FIDES: A Multi-Core Platform to Enhance Robustness of Embedded Systems

INOUE Hiroaki, SATO Naoki

Abstract

High-end embedded systems, such as digital home appliances, mobile phones and automotive information systems, are likely to require a mechanism to extend system functions by adding software after shipment. This paper reports an asymmetric multi-core platform, known as FIDES, which enhances robustness of such embedded systems. The FIDES platform is based on multi-core technology and features high performance with low power consumption. Moreover, the platform helps improve system reliability by separately executing basic functions (e.g., pre-installed applications) and additional functions (e.g., downloaded applications) on different processors.

Keywords

multi-core, native application, dynamic add/execute function, security

1. Introduction

It is no exaggeration to say that performance improvement in digital home appliances, mobile phones and automotive information systems has been supported by high clock frequency based on semiconductor technology scaling. However, the scaling has not only brought such benefits as the improvements in clock frequencies but on the downside, it has also brought about problems such as significant increases in power consumption. As an approach to solving the problem of power consumption, multi-core technology is attracting attention with regard to its capability of improving performance by utilizing parallel processing instead of improving the clock frequency.

NEC and NEC Electronics became aware of the multi-core technology and its power saving capability from a very early stage and became industry leaders in developing a large number of research results in the field of embedded systems. These included the MP211[1-4] mobile application processor with asymmetric multi-core technology, the MPCore that is a symmetric multi-core processor developed jointly with ARM Ltd. and the Pinot that is a control-flow parallel multi-core processor featuring automatic parallel processing[5].

In addition to providing benefits such as performance improvement and power saving by means of multi-core technology, NEC and NEC Electronics are also conducting R&D into multi-core technology that provides new values created by redefining multi-core's characteristics. These include: system robustness, for digital home appliances, mobile phones and automotive information systems that will require functional extensions based on software additions after shipment.

Fig. 1 shows the positioning of multi-core technology at NEC and NEC Electronics. This paper introduces the FIDES multi-core platform[6], which is being developed to meet the functions of dynamic addition (downloading) and execution of native applications that are expected to be supported by various systems in the future.

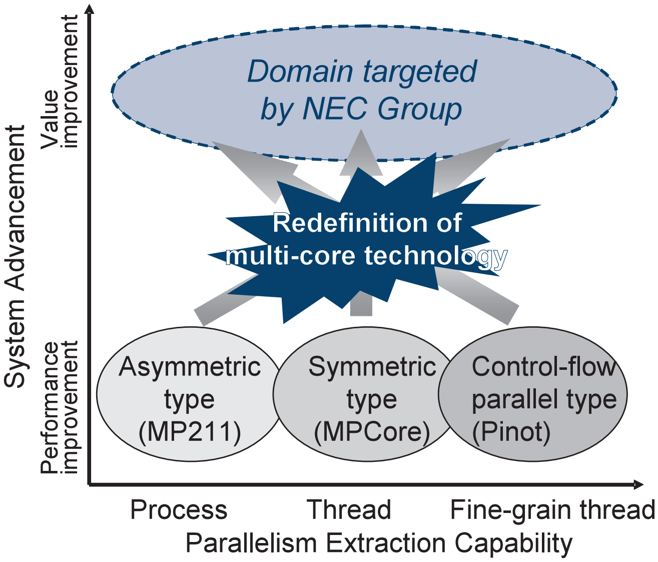


Fig. 1 Positioning of multi-core technology in the NEC Group.

2. FIDES Multi-Core Platform

It is expected that more and more future systems will support functions to enable dynamic addition and execution of native applications. Unlike traditional, non-native applications such as Java, native applications can run in the same execution environment as the basic application of the system so that they can be used to implement functions very quickly and with flexibility. This facility allows users to add the desired functions to the system even when it is in use.

Nevertheless, if a newly downloaded native application is faulty, the system will not be able to operate normally. In addition, if the downloaded application contains a virus, then there will also be a risk of system abuse. In this regard, the flexibility provided by the function for dynamic addition and execution of native applications is accompanied with the potential for problems related to the system robustness.

