System-on-a-Chip with Security Modules for Network Home Electric Appliances

● Hiroyuki Fujiyama

(Manuscript received November 29, 2005)

Home electric appliances connected to the Internet and other networks allow users to easily access a variety of information and services. However, the users of such appliances are increasingly exposed to the threat of information leaks, unauthorized access, and other risks. Therefore, home electric appliances connected to networks must provide adequate security functions. This paper introduces three new Fujitsu system-on-a-chips (SoCs) developed for network home electric appliances. These SoCs provide network, security, and control functions for home electric appliances and peripheral components. The new SoCs can also provide these functions for a digital home system and process the data of the system's devices. Moreover, when connected to an existing system, they can be used as slave processors for network and security processing.

1. Introduction

In the past, very few home electric appliances were connected to a network. However, increasing numbers of these appliances are now being connected to the Internet just like PCs.

Home electric appliances connected to the Internet and other networks allow users to easily access a variety of information and services. However, in contrast with the convenience offered, the users of such appliances are increasingly exposed to the threat of information leaks, unauthorized access, and other risks through networks. Consequently, home electric appliances connected to networks must provide adequate security functions.

This paper introduces three new system-on-a-chips (SoCs) developed for networked home electric appliances. As implied by the name, these devices are complete computer systems on a single chip. SoCs can be used as the CPUs for home electric appliances and peripheral components or to build network and security systems, control devices, and process the data of those devices. Moreover, when connected to an existing system, SoCs can be used as slave processors for network and security processing.

2. Developing SoCs for network home electric appliances

To provide more addresses for the ever-growing Internet and make other improvements, the Internet protocol will be upgraded from the current Internet Protocol Version 4 (IPv4) to IPv6. IPv6 provides sophisticated security as a standard feature and enables easy connectivity. In addition to typical devices such as PCs that are connected to the Internet, home electric appliances are now being connected to enhance convenience for users. Low-cost and easy-to-use networking modules should be developed for home electric appliances to make such connections more popular. Toward this end, Fujitsu has developed these SoCs with security modules for network home electric appliances.

As more and more home electric appliances are connected to networks, it will become increasingly important to have strong security systems that protect the personal data they contain. Moreover, it is preferable for such a security system to be used simply and reliably from applications. The Internet Engineering Task Force (IETF) has developed a security system that meets these requirements. This system, called IPsecurity (IPsec), will be supported by IPv6 as a standard feature. In terms of performance, however, it is difficult to realize IPsec in the embedded microcontrollers used in general home electric appliances because this system requires a lot of processing. Therefore, increasing the level of performance also increases the cost and power consumption.

The new SoCs with security modules for network home electric appliances solve these problems of performance, cost, and power consumption. These SoCs are used in encryption processing to divert the software overhead to hardware, thereby improving the processing efficiency and reducing the CPU load.

The interface function of these SoCs enables network connections based on the microcontrollers generally used in existing home electric appliances. By implementing this interface function and the program group required for networking as firmware, the SoCs enable easy, low-cost network connections.

The following sections describe the three new SoCs developed for network home electric appliances. The SoCs are the MB91401, an advanced general-purpose SoC, and the MB91402 and MB91403, which have embedded RAM.

3. Advanced general-purpose SoC: MB91401 (for evaluation)

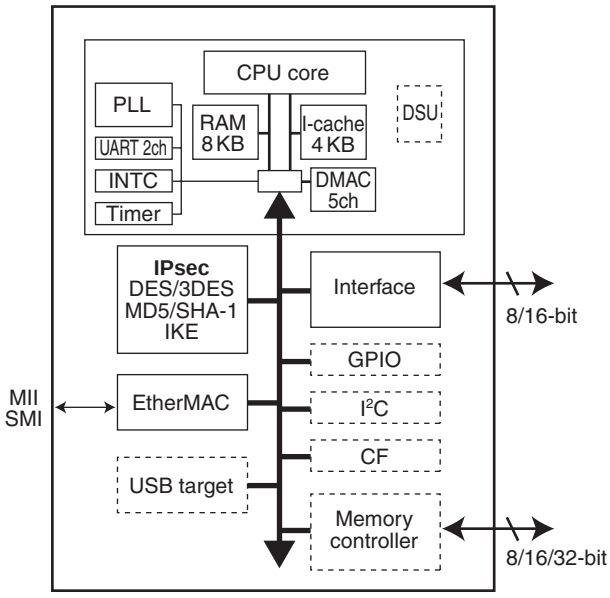
The MB91401 is the first SoC developed for network home electric appliances to have a security system and is designed to be used for ES-level evaluation purposes.

To support network and security systems, the MB91401 uses a Fujitsu-proprietary FR 32-bit RISC microcontroller for its CPU core. The MB91401 is designed to support a security system and IPv6 without placing a burden on the CPU. It also offers various interface features so it can be readily used in many types of home electric appliances. **Figure 1** shows the MB91401's block diagram.

