a standard part. Other customers may want to differentiate themselves from competitors by using proprietary logic. For those reasons, Freescale offers the option of creating a semicustom design based on the MPC834x series.

Changing the lineup of on-chip peripherals is the easiest semicustom job and typically takes only a few months. Integrating proprietary logic is a little more involved, but Freescale says it can spin almost any variation in six to nine months—about half the time usually required for a full-custom ASIC. Customers provide the register-transfer level

(RTL) model or simply the specifications, and Freescale's engineers do the work.

Contracting with Freescale to produce a semicustom chip can be better than spinning a full-custom ASIC for several reasons: it eliminates the need to create a ground-up chip design, maintain a VLSI design team, acquire peripheral cores, pay royalties for licensed intellectual property (IP), assume all the risks for project mishaps, and negotiate with a foundry for manufacturing. Freescale will manufacture the semicustom chips, of course, sometimes using shuttle wafers to combine on a single wafer the low-volume designs from multiple customers.

Performance Is Difficult to Quantify

Freescale hasn't yet released EEMBC benchmark scores for the PowerQuicc II Pro family. The 1.0 version of EEMBC's networking suite isn't especially relevant, anyway, although the newly released 2.0 networking suite includes some applicable benchmarks, such as the IPmark and TCPmark. Meanwhile, Freescale offers some other estimates of performance.

According to Freescale, the Pro chips can execute 1.89 Dhrystone MIPS per megahertz. Unfortunately, the Dhrystone benchmark is strictly a measure of CPU performance and is next to useless for evaluating a communications processor. More to the point, Freescale estimates that Pro chips can process encrypted packets at a rate of about 200–300Mb/s, which is faster than AMD's claimed rate of about 150Mb/s for the recently introduced Alchemy Au1550. (See *MPR 4/5/04-01*, "Alchemy Adds Security Engine.") Another competing chip, Intel's XScale IXP425, can process encrypted packets at up to 70Mb/s. (See *MPR 3/18/02-01*, "Intel Beefs Up Networking Line.")

However, relative performance is difficult to judge without independent benchmarks, because it depends on many factors, including packet sizes and the utilization percentages of the CPU and memory bus. Last January, Motorola published an informative white paper on this subject (*Understanding Cryptographic Performance*) that is available from Freescale upon request.

PowerQuicc II Pro power consumption appears to be in the same ballpark as that of competing processors—although, again, it's difficult to draw conclusions without verified benchmarks. Freescale estimates that Pro chips will typically consume anywhere from 800mW at 266MHz to 1.3W at 533MHz. Intel pegs the typical power consumption of the IXP425 at 1.0–1.5W at 400MHz, and AMD estimates the Alchemy Au1550 will typically consume less than 500mW at 400MHz. Those are "typical" power ratings; maximum ratings will, of course, be higher.

With all on-chip peripherals and I/O buses running full out, Freescale estimates that the MPC8343E will consume 2.6W at 266MHz, and that the '49E will consume 3.5W at 533MHz. Those power estimates are not out of line for communications processors having the performance and integrated features of the PowerQuicc II Pro family.

New PowerQuicc III Has e500 CPU Core

Two new chips in the higher-end PowerQuicc III family are the MPC8541 and '41E—identical except for the SEC 2.0 security engine in the "E" part. These processors are based on the more powerful PowerPC e500 CPU core found in other PowerQuicc III chips, including the MPC8560, which won the *Microprocessor Report* Analysts' Choice Award for Best High-Performance Embedded Processor of 2003. (See *MPR 2/9/04-08*, "MPC8560 Merges Winning Features.")

Thanks to a deeper seven-stage pipeline (the e300 has only four stages), the e500 core runs at 533–833MHz in the MPC8541/E—and up to 1.0GHz in other PowerQuicc III devices manufactured in Motorola's 0.13-micron HIP7b CMOS process. In the next-generation 90nm process, the e500 core should reach 1.5GHz. (Freescale plans to begin sampling 90nm PowerQuicc III chips next year.) Another significant factor in the e500's higher performance is an on-chip 256K L2 cache; PowerQuicc II processors don't have L2 caches.

