Nobuyasu Kanekawa
Eishi H. Ibe
Takashi Suga
Yutaka Uematsu

Dependability in Electronic Systems

Mitigation of Hardware Failures, Soft Errors, and Electro-Magnetic Disturbances

Springer

Dependability in Electronic Systems

Nobuyasu Kanekawa · Eishi H. Ibe · Takashi Suga · Yutaka Uematsu

Dependability in Electronic Systems

Mitigation of Hardware Failures, Soft Errors, and Electro-Magnetic Disturbances

Springer

Nobuyasu Kanekawa
Hitachi Research Laboratory, Hitachi, Ltd.
Hitachi-shi 319-1292, Ibaraki, Japan
nobuyasu.kanekawa.ef@hitachi.com

Eishi H. Ibe
Production Engineering Research
Laboratory, Hitachi, Ltd.
Yokohama-shi 244-0817,
Kanagawa, Japan
hidefumi.ibe.hf@hitachi.com

Takashi Suga
Production Engineering Research
Laboratory, Hitachi, Ltd.
Yokohama-shi 244-0817,
Kanagawa, Japan
takashi.suga.pt@hitachi.com

Yutaka Uematsu
Production Engineering Research
Laboratory, Hitachi, Ltd.
Yokohama-shi 244-0817,
Kanagawa, Japan
yutaka.uematsu.ws@hitachi.com

ISBN 978-1-4419-6714-5 e-ISBN 978-1-4419-6715-2
DOI 10.1007/978-1-4419-6715-2
Springer New York Dordrecht Heidelberg London

Library of Congress Control Number: 2010937189

Preface

The word “dependability” that appears in the title is not used so often to be familiar with. The word has wider meaning and not only means “reliability” but also includes robustness, safety, security, resilience, and so on. Fault-tolerance technology that equips the redundant subsystems or components in preparation for failure in order to improve “reliability” has been used for many decades. In the meantime, J.C. Laprie expanded the term dependability as a wider concept in 1985 [1] because the meaning of “reliability” that the fault-tolerance technology treated had broadened. After then, dependability and dependable have been used in various fields to this day. Based on such situation and as I also belonged to the committees concerning “dependability,” I dare to use “dependability” in this text, thinking it is one of my vocations to spread the term.

As for terms related to reliability, the two terms have been used exclusively in Japanese. The Japanese word *shinrai-do* means quantitative index of reliability and the word *shinrai-sei* means qualitative character of reliability. In my personal opinion, the *shinrai-sei* may fall on the dependability.

As written in the title of this book, mitigation of hardware failures, soft errors, and electro-magnetic disturbances is indispensable in order to realize dependability of electronic systems. This book introduces authors’ original mitigation technologies of soft errors, electro-magnetic interference, and power supply noise, in addition to general mitigation technologies.

The authors have brought up the mitigation technology to realize dependability through a lot of industrial fields such as railroad, atomic energy, and IT networks. The dependable technology starts unifying with the latest LSI technology and being succeeded by the safety processor technology by on-chip redundancy. As a result, great reduction in costs will become possible by the effect of mass production of LSI technology in the future. I am convinced that we can contribute to safety and convenience of our ordinary life using dependable technology in more falimiar field such as automotives.

Lake Hatori, Japan — Nobuyasu Kanekawa
3rd May, 2010

Reference

1. J.C. Laprie, "Dependable Computing and Fault Tolerance: Concepts and Terminology," *Proceedings of the 15th IEEE International Symposium on Fault-Tolerant Computing, Austin, TX, USA*, pp. 2–11 (1985).

Acknowledgements

For Chapter 2, the authors would like to gratefully acknowledge Professors Emeritus T. Nakamura, M. Baba, Professor Y. Sakemi of Tohoku University for their helpful discussions and support for the database on nuclear reactions and high energy neutron irradiation tests. The authors also gratefully acknowledge Professor J. Blomgren and Dr. A. Prokofiev for their support of neutron irradiation experiments in TSL.

Dr. M. Nicolaidis of TIMA Laboratory, Dr. C. Slayman of Ops A La Carte and Dr. D. Alxandrescu of iRoC Inc. have made invaluable discussions toward new standards on neutron testing methods.

For Chapter 5, the authors would like to gratefully acknowledge Prof. Emeritus T. Takano,[1] Prof. T. Yamada, and Mr. K. Shutoh of ISAS (Space and Astronautical Science of Japan)[2] for giving us opportunity to pursue research on fault-tolerance through Hiten Onboard Computer development and its experiments.

The authors wish to express their gratitude to the members of Hiraiso Solar Terrestrial Research Center, Communication Research Laboratory of Japan for furnishing their solar flare data, and the members of the Orbit Planning Group, ISAS for furnishing their orbit data of Hiten.

The authors are grateful to Professors Emeritus Y. Tohma and T. Nanya of Tokyo Institute of Technology, Professors A. Avizienis[3] and D. Rennels of University of California, Los Angeles, Mr. H. Nakanishi,[4] ex-Deputy General Manager, Ohmika-Works, Hitachi, Ltd., and Dr. H. Ihara, ex-Chief Engineer of the Space System Division, Hitachi, Ltd., for their help and advices in pursuing research on fault tolerance.

The authors thank Mr. C. Glaser and the members of Springer for their efforts in publishing this book, and the members of Hitachi, Ltd., for their advices and efforts in implementing dependable systems stated in this book.

---

[1] Currently in Nihon University.

[2] Currently Institute of Space and Astronautical Science, Japan Aerospace Exploration Agency (JAXA).

[3] Currently in Vytautas Magnus University, Lithuania.

[4] Currently, President of Hitachi, Ltd.

After the correction of the text, the authors were informed news with the deepest sadness. We would like to pay a tribute to the memory and contribution of the late Dr. J. C. Laprie, who advocated the term “dependability” ([1] in Preface).

Contents

List of Figures

List of Tables

List of Acronyms

ACCM	AC common-mode conversion
ALARP	as low as reasonably practicable
ATP	automatic train protection
BGA	ball grid array
BOM	bill of materials
BQF	bypass quality factor
CDR	clock data recovery
CHB	checker board
CHBc	checker board complement
CMRR	common-mode reduction ratio
CORIMS	cosmic radiation impact simulator
COTS	commercial off-the-shelf
DDR	double data rate
DMAC	direct memory access controller
DOA	design on average
DOAV	design on average and variation
DOUB	design on upper bound
DRAM	dynamic random access memory
ECC	error correction code
EMC	electromagnetic compatibility
EMI	electromagnetic interference
ENIAC	electronic numerical integrator and computer
ESL	equivalent series resistance
ESL	equivalent series inductance
ESR	equivalent series resistance
FDTIM	frequency-domain target impedance meter
FIT	failure in time, failure unit
FPGA	field programmable gate array
FTMP	fault-tolerant multi-processor
GND	ground
HMR	hybrid modular redundancy
IFDIM	integrated power-supply frequency-domain impedance meter

ISAS	Space and Astronautical Science of Japan, currently Institute of Space and Astronautical Science, Japan Aerospace Exploration Agency (JAXA)
ISI	inter-symbol interference
JAXA	Japan Aerospace Exploration Agency
JPL	jet propulsion laboratory
LSI	large-scale integrated circuit
MASR	modified asymmetrical slew rate
MBU	multi-bit upset
MCBI	multi-coupled bipolar interaction
MCP	multi-chip package
MCU	multi-cell upset
MFTF	mean fluence to failure
MOS	metal oxide semiconductor
MTTF	mean time to failure
MTTR	mean-time to repair, or mean-time to restoration
NMR	N-tuple modular redundancy
OBC	onboard computer
OLTP	online transaction processor
OSPM	operating system power management
PCB	printed circuit board
PCSE	power cycle soft error
PDN	power distribution network
PDS	power distribution system
PI	power integrity
PKG	package
PLL	phase locked loop
PoP	package on package
PWL	piecewise linear
RAM	random access memory
RF	radio frequency
SBU	single-bit upset
SDRAM	synchronous dynamic access memory
SEB	single-event burnout
SEFI	single-event functional interruption
SEGR	single-event gate rupture
SEL	single-event latchup
SER	soft-error rate
SESB	single-event snap-back
SEU	single-event upset
SIFT	software implemented fault tolerance
SIL	safety integrity level
SNV	stepwise negotiating voting
SPICE	simulation program with integrated circuit emphasis
SRAM	static random access memory

SSN	simultaneous switching noise
STAR	self-testing and repairing
TMR	triple modular redundancy
TRON	the real-time operating system nucleus
TTP	time-triggered protocol
USEF	Institute for Unmanned Space Experiment Free Flyer
VRM	voltage regulator module
ZIR	zero-input response
ZSR	zero-state response

Chapter 1
Introduction

1.1 Trends in Failure Cause and Countermeasure

Figure 1.1 shows trends in failure cause with transition of technology. In the industrial history, the major failure modes were permanent fault, malfunction of electronic parts caused by electric and physical stress, and worn-out. As for one of the first computers in the history of electronic numerical integrator and computer (ENIAC), people's eagerness to attain reasonable availability (see Section 5.2.2 for its definition) at that time is well understood [1]. It is said that a couple of vacuum tubes broke weekly, and the availability was 90% with special careful treatment, derating, and keeping the machine turned on. In addition, it is also said that the longest time (not mean time) between failures was 116 h.

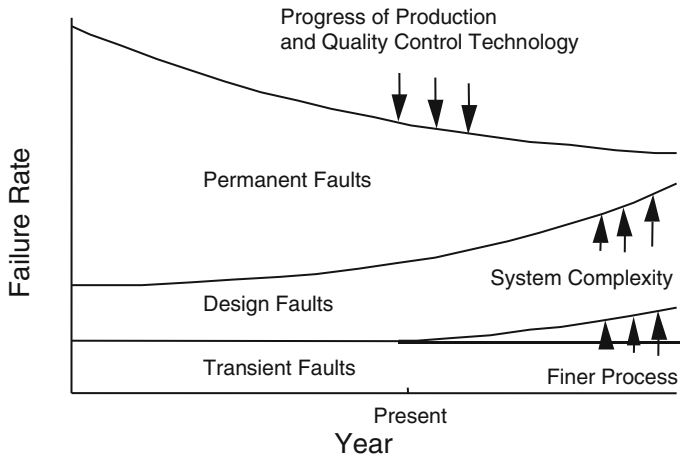


Fig. 1.1 Trends in failure cause

Nobuyasu Kanekawa

N. Kanekawa et al., *Dependability in Electronic Systems*,
DOI 10.1007/978-1-4419-6715-2_1, © Springer Science+Business Media, LLC 2011

Nowadays, failure rate of these failure modes is remarkably decreased, thanks to innovation in production and quality control technology. On the other hand, design fault has become the most important issue these days because of the growth of system scale and complexity.

Furthermore, transient fault is going to be the most important issue in future. The transient faults are induced by ionized or high-energy particles, and by electronic disturbances such as electro-magnetic interference and power supply noise. Especially, transient faults induced by ionized or high-energy particles are called soft errors or single-event upsets.

Moore's Law [2] to which the limit theory was recited from various technical limits many times is still effective now. Far from staying, the integration of the semiconductor has been accelerated by a lot of technical improvements. When semiconductor process size reached below 0.1 μm (100 nm), the unit for semiconductor design rule dive-nosed from μm to as small as nm, and the design rule has become finer as 90, 70, and 45 nm year by year as shown in Fig. 1.2. By such an integration, critical charge (quantity of electric charge that is necessary to cause the inversion of data) decreases. Data error called soft error (a single-event upset) easily occurs due to the decrease of the critical charge and a decrease in the power supply voltage. It was known from the past that soft error by cosmic rays occurred in the outer space. Moreover, it was generally thought that the soft error was only caused by alpha rays that the radioactive isotope of package materials emitted on the ground. In 1996, occurrence of soft error by cosmic rays (in particular, the second cosmic rays caused by neutron collision with atmosphere atoms) was predicted

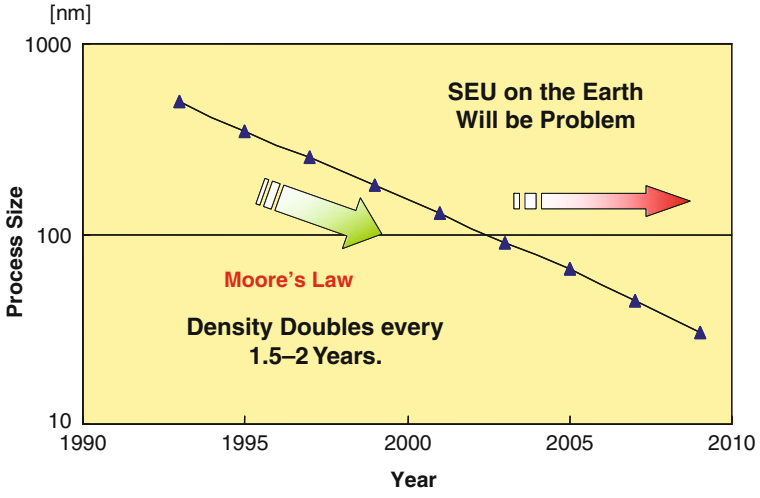


Fig. 1.2 Trends of LSI technology

with the integration of the semiconductor [3]. The prediction has become the reality now [4]. The memory density that the system possesses has also increased by Moore's Law. Frequency of soft error in the memory increases in proportion to the memory size that composes the system even if the upset rate per bit is unchanged. In other words, both an increase in the soft-error rate by finer process of semiconductor described previously and an increase in memory total size make the impact of a soft error by cosmic rays larger. Therefore, dependable technology and study on soft-error mechanism are indispensable in the trend of the semiconductor integration.

With the growth of LSI integration, process size has grown smaller, power supply voltage has became lower, and clock frequency and chip current have been increased. Increases of clock frequency and chip current make the noise intensity larger. Furthermore, increase of clock frequency and decrease of power supply voltage make LSIs more noise-sensitive. Therefore, consideration and mitigation of electro-magnetic disturbances are also indispensable for stable and dependable operation of highly integrated LSIs.

Figure 1.3 shows chronology of events related to dependability in recent couple of decades. We can find several trends in the history. Dependable systems are used to be applied to limited fields such as aerospace and railroad. Moreover, commercial fault-tolerant computer system emerged recently, and availability is used for convenience in more familiar application fields such as video on demand systems and search engines nowadays. Trend of semiconductor integration along with the Moore's Law encouraged innovation of technology for dependability such as satellites using commercial off-the-shelf (COTS) components, on-chip redundancy, and research on terrestrial soft errors caused by cosmic ray and electro-magnetic disturbances and their mitigation countermeasures.

1.2 Contents and Organization of This Book

The book covers practical applications of dependable electronic systems in real industry such as space, train control, automotive control systems, and network servers/routers. Their fundamental technical backgrounds are also provided; compatibility and trade-off between availability and coverage.

The impacts from transient and intermittent errors caused by environmental radiation (neutrons and alpha particles) and electro-magnetic interference (EMI) are introduced together with their most advanced countermeasures, and power integration is included as one of the most important basis of dependability in the systems.

Chapter 2 describes studies and proposals on mitigation measure of terrestrial neutron-induced failures. This chapter starts with basic knowledge on terrestrial neutron-induced soft-error rate (SER), experimental techniques to quantify SER,

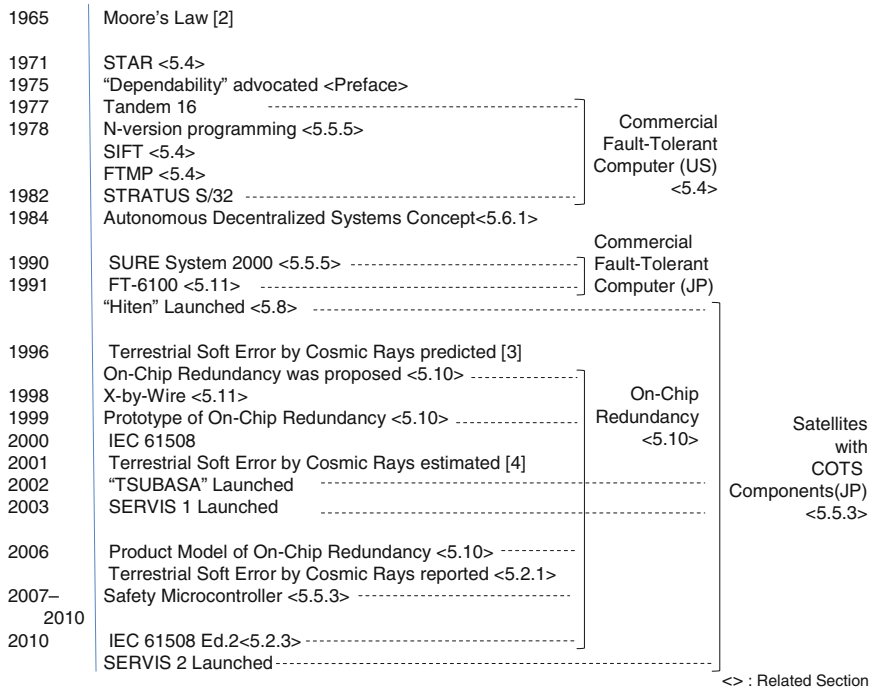


Fig. 1.3 Chronology on dependability

and relevant international standards. In addition, novel multi-cell upset (MCU) characteristics and their significances are introduced. Furthermore, major algorithms relevant to neutron-induced soft error, SRAM device models for Monte-Carlo simulation, and simulation results for scaling effects of SER in SRAMs are presented and discussed. Finally, an example of board-level evaluation and mitigation techniques and hierarchical countermeasures in devices/components/systems are discussed. In-depth considerations are focused on multi-node upset (MNU) that may kill the space redundancy techniques among logic nodes.

For electro-magnetic disturbances, Chapter 3 describes studies and mitigation of electro-magnetic interference and Chapter 4 describes studies and mitigation measures of power supply noise. In Chapter 3, the author presents an overview on electromagnetic compatibility, basic model of interference, and design methodology of printed circuit board, cable, connector, and enclosure.

In Chapter 4, problems of power supply noise for semiconductor devices such as threshold voltage variation and logic error jitter with delay and drivability modulation caused by power supply voltage fluctuation are described. Furthermore, trends of power supply voltage decrease and current increase with trends of CMOS technology are introduced and the target of power integrity design is identified. Also, design methodology of power integrity such as time and frequency-domain analysis and design, printed circuit board design methodology, and example of real design

results are introduced. In addition, principle and experiments on simultaneous switching noise are discussed.

Chapter 5 describes fault-tolerant system technology as a system-level approach for mitigation measure of hardware failures, soft errors, and electro-magnetic disturbances. The usual practice for high reliability is redundancy. This chapter focuses on the technical issues of the high reliability not known in general and introduces the measures through a deeper discussion. In Chapter 5, the metrics for dependability is introduced and misunderstanding on the metrics that is easy to fall into is explained by an example of paradox. In addition, author's industrial approaches are introduced after surveys on fault-tolerant techniques and technical issues. As for technical issue on coverage, the authors took complementary approaches to realize both availability and coverage improvement. The authors proposed misdetection tolerant data selection scheme, SNV method which tolerate imperfect detection coverage, and also self-checking comparator and optimal time diversity to improve fault-detection coverage. Also, fault-tolerance techniques employed by commercial fault-tolerant computer are introduced as examples of techniques to realize high performance and transparency, in addition to dependability. Finally, X-by-Wire is introduced as a current application field, and prospects of cost reduction by scale merit of mass production with LSI technology are discussed.

1.3 For the Best Result

The most important thing and what should be done first are to take primary countermeasures of each malfunction causes. A better result will be obtained by combination with system-level countermeasure, fault-tolerance techniques supplementing each countermeasure.

As for hardware failures, production technology and quality control technique and fault-avoidance technique are the primary countermeasures. In addition, process level, circuit level, chip level, and subsystem level techniques stated in Chapter 2 are the primary countermeasures for soft errors. The better result will be provided by the combination with spatial diversity or redundancy techniques preferably with layout rule and floor planning stated in Section 5.10. For electro-magnetic disturbances, techniques for electro-magnetic compatibility stated in Chapter 3 and power supply integration stated in Chapter 4 are the primary countermeasures, and the better result will be obtained by combination with the optimal time diversity techniques stated in Section 5.9.2.