The following describes the main features of the network and security systems of the MB91401.

3.1 Network system

The MB91401 connects to a network using 10/100 M Ethernet media access control (MAC), which conforms to IEEE802.3. This standard media-independent interface (MII) enables easy connection to general physical layer (PHY)



CF: CompactFlash
DES: Data Encryption Standard
DMAC: Direct Memory Access Controller
DSU: Debug Support Unit
GPIO: General Purpose Input/Output
I^2C: Inter Integrated Circuit bus
IKE: Internet Key Exchange
INTC: Interrupt Controller
MD5: Message Digest 5
SHA-1: Secure Hash Algorithm 1
UART: Universal Asynchronous Receiver Transmitter

Figure 1
MB91401 block diagram.

devices. The internal registers conform to a conventional LAN controller as much as possible to facilitate the use and development of middleware such as drivers.

A major feature of the MB91401 is its support of packet filtering in the L2, L3, and L4 network layers. By accepting only the required packets, this SoC protects its CPU against overloading. This function also enhances security because unnecessary packets can be eliminated without software intervention.

Filtering is done for differences in the protocol headers of IPv4 and IPv6. MAC has an embedded send buffer of 1.5 KB, which is the largest packet size in IPv6. It also has an embedded high-capacity receive buffer of 9 KB so it can instantaneously receive packets at up to 100 Mb/s without error.

3.2 Security system supported by hardware

IPsec is used as the standard protocol security system over the Internet. IPsec uses an encryption function to prevent surreptitious reading, an authentication function to prevent spoofing, and a function for safely exchanging encryption keys. The MB91401 hardware supports these IPsec functions. It also supports Triple DES[note 1)] secret-key cryptosystems and the MD5[note 2)] and SHA-1[note 3)] hash functions. Moreover, it has an embedded processor that can be used for Internet Key Exchange (IKE) and public key cryptosystems.

The MB91401 mainly supports the following security functions:

– DES-ECB, DES-CBC, 3DES-ECB, and 3DES-CB mode
– MD5, SHA-1, HMAC-MD5, and HMAC-SHA-1 mode
– Internet key exchange DH groups: 1 (MODP 768 bits) and 2 (1024 bits)

The MB91401's IPsec Manager processes security data transfers. It provides a fivefold increase in transfer rate compared to that achieved when only the CPU is used and also reduces the CPU load by 80% or more. By leaving the security system to hardware and providing an IPsec Manager, the MB91401 enables high-speed processing. Encryption is about 200 times faster and the key exchange algorithm about 100 times faster than when these processes are done using only software running on the CPU.

The security system can be used by non-IPsec systems on networks. The encryption and hash functions can also be used to secure external memory data. By providing the appropriate device drivers, these functions can easily be used from applications.

3.3 External interfaces

The MB91401 can be used independently as a controller for home electric appliances because its CPU core contains standard peripheral circuits such as an interrupt controller (INTC), timer, DMA controller (DMAC), and serial interface (UART). When mounted in a home electric appliance or another system, the MB91401 can provide network connectability with strong security measures.

The MB91401 has an interface for easy connection to the system memory bus. This interface uses high-capacity send and receive FIFOs and a communication register. These components make it easy to add a network function to an existing system. Moreover, the MB91401 can readily provide system security when connected to an existing system as a slave processor.

3.4 Peripheral interface

The MB91401 provides a USB target

note 1) "DES" is an abbreviation for the Data Encryption Standard: a widely used secret key cryptosystem. Triple DES repeats DES three times to enhance encryption strength.
note 2) Abbreviation of Message Digest 5: a widely used hash function.
note 3) Abbreviation of Secure Hash Algorithm 1: another widely used hash function.

function, card interface, inter-IC interface, and a network function. Therefore, the appropriate connection method can be selected for the device. The MB91401 can be used as a file encryption engine via USB or connected to a wireless LAN card via the card interface.

4. Two SoCs with embedded RAM: MB91402 and MB91403

With its various interfaces, the MB91401 is designed to connect a wide range of devices to a network. The MB91402 and MB91403 are designed to be embedded in home electric appliances for relatively inexpensive connection to a network or factory automation (FA) system. The MB91402 and MB91403 have an embedded high-capacity RAM. **Figure 2** shows the block diagram of the MB91402/MB91403.

A major difference between these SoCs and the MB91401 is their high-capacity 64 KB RAM. Also, the USB and card interface of the MB91401 have been omitted, and its pin count has been reduced from 240 to 144 so it can be packaged using a QFP (Quad Flat Package). A single 3.3 V power supply is used for system downsizing and cost reduction. In addition, the AES,[note 4)] which is becoming increasingly popular as a next-generation encryption standard, has been added to improve over security systems such as Triple DES. The embedded memory is effective in terms of cost reduction and security measures because data can be processed within the SoC. If more memory is required, the MB91402 and MB91403 can support external memory through a mode setting. Furthermore, these SoCs can be used in conjunction with an external, rewritable flash memory.

