社団法人　情報処理学会　研究報告
IPSJ SIG Technical Reports

2007－ＳＬＤＭ－132（13）
2007／11／21

[フェロー記念講演] 社会情報基盤と Dependable VLSI

安浦　寛人†

†九州大学システム LSI 研究センター　〒819-0395 福岡市西区元岡 744
E-mail:　†yasuura@slrc.kyushu-u.ac.jp

あらまし　我々の日常生活は、大量の VLSI チップを内蔵した巨大な社会情報基盤に支えられている。その中で、種々のシステム障害が、物理的な故障、設計や製造や運用時の人的な誤り、あるいは悪意ある攻撃によって引き起こされている。本講演では、これらの VLSI システムにおける障害の原因とそれに対する対策について議論し、社会情報基盤を支えるディペンダブルな VLSI を設計する新しい技術に関する研究の方向性を示す。事例として、電子マネーシステムを取り上げて議論する。

キーワード　ディペンだビリティ、故障、社会情報基盤、価値、信用、VLSI

[Fellow Memorial Lecture]

Social Information Infrastructure and Dependable VLSI

Hiroto YASUURA†

† System LSI Reserch Center, Kyushu University　744 Motooka, Nishi-ku, Fukuoka, 819-0395 Japan
E-mail:　†yasuura@slrc.kyushu-u.ac.jp

Abstract　Our daily lives heavily depends on the social information infrastructure, which includes a huge numbers of VLSI chips. Various system failures are caused by physical faults in the circuits, human errors in design/fabrication/operation and malicious attacks.　In this talk, the causes and countermeasures of these failures of VLSI systems are summarized. The discussion leads a new direction of researches of design technology of dependable VLSI systems for social information infrastructures. As an example of social information systems, e-money systems are discussed in detail.

Keyword　dependability, failure, social information infrastructure, value, trustworthy, VLSI

1. Introduction

Information technology is now supporting various social systems including lifelines, traffic systems, governmental services, communication systems, economic systems and business systems. VLSI, software including embedded software, and information networks are the most important key components of the information technology constructing the social systems. We can call them social information infrastructure (see Figure 1) [1].

Since our daily lives heavily depend on the social systems, a failure or a suspension of the social information infrastructure has harmfully influences on life, property and privacy of each citizen. *Dependability* is a concept covering *availability, reliability, safety, confidentiality, integrity* and *maintainability* of the systems. The failures are caused by physical faults, human errors in design, fabrication and operation stages, and malicious attacks. Recently, social systems, most of which were designed before invention of information technology, are redesigned under the assumption of effective usage of information technology, which has

been developed and progressed in the last 50 years. In this context, establishing methodology of dependable social information infrastructures is urgent requirement [2].

In this paper, the causes of the failures of VLSI for social information infrastructures are analyzed in each stage of its life cycle. Countermeasures against causes of the system failures have been developed in the different fields, such as, fault-tolerant technologies for physical faults, verification and validation for human design errors, and security technology for malicious attacks. Unfortunately, since each technology has been developed independently, some measures interact with synergistic effects but some cancel out each other.

Firstly, we are discussing on requirements of dependability of social information infrastructure. As an example social information infrastructure, e-money systems and dependability of VLSI in it are discussed.

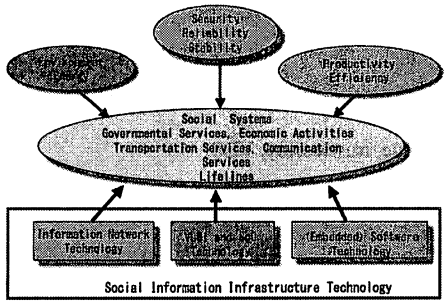

Figure 1. Social Information Infrastructure

2. Social Information Infrastructure [2,3]

In the 20th century, many *information and communication technologies* (ICT) were developed and introduced in various social systems. Since the rapid progress of these ICT causes the drastic reduction of time and space of information transfer, processing and storage, new schemes of social systems are redesigned on dependable social information infrastructure. The dependability is implemented based on reliable hardware, qualified software and secure networks. To develop dependable social information infrastructure, it is important that engineering solutions should provide information technologies on which society and human being can be safely depend.