References

1. Alexander Randall 5th, "A Lost Interview with ENIAC Co-inventor J. Presper Eckert," *Comput. World,* 14 February 2006. http://www.computerworld.com/printthis/2006/0,4814,108568,00.html.
2. G.E. Moore, "Cramming More Components onto Integrated Circuits," *Electron. Mag.*, Vol. 38, No. 8, pp. 114–117 (1965).

3. T.J. O'Gorman, et al., "Field Testing for Cosmic Ray Soft Error in Semiconductor Memories," *IBM J. R & D,* Vol. 40, No. 1, pp. 41–50 (1996).
4. E. Ibe, "Current and Future Trend on Cosmic-Ray-Neutron Induced Single Event Upset at the Ground Down to 0.1-Micron-Device," *The Svedberg Laboratory Workshop on Applied Physics, Uppsala, May 3*, No.1 (2001).

Chapter 2
Terrestrial Neutron-Induced Failures in Semiconductor Devices and Relevant Systems and Their Mitigation Techniques

2.1 Introduction

2.1.1 SER in Memory Devices

Scaling down of semiconductor devices to sub-100 nm technology encounters a wide variety of technical challenges like V_{th} variation [1], negative bias temperature instability (NBTI) [2], short-channel effect [3], gate leakage [4], and so on. Terrestrial neutron-induced single-event upset (SEU) is one of such key issues that can be a major setback in scaling.

SEU research in memory devices has initially focused on DRAM but the reliability of SRAMs became very poor in late 1990s [5], triggering intense researches on SRAM SER.

JESD89A [6] was issued in 2003 as the revised version of JESD89, in which alpha-ray, thermal neutron, spallation neutron, (quasi-mono) energetic neutron, and high-altitude/underground field tests are described in a more reasonable way compared to the original JESD89. SERs in logic devices and field programmable gate arrays (FPGAs) were discussed there to a certain degree but test methods were not defined. EIAJ EDR4705 [7] was issued in 2005 with a similar scope with JESD89A as the Japanese guideline. IEC60749-38 [8] was issued with similar scope with JESD89A in 2008. Basic concepts in JESD89A are accepted worldwide as such. Some recent works after 2009, however, have revealed that basic assumptions in JESD89A as exemplified below may not be true anymore beyond 90 nm generations.

Recent works show that some evolution of the standards may be needed. For instance

- The contribution of low-energy proton as the secondary ions from nuclear spallation reaction is significant and will be much greater in smaller generations.
- The SEU cross-section has high peak below 10 MeV due to secondary protons and the peak height continues to be higher as devices scale down.

Eishi Ibe

N. Kanekawa et al., *Dependability in Electronic Systems*,
DOI 10.1007/978-1-4419-6715-2_2, © Springer Science+Business Media, LLC 2011

Also, SER tests for automotive LSIs with memories over 1 Mbits are strongly recommended in AEC-Q100-Rev.G [9]. The impacts from AEC-Q100-Rev.G were discussed in the IOLTS2008 special session [10].

2.1.2 MCU in Memory Devices

In particular, "multi-cell upsets (MCUs)," which are defined as simultaneous errors in more than one memory cell induced by a single event, have been under close scrutiny [11–16]. The concept of MCU, therefore, contains both upsets that can be corrected by error detection/error correction code (EDAC/ECC) as well as those which cannot. The latter is called "multiple bit upset" or "multi-bit upset" (MBU) of memory cells in the same word, and can lead, for example, to hang-ups of computer systems. Though MBUs can be avoided by a combination of ECC and the interleaving technique [2.16], MCUs may still be problematic in high performance devices such as contents addressable memories (CAMs) [17] used in network processors and routers. In the case of system design, it is therefore very important to evaluate MCUs as well as soft-error rates (SERs) of the device in design phase.

Historically, MCUs are understood as taking place when two or more storage nodes are hit by one secondary ion from nuclear spallation reaction in a device. As device scaling down proceeds, novel MCU modes are being reported as "charge sharing among memory storage nodes in the vicinity [15, 18–20] or bipolar effects in p-well [16, 21, 22]." Ibe et al. have proposed multi-coupled bipolar interaction (MCBI) for one of the bipolar MCU mechanisms that is regarded as a parasitic thyristor effect triggered by a single-event snapback (SESB) in the p-well and causes MCU multiplicity of more than 10 bits [16]. It is also reported that MCU physical address pattern differs depending on written data patterns typically between the groups ALLX (all "1" or all "0") and Checkerboard (CHB or its complement CHBc).

2.1.3 SET and MNU in Logic Devices

Concerns on SEUs are shifting to logic devices. Quantification efforts of SER in logic devices are being developed. Gate-chain methods are among such techniques, where logic gates like inverters [23, 24], NAND [25], NOR [25, 26] gates are connected in series with FFs in-between. Single-event transients (SETs) that take place in some of the gates may be latched in FFs and stored.

Data corruption in radiation hardened-by-design (RHBD) flip flops (FFs) such as DICE [27] is getting recognized as a real threat due to the multi-node upset (MNU) mechanisms caused by the charge-sharing or potential elevation in wells by bipolar events. Some novel RHBD FF designs are proposed to encounter this emerging threat [28–30]. Errors due to glitches in global control line such as clock [31]/SET/REST [32] lines are also being recognized.

2.1.4 Chip/System-Level SER Problem: SER Estimation and Mitigation

MCU and MNU can be a threat in mission-critical systems with an extreme number of logic devices that are mainly protected by spatial or time. Typically, redundancy circuits such as triple module redundancy (TMR) [33], duplication and comparison [34], replication [35] are applied to realize such protection. However, space redundancy techniques cause power, speed and area overhead.

In the actual electronic components, direct estimation of component-layer SER from the database of such logic/memory-level SERs is quite a difficult and painful work. Masking or derating factor must be quantified for such works. Even though such factors are obtained, the estimated component-layer SER must have very wide variation depending on circuits and applications. The variation is not originated from random process so that any statistical cannot be applied, in principle.

2.1.5 Scope of This Chapter

The statistics in SEUs and MCUs in static random access memories (SRAMs) are predicted down to 22 nm process by using the Monte-Carlo simulator CORIMS [36, 37]. It is shown that the impact of MCU and neutrons with energy of less than 10 MeV becomes harsh as the scaling proceeds.

All of the new threats make device/component/system design much more complicated and difficult. To cope with the new threats, they have to be quantified first. New standards for characterization of the fault/error modes in memory/logic devices, components and system may be necessary in order to

(1) obtain the target level of raw SER (SER without any masking effects) in designing devices for device vendor;
(2) design cost-effective, low-power, and acceptably reliable components and systems starting with the raw SER databases.

This chapter also discusses and proposes novel approaches with the following features that can overwhelm the setbacks mentioned above:

(i) Overall reduction approach in component-layer SERs.
(ii) Experimental approach by which SERs in the component or board layer can be quantified and reduced.
(iii) Inter-layer built-in reliability (LABIR) that potentially detects and reduces SERs with very low additional spatial overhead, power dissipation, and costs.

In Section 2.2, basic knowledge on terrestrial neutron-induced SER is reviewed. In Section 2.3, experimental techniques to quantify soft-error rate (SER) and relevant international standards are reviewed. In Section 2.4, novel MCU characteristics and their significances are introduced. The physical model, major algorithms relevant to neutron-induced soft-error and SRAM device models for Monte-Carlo

simulation are described in Section 2.5. In Section 2.6, simulation results for scaling effects of SER in SRAMs are presented and discussed. In Section 2.7, quantification methods of SEEs in sequential and combinational logic devices are introduced and possible and necessary revisions in the international standards are discussed. Section 2.8 shows an example of board-level evaluation and mitigation techniques. Section 2.9 discusses hierarchical countermeasures in devices/components/systems. Section 2.10 proposes LABIR and its concept is introduced. Section 2.11 summarizes this chapter.

2.2 Basic Knowledge on Terrestrial Neutron-Induced Soft-Error in MOSFET Devices

2.2.1 Cosmic Rays from the Outer Space

High-energy neutrons, protons, pions, muons, and neutrinos are primarily produced by nuclear spallation reactions of extremely high-energy cosmic rays (mainly protons) with atmospheric nuclei (nitrogen and oxygen) as illustrated in Fig. 2.1 [38]. Charged particles are halted in a relatively short range, but neutrons produce a cascade of spallation reactions (air shower) that eventually make terrestrial neutrons at the ground level. Since charged particles twine around magnetic force lines, the geomagnetic and heliomagnetic fields act as shields against low-energy cosmic rays. Air also acts as a shield against neutrons, so that neutron flux varies with the location on the Earth and solar activity. The neutron energy spectrum at the sea level in NYC is shown in Fig. 2.2 [6]. The terrestrial neutron flux at the sea level is about $20\,\mathrm{n/cm^2/h}(E_\mathrm{n} > 1\,\mathrm{MeV})$.

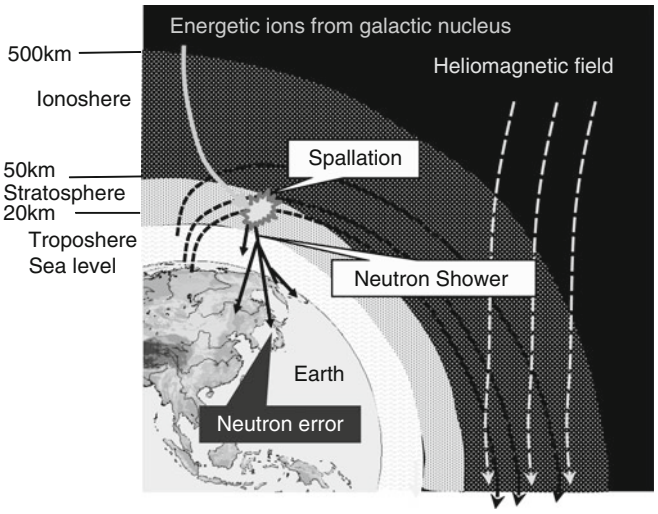


Fig. 2.1 Macroscopic neutron-induced soft-error mechanism

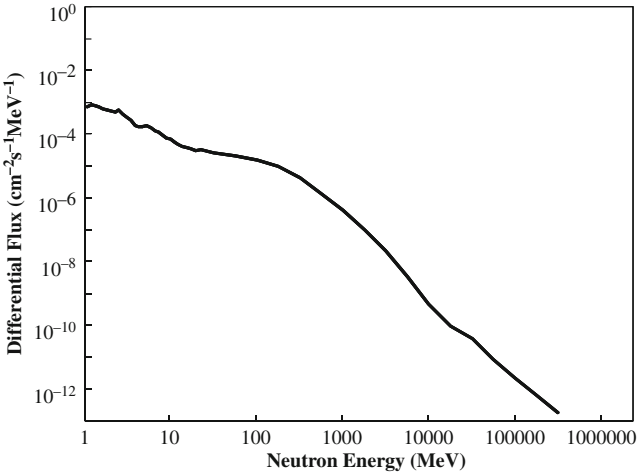


Fig. 2.2 Neutron differential flux spectrum at the sea level in NYC (JESD89A) [6]

2.2.2 Nuclear Spallation Reaction and Charge Collection in CMOSFET Device

A simplified bird's eye view of one-bit CMOS-SRAM (static random access memory) cell is illustrated in Fig. 2.3, with a physical model of neutron-induced soft-error. The n-well (pMOSFET) is placed at the center of the SRAM device sandwiched by p-wells (nMOSFETs). The MOSFET channels are isolated by shallow trench isolation (STI). When a nucleus in the device undergoes a collision with a ballistic neutron, a nuclear spallation reaction, in which the nucleus breaks into

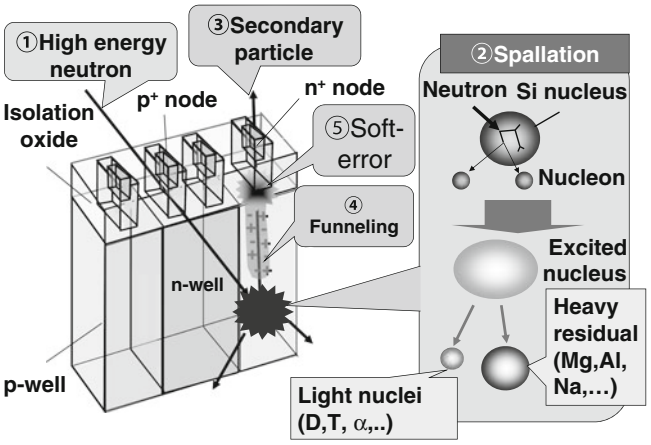


Fig. 2.3 Microscopic mechanism of neutron-induced soft-error in a SRAM bit. Secondary ions are produced by nuclear spallation reaction and soft-error takes place when enough amount of charge is collected to the n^+ storage node

secondary fragments, can take place with a certain probability. Similar to alpha-ray soft-error, when the storage node (diffusion layer) is hit by a secondary ion, a certain amount of electrons/holes produced along the ion track are collected to the nodes, typically by the funneling mechanism [39] and/or the drift-diffusion process. An SEU takes place when charge collected to the node exceeds the critical charge Q_{crit} over which the data "1 (high)" in the node changes to "0 (low)."

2.3 Experimental Techniques to Quantify Soft-Error Rate (SER) and Their Standardization

2.3.1 The System to Quantify SER – SECIS

The SER evaluation techniques using high-energy particle accelerators are integrated as an SER evaluation system, self-consistent integrated system (SECIS for SER evaluation system) [40, 41], combined with field testing and measurements of environmental factors. SECIS consists of five closely interlinked key techniques: (i) field testing of typical devices, (ii) measurement of SEU cross-section as a function of neutron energy (E_n) using mainly quasi-mono-energetic neutron beams [40–44] along with a necessary correction using the numerical simulation package CORIMS (developed for nuclear spallation and charge collection physics in the device) [45], (iii) measurement of the terrestrial neutron spectrum at a specific location, (iv) measuring geographic coordinates and terrestrial neutron dose in the field, and (v) a numerical simulation by CORIMS of field testing and accelerator testing of memory devices [38]. The ultimate goal of this system is to evaluate SER of devices directly by the simulator CORIMS. It is expected that repetition of the procedure from (i) to (v) converges the evaluated value of SER obtained by SECIS with a high degree of accuracy. In order to confirm the usefulness of SECIS, a comparison among SER values obtained by field testing, accelerator testing, and simulation is carried out. Figure 2.4 demonstrates the series of the SER values of low power consumption CMOS SRAM with 180 nm process technology at three different locations

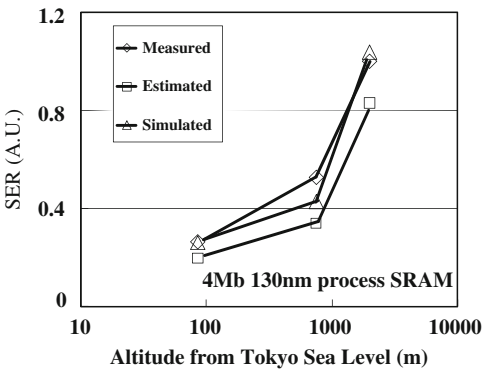


Fig. 2.4 Altitude dependency of field SER measured in three locations in Japan. Accuracies of estimated field SER with (quasi-)mono-energetic neutron method and simulated field SER with the simulator CORIMS are demonstrated (© 2002 IEEE)

in Japan at altitudes of 86, 755 and 1988 m. The simulation results obtained by using CORIMS are also shown [38].

2.3.2 Basic Method in JESD89A

2.3.2.1 Spallation Neutron Methods

First, define the neutron energy range $E_{\min}$ and $E_{\max}$ of the accelerator. In JESD89A, $E_{\min} = 10\,\text{MeV}$ and $E_{\max} =$ maximum energy of the spallation neutron source. Second, obtain the effective SEU cross-section based on the test results:

$$\sigma_{\text{seu}}^{\text{eff}} = \frac{N_{\text{err}}}{\int_{E_{\min}}^{E_{\max}} \frac{\partial \varphi}{\partial E_n} dE_n} \tag{2.1}$$

where N_{err}: number of errors in the OUT for total neutron irradiation and φ fluence for neutron energy range between E_{n} and $E_{\text{n}} + \text{d}E_{\text{n}}$.

Finally, estimate real-time SER (RTSER) from

$$\text{RTSER} = \sigma_{\text{SEU}}^{\text{eff}} \times \phi(E_{\min}, E_{\max}) \tag{2.2}$$

where $\phi(E_{\min}, E_{\max})$ flux of neutron with energy range between $E_{\min}$ and $E_{\max}$ at the sea level in NYC. $E_{\min} = 10$ MeV is recommended in JESD89A.

2.3.2.2 (Quasi-)Mono-Energetic Neutron Test

The quasi-mono-energetic neutron test is applied, where neutron beams with a flux peak at specific neutron energy are exemplified in Fig. 2.5. Some of the neutron spectra have plateaus in the lower energy range, which is called as "tail." The SEU cross-section σ_{seu} for the peak flux contribution is defined and obtained by

$$\begin{aligned} \sigma_{\text{seu}} &= \frac{N_{\text{err}}^{\text{peak}}}{\Phi_{\text{peak}}} = \frac{R_{\text{err}}^{\text{peak}}}{\phi_{\text{peak}}} \\ &= \frac{N_{\text{err}}^{\text{peak}}}{\Phi_{\text{total}}} \times C_{\text{peak}} \end{aligned} \tag{2.3}$$

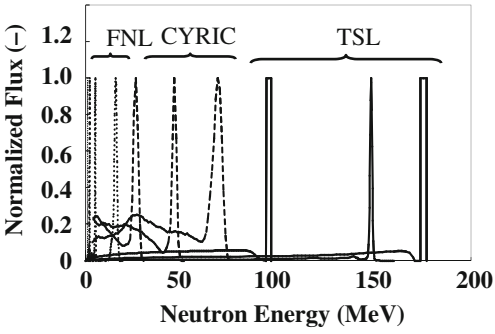


Fig. 2.5 Quasi-mono-energetic neutron energy spectra in various facilities (FNL, CYRIC, and TSL)

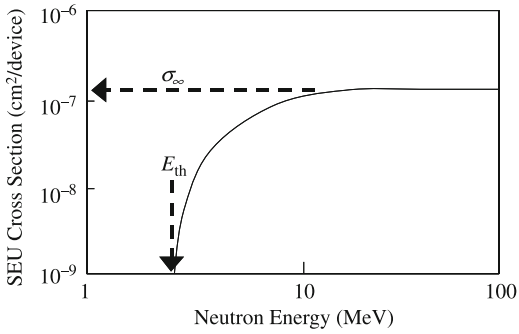


Fig. 2.6 Typical conventional Weibull Fit curve

where $N_{\mathrm{err}}^{\mathrm{peak}}$: number of errors caused by neutrons in the peak flux area (errors); Φ_{peak}: fluence in the peak flux area (n/cm^2); $R_{\mathrm{err}}^{\mathrm{peak}}$: error rate caused by neutrons in the peak flux area (errors/h); ϕ_{peak}: flux in the peak flux area (n/cm^2/h); $N_{\mathrm{err}}^{\mathrm{total}}$: number of errors caused by total neutrons (errors); Φ_{total} total neutron fluence (n/cm^2); and C_{peak}: tail correction factor.

The tail correction factor eliminates the contribution of the tail to the total number of errors and can be obtained either by unfolding experimental data obtained for several (at least four) different energy peaks [42] or soft-error simulator CORIMS [41].

The SEU cross-section $\sigma_{\mathrm{seu}}(E_n)$ is thus measured as a function of the neutron energy. The measured data are approximated by the Weibull Fit-type excitation function $\sigma_{\mathrm{seu}}(E_n)$ as

$$\sigma_{\mathrm{seu}}(E_n) = \sigma_{\infty}\left[1 - \exp\left\{-\left(\frac{E_n - E_{\mathrm{th}}}{W}\right)^S\right\}\right] \tag{2.4}$$

where σ_{∞}: saturation value of SEU cross-section (cm^2); E_{n}: neutron energy at the flux maximum (MeV); E_{th}: threshold energy (MeV); W: width factor (MeV); and S: shape factor (–).