The MB91402 was developed for applications that require no security, for example, IPv4 or an internal gateway. This SoC has exactly the same features as the MB91403 except for the security function. The MB91402 can be replaced with the MB91403 when a system needs security because they are pin-compatible. **Table 1** shows a functional comparison of the MB91401 and MB91402/MB91403.

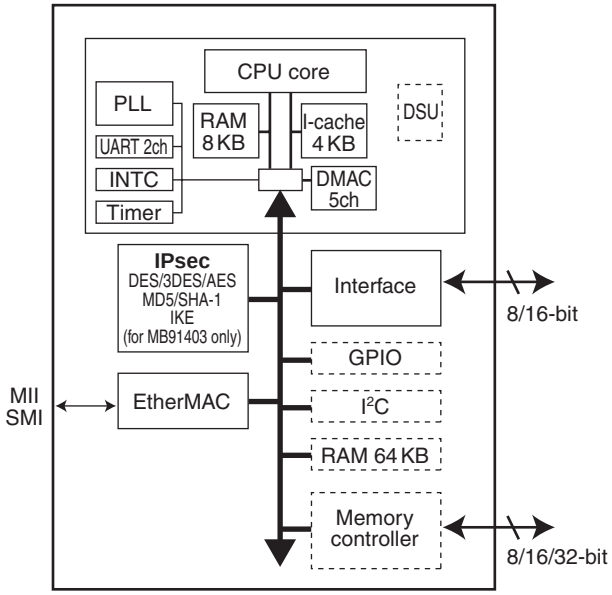


Figure 2
MB91402/MB91403 block diagram.

5. Software products and development environment

This section describes some software products that take advantage of the performance and functions offered by these SoCs and a development environment for employing these SoCs in digital home electric appliances.

5.1 Software products

To achieve the network function, a TCP/IP protocol stack that supports IPv4 and IPv6 is also provided along with the SoCs (**Figure 3**). The security cryptosystem's DES, AES, and hash functions were developed as drivers to enable easy use as functions from applications. Moreover, software products to support various types of encryption applications, including RSA applications, are now being prepared.

note 4) Abbreviation of Advanced Encryption Standard: a secret key cryptosystem established by the National Institute of Standards and Technology (NIST) as the successor to DES.

Table 1
Functional comparison of MB91401 and MB91402/MB91403.

			MB91401	MB91402	MB91403
CPU	CPU core		FR60 series core	FR60 series core	FR60 series core
	Instruction cache		4 KB	4 KB	4 KB
	Data RAM		8 KB	8 KB	8 KB
	UART		2 channels	2 channels	2 channels
	External interruption		3 channels + NMI	2 channels	2 channels
	DMA (without external terminal)		5 channels	5 channels	5 channels
	Reload timer		3 channels	3 channels	3 channels
	DSU		3	3	3
Peripheral module	MAC controller		○	○	○
		Receivable FIFO size	9 KB	3 KB	3 KB
	External IF		○	○	○
		Receivable FIFO size	3 KB	1.5 KB	1.5 KB
	Memory IF		○	○	○
		Address bits	24 bits	23 bits	23 bits
		Data bits	8 bits/16 bits/32 bits	8 bits/16 bits	8 bits/16 bits
		Chip selection	3	2	2
		Applicable device	ROM/RAM	ROM/RAM/SDRAM/FCRAM	ROM/RAM/SDRAM/FCRAM
	I^2C IF		○	○	○
		Applicable mode	Typical (100 kb/s)	Typical/high-speed (400 kb/s)	Typical/high-speed (400 kb/s)
	GPIO		8 pins max.	26 pins max.	26 pins max.
		Input change interruption port	—	○ (4 pins)	○ (4 pins)
	Encryption/authentication macro		○	—	○
		DES/3DES	○	—	○
		AES	—	—	○
		HMAC-MD5/SHA-1	○	—	○
		REDC	○	—	○
		IPsec Manager	○	—	—
	Internal RAM		—	○ (64 KB)	○ (64 KB)
	USB IF		○ (FS mode)	—	—
	CARD IF		○ (CF card)	—	—
Package			FBGA-240	LQFP-144	LQFP-144
Operating frequency			66 MHz max.	33 MHz max.	33 MHz max.
Power supply			2 power supplies (1.8 V/3.3 V)	1 power supply (3.3 V)	1 power supply (3.3 V)