As with the PowerQuicc II Pro, the new PowerQuicc III chips have DDR SDRAM controllers (64 bits wide, up to 333MHz effective bus frequency) and dual Gigabit Ethernet controllers. However, the PowerQuicc III processors have two additional 10–100Mb/s Ethernet controllers (as well as SPI and I^2C serial interfaces) as part of their communications-processing module (CPM), an on-chip coprocessor. The PCI controller can operate as a 66MHz, 64-bit interface or as two 32-bit interfaces.

Missing from the MPC8541/E are a few features found in some other PowerQuicc III processors, most notably PCI-X, RapidIO, ATM, and Utopia 2. The MPC8541/E is obviously intended for lower-end applications—such as network appliances and gateways in homes and small businesses—that nevertheless demand higher performance than the PowerQuicc I and II families can deliver. Freescale says the MPC8541/E can process encrypted packets at about 400–600Mb/s, roughly twice the rate of the PowerQuicc II Pro. Table 1 compares the features of the PowerQuicc III MPC8541/E with those of the PowerQuicc II Pro family, an existing PowerQuicc II processor (the MPC8272), and two competing communications processors.

Alchemy's MIPS32-based Au1550 will probably offer Freescale the stiffest competition. It's scheduled to hit the market about a year before the new PowerQuicc Pro processors, and it crams a SafeXcel IP security engine (licensed from SafeNet), a DDR SDRAM controller (slightly faster at 400MHz), a USB host/device controller, and two Ethernet controllers into a smaller package. Nevertheless, the new PowerQuicc II Pro processors have several advantages over the Au1550: higher core clock frequencies; larger CPU caches; Hi-Speed USB (40 times faster than USB 1.1); Gigabit Ethernet; and—in some parts—64-bit PCI and DDR SDRAM interfaces. The PowerPC cores also have a 64-bit FPU, although floating-point math is less useful for communications than the 32 × 16-bit multiply-accumulate unit in the Au1550's MIPS32 core. On balance, the PowerQuicc