To deal with this problem and improve the system reliability, NEC and NEC Electronics have developed a multi-core platform that makes it possible to execute the basic functions of the system as well as additional functions, which include downloaded applications, on different processors. The multi-core platform is named “FIDES” after the Latin word that means trust.

Fig. 2 shows the configuration of the FIDES asymmetric multi-core platform that is composed of three processor cores. In this example, execution environments called the base domain; trusted domain and the untrusted domain are running on each processor. Here, the base domain is provided in order to execute the applications for the basic functions of the system. Thus, the externally downloaded native applications are never executed in the base domain. On the other hand, the trusted domain and the untrusted domain are provided in order to execute additional functions such as downloaded applications, with the trusted domain executing the applications that are guaranteed to be trustworthy and the untrusted domain for executing any suspect applications. This configuration makes it possible to ensure a higher safety level between the additional functions as well as between the basic and the additional functions.

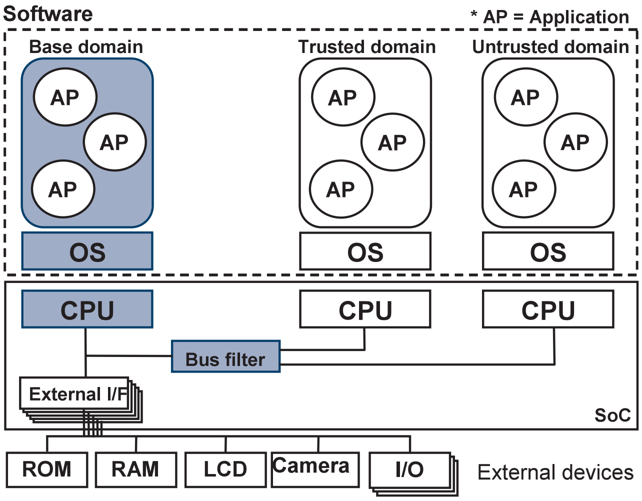


Fig. 2 FIDES multi-core platform.

The platform is characterized by the provision of executing environments using different core processors according to the reliability of the native applications. As a result, even when a downloaded application contains a bug or virus, its effects are limited to within the trusted or untrusted domains and the applications in the base domain are not affected. Furthermore, since the trusted and untrusted domains are working on different core processors, even if a domain is affected by a bug or virus, it can be restored independently from the base domain.

3. Technology Supporting the FIDES Platform

The FIDES multi-core platform that was introduced in Section 2 above was implemented by overcoming the following three major technical issues.

1) Separation of the resources shared by the core processors.
2) Increase in the memory required by the multiple execution environments.
3) Control of the security levels of the core processors.

NEC and NEC Electronics have recently developed a world-first highly reliable multi-core platform for embedded systems in solving the above problems by combining the appropriate technologies owned by the two corporations. The following sections will describe each of these technologies in detail.

3.1 Bus Filter Logic

In ordinary multi-core platforms, external resources such as the memory, LCD and camera are designed to be shared by all of the core processors as shown in Fig. 2. However, if a bug or virus is included in a downloaded application in the trusted or untrusted domains, its result would be to affect the basic applications in the base domain via these shared resources. For example, with the memory resource, a bug or virus is capable of halting the operation of the basic functions by destroying the memory area used by the applications in the base domain. This makes it necessary to use a technology for restricting illegal access to the shared resources, which is the bus filter logic.

Fig. 3 shows the configuration of the bus filter logic. It is connected to the system bus on the chip and monitors illegal access to the shared resources based on given setting information. The setting information for specifying the range of external resources that are accessible by each of the core processors can be updated only from the base domain. Namely, in Fig. 3, CPU #1 can read or write the memory in the address range #0 but it is allowed to read only the memory in the address range #1. This configuration protects the base domain from illegal access from either the trusted or untrusted domains.