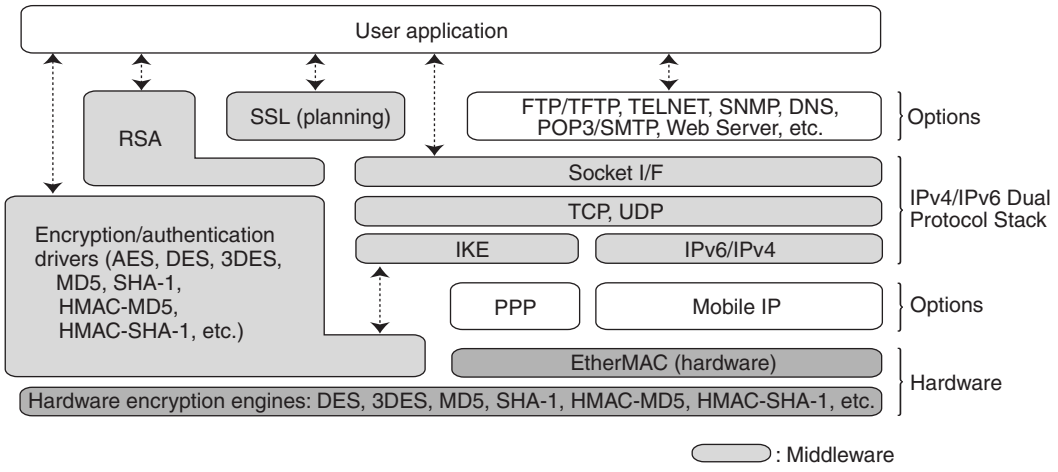


Figure 3
Software components for network and security functions.

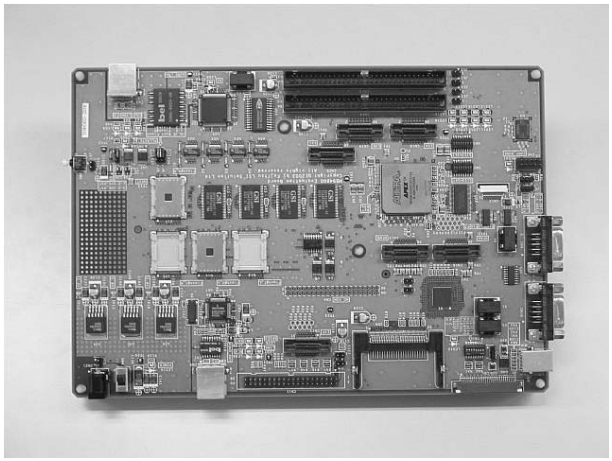


Figure 4
MB91401 evaluation board.

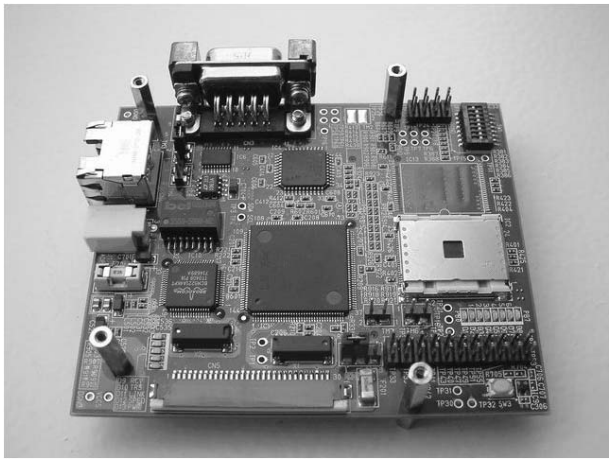


Figure 5
MB91402/MB91403 evaluation board.

5.2 Development environment

These SoCs can operate in Fujitsu's SOFTUNE V6 integrated development environment. This environment supports the MB2198-01 series of FR family emulators to enable real-time debugging.

Figure 4 shows the MB91401 evaluation board. This board has USB connectors and card slots to enable the use of various MB91401 peripheral interfaces. Also, to facilitate the addition of circuits, it has an FPGA with which circuits can be written and placed on the memory bus.

Figure 5 shows the MB91402/MB91403 evaluation board. This downsized board has the minimum evaluation features required to make full use of the MB91402 and MB91403. If necessary, the board can be embedded in a device for evaluation.

6. Conclusion

This paper introduced three new Fujitsu SoCs with security modules developed for network home electric appliances: the MB91401, MB91402, and MB91403. These SoCs overcome the previous performance and security obstacles so that devices can now be safely and easily connected to

networks.

In the future, as home information appliances are put to increasingly diverse uses in the growing network society, SoC performance and functions will be further optimized. In addition, simpler and more secure network application technologies will be provided.

Hiroyuki Fujiyama, *Fujitsu Ltd*.
Mr. Fujiyama joined Fujitsu Ltd. in 1986, where he has since been engaged in research and development of microprocessors. His current focus of work is on network and security system LSIs.