Feature	Freescale MPC8349E	Freescale MPC8347E	Freescale MPC8343E	Freescale MPC8541E	Freescale MPC8272	AMD Au1550	Intel IXP425
General Features							
Chip Family	PowerQuicc II Pro	PowerQuicc II Pro	PowerQuicc II Pro	PowerQuicc III	PowerQuicc II	Alchemy	XScale
CPU Core	PowerPC e300	PowerPC e300	PowerPC e300	PowerPC e500	PowerPC 603e	Enhanced MIPS32	StrongARM
Core Freq	400–667MHz	266–667MHz	266–400MHz	533–833MHz	266–400MHz	333–500MHz	266–533MHz
Bus Freq (external)	133–167MHz	133–167MHz	133–167MHz	133–167MHz	33–100MHz	100–200MHz	133MHz
DDR Freq	266–333MHz	266–333MHz	266–333MHz	266–333MHz	—	200–400MHz	—
L1 Cache (I/D)	32K/32K	32K/32K	32K/32K	32K/32K	16K/16K	16K/16K	32K/32K
L2 Cache	—	—	—	256K	—	—	—
FPU	64-bit	64-bit	64-bit	64-bit	64-bit	—	—
MAC Unit	—	—	—	—	—	32 x 16-bit	—
MMU	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Voltage (Core)	1.2V	1.2V	1.2V	1.2V	1.5V	1.2V	1.3V
Voltage (I/O)	3.3V I/O 2.5V DRAM	3.3V I/O 2.5V DRAM	3.3V I/O 2.5V DRAM	3.3V I/O 2.5V DRAM	3.3V	3.3V I/O 2.5V DRAM	3.3V
Power (typical)	~0.8–1.3W	~0.8–1.3W	~0.8–1.3W	3.2–5.4W	1.2W @ 400MHz	<500mW @ 400MHz	1.0–1.5W @ 400MHz
Package	TBGA-672 35 x 35mm	TBGA-672 35 x 35mm PBGA-556 29 x 29mm	PBGA-556 29 x 29mm	PBGA-783 29 x 29mm	PBGA-516 27 x 27mm	PBGA-483 21 x 21mm	PBGA-492 30 x 30mm
Production	2Q05	2Q05	2Q05	4Q04	Now	2Q04	Now
Price (10K)	See Price & Availability Box			$72–102	$23.33–31.64	$21.26–33.75	n/a
On-Chip Peripherals							
DRAM Controller	DDR/SDRAM	DDR/SDRAM	DDR/SDRAM	DDR/SDRAM	SDRAM	DDR/SDRAM	SDRAM
Bus Width	32/64 bits	32/64 bits	32 bits	64 bits	64 bits	16/32 bits	32 bits
ROM-SRAM-Flash I/F	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DMA Controller	Yes	Yes	Yes	Yes	Yes	DMA + DDMA	PCI only
Serial Controllers	3	3	3	3	5	4	2
Serial Protocols	I^2C, SPI	I^2C, SPI	I^2C, SPI	I^2C, SPI	I^2C, SPI, TDM	AC'97, I^2S, SPI, SMBus	n/a
PCI Controller	2 x 33/66MHz*	1 x 33/66MHz	1 x 33/66MHz	2 x 33/66MHz*	1 x 33/66MHz	1 x 33/66MHz	1 x 33/66MHz
USB Controller	1x Host/device** 2.0 1x Host 2.0	1x Host/device** 2.0 1x Host 2.0	Host/device** 2.0	—	Host/device 1.1	Host/device* 1.1	Device 1.1
Ethernet MAC	2 x Gigabit	2 x Gigabit	2 x Gigabit	2 x Gigabit 2 x 10/100	2 x 10/100	2 x 10/100	2 x 10/100
Utopia 2 I/F	—	—	—	—	Yes	—	Yes
UART	2	2	2	2	1	3	2
GPIO (Max)	~64	~52	39	~32	83	43	16
Real-Time Clock	1	1	1	1	1	1	—
Time-of-Year Clock	—	—	—	—	—	1	—
Security Engine	Freescale SEC 2.0	Freescale SEC 2.0	Freescale SEC 2.0	Freescale SEC 2.0	Freescale SEC 1.0	SafeNet SafeXcel IP	Intel
HW Random Num	Yes	Yes	Yes	Yes	Yes	Yes	—

Table 1. Freescale's new PowerQuicc II Pro family and the new PowerQuicc III chips boast higher clock speeds, faster memory systems, and gigabit network interfaces—at the cost of larger packages. To conserve space, this table omits the four new PowerQuicc chips that lack a built-in security engine; their part numbers omit the "E" suffix, but, otherwise, the chips have the same features. For comparison, the table shows an existing PowerQuicc II (the MPC8272), AMD's Alchemy Au1550, and Intel's XScale IXP425. *The two 32-bit PCI interfaces can operate as a single 64-bit PCI interface. **The USB 2.0 host/device controllers also support the USB On-the-Go standard. n/a: not available.

processors are capable of delivering much more I/O throughput than the Au1550 can, but they will ship about a year later.