Typical example of this type of excitation curve is described in Fig. 2.6. The curve starts from E_{th} and increases gradually to the saturation value σ_{∞}.

SER in any location on the Earth can be obtained from integration of the Weibull Fit and differential flux over the energy range from E_{th}.

$$\mathrm{SER} = 10^9 \times \int_{E_{\mathrm{th}}}^{\infty} \sigma_{\mathrm{seu}}(E_n)\frac{\partial \phi(E_n)}{\partial E_n} dE_n \tag{2.5}$$

where SER: soft-error rate (FIT) and $\phi(E_{\mathrm{n}})$: neutron flux (n/cm^2/h).

Recently, extension of the Weibull Fit is found to be necessary and modified Weibull Fit (MWF) will be introduced in Section 2.7.

2.3.3 SEE Classification Techniques in Time Domain

Figure 2.7 shows the sequential test algorithm basically to classify the nature of SEU [16, 43]. One normal *write*/*read* cycle takes 8–9 s for all bits in a DUT. Two or more errors in the same sampling interval are basically regarded as MCU. Once the data in a certain bit is in an error, then the error classification algorithm is applied thereafter. If the data is recovered by re-reading, the error is regarded as a transient error. If the error is not a transient error, then compliment data is written to the bit in the phase II. If the bit is re-writable, then the error is regarded as "static soft error" part of which may be MCBI as discussed later or SEFI if it can be corrected by resetting. After all the bits are checked and if there are any error bits which are not re-writable or cannot be corrected by resetting, the DUT power is turned off and then turned on to see if the bit is re-writable in the phase III. If the bit is re-writable after power cycle, the errors are categorized as the "power cycle soft error" (PCSE) [6]. Non-destructive SEL may be among PCSE mode. If the errors cannot be corrected even by power cycle, then those errors may be classified as hard error (HE). I_{DD} current and device temperature are measured within a certain time interval independently.

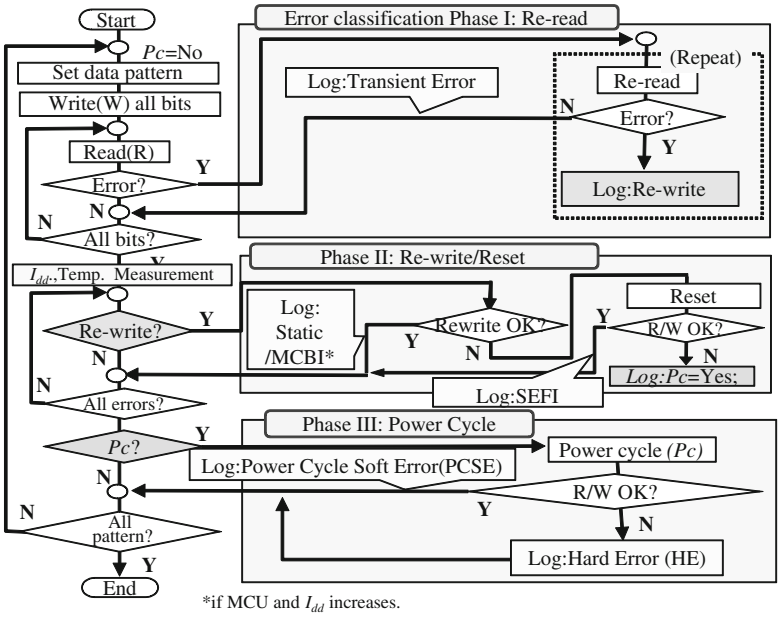


Fig. 2.7 Sequential classification algorithm of SEE in time domain (© 2006 IEEE)

2.3.4 MCU Classification Techniques in Topological Space Domain

A space-domain topological classification algorithm, which automatically identifies and classifies MCUs within a single sampling time window, is implemented in a specially designed program MUCEAC [43].

Figure 2.8 outlines the basic algorithms in MUCEAC. Any two errors within a certain distance along both BL and WL directions in the same time interval are regarded as contained in an MCU. If any two errors in different MCUs satisfy these criteria, the two MCUs make a single MCU. This procedure is continued until all the SEU/MCUs are isolated.

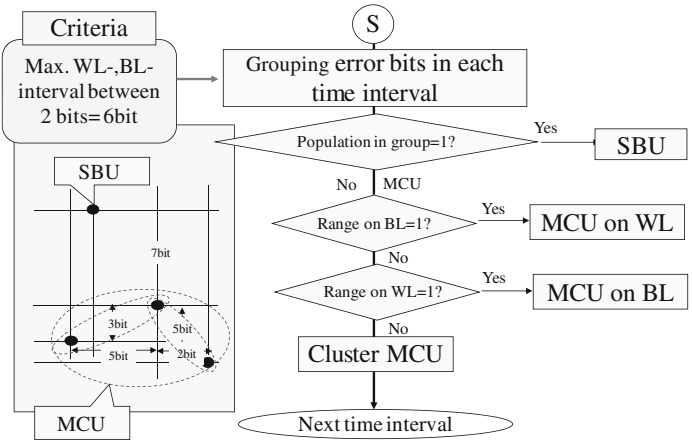


Fig. 2.8 Topological classification algorithm of MCU in space domain (© 2006 IEEE)

As proposed in the MCBI experimental analyses [16, 43], the following MCU classification rules are also applied in CORIMS:

(1) MCU pattern is classified into three basic categories, like a single line along BL (category "b"), a single line along WL (category "w"), and cluster (an MCU that has two or more bits along both BL and WL directions; category "c").
(2) MCU code that can be almost uniquely relevant to physical address pattern in an MCU is given as:

$$C\_N_1\_N_2\_N_3\_N_4\_P$$

where C: category (b/w/c); N_1: MCU size($= N_3 \times N_4$); N_2: bit multiplicity in an MCU; N_3: width in the BL direction (bits); N_4: width in the WL direction (bits); and P: parity (A1: initial data in an MCU bits are all "1"; A0: initial data are all "0"; MX: initial data are a mixture of "0" and "1").

Figure 2.9 depicts examples of MCU categories and codes. An MCU code can be almost uniquely assigned to a specific error bit pattern as far as MCU size is not so

Category	Code	Error bit pattern example
On single BL	B_2_2_2_1_ any parity	
On single WL	W_2_2_1_2_ any parity	
Cluster	C_4_2_2_2_ any parity	
	C_6_2_2_3_ any parity	
	C_6_2_3_2_ any parity	
	C_6_3_3_2_ any parity	
	C_8_2_4_2_ any parity	
	C_9_3_3_3_ any parity	

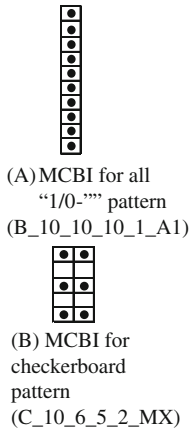


Fig. 2.9 Example of MCU codes and categories

large. MCU categories or codes can be very effective hints to identify the underlying mechanism. As for MCBI, all "high" (data "1") nodes in the vicinity of the MCBI in the p-well fail so that very specific error bit patterns appear depending on the data pattern, (A) FF (all "1") or (B) CHB, as illustrated in Fig. 2.9.

2.4 Evolution of Multi-node Upset Problem

Peculiar MCU mode was found in 130 nm 8 Mbit SRAM by 70 MeV quasi-mono-energetic neutron test in CYRIC [14] before its flux was intensified to world-top class in 2007 [44]. Most MCUs turned out to be two-bit MCUs in adjacent position along WL. More detailed study was carried out with 130 nm SRAMs in TSL. The new MCU mode was defined as multi-coupled bipolar interaction (MCBI) and threat of MNUs in logic devices due to MCBI was recognized.

2.4.1 MCU Characterization by Accelerator-Based Experiments

2.4.1.1 DUTs and Neutron Beams

For the irradiation test, 130-nm 16-Mbit SRAM is used. The layout and structure is schematically shown in Fig. 2.10. The test was carried out in Theodore Svedberg Laboratory (TSL) of Uppsala University [45] with neutron peak energies E_p of

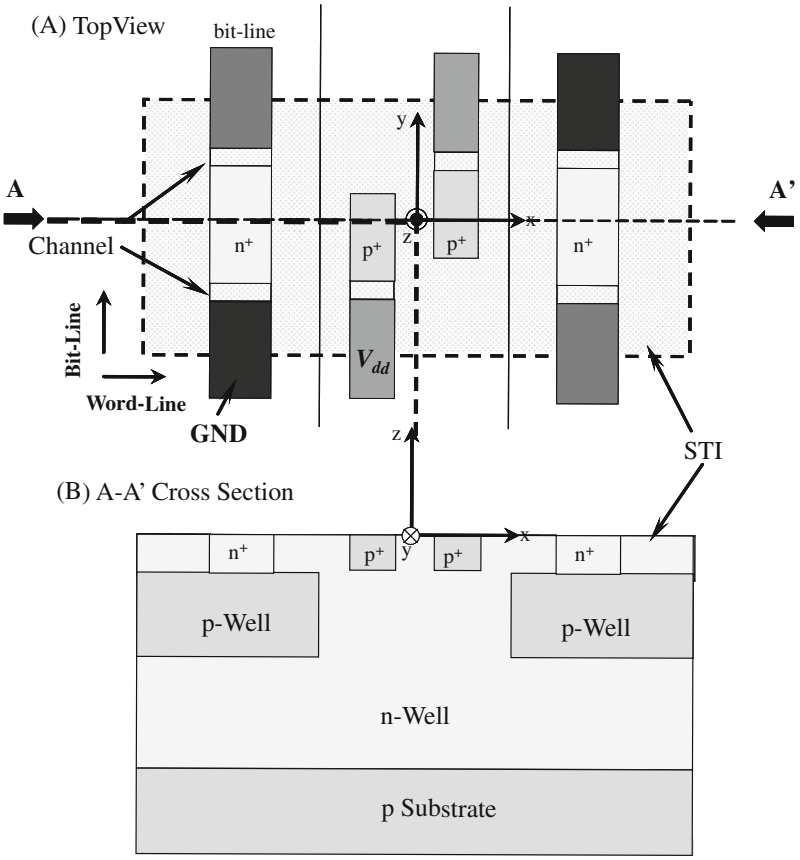


Fig. 2.10 Triple-well structure of the one-bit SRAM cell model (© 2005 IEEE)

21, 46, 96, and 176 MeV. Beam flux and energy peak in TSL are the highest so that better statistics is expected to be obtained with new MCU mode. The automatic data analysis sequences are applied in space and time domains as described in Section 2.3 [42].

2.4.1.2 MCU Patterns

Of MCUs 2564 were identified in total without any MBUs. All MCUs are found to be re-writable so that they are neither MCBI nor SEL. It was also found that all multiple errors along single word line were only two adjacent bits so that the new MCU mode cannot be any cause of failures by applying conventional interleaving with interval of three or more bits and ECC in memories. Based on topological analysis of MCUs, as partly exemplified in Fig. 2.9, the following implications are also obtained:

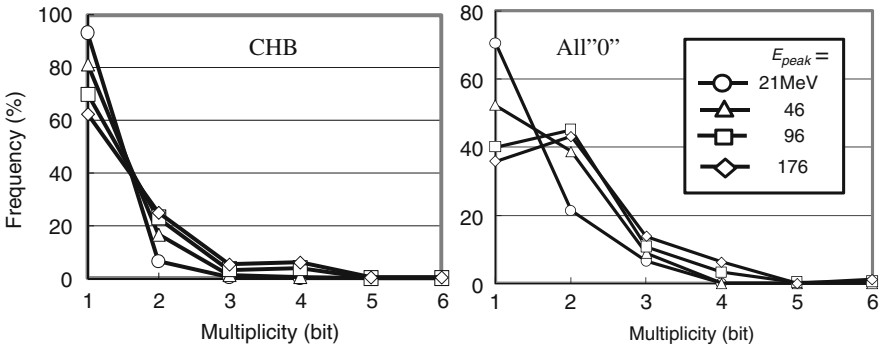


Fig. 2.11 Bit multiplicity of MCU in 130 nm SRAM measured at TSL (© 2006 IEEE)

(1) For CHB/CHBc, MCU with two error bits aligns along with the word line (WL), as seen in (B) in Fig. 2.9.
(2) As rare cases for CHB and CHBc, the clusters cover multi BLs and WLs.
(3) For ALL0/ALL1, MCU normally makes a single successive straight line along BL, as seen in (A) in Fig. 2.9, which implies "high" nodes aligned in the same p-well are subject to fail. As many as 12 successive MCEs are observed at the maximum as in (A).
(4) Likewise for CHB and CHBc, "high" nodes in p-well are subject to fail showing "leap-frog" cluster error bit pattern along a BL as triple leap-frog pattern in (B).

Figure 2.11 shows unnatural multiplicity observed in the test results. For all "0," it is found that the number of double-bit error exceed those of single-bit error when the neutron energy becomes higher, while the trends for CHB seems rather normal. For CHB, there is a slight increase in quad-bit MCU, suggesting an increase in double leap-frog-type MCUs.

2.4.1.3 Influence of Tap Locations

Figure 2.12 shows error population of (a) single-bit upset (SBU) and (b) MCU errors along BL with modified address (Mod 128) to see the effects of tap locations [16]. Clear dependency with 32-bit intervals appears only on MCUs along BL direction, where tap for bias is located with 32-bit interval. This implies that

(i) MCU probability is low at the 2–3-bit vicinity of the tap position, which implies that the resistance to the tap governs MCU.
(ii) Major mechanism of MCUs is different from SBUs. For SBUs, major SEU mechanism may be attributed to charge collection–diffusion or simple snap-back mechanism, while that of MCUs must be related to bipolar action, where resistance between parasitic transistors and taps plays a major role.

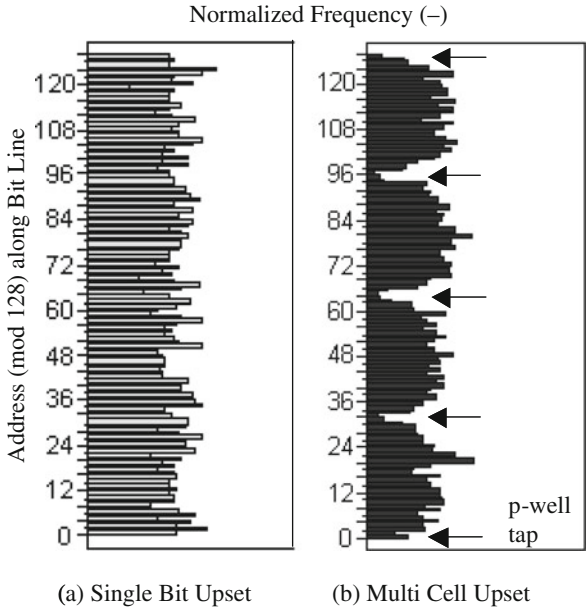


Fig. 2.12 Distribution of SEUs along with bit line. *Arrows* indicate p-well tap locations where V_{SS} is supplied. (**a**) Single-bit upset (**b**) Multi-cell upset (© 2006 IEEE)

The other evidence indicating bipolar action is stepwise distribution of I_{DD} increase [16]. The number of discrete steps increases with the peak neutron energy and is believed to depend on the MCU bit-multiplicity.

2.4.1.4 MCU Category

Figure 2.13 shows the ratio of MCU categories as a function of neutron peak energy for CHB, CHBc, all "0" and all "1" data patterns. CHB and CHBc have almost the same trends, showing that MCU on WL is not changed so drastically with neutron energy, but MCU on BL decreases while cluster MCU increases. As for all "0" and all "1," trends are also almost the same between two patterns. Almost all MCUs are MCUs on BL with a slight increase in cluster.

2.4.1.5 MCU Code

Figure 2.14 summarizes classification results by MCU code for MCUs of size 6 bits. It is seen that

(i) Major codes for group A (CHB, CHBc) are C_&_3_3_2_MX and C_6_4_2_3_MX (correspond to double leap-frog patterns as shown in the left bottom of Fig. 3.14) and they increase as neutron energy increases.
(ii) As for group B (all "0" and all "1"), no particular MCU code appears for the MCU size of 6 bits.

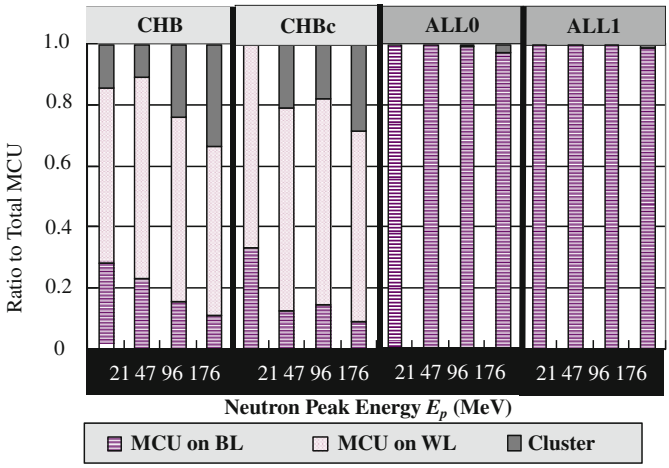


Fig. 2.13 Three categories identified in each run. For *bars* in each data pattern correspond to neutron energies of 21, 46, 96, 176 MeV, respectively, from *left side* (© 2006 IEEE)

Code	Data pattern							
	Group A				Group B			
	Ep= 21	47	96	176	21	47	96	176
C_6_2_3_2_MX	1	1	1	2				
b_6_2_6_1_MX	1							
C_6_3_3_2_MX	1	15	49	77				
C_6_3_2_3_MX				2				
C_6_3_3_2_A0								1
C_6_3_3_2_A1								2
C_6_4_3_2_MX		7	57	100				
C_6_4_2_3_MX		1		3				
b_6_6_6_1_A0							1	2
b_6_6_6_1_A1								2
Typical Error pattern ● (data = "1"), ○ (data = "0")	(C_6_4_3_2_MX)				(b_6_6_6_1_A1)			

Fig. 2.14 MCU code dependency in data pattern and neutron peak energy for group A (CHB) and group B (all 0)

2.4.2 Multi-coupled Bipolar Interaction (MCBI)

The error-bit pattern and IDD increase in the new MCU mode are clearly reproduced in multi-cell TCAD simulation and the mode is turned out to be parasitic thyristor effect triggered by single-event snapback in the p-well. The mechanism is

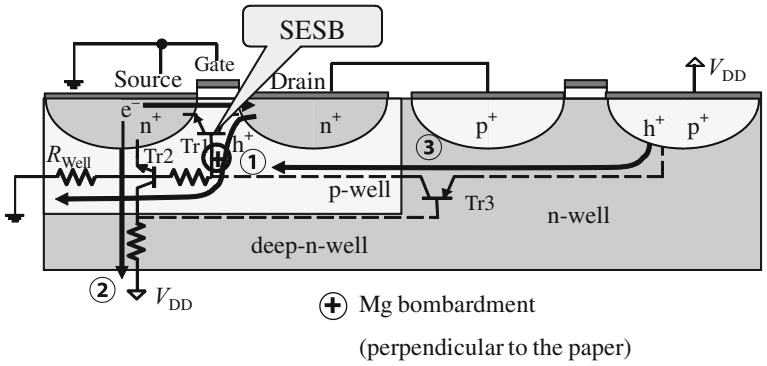


Fig. 2.15 Mechanism of MCBI (© 2005 IEEE)

illustrated in Fig. 2.15 [16]. When the secondary ion penetrates into pn-junctions surrounding the p-well, electrons produced in the ion track move outside the p-well, and the holes remain in the p-well to raise potential in the p-well and form a parasitic transistor Tr1. The potential increase turns on the transistor and high-state drain data flips. If holes continue to be supplied from the drain by impact ionization mechanism, high potential is kept to turn on the parasitic transistor Tr2. Electrons that flow into the deep *n*-isolation region reduces the potential in the *n*-region to turn on the parasitic transistor Tr3 to supply holes to the channel in Tr1, resulting in an increase in I_{DD} current. We call this mechanism multi-coupled bipolar interaction (MCBI). Figure 2.16 demonstrates that only MCBI can explain the MCU pattern

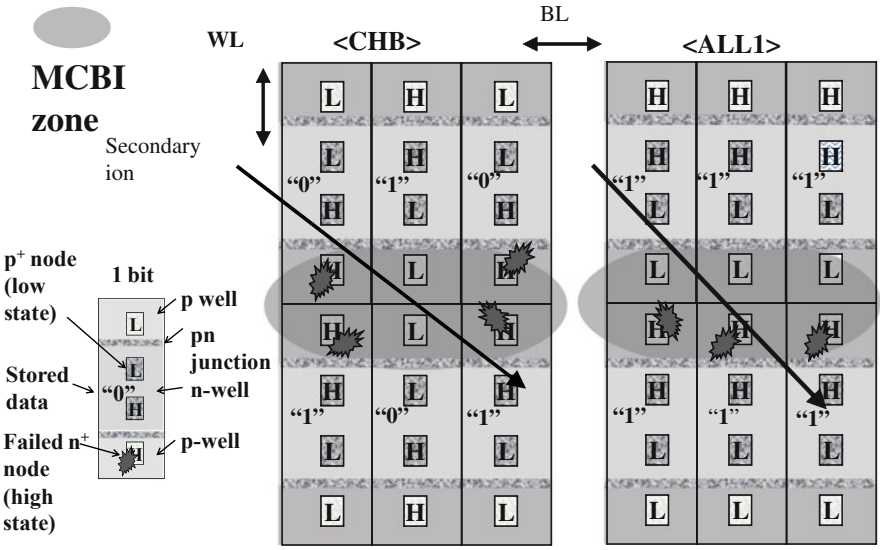


Fig. 2.16 Mechanism of error bit pattern dependency on data pattern

Table 2.1 Comparison of bipolar action mechanisms in CMOSFET device

Features	Single event latchup (SEL)	Multi-coupled bipolar interaction (MCBI)
Multiplicity	No limit over WL/BL direction (within peripheral circuit)	10–20 bits maximum mainly in one or adjacent well (s)
Correction method	Power cycle	Re-writing
I_{DD} current	High, 10–5 mA stepwise increase (2–3, three steps)	Low, 2–10 mA stepwise increase depending on multiplicity
Tap location dependency	High	High except for single bit upset
Mechanism	Direct switch-on of parasitic thyristor	Parasitic thyristor triggered by neutron-induced snapback

dependency on data pattern: p-wells are commonly owned by two adjacent memory cells. For CHB, two adjacent "high"-state storage nodes line up along WL with two-bit interval along BL. If a certain region in p-well is affected by MCBI, "high"-state storage nodes in the area flip to make leap-frog pattern. As for all "0" and all "1" data patterns, "high"-state nodes align continuously in one side of p-well to make a line of failed bit along BL.