3.2 XIP Kernels

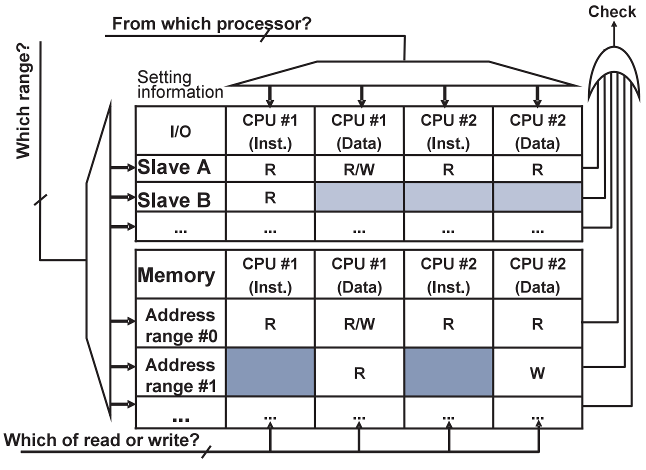
With ordinary multi-core platforms, the provision of an execution environment (kernel) for each processor can increase the system robustness but also results in an increase in the memory requirement, a characteristic that leads to an increase in the costs of embedded systems. The memory requirement of a single-processor kernel has traditionally been reduced using the XIP (Execute-In-Place) technology, which places the instruction area of the kernel and read-only data on the ROM and copies the normal data area in the RAM. At NEC, being aware of the memory requirement reduction capability of the single-processor kernel XIP technology and in order to reduce the memory requirement for the multi-core platform we developed the XIP kernels technology by extending the XIP technology for use in the multi-core platform.

Fig. 4 shows the concept of the XIP kernels technology. With this technology the instruction areas and read-only data areas of individual kernels in the ROM are shared by multiple kernels, and the normal data area is copied in the RAM area specific to each kernel in order to reduce the total amount of memory required by the multi-core platform. Each kernel is naturally capable of operating by using the same virtual addresses as the kernel in a single-core processor. This design makes it possible when the Linux kernel is used as the OS to reduce the static memory requirement by about 182% compared to the configuration in which the XIP kernels technology is not applied.

3.3 Security Domain Separation Technology

When downloading a native application and running it on a terminal, it is necessary to determine whether it should be run in the trusted or untrusted domains. FIDES employs a certification for identifying the domain running each native application. A native application is downloaded in the trusted domain when it is downloaded together with a certificate that it is trustworthy and in the untrusted domain when it is downloaded without a certificate. The downloading and certification checks are performed by the software named as the application manager in the base domain. The application manager is also used to assign the trusted or untrusted domains when the downloaded application is launched.(**Fig.5**)

When running an application, the system is required to control the available libraries, system calls and accessible files according to the reliability of the application. FIDES performs the control procedures for the access to the libraries, system calls and files by the software at the OS level as well as the control of the shared resource access using the bus filter logic



I/O	CPU #1 (Inst.)	CPU #1 (Data)	CPU #2 (Inst.)	CPU #2 (Data)
Slave A	R	R/W	R	R
Slave B	R			
...	...	...	...	...

Memory	CPU #1 (Inst.)	CPU #1 (Data)	CPU #2 (Inst.)	CPU #2 (Data)
Address range #0	R	R/W	R	R
Address range #1		R		W
...	...	...	...	...

Fig. 3 Bus filter logic.

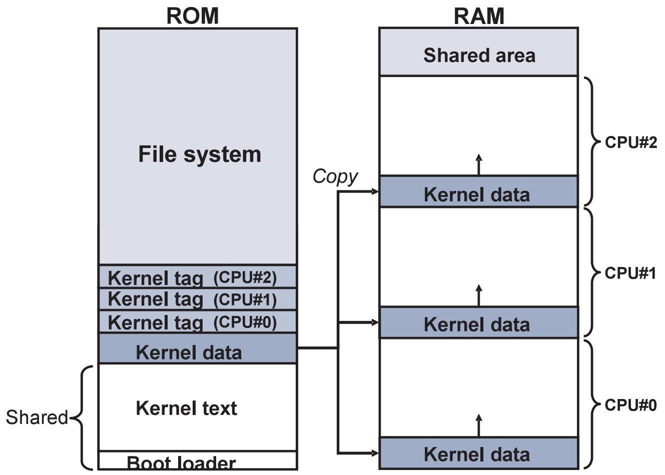


Fig. 4 XIP kernels.