There are various threats to dependability of information infrastructure.

Natural threat: Deep-submicron, high-speed and ultra-low-power technologies for hardware of information infrastructure are exposed to the treat of uncontrollable physical uncertainty caused by variation of fabrication and circumstances. Reliability and lifetime control are also important challenges in hardware design.

Threat of human errors: There are various threats of human errors in specification, design, fabrication and test processes of information systems and devices. Human errors in operation are the most critical problems of the social information infrastructure.

Threat of malicious attacks: Information systems are always exposed to the threats of malicious attacks by virus, worms and hacking. Attacks to the design data and illegal production also become serious problems in social systems.

In Figure 2, distribution of the threats is summarized in the different levels of systems, VLSI fabrication process, VLSI circuits, software and networks. In the process technology level, process variation causes uncertainty of circuit behavior, which is amplified by miniaturization of the

fabrication process. In the circuit level, variations of supply voltage and temperature also affect speed and correctness of circuit behavior. Design technologies called DFM (Design for Manufacturability) and DFT (Design for Testability) have been developed to conquer the difficulties. In the software and circuit layers, the numbers of design bugs are increasing in large and complicated system design. Verification and validation techniques have been developed and used in the practical design but increase of complexity of circuits and software brings rapid increase of design bugs. Moreover, systems are connected each other through networks and applications and environments of the systems are changing day by day. Thus it is inherently hard to define complete specifications of the systems in their design stages. Through the network and new application software down loaded in the systems, there are various threats of malicious attacks. Security is also a very important issue of system design.

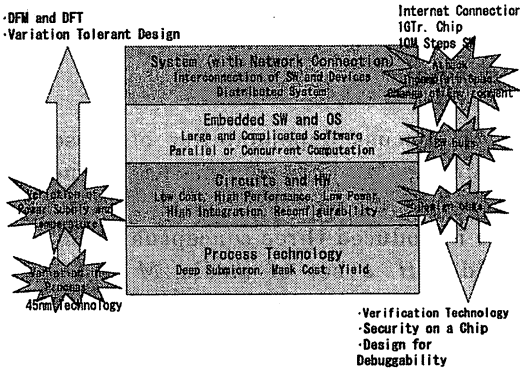

Figure 2. Threats of Social Information Infrastructure

In construction of social information infrastructure, we have to develop techniques to cope with the difficulties by these threats.

3. Dependability of VLSI

Dependability is defined as a property that a system sustains its service in allowance of users against physical faults by natural threats, human errors, and malicious attacks, in the parts of the system, the system itself and its environment. The causes of troubles are various physical faults in hardware, human errors in design/production /test/operation stages and attacks by virus, warms and hacking. The causes are called *faults* in general. A *fault* in a system may cause an *error*; a status of the system, which may causes a *failure* of the system. The *failure* degrades or stops the service of the system. A failure in the lower system becomes a fault of the upper system. A hierarchical dependability causal chain is depicted in Figure 3.

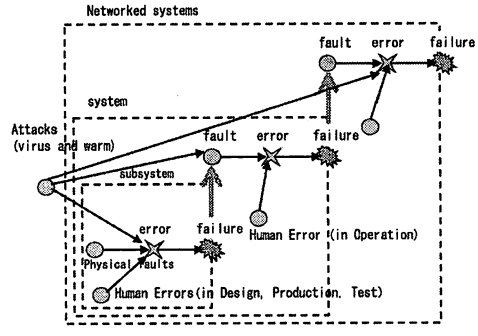

Figure 3. Hierarchy of Dependability in Systems

To implement a system with high dependability, we have to establish technologies for forecasting, detecting, suppressing, masking, preventing and repairing faults and /or errors (see Figure 4). If a failure happens, localization of its effect and quick recovery are also required.

The technologies for dependability have been developed as *FTC* (Fault Tolerant Computing) and *security*. Establishing the concept of dependable system design, we

should reorganize the concepts of *availability, reliability, safety, confidentiality, integrity* and *maintainability*. *Functional safety* is also an important concept in dependability [4].