Table 2.1 compares the features of bipolar actions, snapback, MCBI, and latchup. The biggest difference of MCBI from latchup is that MCBI is re-writable, neither destructive nor PCSE. Failures due to MCBI can be avoided by interleaving and ECC for memories. It has, however, potentially critical influences on the logic devices. MNU in logic gates can be caused by MCBI, resulting in failures in component/system with a number of logic gates.

2.5 Simulation Techniques for Neutron-Induced Soft Error

2.5.1 Overall Microscopic Soft-Error Model

In Fig. 2.3, a schematic of microscopic soft-error model for a SRAM cell is depicted. The SRAM has two n^+ nodes in the p-well and two p^+ storage nodes in the n-well. Two sets of adjacent n^+ and p^+ nodes correspond to two potential states "high" or "low." The memory data "1" or "0" is assigned to the side (right or left) that has high potential. Once a ballistic neutron penetrates into the SRAM, nuclear spallation reaction may take place between the neutron and the nucleus (mostly Si) in the device. As a prompt reaction, nucleons (protons and neutrons) collide with each other in the nucleus. Some of the nucleons may escape from the nucleus when they have enough kinetic energies. This process is called as intra-nuclear cascade (INC) [46]. After this prompt process, light nuclei may be "evaporated" from the residual excited nucleus [47]. As a consequence, nucleons, light nuclei, and the residual nucleus run inside the SRAM cell producing electron-hole pairs along with the ion track. Energy necessary to produce one pair of electron and hole is 3.6 eV in Si.

When one of such secondary ions hit the storage nodes, some of the charges are collected to the storage node mainly through funneling effect [39] and drift/diffusion process. If the amount of charges exceeds the critical charge that can flip the logical state of the SRAM, a soft error takes place in the SRAM.

2.5.2 Nuclear Spallation Reaction Models

Monte Carlo single-event simulator, cosmic ray impact simulator (CORIMS) [14, 16, 36–38, 48], is equipped with numerical solutions for nuclear spallation reactions of silicon, ion track analysis in an infinite layout of memory cells in a semiconductor device, and charge collection to the diffusion layer of the device. The model of the nuclear spallation reaction is based on the intra-nuclear cascade (INC) model and the evaporation model by Weisskopf and Ewing. The INC model is applied to prompt collision process, where many-body collisions among nucleons (neutron and proton) are treated numerically as a cascade of relativistic binary collisions between two nucleons in the target nucleus. The evaporation model of light particles from excited nucleus is also applied for delayed nuclear reaction process, where nucleons (n and p), deuterons (^{2}H or D), tritons (^{3}H or T), helium and residual nucleus are released into the substrate. The inverse reaction cross-section necessary for determination of an evaporation channel (a set of evaporated light particle and residual nucleus) is calculated based on the GEM model [49]. Nucleus type, energy and direction of each secondary ion produced in a spallation reaction are thus determined and reaction locations are randomly set in the device model. The details of the nuclear reaction data are summarized elsewhere [38].

Accuracy of nuclear reaction model is validated through comparison of nuclear reaction data of high-energy proton and aluminum [50]. SER in the device under any neutron spectra can be simulated. In the case of simulation at a specific location at ground level on the Earth, the terrestrial neutron spectrum at the location is corrected in accordance with the geomagnetic latitude and the altitude based on the standard neutron spectrum at the sea level in New York City as shown in Fig. 2.2 [6].

Figure 2.17 shows an example of outputs from CORIMS for energy spectra of secondary ions produced directly from Si substrate with the neutron spectrum shown in Fig. 2.2. It is noteworthy that

(i) Light particles such as proton and helium (or alpha particle) have high production rates and high energies up to a few hundreds to 1,000 MeV
(ii) Heavier particles such as Mg and Al have also relatively high production rates but do not have high energies with maximum energies of 10–100 MeV.

2.5.3 Charge Deposition Model

Figure 2.18 shows calculated charge deposition density for the relevant ions based on the SRIM tables (http://www.srim.org/).

It is also noteworthy that

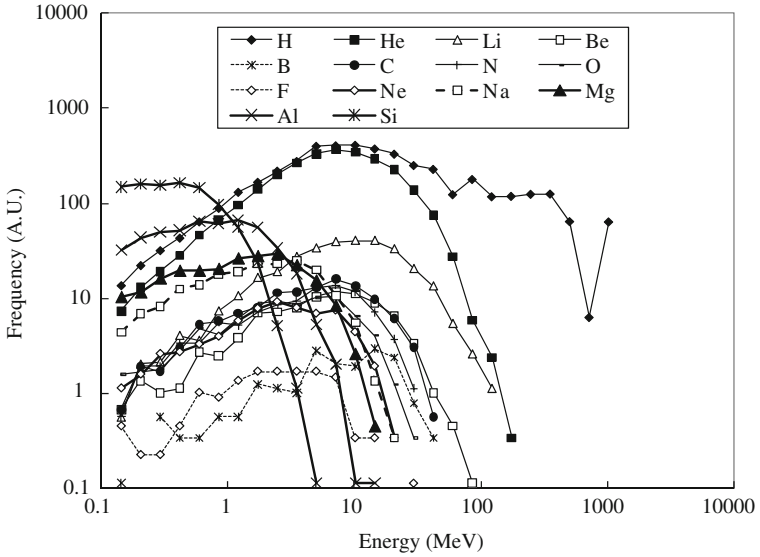


Fig. 2.17 Energy spectra of secondary ions produced from Si by neutron spallation reaction with neutron energy spectrum in NYC (© 2010 IEEE)

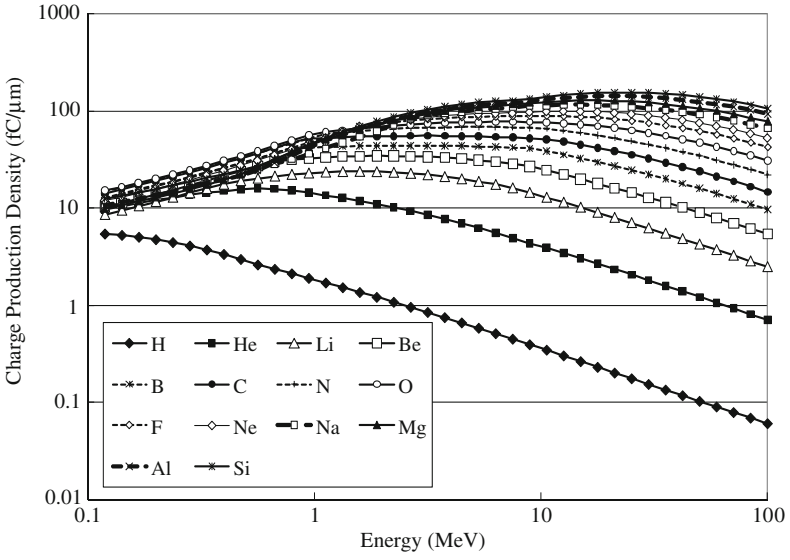


Fig. 2.18 Charge density spectra in Si of secondary ions as functions of energy (© 2010 IEEE)

(i) The charge production density by proton and alpha becomes lower when the energy is higher beyond 0.1–1 MeV. This implies that protons and alpha particles with high energy demonstrated do not have high contribution to soft error in SRAMs.

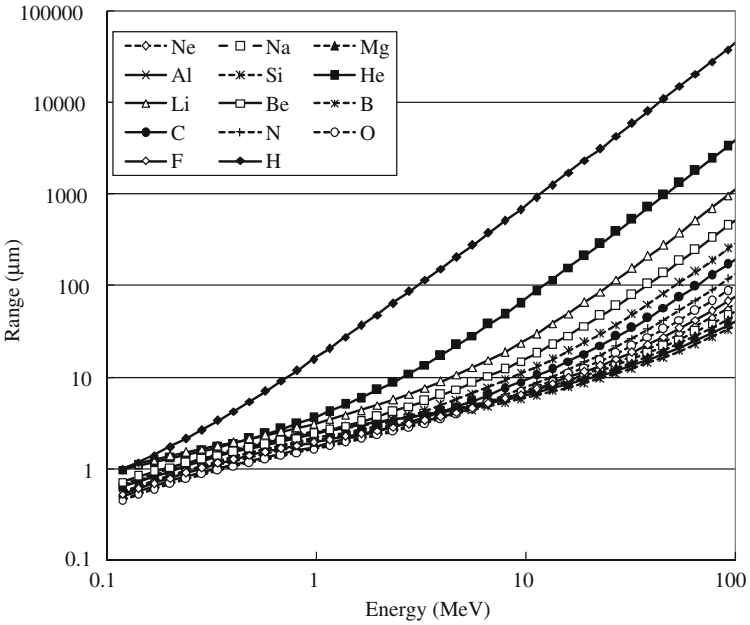


Fig. 2.19 Mean range of secondary ions in Si as functions of energy (© 2010 IEEE)

(ii) The charge production density by heavier ions becomes larger when the ion energies increase in the relevant energy range.

Figure 2.19 shows the average range of ion as a function of kinetic energy also based on the SRIM tables.

It can be seen that

(i) Light particles have as long range as 10–100 μm in Si substrate in the relevant energy range
(ii) Heavier particles have much shorter ranges of 1–100 μm.

2.5.4 SRAM Device Model

The model layout of MOSFET SRAM cell is illustrated in Fig. 2.10. Since the active regions are isolated by STI oxide in lateral direction and wells line up across the word lines, charge collection in the lateral direction is tightly limited in the present device. Bits in a word are aligned along a word line so that MBUs in this device are tightly limited eventually. When an ion passes through the depletion layer under the storage node, the funneling model is applied to calculate the charge collected to the storage node. When the ion passes through the p–n junction at the bottom

of p-well, funneling also takes place so that the charge deposited in the p-well is distributed to the storage node and p-substrate below the p-well. The funneling effect becomes larger when the ion track runs along with the p-well (BL direction) because there is less probability that the ion passes through the other p–n junction in the p-well. Drift–diffusion layer of 100 nm thickness is assumed to be located under the storage node. When an ion passes through only the drift–diffusion layer, the amount of charges in the layer is assumed to be collected by the storage node. The charge deposited inside the storage node and oxide is assumed to recombine and not to contribute to soft error. Any 3-D device models, including SRAMs, can be constructed automatically from device layout data in GDS2 files [51] by using a specially designed tool. Ion tracks through components in a device are analyzed with the help of computer geometry techniques in CORIMS.

2.5.5 Cell Matrix Model

Naturally, a model with the fixed number of physical cell models may be applied to investigate MCU effects. Such a method, however, has inherent limitations on the memory and speed of the simulations. We have developed a dynamic cell-shift (DCS) method to overcome such limitations.

Figure 2.20 shows the basic idea of the dynamic cell-shift method. When an ion crosses a memory cell matrix along the line A–B–C–D, the track of the ion may be traced as long as the ion has a possibility to hit the sensitive components. This method requires a cell matrix that is wide enough compared to the ion range. The

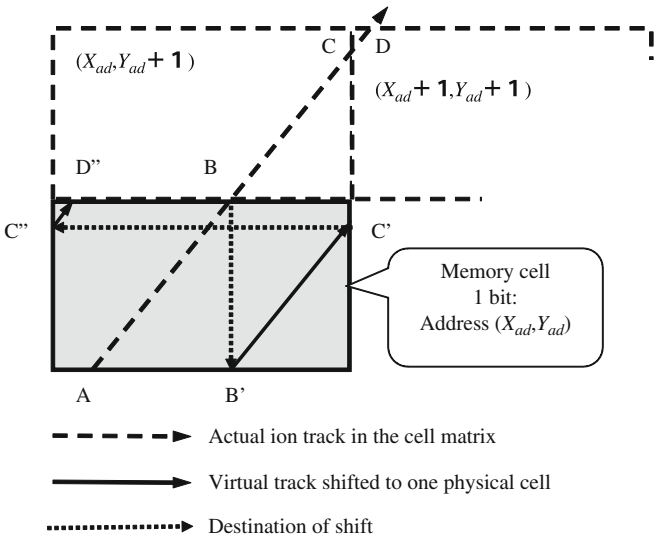


Fig. 2.20 Dynamic cell shift (DCS) method to track ion trajectory in the infinite cell matrix (© 2010 IEEE)

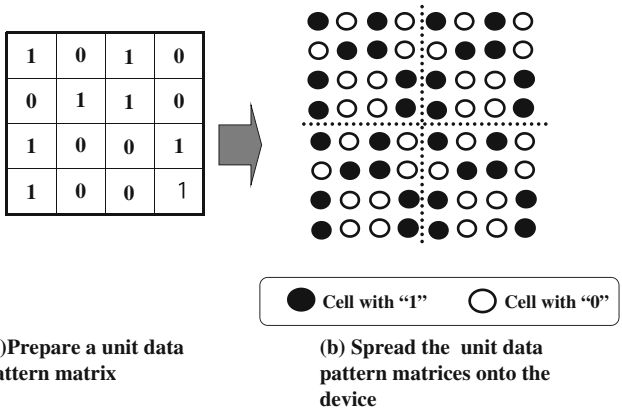


Fig. 2.21 Method to set any data pattern on the cell matrix

proposed method does not need an actual cell matrix. Instead, it utilizes only one physical cell model. When an ion reaches the boundary at B, for example, the track is virtually shifted to B′–C′ by using a shift in the *Y*-coordinates and physical address of *Y*-direction Y_{ad} is incremented by 1 bit. Similarly, when the actual ion crosses C–D, virtual track is shifted to C′–D′ and the physical addresses of *X*- and *Y*-directions are incremented by 1 bit from the original address. In this way, any ion track can be traced until it stops, regardless of the length of the ion's range. In the present device, the condition of data "1" or "0" corresponds to the position (left or right) of "high" node in one bit of SRAM and the layout of the SRAM is symmetry to its center, all "1" and all "0" have the same feature and susceptibility to neutron impacts.

To save the area penalty, some nodes connected to V_{DD} or V_{SS} are commonly shared between adjacent bits. In this case, the bit layout is folded symmetrically along the boundary between the two bits. This technique is sometimes called "mirroring." The DCS method implemented in CORIMS is applicable to this type of mirroring.

Any cyclic data pattern in a rectangular zone can be implemented in CORIMS. The basic idea is illustrated in Fig. 2.21. Once after the data "1" and/or "0" pattern is set in a unit rectangular zone, the unit is close-packed infinitely in the WL and BL directions. Interleaving effects with any bit layout in the same word can also be analyzed with CORIMS, which is desirable for ECC design.

2.5.6 Recycle Simulation Method

In extreme cases, CPU time may exceed several days. This makes parametric survey study difficult in wide scope. To cope with this problem, CORIMS saves the virtual single events with extremely low critical charge with a certain input conditions, and re-runs later to recycle them for parametric survey on the effects of different critical charge, data pattern, and interleaving within 1 h CPU time.

2.5.7 Validation of SRAM Model

SRAM models in CORIMS have been validated to have less than 20% variations from experimental data of 250–130 nm SRAMs in a wide variety of neutron fields like field tests [40] and accelerator tests in LANSCE [52], TSL [45] ,CYRIC [44], and FNL[53], as shown in Fig. 2.22. Figure 2.4 also demonstrates such an example of justification of 130-nm SRAM simulation with measured data in three locations with different altitudes in Japan [38].

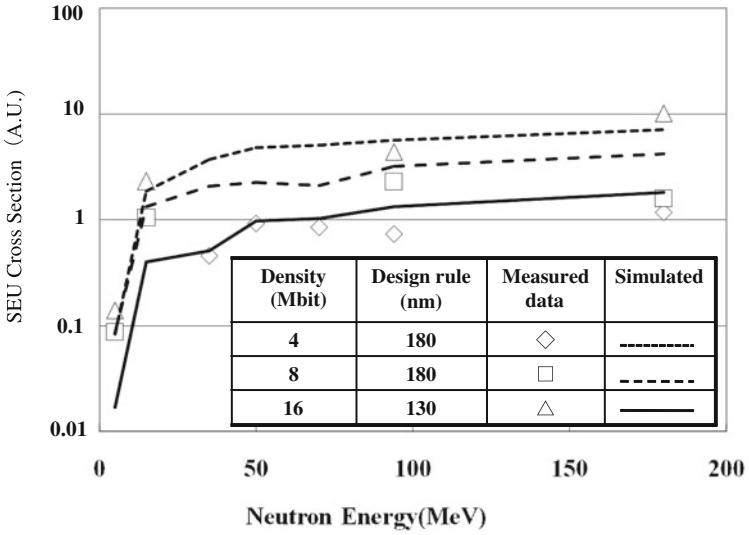


Fig. 2.22 Comparison of SEU cross-sections measured by (quasi-) monoenergetic neutron test and simulated by using CORIMS

2.6 Prediction for Scaling Effects Down to 22 nm Design Rule in SRAMs

2.6.1 Roadmap Assumption

Table 2.1 summarizes the typical roadmap parameters in 20–130 nm SRAM assumed based on ITRS2007 (http://www.itrs.net/Links/2007ITRS/Home2007.htm). Lateral two-dimensional scaling is assumed to reduce area by a factor of 2 by each generation. Depth profile is assumed to be constant due to lack in the roadmap information and also because of difficulty in making shallow profile. As parasitic capacitance is basically in proportion to device area, critical charge is also assumed to decrease by a factor of 2 by each generation. Although reduction in the supply voltage V_{DD} is preferable for reducing power consumption,

it is actually being limited in order to ensure enough margin from the upper bound of V_{th} variation [1] and, therefore, assumed to be constant. The critical charge will decrease more rapidly if the V_{DD} is reduced by generation, leading to increase in SER.