Intel's XScale IXP425 is another similar processor with a built-in security engine, albeit without a hardware random-number generator. Its StrongARM-derived core can reach 533MHz, which is less than the PowerPC e300 and e500 cores but still adequate for the intended applications. Like the Au1550, the IXP425 is handicapped by slower network interfaces (no Gigabit Ethernet); a USB 1.1 controller (device only, requiring an external host controller); and, additionally, a

New PowerPC Cores Promise Higher Performance

Freescale's roadmap for the PowerQuicc line shows a transition to four PowerPC cores: the e300, e500, e600, and e700. By surrounding these cores with different combinations of on-chip peripherals and I/O interfaces, Freescale plans to offer a PowerQuicc family for almost every conceivable communications application. The overall trend is toward higher performance on all fronts: CPUs, memory systems, peripheral I/O, and network connections. In addition, Freescale will create PowerQuicc-based semicustom designs for customers that want something a little different.

The PowerPC e500 core was announced at Embedded Processor Forum 2001 (see *MPR 7/16/01-01*, "Speedier Book E Encore") and was the first Motorola PowerPC core to support the Book E embedded-processing extensions that IBM and Motorola added to the PowerPC architecture in 1999. (See *MPR 5/10/99-02*, "PowerPC Architecture Gets Makeover.") Later in 2001, Motorola announced the PowerQuicc III MPC8540, the first processor to use the e500 core. (See *MPR 12/17/01-01*, "Motorola's MPC8540 Parts OCeaN.") All PowerQuicc III chips use the same core, differing only in their clock frequencies, mix of on-chip peripherals, and I/O interfaces.

Freescale's PowerQuicc II Pro family marks the debut of the PowerPC e300 core. It is derived from the PowerPC 603e, an embedded version of a low-power desktop processor found in some early Power Macs. The e300 has several performance enhancements over the 603e. Its instruction and data caches are twice as large (32K vs. 16K), with greater set-associativity (eight-way vs. four-way) and parity checking. Core frequencies will reach 667MHz for PowerQuicc II Pro chips manufactured in Motorola's HIP7b 0.13-micron CMOS process, as opposed to 400MHz for existing PowerQuicc II chips in the same process.

The PowerPC e600 and e700 cores have yet to appear in any chips. The e600 will be a fully compatible 32-bit derivative of the PowerPC G4 core in Motorola's current MPC74xx-series processors. (Don't confuse the Motorola G4 with the 64-bit IBM PowerPC 970 processor found in Macintosh G4 desktop computers and blade servers.) The e600 will also support multicore designs. Freescale's roadmap calls for the e600 to surpass 2.0GHz in future MPC86xx-series processors, but the roadmap is vague about dates.

Even greater performance is expected of the PowerPC e700 core, a 32/64-bit CPU that aims at clock speeds exceeding 3.0GHz in a 90nm fabrication process. It will appear in future MPC87xx-series processors, but the roadmap doesn't say when. *MPR* doesn't expect it before 2006. Freescale needs time to port existing designs to 90nm and emerge from the distractions of its spinoff from Motorola and its anticipated initial public offering.

slower memory system (SDR SDRAM at 133MHz). The IXP425 is two years old and due for a refresh.

PowerQuicc Stays the Course

Motorola was among the first companies to anticipate the explosive demand for communications processors in the 1990s. The first PowerQuicc was the MPC860 of 1993, which improved upon Motorola's earlier 68K Quicc family by substituting a PowerPC CPU core for the 68360. (See *MPR* 5/10/93, p. 13, "68360 Provides Sophisticated Communications.") The PowerQuicc chips soon accounted for most of Motorola's embedded PowerPC sales and continue to be strong sellers, even after many other companies rushed into the market in the late 1990s. When the market imploded during the tech recession, Motorola stuck with its long-term strategy and never stopped improving the product line.

With these latest introductions, Motorola's semiconductor group—now spun off as the wholly owned Freescale subsidiary, pending an initial public offering—is renewing its commitment to the PowerQuicc line. Instead of downsizing its vision, Freescale is touting a roadmap that forecasts even higher performance and more-powerful CPUs. No other vendor offers such a broad selection of communications processors. If Freescale can manage the formidable business challenge of spinning off from Motorola and maintaining its rapid pace of product development, the company will be well poised to take advantage of the coming market rebound.