Faults by the threats are caused in various stages in a life cycle of a system. The stages are *planning, design, fabrication, testing, distribution, operation* (or usage), and *abandonment.*

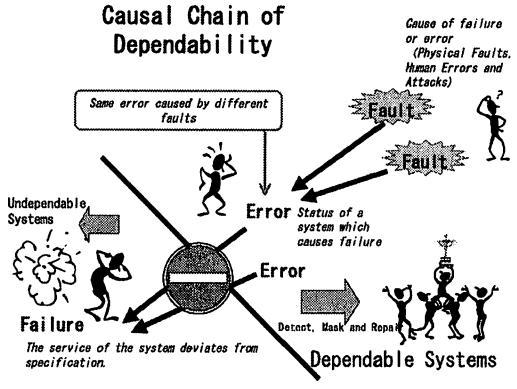

Figure 4. Dependable System

4. Dependability of *e-Money* System

Money system is one of the most important social systems which supporting our daily economic activities. As shown in Figure 5, human beings used *metal coins* more than 2,000 years as a medium of money. Value of money is guaranteed by metal itself, which is gold, silver or cupper. Conservation of total amount of value in the money exchanges is also guaranteed by the low of the indestructibility of the metals. In the 10th century, Chinese people invented *paper bills*. In the paper bill system, value is represented as printed information. To guarantee value and the money system, an issuer of the bills, which is mostly a government, arranged laws and technologies against counterfeits. Conservation still depends on the low of the indestructibility of papers.

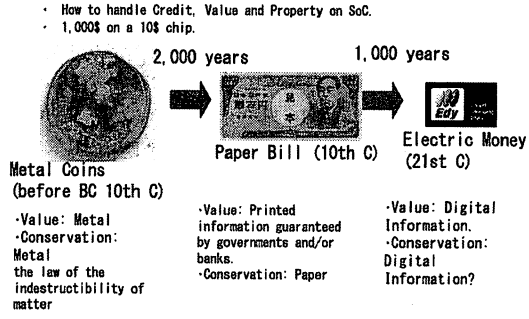

Figure 5. History of Money System

Now, we are introducing electric money (*e-money*) systems. Many trials and commercial usages of e-money are started. In e-money system, value is represented by digital data, which is inherently copy-free. Conservation of the total amount of money also depends on digital technology. Various techniques are adopted to keep the security of e-money system, but it has not been proven that e-money system is dependable as well as the existing money system based on metal coins and paper bills.

To discuss dependability of these money systems, we have defined a mathematical model of money systems (see Figure 6)[5]. We introduced three conceptual sets, a set of holder H, a set of media M and a set of values V. Coins, bills and smart cards (or VLSI chip in the cards) are the holders. The metal of coins, the printed information on the bills and digital data representing the values are the media, which are corresponding to the real values in the money systems. Using this model, we can compare these three money systems and discuss differences of dependability of each system.

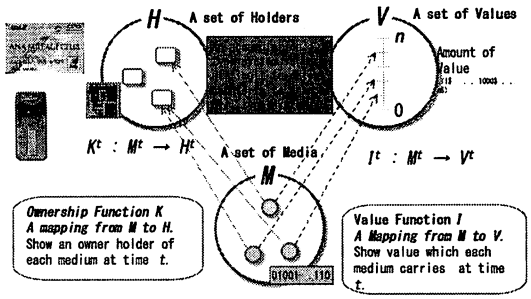

Figure 6. A Mathematical Model of Money System

From the discussions using the money model, we have a question whether the VLSI storing the value of money in a smart card is a part of money or mere purse. Holders of the coin and bill systems, coins and bills, are parts of money and designed, fabricated and issued by governments or central banks. But there is no discussion of mint bureau for VLSI for e-money. The discussion contains various social problems on e-money system. We also proved that the most popular e-money system, which is a stored value type storing only total amount of value, has a shortcoming on tolerance for inflation by introduction of counterfeits.

In Table 1, threats of VLSI for e-money systems are summarized. We suppose VLSI in smart cards, mobile phones, readers and writers of money exchange, and backend systems.

In planning stage, specification errors and theft of the specification are main threats. In design stage, design bugs and errors of assumptions may be major human errors. Estimation of the life span of the chip and effects of aging is an example of the important assumptions of design. Theft of design and illegal insertion of circuits are possible attacks. Since several circuits such as scan path for DFT are inserted in the design without direct control of designers automatically, insertion of extra circuits to read out the secret information or to write data illegally is possible fatal attack.