2.6.2 Results and Discussions

2.6.2.1 Overall Trends

Major simulation results are summarized in Tables 2.2 and 2.3 for data pattern of CB and all "1," respectively. The maximum MCU size expands to the order of as many as million bits with the maximum MCU multiplicity of over 100 bits in 22–32 nm generations. The ratio of MCU to SEU will increase up to as high as about 50%. It is noteworthy that the maximum MCU size and multiplicity are statistically very rare case, showing only rough trends with generation (Table 2.4).

Table 2.2 Assumed roadmap of SRAM parameters

	SRAM property		
Design rule	Normalized cell area	Density	Normalized Q_{crit}
nm	AU	Mbit	AU
250	7.45	4	12.8
180	3.84	8	6.4
130	2.01	16	3.2
90	1.00	32	1.6
65	0.49	64	0.8
45	0.24	128	0.4
32	0.12	256	0.2
22	0.06	512	0.1

Source: (© 2010 IEEE)

Table 2.3 General trends obtained from simulation (CHB)

	Soft error rate				
Design rule			MCU ratio	MCU maximum size	Maximum MCU multiplicity
nm	Per device	Per Mbit	%	Bit	Bit
250	0.06	0.48	0	1	1
180	0.26	1.04	5.3	112	2
130	0.50	1.01	7	459	10
90	1.00	1.00	14.8	14,940	16
65	1.62	0.81	21.2	114,170	19
45	2.31	0.58	29.1	288,864	26
32	3.06	0.38	38.5	1932,765	52
22	3.53	0.22	46	463,638	175

Source: (© 2010 IEEE)

Table 2.4 General trends obtained from simulation (All1)

Design rule	Soft error rate		MCU ratio	MCU maximum size	Maximum MCU multiplicity
nm	Per device	Per Mbit	%	Bit	Bit
250	0.06	0.47	0	1	1
180	0.21	0.85	3.6	5,472	4
130	0.53	1.06	6.6	396	4
90	1.00	1.00	12.2	8,096	11
65	1.70	0.85	18.4	31,860	29
45	2.31	0.58	27.8	84,525	27
32	3.06	0.38	34.7	77,216	39
22	3.75	0.23	44.7	3,659,296	87

Source: (© 2010 IEEE)

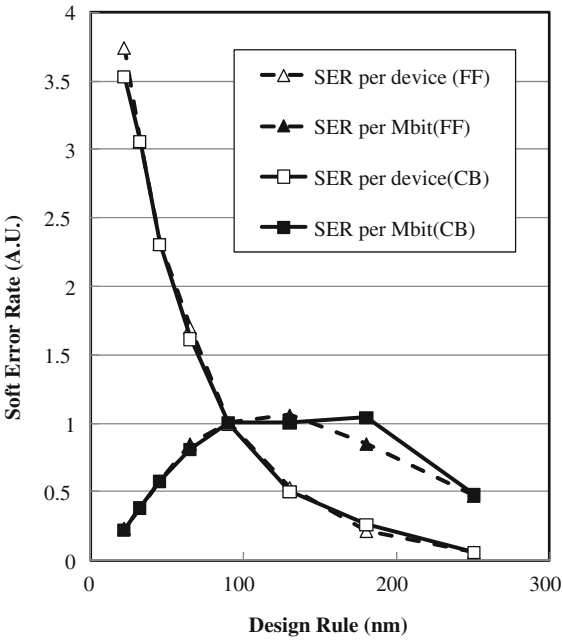


Fig. 2.23 Predicted trends in SER per device and Mbit (© 2010 IEEE)

Typical trends for SER/device and SER/Mbit are plotted for the data patterns CB and FF in Fig. 2.23. Trends in MCU ratio and the maximum MCU multiplicity are also plotted in Fig. 2.24 for the data patterns CB and FF. It is seen that

(i) SER/Mbit increases drastically from 250 to 180 nm. This is quite consistent with the observation that SER in 4 Mbit SRAM increases drastically beyond

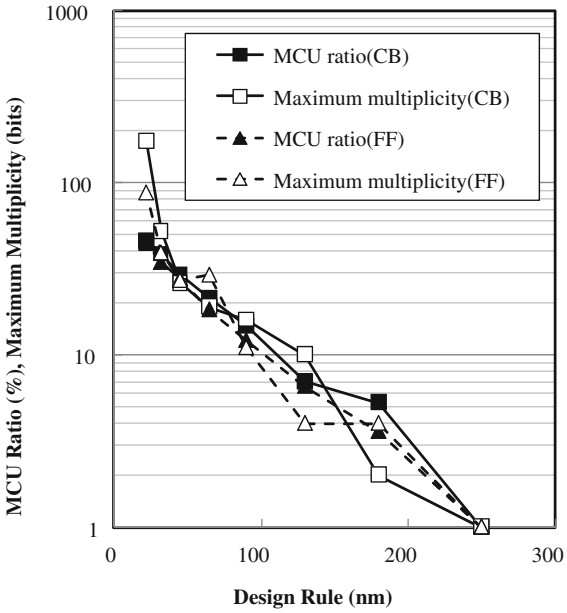


Fig. 2.24 Predicted trend in MCU ratio and maximum bit multiplicity in MCU (© 2010 IEEE)

that in DRAMs, whose SERs have been problematic until late 1980s [38]. SER in SRAMs decreases mildly from 130 nm down to 22 nm. The decrease is also quite consistent with the recent experimental data [54].

(ii) Although SER/Mbit decreases beyond 130 nm, SER/device increases by a factor of as much as 6–7 both for CB and all "1" due to an intense increase in density.

(iii) MCU ratio and multiplicity increase exponentially as scaling proceeds.

(iv) There are only minor differences between CB and FF data patterns.

Table 2.5summarizes the trends in MCU categories for data patterns (A) CB and (B) FF. Typical MCU codes and the number of unique codes are also shown in the table. The figures in the cells are ratio to the total MCUs in percentage. Most MCU error patterns for MCU codes are shown before in Fig. 2.9. Some substantial differences can be seen between the data patterns:

(i) The ratios of the category W (On single WL) for CB patterns are higher than those for FF patterns by a factor of about 2. This is due to the fact that two "high" nodes locate in the same p-well of two adjacent bits in WL direction for CB patterns so that two adjacent bits in WL direction are easily corrupted. This is also seen in the ratios of the MCU code W_2_2_1_2_any parity.

(ii) The ratios of the code C_4_2_2_2_A1 for FF patterns are substantially higher than those for CB patterns.

(iii) The differences between the ratios of categories seem to be clear for larger generations (180 and 130 nm). This has been clearly observed in our preceding

Table 2.5 Major predicted categories and MCU codes

(A) Data pattern CB		Design (nm)							
		250	180	130	90	65	45	32	22
Total MCU even[a]		0	11	49	215	475	980	1,697	2,478
Category	On single BL (B)	0	36.4	12.2	16.7	16.1	14.7	12.0	10.8
	On single WL (W)	0	182	16.3	14.9	14.6	10.5	9.4	8.0
	Cluster (C)	0	45.5	71.4	68.4	69.2	74.8	78.6	81.2
Code[b]	C 4 2 2 2 A1	0	18.2	6.1	4.7	2.1	3.6	2.7	2.2
	C 4 2 2 2 A0	0	0.0	12.2	3.3	3.3	2.3	1.6	2.2
	B 2 2 2 1 MX	0	36.4	12.2	11.6	11.7	10.5	9.1	7.7
	C 6 2 3 2 MX	0	9.1	4.1	6.0	2.9	3.1	1.9	2.5
	W 2 2 1 2 MX	0	18.2	12.2	14.0	12.1	9.3	7.7	6.7
	C 12 2 4 3 MX	0	0.0	0.0	1.9	1.0	0.9	1.1	0.4
	C 6 2 2 3 MX	0	0.0	2.0	1.4	2.5	1.6	1.5	1.3
	Number of unique codes	1	8	30	107	243	483	917	1457
(B) Data pattern FF		Design (nm)							
		250	180	130	90	65	45	32	22
Total MCU even[a]		0	10	49	177	436	932	1,526	2,554
Category	On single BL (B)	0	30.0	22.4	11.3	11.9	9.8	9.4	7.6
	On single WL (W)	0	0.0	12.2	11.3	8.0	4.5	5.2	5.3
	Cluster (C)	0	70.0	65.3	77.4	80.0	85.7	85.4	87.0
Code[b]	C 4 2 2 2 A1	0	0.0	18.4	7.3	11.7	9.4	7.5	6.0
	C 8 2 4 2 A1	0	0.0	0.0	3.4	2.1	1.7	1.2	1.8
	B 2 2 2 1 A1	0	20.0	14.3	7.3	7.3	6.3	6.3	5.3
	C 6 2 3 2 A1	0	10.0	8.2	5.6	7.1	4.8	5.1	4.1
	W 2 2 1 2 A1	0	0.0	8.2	9.6	6.0	3.2	3.7	3.5
	C 9 3 3 3 A1	0	0.0	4.1	2.3	0.5	2.5	1.0	1.1
	C 6 2 2 3 A1	0	0.0	2.0	2.8	2.3	1.7	2.7	1.3
	Number of unique codes	1	8	27	96	220	508	837	1,440

[a] Total number of neutrons reacted: 58,003

[b] Code = Category(Initial)_MCU size_Multiplicity_BL width_WL width_Parity of initial data (A0:all“0”, A1:all“1”.MX:mixture)

Source: (© 2010 IEEE)

work for 180 nm SRAMs [14]. The differences are getting unclear for smaller generations. This may be due to the fact that the SRAM cells are easily corrupted by the charge deposited only in the depletion layer as the critical charge becomes smaller and the memory cells are more tightly packed in the smaller generations. The directional effects become weak for smaller generation, since the contribution from charge collection by the directional funneling effects as mentioned before becomes smaller.

The result that MCU ratio drastically increases as scaling proceeds means that multi-node upset (MNU) in which multiple logical nodes of sequential or combinational logic device are corrupted must increase as well. This may cause serious impacts in reliability design of logic devices, since MNUs would make error detection impossible. This would make the redundancy SER mitigation techniques extremely vulnerable to MNU.

2.6.2.2 Charge Deposition Density for Secondary Ions

The frequencies of charge deposition density per unit track length at the boundary of the storage node by secondary ions are shown in Fig. 2.25 for proton, alpha particle, heavier particles (atomic number is 10 or more) and total particles. Basically, there are no differences in the shape of spectra with generation, with the maximum deposition density of about 110 fC/μm. This means that any device which can tolerate the density of 110 fC/μm can be perfectly soft-error immune. Heavy ions cause high density (10–110 fC/μm) charge deposition but their frequencies are relatively

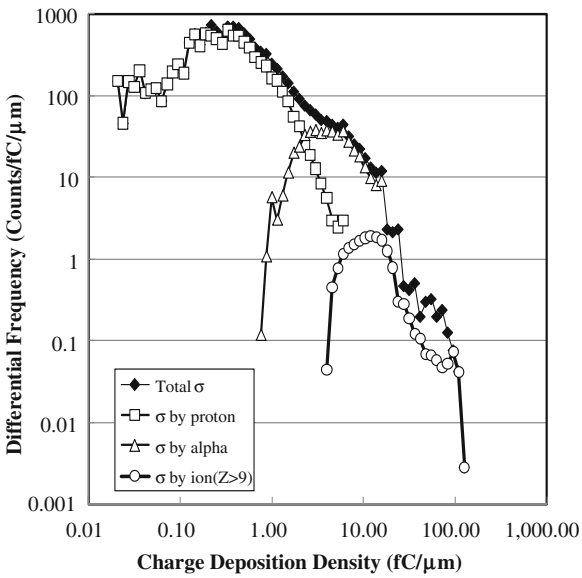


Fig. 2.25 Charge deposition density spectra when secondary ions penetrate the storage node (© 2010 IEEE)

low. Lighter particles (proton and alpha particle) play major roles for the deposition density below 10 fC/μm.

2.6.2.3 Total Charge Collected to Storage Node

Figure 2.26 shows the spectra of the total charge collected to the storage nodes for 22 and 130 nm SRAMs. When the collected charge excess the critical charge, SER takes places. In contrast to the charge deposition density, there are differences among different generations. The maximum collected charge decreases from 130 nm SRAM (36 fC) to 22 nm SRAM (20 fC), though the difference may not be so significant (16 fC).

In contrast, the soft-error susceptibility improves only slightly when the critical charge increases from 5 fC to 10 fC for 130 nm, but the change in the critical charge of $1 \rightarrow 2 \rightarrow 4 \rightarrow 10$ fC improves the susceptibility by one order of magnitude for each step for 22 nm SRAM, since protons and alpha particles play major role when the critical charge is relatively low. The range in the collected charge becomes lower as scaling proceeds.

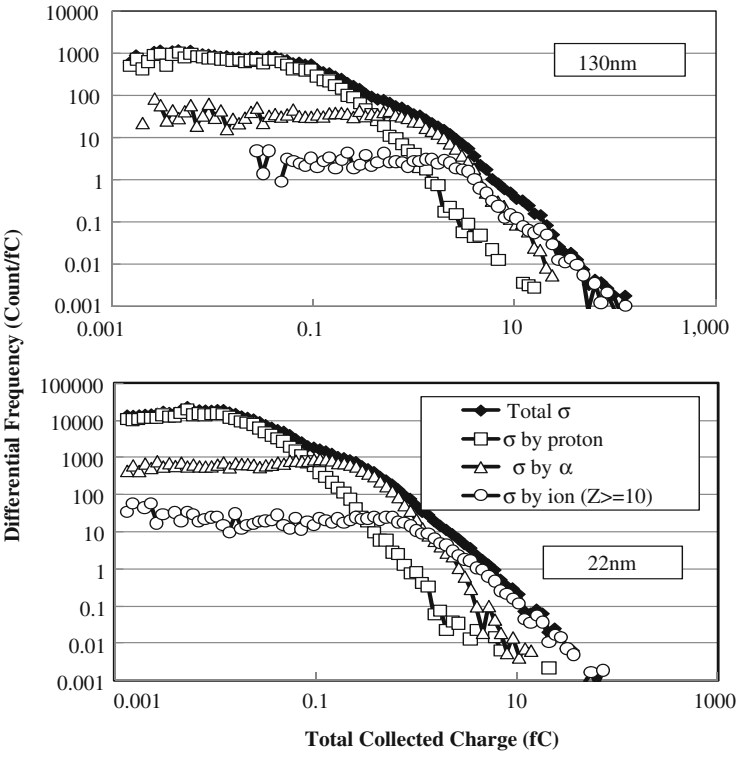


Fig. 2.26 Total collected charge spectra for 130 and 22 nm process SRAM (© 2010 IEEE)

2.6.2.4 Failed Bit Map (FBM)

Figure 2.27 shows the distribution of total failed bit map in the BL (perpendicular axis) and WL (vertical axis) address space when about 58,000 nuclear reactions take place in the four bits near the origin for the data pattern CB. It is seen that the area densely affected drastically increases from 130 nm (about 50 × 50 bits) to 22 nm (about 500 × 500). The automatic MCU classification tool, MUCEAC, has been introduced to make the statistic calculations from a number of MCUs and demonstrated for mainly 130 nm SRAM test results [16]. The extremely widened range of FBMs, however, would make the statistic calculations for MCU in neutron accelerated testing for 45–22 nm SRAM very painful or almost impossible task unless any ultra-high-speed automatic classification tool is developed.

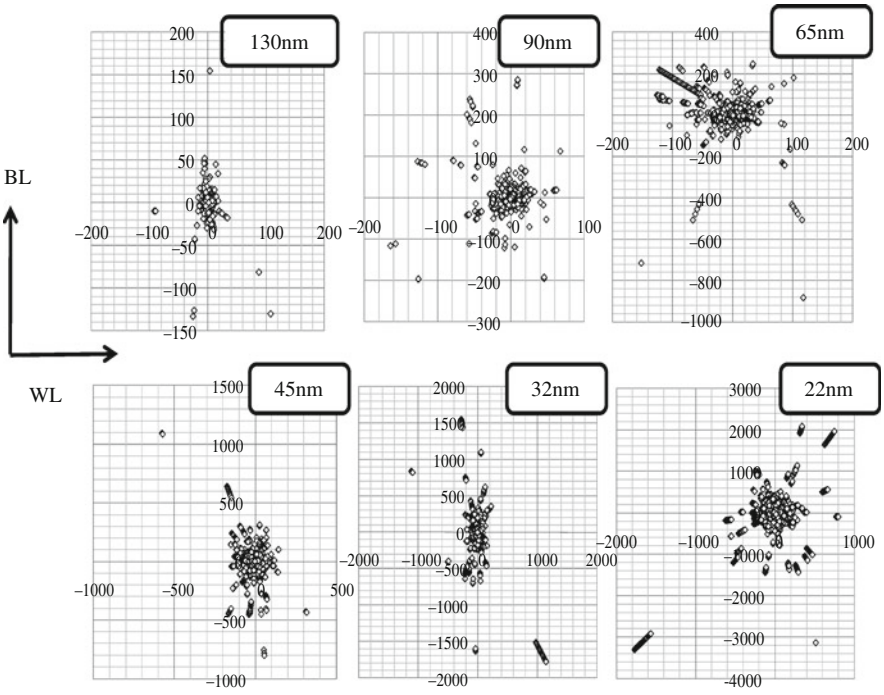


Fig. 2.27 Failed bit map for 58,000 nuclear spallation reaction with NYC sea level neutron spectrum from 130 nm SRAM to 22 nm SRAM (© 2010 IEEE)

2.6.2.5 Energy Dependency of SEU/MCU Cross-Section

SEU and MCU cross-sections for each generation are shown as a function of neutron energy in Figs. 2.28 and 2.29, respectively.

As scaling proceeds, the contribution of neutrons with energy lower than 10 MeV drastically increases due to increase in contribution of lighter particles as scaling

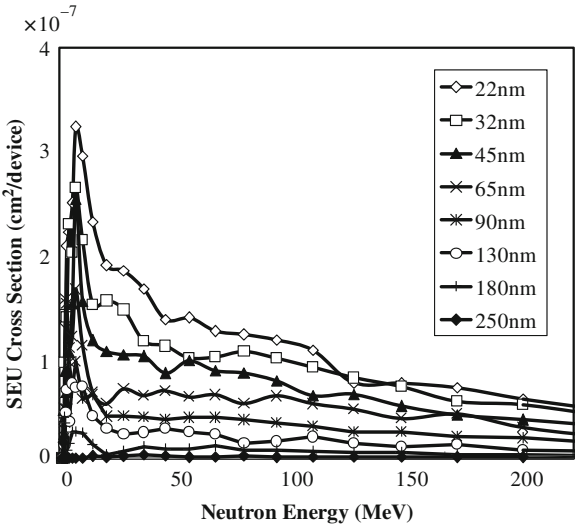


Fig. 2.28 Change in SEU cross-section curves from 250 nm SRAM to 22 nm SRAM (© 2010 IEEE)

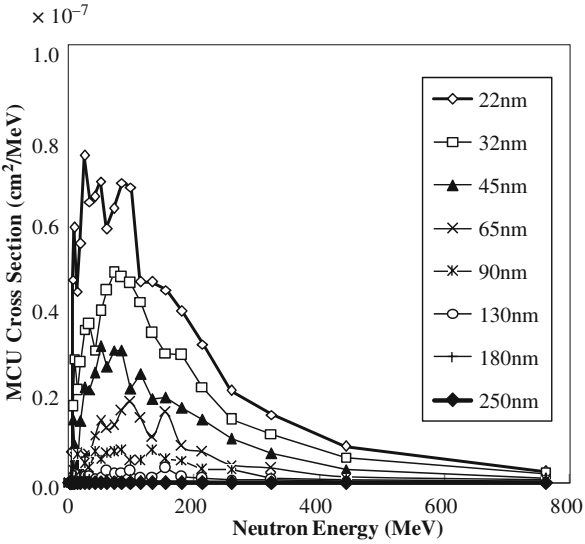


Fig. 2.29 Change in MCU cross-section curves from 250 nm SRAM to 22 nm SRAM (© 2010 IEEE)

proceeds. Recent experimental results with low-energy protons showed quite consistent trends with the predicted trends, where SEU cross-section has sharp peak for protons with energies lower than 10 MeV [57, 58]. This implies that two essential changes may be needed in the standard methods including JESD89A to estimate SER from accelerator-based testing, namely

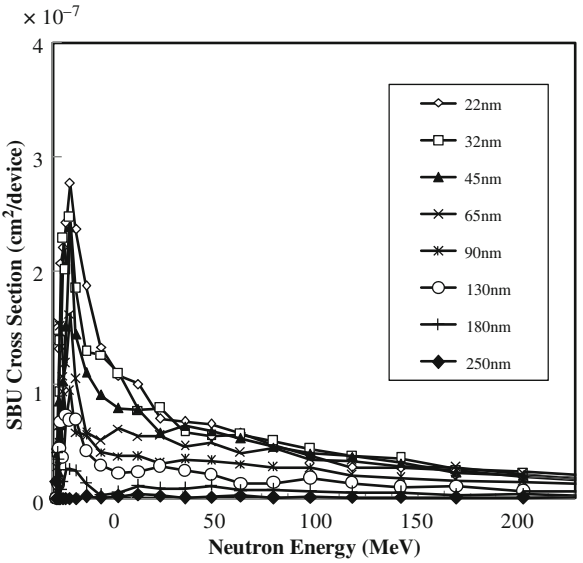


Fig. 2.30 Change in SBU cross-section curves from 250 nm SRAM to 22 nm SRAM (© 2010 IEEE)

(1) to include the contribution of neutrons with energy lower than 10 MeV to avoid large error in SER estimation when the spallation neutron sources are used;
(2) the ordinary excitation function with saturated cross-section should be modified to have a sharp peak at low neutron energy when the (quasi-) mono-energetic neutron sources are used.