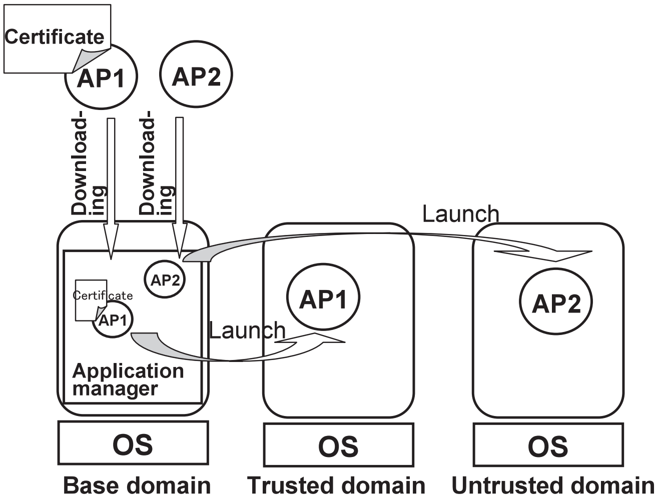


Fig. 5 Application manager

technology. The access control is performed according to the guidelines that are provided individually for the trusted and untrusted domains. This function enables for example, a control with which a system file is accessible only from the trusted domain and is inaccessible from the untrusted domain. The access controls at the hardware and OS levels are combined in order to provide the system with a higher reliability.

4. Conclusion

In this paper, we introduced the FIDES multi-core platform, which offers an enhanced level of reliability (robustness) for digital home appliances, mobile phones and automotive information systems that require functional extensions based on the addition of software after shipment.

We also described the highly reliable capability of FIDES by taking as an example the function for dynamic addition and execution of native applications, in which the basic functions of the system and its additional functions enabled by downloaded applications are executed on different processors.

The innovative technologies of NEC and NEC Electronics were also introduced as solutions for the three major technical issues that had to be overcome for the multi-core platform implementation. These included the bus filter logic technology, the XIP kernels technology and the security domain separation technology.

In the future, our R&D will be advanced in wider ranging applications fields, which will include digital home appliances, mobile phones and automotive information systems.

References

1) Edahiro, M. et al.: "MARUCHI-KOA MUKE SOHUTOUEA PURATTOFOOMU WO KAIHATSU SHI, KEITAI DENWAKI NI TEKIYO (Development of Software Platform for Multi-core Software, Its Application in Mobile Phone)," NIKKEI ELECTRONICS, March 28, 2005 issue, pp.125-136, 2005.
2) Torii, S. et al.: "Asymmetric Multi-Processing Mobile Application Processor MP211," NEC Journal of Advanced Technology, Vol.2, No.3, pp.204-210, 2005. URL http://www.nec.co.jp/techrep/en/r_and_d/a05/a05-no3/a0503p204.html
3) Torii, S. et al.: "A 600 MIPS, 120mW, 70μA Leakage Triple-CPU Mobile Application Processor Chip," ISSCC 2005 Proceedings, pp.136-137, 2005.
4) Sakai, J. et al.: "Multi-tasking Parallel Method on MP211 Multi-core Application Processor," COOLChips VIII Proceedings, pp.198-211, 2005.
5) Ohsawa, T. et al.: "Pinot: Speculative Multi-threading Processor Architecture Exploiting Parallelism over a Wide Range of Granularities," MICRO-38 Proceedings, pp.81-92, 2005.
6) Inoue, H. et al.: "FIDES: An Advanced Chip Multiprocessor Platform for Secure Next Generation Mobile Terminals," CODES+ISSS 2005 Proceedings, pp.178-183, 2005.
7) Hieda, S. et al.: "KEITAI TANMATSU-YO LINUX NI OKERU RISOOSU KANRI NO JITSUGEN (Implementation of Resource Management for Mobile Terminal Linux)," Journal of Information Processing Society of Japan "COMPUTING SYSTEMS," Vol. SIG03 (ACS8), No. 1, pp.1-11, 2005.

Authors' Profiles

INOUE Hiroaki
Assistant Manager,
System Devices Research Laboratories,
Central Research Laboratories,
NEC Corporation

SATO Naoki
Senior Manager,
System Platforms Research Laboratories,
Central Research Laboratories,
NEC Corporation

●**The details about this paper can be seen at the following.**
http://www.labs.nec.co.jp/Overview/soshiki/device/systemlsi.html