	Natural Threats	Human Errors	Attacks
Plan		Bug in Specification	Theft of Plan
Design		Design Bugs Errors in Assumptions	Theft of Design, Insertion of Illegal Circuit (IPs)
Fabrication	Process Variation	Errors in Fabrication	Illegal Sale of Extra Products
Test	Intermittent Faults	Errors in Test	Illegal Sale of Good Products
Distribution	Variation in Packaging	Mixture of Defectives Installation of Buggy Software	Theft Insertion of Illegal Software
Operation	Ageing and Particles Temperature and Supply Voltage Variation	Errors and Misunderstanding in Usage	Phishing, Virus Tampering, Tapping
Abandonment		Mis-Arrangement in Replacement	Theft of Logged Information

Table 1. Threats of LSI for e-Money Systems

Effects of process variation and human errors of fabrication are major threats in the fabrication stage. Fabrication is often done in factories independent from design organization by sending mask data to the factories. It is very hard to check by the designers how many wafers are really fabricated. There is a possibility that the fabrication people cheats designers and produce extra chips and sell them to a black market. How to control the number of fabricated chips is a very important problem of VLSI production for e-money systems. In test stage, we also have a similar problem that good chips are illegally classified as faulty chips and sell to the black market. Intermittent faults and detection errors are also problems.

In distribution stage, variations in packaging process and changes of environments will affect dependability of VLSI. Software is other source of bugs and attacks. In operation stage, since ordinal users used the system, misunderstanding of usage by users are major threats. How to design a system to avoid the misunderstanding is very important issue.

Variations of environments are threats of physical side, and phishing, virus and tampering are threats of malicious attacks.

Abandonment is the final stage of the life cycle of the chip. Theft of logged information from abandoned chips is also dangerous. How to erase information from the chip in abandonment is a design issue. Continuity is another important requirement of the social information infrastructure and the chip should be designed to move a new updated system with smooth replacement protocols.

5. Conclusion

We have discussed dependability of VLSI, which is used in social information infrastructure. Since fault tolerance, verification and security are discussed in the different societies, merging and unification of the concepts and techniques under the concept of dependability of whole VLSI system is requested.

As an example of the social information infrastructure, we discussed on e-money systems. From the discussion, we have clarified several requirements and problems for VLSI design and fabrication for e-money systems.

Dependability is a new value added feature of VLSI different from cost, performance and power consumption. Definition of the measure of dependability has not been concretely defined. We have to make the measure of dependability and to establish methods to estimate dependability in the early stage of design. Optimization techniques considering tradeoff among cost, performance, power and dependability are the first research goal.

Acknowledgement

The author expresses his sincerely application to the members of System LSI research center and SoC Lab. of Kyushu University for their discussions. He also thanks to researchers of JST CRDS for their discussions on the concept making of dependability. This work has been partly supported by the Grant-in-Aid for Creative Scientific Research No.1920004 and CREST DVLSI.

References

[1] Hiroto Yasuura, ``[Invited Paper] Toward Information Technology Treating "Value" and "Trust"'', *The 19th Workshop on Circuits And Systems in Karuizawa*, pp.313-318, Apr. 2006.

[2] Hiroto Yasuura, ``Dependable Computing for Social Systems (in japanese)'', *The Journal of IEICE*, Vol.90, No.5, pp.399-405, May. 2007.

[3] Hiroto Yasuura, "Dependability of VLSI for Applications in Social Information Infrastructure", International SoC Design Conference 2007, Oct. 2007.

[4] IEC TC65, "Functional safety of electrical /electronic /programmable electronic safety-related systems – Part 0 Functional safety and IEC 61508", *IEC/TR 61508-0*, Ed. 1.0, 2005.

[5] Kenichiro Oyama, Shunsuke Inenaga, and Hiroto Yasuura, "Modeling Electronic Money System Considering Its Value Preservation Formats (in Japanese)", IPSJ SIG Notes, 2007-MPS-63-(14), vol.2007, no.19, pp.53-56, march 2007.