In contrast, there are no essential changes in MCU cross-section shapes. This can be understood from the fact that the contribution of lighter particle to MCU is relatively low. Instead, the sharp peak is understood to originate from single-bit upset (SBU) as shown in Fig. 2.30. The cross-section curve for SBU can be obtained by subtraction of MCU cross-section in Fig. 2.29 from the SEU cross-section in Fig. 2.28.

2.6.2.6 Trends in MCU Ratio

Figure 2.31 shows the trends in MCU ratio to the total SEU. The ratio generally increases as neutron energy increases and scaling proceeds. When the neutron energy increases, heavy ions with higher energy are produced, flipping multiple memory cells. If the memory cells are packed more densely, the number of flipped MCU bits is naturally increased. The maximum ratio exceeds as high as 0.5 for 22 nm SRAM, indicating the MCU and MNU impacts become more serious.

2.6.2.7 Trends in MCU Multiplicity Distribution

Figure 2.32 shows the changes in MCU multiplicity distributions. It is seen that the multiplicity shifts to larger number of bits as scaling proceeds. The ratios of SBU

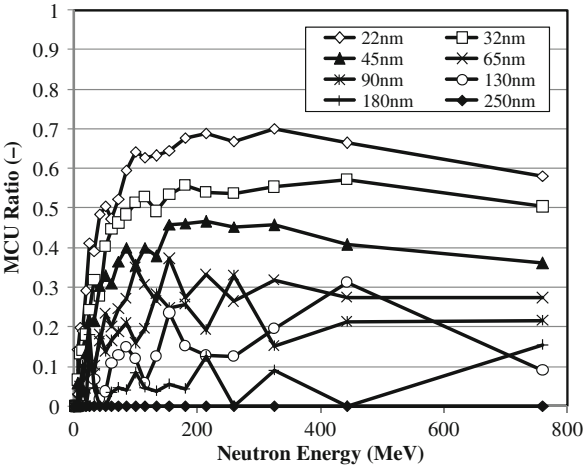


Fig. 2.31 Change in MCU ratio as a function of neutron energy from 250 nm SRAM to 22 nm SRAM (© 2010 IEEE)

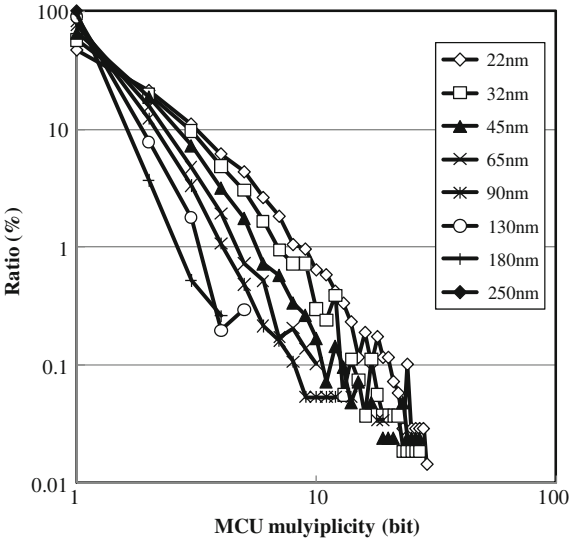


Fig. 2.32 Change in MCU bit multiplicity from 250 nm SRAM to 22 nm SRAM (© 2010 IEEE)

and lower multiplicity MCUs reduce correspondingly. The maximum multiplicity is well beyond tens of bits when scaling proceeds beyond 32 nm as mentioned before.

2.6.3 Validity of Simulated Results

In the present model, the depth profile of impurities and the maximum funneling length are fixed for all generation. But in reality, depth profile will be shallower and funneling length will also be shorter as concentration of impurities become higher.

These effects would work for suppressing SER. On the other hand, operation voltage may be reduced in reality as scaling proceeds. This works for worsening SER.

Change in the material in the device would make wider variation in the prediction. If the high-*k* material is used for gate oxide like HfO, the critical charge is increased to result in lower SER. Meanwhile, if the low-*k* material is used for interlayer oxide, parasitic capacitance is reduced, resulting in lower critical charge and higher SER.

The bipolar effects, which are not implemented in CORIMS at present, are somewhat in the trade-off relationship with the charge collection mode. When the operation voltage is reduced, the bipolar mode would decrease. When p-well size is shrunk, charge collection mode would be minor but bipolar mode would be activated due to shrinkage of distance of p–n junctions. Even when the bipolar effects are implemented into the CORIMS model, the total trends may not differ so significantly. This point will be more clearly shown in the future work.

2.7 SER Estimation in Devices/Components/System

2.7.1 Standards for SER Measurement for Memories

Reliability of CMOS devices are being impaired by environmental radiation sources such as alpha-ray emitting impurities in device packages and terrestrial high-energy neutrons. In late 1990s, terrestrial neutron-induced soft error in SRAMs has become one of the major concerns in reliability issues, overwhelming concerns in DRAM soft errors and alpha-ray-induced soft-errors [5]. In around 2000, data corruption in SRAMs in network components has emerged as serious threats for network reliability [55, 56]. Establishing standard testing methods was urgent for the device vendors and users to make databases for reliable design. JESD89 has been established in 2002 in order to fulfill this requirements based on in-depth discussions among experts in relevant fields. JESD89A [6] has been issued in 2003 as the revised version of JESD89, in which alpha-ray, thermal neutron [57], spallation neutron [52, 58–61], (quasi-mono) energetic neutron [44, 45, 53], and high-altitude/underground field tests [41, 62–66] are described in a more reasonable way compared to the original JESD89. SERs in logic devices and field programmable gate arrays (FPGAs) were discussed to a certain degree but test methods were not defined.

As the devices scaled down below 130–90 nm, concerns in alpha-ray-induced soft errors are rebooted mainly due to decrease in the critical charge Q_{crit}. Evidences in SERs in logic devices such as peripheral circuits in DRAMs are emerging as well.

2.7.2 Revisions Needed for the Standards

Recent works [36, 37, 67–71] show that SEU cross-section has high peak below 10 MeV due to secondary low-energy protons and the peak height continues to be higher as devices scale down. Such examples in a simulation work are shown in

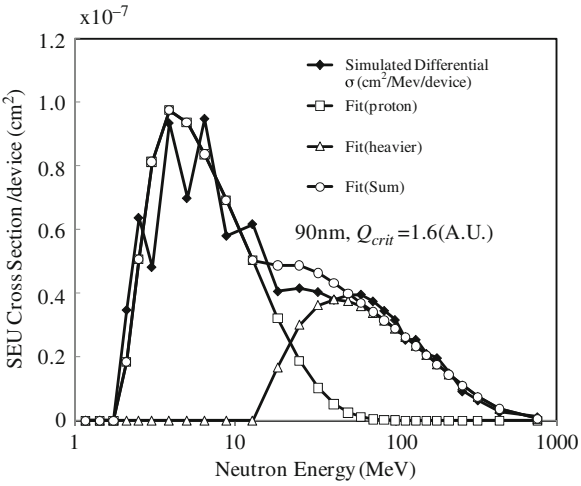


Fig. 2.33 Example of simulated excitation function of the 90 nm SRAM and fitted curve with sum of two (for proton and heavier ions) modified Weibull Fit curves

Fig. 2.33 [36, 37]. Compared to the shape of excitation function shown in Fig. 2.6, obvious large peaks appeared in the energy range below 10 MeV. Two peaks correspond to proton and alpha contributions that emerged from nuclear spallation reaction of neutron and silicon nucleus. It is seen that the peak heights get higher and threshold energies get lower as feature size becomes smaller, mainly due to decrease in the critical charge. $E_{\min}$ less than 10 MeV should be used in Eqs. (2.1) and (2.2) for devices with design rule smaller than 90 nm. The validation for the reason why the range is applicable has to be shown quantitatively. The range may differ depending on the combination of the object under test (OUT) and spallation neutron sources.

In quasi-mono-energetic test, approximation function of excitation function in Eq. (2.4) must be changed. The following function may be applied:

$$\sigma_{\mathrm{SEU}}(E_n) = \sigma_{\infty} \exp(-\lambda E_n) \left[1 - \exp \left\{ \left(\frac{E_n - E_{\mathrm{th}}}{W} \right)^s \right\} \right] \tag{2.6}$$

where λ is a decay constant (1/MeV).

Equation (2.4) in JESD89A is the simplest case with $\lambda = 0$. As shown in Fig. 2.33, two or more curves are recommended to fit proton/alpha and heavier secondary ion contributions. Sum of those curves can give overall excitation function. The excitation function may be given in the style of a look-up table also.

Logic gates (inverters, AND, OR, NOR, adder, ...) chain as shown in Fig. 2.34 with FFs in-between irradiated in neutron field can be used to obtain raw SERs in combinational and sequential logic gates [23–26]. Raw SER can be obtained after corrections for masking effects and errors in FF themselves are made.

Current major stream in the system SER evaluation focuses on the masking effects to obtain mean system SER value accurately [72].

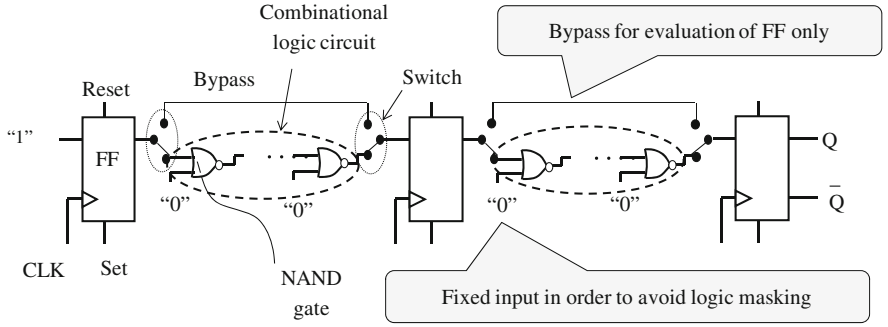


Fig. 2.34 Chain of NAND gates with FFs in-between to measure gate-level SER in NAND and FFs. By-pass is used by switching to measure SER in FF only

2.7.3 Quantification of SER in Logic Devices and Related Issues

Quantification in the chip-level SER evaluation may start with total raw SER of the system as expressed in Eq. (2.7):

$$\mathrm{SER_{UB}} = \sum_j (\mathrm{SER}_j^G \times N_j^G) + \sum_j (\mathrm{SER}_i^M \times N_i^M) \tag{2.7}$$

where $\mathrm{SER}_j^{\mathrm{G}}$: SER of a jth gate; N_j^{G}: number of jth gates; $\mathrm{SER}_i^{\mathrm{M}}$: SER of a ith memory and N_i^{M}: number of ith memories.

Contribution of combinational (inverters, AND, OR, NOR, adder, ...) and sequential (FF and latch) logic gates to the chip-level SER can be twofold: (a) direct incidence sequential gates from inside, clock or set/reset channel and (b) indirect incidence from input as indicated in Fig. 2.35. As for indirect incidence, SET noise may not be latched to the flip/flops due to three masking mechanisms such as window (timing), logic, and electric masking. Electric masking refers decay effect of pulse height by which the logical state of SET pulse is changed. Window masking refers non-active duration of FF input relevant to clock timing and clock

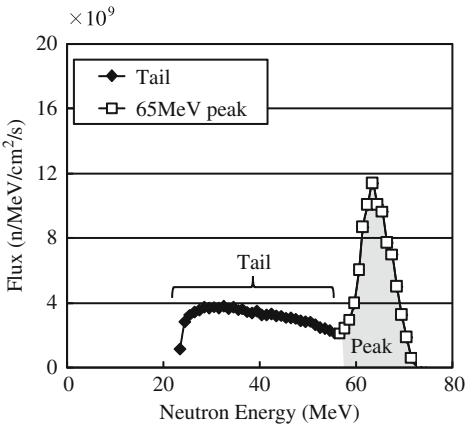


Fig. 2.35 Neutron spectrum used for the partial irradiation test in CYRIC. Peak flux is obtained at about 65 MeV (© 2010 IEEE)

width. Logical masking refers the effect of priority input in multi-input gate, by which SET pulse is disregarded.

(1) Methods to measure SER_j^M are almost established as in [6]. Some further development may be needed for MCU or bipolar effects except for the usage of MWF.
(2) Methods to measure SER_j^G have not been fully established, but logic gates chain methods, as typically shown in Fig. 2.34, are gaining popularity and seem attractive. The chain with FFs connected in-between can be used to obtain raw SERs in combinational and sequential logic gates. Usually, tremendous types of gates are implemented in a ULSI chip so that obtaining all SER_j^G by irradiation experiments is inevitably impossible. Instead, simulation tools like CORIMS validated in field can be used to evaluate SER_j^G .
(3) Quantification and mitigation methods for global control lines (clocks, SET/REST). In gate chain tests, dual-interlocked cell (DICE) is used assuming SER immune FFs. But this is not true at present. Some mitigation techniques are proposed for DICE-type FFs as mentioned before.
(4) More direct quantification by chip/board-level irradiation tests are also pursued [73–76]. An example of this type of test is described in Section 2.9. This method is quite straightforward, but time and cost consumption cannot be avoided. Some effective guidelines are needed for this type of tests to generalize the test results.

2.8 An Example of Chip/Board-Level SER Measurement and Architectural Mitigation Techniques

2.8.1 SER Test Procedures for Network Components

2.8.1.1 Full and Partial Board Irradiation Test

System-level neutron irradiation test was proposed first by Ibe et al. in 2005 [77] in order to identify problematic system first and then problematic components in the system. Full-chip irradiation test has been done with microprocessors, servers, and routers [73–75]. Partial board irradiation test for routers is first carried out by Shimbo et al. [76].

Merits and demerits are summarized in Table 2.6 for partial and full-board irradiation tests, respectively.

Table 2.6 Merits and demerits of full and partial board irradiation

	Full board irradiation	Partial board irradiation
Merit	-Can simulate natural terrestrial neutron radiation environments	-Can pinpoint susceptible components
Demerit	-Difficult to pinpoint susceptible components -Wide neutron beam is required	-Test results for the components may vary from the full board irradiation test

2.8.1.2 Neutron Facility

The quasi-mono-energetic neutron facility at CYRIC (cyclotron radio-isotope center) of Tohoku University [44] was utilized for the irradiation tests with neutron peak energy of 65 MeV. The neutron energy spectrum is shown in Fig. 2.35. Tail and peak parts are indicated in the figure. Neutron beams with other energy peaks are not utilized due to limit of machine time. The parameters summarized in Table 2.7 for the Weibull Fit are estimated from the 130 nm generation SRAM experimental data measured at neutron energies 1, 2, 5, 15 MeV in FNL [45], 30, 65 MeV in CYRIC [44], and 95, 170 MeV in TSL [54]. σ_∞ is fixed so that the Weibull Fit curve goes through the measured SEU cross-section at 65 MeV. Error in estimated SER due to this simplified procedure will be evaluated in Section 2.8.2.3. Figure 2.36 shows a schematic of irradiation room connected to the No. 3 TR 32 line. High-energy protons are bombarded to thin Li target from which neutron in the Li nuclei with almost same energy as the protons are evolved. Neutron beams are collimated by the concrete collimator into 10 cm $\times$ 10 cm square cross-section.

Figure 2.37 illustrates the layout of the test equipment. The board under test (BUT) is set up perpendicular to the neutron beam whose center is at 125 cm high from the floor surface and 40 cm apart from the aperture of the neutron collimator.

Table 2.7 Parameters used for conventional Weibull Fit and their possible ranges

Weibull Fit parameter	This study	Minimum	Maximum
σ_∞	Fitted to 65 MeV data	←	←
E_{th}	2	1	5
W	18.9	10	20
S	1.4	1	2

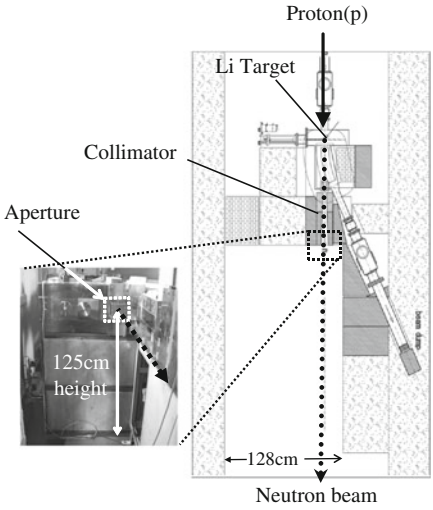


Fig. 2.36 Layout of irradiation room and a photograph of neutron beam aperture (© 2010 IEEE)

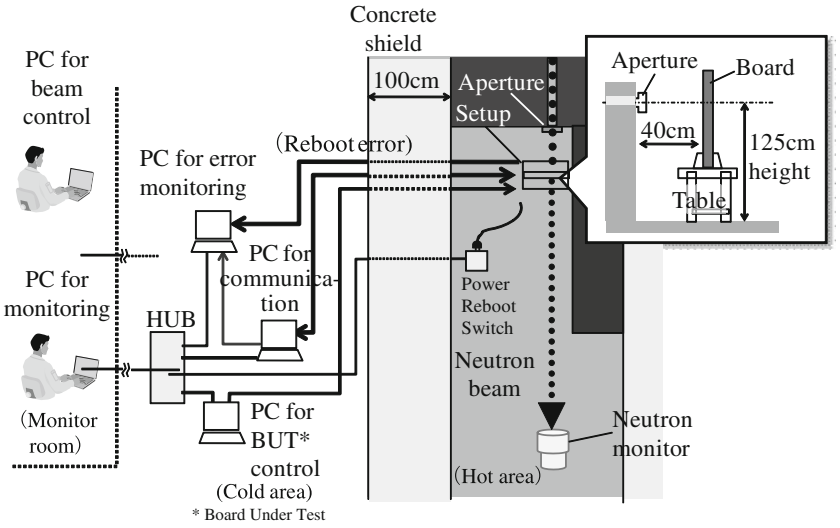


Fig. 2.37 Board setup and conceptual layout of experimental components (© 2010 IEEE)

The position of the table on which the BUT is set up is changed according to the part to be irradiated.

The failures are monitored with a PC placed in the cold (no neutrons) area just outside of 100 cm thick concrete wall. PCs for communication and BUT control are also placed in the same area. The signals from these PCs are connected to an Ethernet hub and monitored in the air-conditioned monitor room. A power rebooting switch is placed apart from neutron beam center and covered by Pb blocks in the irradiation room so as to minimize the influence on the switch from neutrons.

2.8.1.3 Architecture of Test Component

An FPGA chip, a CPU chip, and memory (SRAMs and SRAMs partially replaced by DRAMs) chip are chosen as partial irradiation parts on the board because they are believed to be the most vulnerable parts to neutron-induced soft error which can be recognized as system rebooting. The mechanisms of rebooting through stack, bus stack, and parity error are illustrated in Fig. 2.38.

Layout of parts in the board is shown in Fig. 2.39. The neutron beam areas for three chips are also shown in Fig. 2.39. Figure 2.40 shows the front view of the casing (430 mm hight × 700 mm width × 40 mm thickness) where the main board (285 mm height × 400 mm width) is located. Two types (sets A and B) of memory architectures are prepared as shown in Fig. 2.40. The CPU consists of 16 micro engines (MEs). Each ME contains an ME core and 32 KB internal memory. Part of SRAMs (10 MB) is not irradiated because of layout limit.

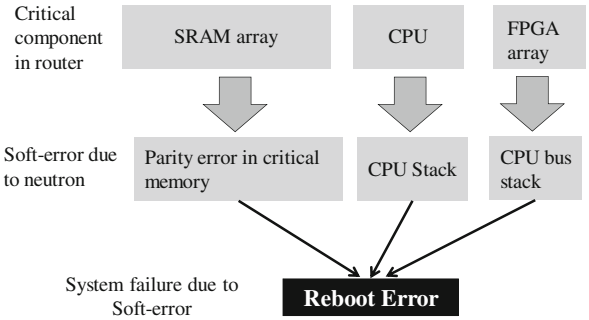


Fig. 2.38 Selection of critical components and mechanisms that cause rebooting the BUT (© 2010 IEEE)

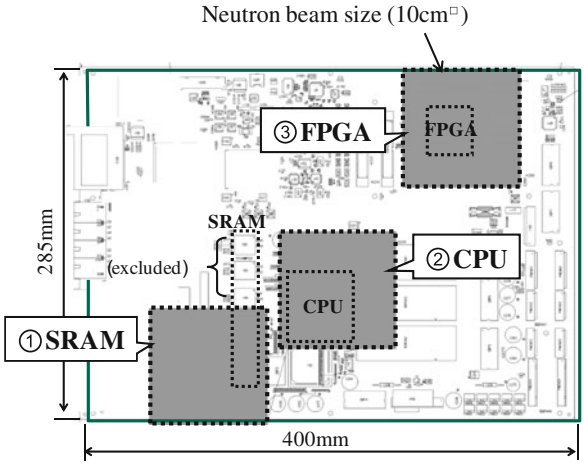


Fig. 2.39 Critical chip layout and irradiation area on the BUT (© 2010 IEEE)

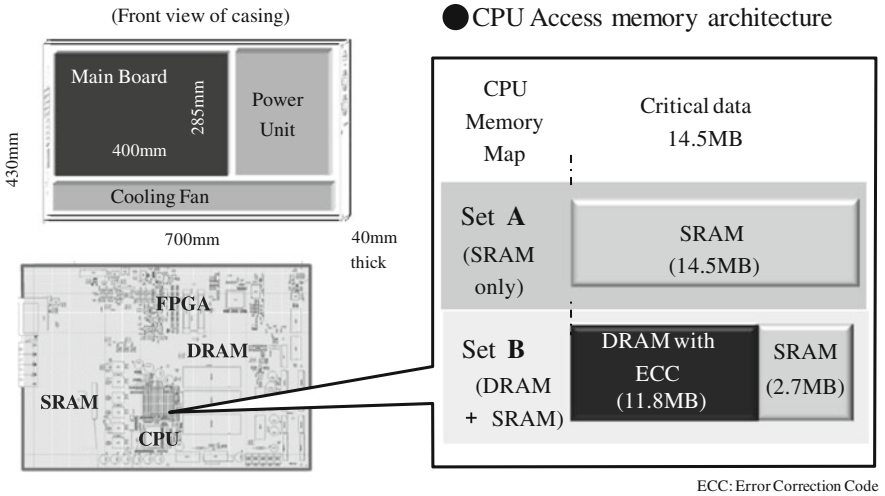


Fig. 2.40 Board casing and CPU access memory map for set A and set B (© 2010 IEEE)

In the memory chip, all 48 MB memory cells are SRAMs for the set A, while 12.5 MB memory cells for timer information which does not require high-speed operation are replaced by DRAMs in the set B. The rest 25.5 MB SRAM memory cells are unchanged because they are utilized to handle the session information and high-speed operation is required. Overall performance is almost equivalent between the sets A and B. Actual size of SRAMs in the test application are 14.5 and 2.7 MB for sets A and B, respectively. Contribution of DRAMs to overall failures is neglected because it is believed to be low enough compared to SRAMs [75].

2.8.1.4 Test Procedures

Direct error detection in each chip is not made, since only BUT failures, namely rebooting, can be commonly used for soft-error susceptibility among three types of chips. System rebooting is found automatically by a PC for error monitoring outside the shielding wall, as shown in Fig. 2.37. Figure 2.41 shows the flowchart of the test procedure. First, the location of the BUT is adjusted to make the neutron beam located on the target chip. A red laser light is used for accurate positioning. After the communication between the BUT and the monitor room is established by using a test program, neutron beam is turned on. Immediately after the neutron beam is on, the timer is turned on to measure time to failure (TTF). When a reboot takes place, error-log and BUT status data are collected. The present BUT is supposed to reboot itself automatically for self-testing if rebooting is successfully done. If automatic

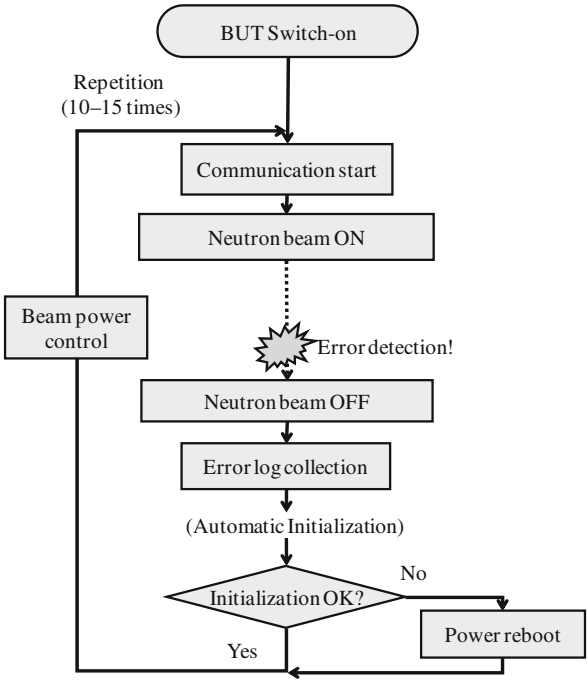


Fig. 2.41 Flowchart of irradiation test (© 2010 IEEE)

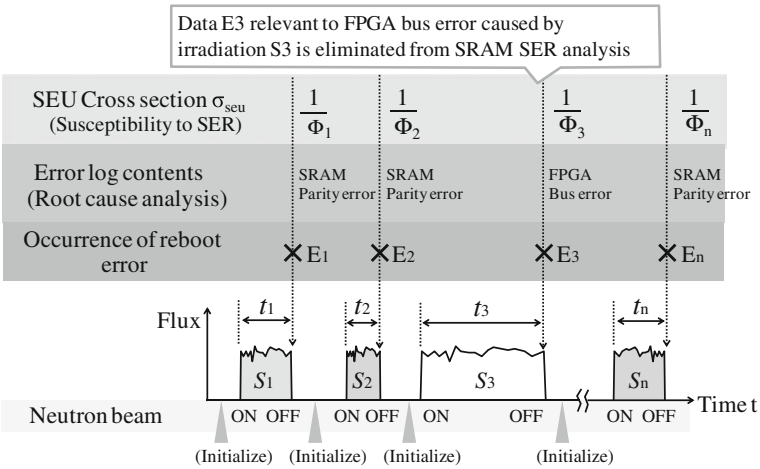


Fig. 2.42 Image of data acquisition and handling (© 2010 IEEE)

reboot is not done due to error in the BUT, BUT is forced to reboot by the rebooting switch.

This procedure is repeated about 10 times to obtain the average cross-section for each chip. Figure 2.42 illustrates an image of data acquisition. Neutron flux is roughly stable as shown in the bottom. The neutron beam is shut off when rebooting take places due to, for example, parity error in SRAMs and its fluence $\boldsymbol{\Phi}_i$ in ith irradiation period is estimated. Here, we define $\boldsymbol{\Phi}_i$ as (ith) fluence to failure (FTF). Only if the neutron flux ϕ is very stable (this is not the case in many neutron facilities), FTF can be calculated by

$$\mathrm{FTF} = \phi \mathrm{TTF} \tag{2.8}$$

Otherwise, FTF is estimated from total proton charge bombarded to the Li target to ith TTF. If rebooting is found through root cause analysis to be caused by other parts, for example, FPGA bus error as shown in Fig. 2.42, that are not directly irradiated, the data is eliminated from data analysis for the relevant chip.

As each irradiation cycle corresponds to one failure, mean SEU cross-section σ_{seu} can be obtained in the following manner:

First, mean FTF (MFTF) can be calculated by

$$\mathrm{MFTF} = \frac{1}{n}\sum_{1}^{n} \Phi_i. \tag{2.9}$$

Then,

$$\sigma_{\mathrm{seu}} = \frac{1}{\mathrm{MFTF}} \tag{2.10}$$

where n is the total number of cycles for the relevant chip or board.

2.8.2 Results and Discussions

2.8.2.1 Test Results

Test results of estimated SER in Tokyo sea level are summarized in Table 2.8for total, SRAM, CPU, and FPGA in sets A and B, respectively. The RTSER (system reboot) measured in Tokyo sea level for about 1 year is also shown for sets A and B in the table.

Table 2.8 Test results of SER normalized at Tokyo sea level for set A and B in accelerated and field tests

		SER Estimated at Tokyo sea level (AU)				
			Accelerated Test			
Set	SRAM Density Use (MB)	Field Test Board	Board	Chip	SER	Ratio (%)
A	14.5	46.8	7.6	SRAM	7.22	95
				CPU	0.38	5
				FPGA	–	–
B	2.7	5.2	1.0	SRAM	0.96	96
				CPU	0.03	3
				FPGA	0.01	1

Source: (© 2010 IEEE)

The architectural mitigation method is found to be effective and it can reduce SER in the BUT by a factor of about 8–9. As also shown in Fig. 2.43, this reduction ratio is consistent between the field and accelerator tests.

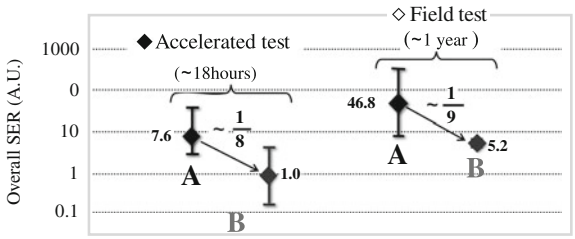


Fig. 2.43 Comparison of estimated SER in accelerator test and measured SER in field for sets A and B (© 2010 IEEE)

2.8.2.2 Efficacy of Partial Board Irradiation Test

It is seen that the most vulnerable part among three types of parts is identified as SRAM (about 95% of total rebooting events) by partial board irradiation test. Vulnerability in CPU seems to be low but care must be taken that vulnerability depends on the run in CPU and the number of FPGAs actually operated. In the present BUT, the number and operating ratio of FPGAs are relatively small.

Total irradiation duration in accelerated test is only 18 h, showing the efficacy of partial irradiation test compared to 1 year field test.

2.8.2.3 Correlation Between the Irradiation Test and Field Data

It is seen that the architectural mitigation method can reduce SER consistently in field and accelerator tests by a factor of about 10. The absolute values, however, are not consistent with each other: the SER in the field is higher than that in the accelerator test by a factor of 6 or 7.

Three factors that may cause this discrepancy are evaluated below:

(i) SER estimation error from the accelerator test due to possibly over-simplified procedure is explained in Section 2. Possible range of Weibull Fit parameters S, W, E_{th} are estimated empirically based on 130 nm generation SRAM data as also summarized in Table 2.7. Possible range of the error is estimated according to the parameter range. Maximum error in estimated SER is turned out to be about 15% so that the discrepancy seems to be difficult to explain due to this mechanism.

(ii) Difference in applications run on the CPU: The application applied to the accelerator test is simple once-write-and-read-many type operation. There is a possibility that the timing of start irradiation was too early compared to the timing by which the critical data (that cause rebooting) in SRAMs are stabilized and the number of SRAMs with critical data may be less than expected. Meanwhile, the application applied to the field is for normal commercial operation. The discrepancy may be explained by this kind of operating rate and more detailed study will be made in future.

(iii) Effect of low-energy neutrons.

Recent study made by Ibe et al. revealed that contribution of low-energy (1–10 MeV) neutron to SER is surprisingly enhanced as device scaling proceeds from 90 to 22 nm [36, 37], and revision of the Weibull Fit is obviously necessary. Experimental data for low-energy proton and some theoretical works that support the prediction are accumulating rapidly [67–71].

Typical SEU excitation curve simulated for a 90 nm SRAM is shown with a very high low-energy peak in Fig. 2.33, which is clearly different from the curve shown in Fig. 2.6. The low-energy peaks appeared in proton experiments are much higher (one or two orders of magnitude higher than higher energy part) than that predicted in the simulation. The simulation may under-estimate for some reason related to the device layout, structure, and electrical properties including Q_{crit}.

The simplified method assumes the conventional Weibull Fit curve using 3.5 MeV neutron data and eventually ignores the low-energy peak. This deficit may result in the discrepancy. As also indicated in Fig. 2.33, the simulation curve can be fitted by overlapping two newly proposed modified Weibull Fits (MWFs).

By using the MWF curve, the discrepancy can be reduced to a factor of three. As mentioned above, the simulation curve is obtained for our known design SRAMs. Actual layout, structure, and electrical properties, including Q_{crit} of the SRAMs in BUT, are not known and are very likely different from our known device to give a different MWF. Figure 2.44 shows (i) the conventional WF curve, (ii) a fitted MWF curve to the simulation results, and (iii) the MWF curve whose parameters in Eq. (2.6) are intentionally adjusted to cancel the discrepancy. Compared to the height for low-energy peak in the excitation function for the proton experiments, the peak height in the curve (iii) seems acceptable.

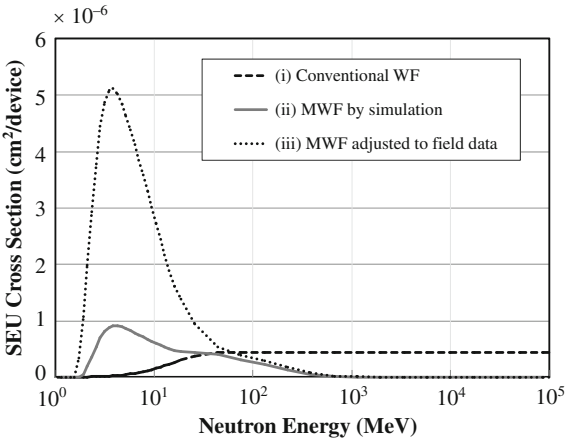


Fig. 2.44 Conventional WF curve, an MWF curve shown in Fig. 3.12, and an MWF curve adjusted to make SER estimate based on Eq. (2.3) consistent with the field data (© 2010 IEEE)

2.9 Hierarchical Mitigation Strategies

2.9.1 Basic Three Approaches

From a reliability viewpoint, mitigation design based on the average chip-level SER estimation methods mentioned in Section 2.7, however, somewhat dangerous if the variation due to circuits and applications (i.e., masking effects) is large as exemplified in Fig. 2.45a. Without certain knowledge of the variation (not necessarily

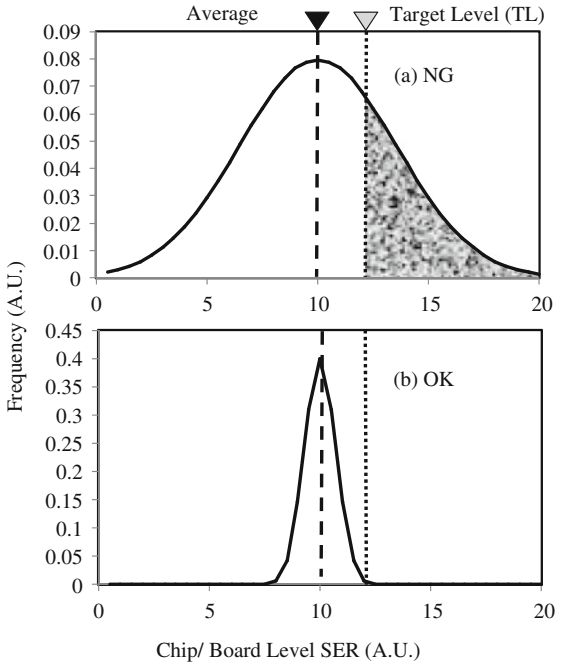


Fig. 2.45 Concept of availability of tolerable level set for chips. Availability depends significantly on the range of variation (© 2010 IEEE)

Poisson distribution) one may design an electronic product with too low SER tolerable level, which leads to under design.

If the variation is small enough, the margin can be small, as shown in Fig. 2.45b. Mitigation strategies can, therefore, be threefold as summarized in Table 2.9. First, current major strategy is design on the average (DOA), which determines the target SER level without the knowledge of variation. Second one is design on average with knowledge of variation (DOAV). Just design (cost, power, speed, and reliability) may be realized through this approach. This strategy including evaluation of logic-masking (or derating) is, however, quite difficult and time/cost consuming to realize because of possible wide variation depending on the circuits and applications.

Assuming Poisson distribution for memory errors, upper limit of device-level SER, SER_{ul} is given by the following equation [6]:

$$SER_{ul} = \frac{\chi^2_{(\alpha/2):k}}{2NT_r} \times 10^9 \tag{2.11}$$

where $\chi^2_{(\alpha/2):k}$: chi-square value given according to parameters α and k; α: ratio of population outside of the Poisson distribution, depending on the confidence level (CL). If CL = 95%, $\alpha = 0.1$ since CL $= 1 - \alpha/2(\%)$; k: degree of freedom $= 2(N_{err}+1)$; N_{err}: number of errors found at the time T_r (h); and N: number of devices tested.

As for chip-level SER, the variation is originated from circuits and applications. Since it is not a random process, this kind of statistical theory seems to be very difficult to establish.

The third strategy believed to be worthwhile to pursue is design on the upper bound (DOUB).

2.9.2 Design on the Upper Bound (DOUB)

The entire scope of DOUB is summarized in Fig. 2.46. Upper bound chip-level SER can be given by the simple summation of all raw SERs of gates and memories as already shown in Eq. (2.5). If the sum SER for a chip is acceptable from reliability viewpoint, no further action is needed for the chip. If not, simple countermeasure (simple exchange of weak gates/memory devices to stronger ones based on the raw SER database) would be applied stepwise.

If the contribution of memories to total chip-level SER is high, ECC with interleaving is effective mitigation technique. If the contribution of logic parts is high, more precise evaluation of the upper bound may be necessary first. Upper bound of masking effects or effects of some other factors independent of circuits and application may be implemented to the Eq. (2.5). Depth of pipe-line, number of bits in a word, number of cache layers maybe such factors.

Table 2.9 Concepts of mitigation design of chip-level SER

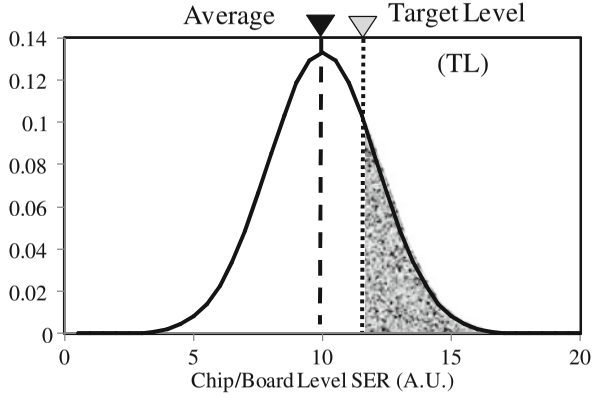
Class	Concept	Merit	Demerit
Design on average (DOA)		• Comparatively simple	• Risk of under design • Depends on circuits and application

Table 2.9 (continued)

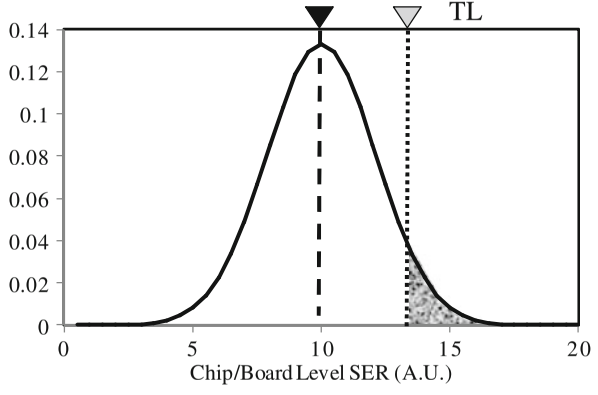
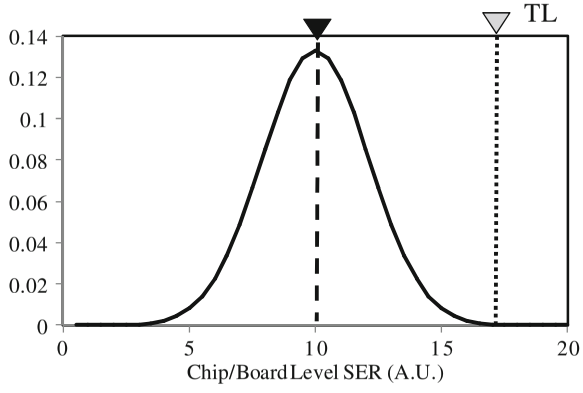
Class	Concept	Merit	Demerit
Design on average and variation (DOAV)		• Just design	• Depends on circuits and applications • High cost

Table 2.9 (continued)

Class	Concept	Merit	Demerit
Design on upper bound (DOUB)		• Simple • Does not depend on circuits and application • Low cost	• Risk of over design

Source: (© 2010 IEEE)

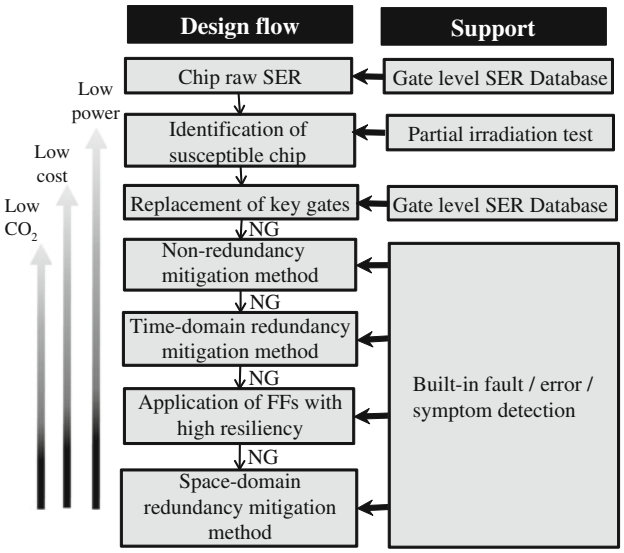


Fig. 2.46 General design flow of stepwise reduction in SER under the design on upper bound concept. Power consumption, cost, and global warming are key issues (© 2010 IEEE)

Upper bound masking factor, whose underlying physics is not necessarily the same as the conventional average masking factor and can be much more simple, may be defined and implemented. Operations that do not require high speed can be carried out with slower but more resilient gates or memories. Architectural countermeasure considering the best matches in trade-offs is one of the steps. The mitigation method described in Section 2.8 is one of such examples.

Further steps are applications and optimization of non- or small-redundancy mitigation method, time domain redundancy methods, and robust FF to SEUs and MNUs. Space redundancy methods may cause high cost and power dissipation, so that application of such techniques has to be avoided or limited to very small portion. Moreover, power consumption of network systems including data centers is becoming one of the top priority issues for future world-wide infrastructure to reduce carbon oxide. As high as 10% of total power consumption will be dedicated to network systems until 2020 unless effective countermeasures are applied (http://www.gimmiethescoop.com/data-center-power-consumption-global-warming-will-the-web-crash). Fault/error/symptom detection device or circuits may be effective for recovery if they are built-in at design phase. One of such recovery scheme LABIR is introduced in the following section.

2.10 Inter Layer Built-In Reliability (LABIR)

Even if space redundancy techniques are applied, they are intrinsically vulnerable against MNUs as mentioned before. Effective countermeasure listed in Fig. 2.47

Stack Layer	SLHBD (Single Layer Hardened-by-Design)	LABIR
Application	・Error aware software for multi-thread processor	・Error recovery algorithm
System	・Multi-boards or components (parallel operation and switching)	
Board	・Replacement of susceptible chip	・Neutron error log
Chip	・TMR ・Duplication+Comparison ・Replication+rollback	・Neutron error log
Circuit	・Error aware synthesis EDA tool ・Layout aware system simulation ・RAZOR, DICE, SEUT ・ECC	・BIST
Device	・Optimized well/node structures	・BICS/BIPS

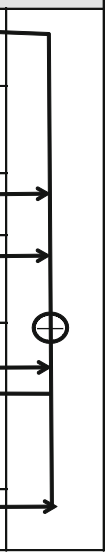


Fig. 2.47 Single layer hardened-by-design and examples of LABIR

and implemented in a single stack layer (device, chip, board, . . .) seems to be almost impossible as the device scaling proceeds.

Obviously, MNU cannot be controlled in the device layer. Specially designed items that make reliability-related communication and action possible between two or more layers may be effective for overall reliability. We call this kind of our approach as LABIR. Concept of a similar approach has been introduced in SELSE VI [78].

LABIR concept is also illustrated in Fig. 2.47. LABIR proposes interactive or communicative mitigation techniques in which a recovery action such as rollback to the checkpoint ignited when a layer finds any error symptom, not necessarily error or fault itself. Built-in self-test (BIST) [79–81], built-in current (pulse) sensor (BICS [82], BIPS)) can be used for such kind of technique. By using BIPS, a pulse propagated from a multi-coupled bipolar interaction (MCBI) [16] zone in p-well is supposed to be detected and ignite the rollback operation in the ULSI chip.

2.11 Summary

Trends in terrestrial neutron-induced soft error in SRAMs down to 22 nm process are predicted by using the Monte-Carlo simulator CORIMS, which is validated to have less than 20% variations from experimental data in a wide variety of neutron

fields like the low and high-altitude field tests and the accelerator tests in LANSCE, TSL, and CYRIC.

The following results are obtained:

(1) Soft-error rates per device in SRAMs will increase 3–7 times from 130 nm to 22 nm process.
(2) As SRAM is scaled down to smaller size, SEU is dominated more significantly by low-energy neutrons (<10 MeV). But MCU does not change drastically.
(3) The area affected by one nuclear reaction spreads well beyond 1 M bits area and multiplicity of multi-cell upset become as high as 100 bits and more.

The discussions are extended to the MNUs of logic devices/systems and countermeasures to them. New bipolar SEU mode is investigated by (quasi-)mono-energetic neutron test and Monte-Carlo and TCAD simulations. The mode turned out to be caused by penetration of secondary ions through p–n junctions (not necessarily storage nodes) and be a parasitic thyristor action triggered by single-event snapback in p-well. The mode can also cause MNU with high probability.

Recent novel trends and data with device scaling below 100 nm are reviewed and the following shortages in current SER test standards are pointed out:

(1) Contributions of neutrons with energies lower than 10 MeV are becoming significant as predicted by simulation mentioned above. The energy range for the spallation neutron tests has to be reconsidered. The shape of SEU excitation function is also subject to be revised.
(2) Standard test methods for logic gates should be determined. Effects of SETs in the global control line for FFs (clock, set/reset lines) have to be taken into account.
(3) MNUs in combinational logic device have to be taken into consideration.
(4) Chip or board-level SER tests may be included with mitigation strategies in new SER standards.

A novel chip-level to board-level SER evaluation method for network routers is introduced by using 65 MeV quasi-mono-energetic neutron beams. Architectural mitigation technique against terrestrial neutron SER for the router is demonstrated. The method is based on the replacement of SRAMs to DRAMs in a chip where speed is not first priority considering operating ratio and showed about 10 times reduction in board-level SER. This reduction ratio is consistent with the field data for about 1-year commercial operation. The absolute SER level estimated from the accelerated test is, however, 6–7 times lower than the field data. Low-energy neutron contribution is pointed out as the most probable root of this discrepancy.

A generic strategy for low cost and low power consumption mitigation of chip and board-level SER based upon the stepwise upper bound reduction is proposed. Partial irradiation method is one of key techniques in this strategy. Inter-layer built-in reliability (LABIR) in which communicative mitigation techniques are applied

to among stack layers is also proposed as another key technology. LABIR can be robust against multi-node upsets (MNUs) in logic parts with low overhead in power, speed, cost, and area.

References

1. N. Sugii, R. Tsuchiya, T. Ishigaki, Y. Morita, H. Yoshimoto, K. Torii, and S. Kimura, "Comprehensive Study on V_{th} Variability in Silicon on Thin BOX (SOTB) CMOS with Small Random-Dopant Fluctuation: Finding a Way to Further Reduce Variation," *IEDM, San Francisco, December 15–17,* pp. 249–253 (2008).
2. R. Duarte, L. Martins-Filho, G. Knop, and R. Prado, "A Fault-Tolerant Attitude Determination System Based on COTS Devices," *IOLTS 2008, Greece, July 6–9, 2008*, No.4.3, pp. 85–92 (2008).
3. D. Villanueva, A. Pouydebasque, E. Robilliart, T. Skotnicki, E. Fuchs, and H. Jaoue, "Impact of the Lateral Source/Drain Abruptness on MOSFET Characteristics and Transport Properties," *2003 IEDM, Washington, DC, December 7–10, 2003*, No.9.4 (2003).
4 H.-S. P. Wong, "Beyond the Conventional Transistor," *IBM J. Res. Develop.*, Vol. 46, No. 2/3, pp. 133–168 (2002).
5. E. Ibe, "Current and Future Trend on Cosmic-Ray-Neutron Induced Single Event Upset at the Ground Down to 0.1-Micron-Device," *The Svedberg Laboratory Workshop on Applied Physics, Uppsala, May 3, 2001,* No.1 (2001).
6. JEDEC, "Measurement and Reporting of Alpha Particles and Terrestrial Cosmic Ray-Induced Soft Errors in Semiconductor Devices: JESD89A," *JEDEC STANDARD, JEDEC Sold State Technology Association, Arlington, VA., USA*, No.89, pp. 1–85 (2006).
7. JEITA, "JEITA SER Testing Guideline," *EIAJ EDR-4705, Tokyo, Japan*, pp. 1–62 (2005).
8. IEC, "Part 38: Soft Error Test Method for Semiconductor Devices with Memory," Semiconductor Devices. Mechanical and Climatic Test Methods," *IEC60749-38*, Edition 1.0, pp. 1–9 (2008).
9. Automotive Electronics Council, "Failure Mechanism Based Stress Test Qualification for Integrated Circuits," AEC-Q100-Rev.G, May 14 (2007).
10. T. Heijmen, E. Ibe, P. Roche, F. Vermunt, and A. Bougerol, "Panel:SER in Automotive: What is the Impact of the AEC-Q100-G Spec?," *IOLTS 2008, Greece, July 6–9, 2008*, No.S3, p. 161 (2008).
11. D. Radaelli, H. Puchner, P. Chia, S. Wong, and S. Daniel, "Investigation of Multi-Bit Upsets in a 150 nm Technology SRAM Device," *Trans. Nucl. Sci.,* Vol. 52, No. 6, pp. 2433–2437 (2005).
12. O. Musseau, Gardic P. Roche, T. Corbiere, R.A. Reed, S. Buchner, et al., "Analysis of Multiple Bit Upsets in a CMOS SRAM," *Trans. Nucl. Sci.,* Vol. 43, No. 6, pp. 2879–2888 (1996).
13. J. Maiz, S. Hareland, K. Zhang, and P. Armstrong, "Characterization of Multi-Bit Soft Error Events in Advanced SRAMs," 2*003 IEEE International Electron Devices Meeting, Washington, DC, December 7–10, 2003,* No.21.4 (2003).
14. E. Ibe, H. Kameyama, Y. Yahagi, K. Nishimoto, and Y. Takahashi, "Distinctive Asymmetry in Neutron-Induced Multiple Error Patterns of 0.13 μm Process SRAM," *The 6th International Workshop on Radiation Effects on Semiconductor Devices for Space Application, Tsukuba, October 6–8, 2004,* pp. 19–23 (2004).
15. N. Seifert, and V. Zia, "Assessing the Impact of Scaling on the Efficacy of Spatial Redundancy Based Mitigation Schemes for Terrestrial Applications," *SELSE3, Austin, TX, April 3, 4, 2007* (2007).
16. E. Ibe, S. Chung, S. Wen, H. Yamaguchi, Y. Yahagi, H. Kameyama, S. Yamamoto, and T. Akioka, "Spreading Diversity in Multi-Cell Neutron-Induced Upsets with Device Scaling," *2006 CICC, San Jose, CA, September 10–13,* pp. 437–444 (2006).

17. K. Pagiamtzis, N. Azizi, and F. Najm, "A Soft-Error Tolerant Content-Addressable Memory (CAM) Using An Error-Correcting-Match Scheme," *Idem.*, pp. 301–304 (2006).
18. B.D. Olson, D. Ball, K.M. Warren, L.W. Massengill, N.F. Haddad, S.E. Doyle, and D. McMorrow, "Simultaneous Single Event Charge Sharing and Parasitic Bipolar Conduction in a Highly-Scaled SRAM Design," *Trans. Nucl. Sci.,* Vol. 52, No. 6, pp. 2132–2136 (2005).
19. O.A. Amusan, L.W. Massengill, B.L. Bhuva, P.R. Fleming, and M.L. Alles, "Charge Collection and Sharing in a 130 nm CMOS Technology," *Trans. Nucl. Sci.,* Vol. 53, No. 6, pp. 3253–3258 (2006).
20. O.A. Amusan, L.W. Massengill, M.P. Baze, B.L. Bhuva, A.F. Witulski, J.D. Black, A. Balasubramanian, M.C. Casey, D.A. Black, J.R. Ahlbin, R.A. Reed, and M.W. McCurdy, "Mitigation Techniques for Single Event Induced Charge Sharing in a 90 nm Bulk CMOS Process," *IRPS 2008, Phoenix, Arizona, April 27–May 1,* No.5A.1 (2008).
21. K. Osada, K Yamaguchi, Y. Saitoh, and T. Kawahara, "Cosmic-Ray Multi-Error Immunity for SRAM, Based on Analysis of the Parasitic Bipolar Effect," *Symp. VLSI Circuits Dig.,* pp. 255–256 (2003).
22. T. Nakauchi, N. Mikami, A. Oyama, H. Kobayashi, H. Usui, and J. Kase, "A Novel Technique for Mitigating Neutron-Induced Multi-Cell Upset by Means of Back Bias," *IRPS 2008, Phoenix, Arizona, April 27–May 1, 2008,* No.2F.2, pp. 187–191 (2008).
23. M. Baze, J. Wert, J. Clement, M. Hubert, A. Witulski, O.A. Amusan, L. Massengill, and D. McMorrow, "Propagating SET Characterization Technique for Digital CMOS Libraries," *Trans. Nucl. Sci.*, Vol. 53, No. 6, pp. 3472–3478 (2006).
24. V. Ferlet-Cavrois, V. Pouget, D. McMorrow, J.R. Schwank, N. Fel, F. Essely, R.S. Flores, P. Paillet, M. Gaillardin, D. Kobayashi, J.S. Melinger, O. Duhamel, P.E. Dodd, and M.R. Shaneyfelt, "Investigation of the Propagation Induced Pulse Broadening (PIPB) Effect on Single Event Transients in SOI and Bulk Inverter Chains," *Trans. Nucl. Sci.,* Vol. 55, No. 6, pp. 2842–2853 (2008).
25. E.H. Cannon, and M., Cabanas-Holmen, "Heavy Ion and High Energy Proton-Induced Single Event Transients in 90 nm Inverter, NAND and NOR Gates," *Trans. Nucl. Sci.,* Vol. 56, No. 6, pp. 3511–3518 (2009).
26. T. Makino, D. Kobayash, K. Hirose, D. Takahashi, S. Ishii, M. Kusano, S. Onoda, T. Hirao, and T. Ohshima, "Soft-Error Rate in a Logic LSI Estimated from SET Pulse-Width Measurements," *Idem.*, pp. 3180–3184 (2009).
27. T. Calin, M. Nicolaidis, and R. Velazco, "Upset Hardened Memory Design for Submicron CMOS Technology," *Trans. Nucl. Sci.,* Vol. 43, No. 6, pp. 2874–2878 (1993).
28. S. Mitra, M. Zhang, N. Seifert, T. Mak, and K.S. Kim, "Built-In Soft Error Resilience for Robust System Design," *ICICDT2007, Austin, TX, May 18–20*, pp. 263–268 (2009).
29. T. Uemura, Y. Tosaka, H. Matsuyama, K. Shono, K. Takahisa, M. Fukuda, and K. Hatanaka, "Robust Against Soft-Error Latch for Protecting SEU by Charge Sharing and SET on Inter-Clock," *IRPS 2010, Anaheim, CA, USA, May 2–6* (2010).
30. H.-H. Lee, K. Lilja, and S. Mitra, "Design of a Sequential Logic Cell Using LEAP: Layout Design Through Error Aware Placement," *SELSE6, Stanford University, Stanford, CA, USA, March 23, 24* (2010).
31. M. Cabanas-Holmen, E.H. Cannon, A. Kleinosowski, J. Ballast, J. Killens, and J. Socha, "Clock and Reset Transients in a 90 nm RHBD Single-Core Tilera Processor," *Trans. Nucl. Sci.,* Vol. 53, No. 6, pp. 3505–3510 (2009).
32. N. Seifert, B. Gill, M. Zhang, V. Zia, and V. Ambrose, "On the Scalability of Redundancy Based SER Mitigation Schemes," *ICICDT2007, Austin, TX, May 18–20,* No.G2, pp. 197–205 (2007).
33. A. Lesea, and K. Castellani-Coulie, "Experimental Study and Analysis of Soft Errors in 90 nm Xilinx FPGA and Beyond," *2007 RADECS, Deauville, France, September 10–14*, No.DWL-13 (2007).
34. D. Skarin, and J. Karlsson, "Software Mechanisms for Tolerating Soft Errors in an Automotive Brake-Controller," *WDSN, Estoril, Lisbon, Portugal, June 29, 2009*, pp. D34–D38.

35. S. Wen, A. Silburt, and R. Wong, "IC Component SEU Impact Analysis," *SELSE4, University of Texas at Austin, Austin, TX, March, 26, 27* (2008).
36. E. Ibe, H. Taniguchi, Y. Yahagi, K. Shimbo, and T. Toba, "Scaling Effects on Neutron-Induced Soft Error in SRAMs Down to 22 nm Process," *WDSN, Estoril, Lisbon, Portugal, June 29* (2009).
37. E. Ibe, H. Taniguchi, Y. Yahagi, K. Shimbo, and T. Toba, "Impact of Scaling on Neutron-Induced Soft Error in SRAMs from a 250 to a 22 nm Design Rule," *IEEE Trans. Electron Devices*, Vol. 57, No. 7, pp. 1527–1538 (2010).
38. T. Nakamura, M. Baba, E. Ibe, Y. Yahagi, and H. Kameyama, "Terrestrial Neutron-Induced Sift-Errors in Advanced Memory Devices," *New Jersey, World Scientific* (2008).
39. C. Hu, "Alpha-Particle-Induced Field and Enhanced Collection of Carriers," *IEEE Electron Device Lett.*, EDL-3, No. 2, pp. 31–34 (1982).
40. E. Ibe, Y. Yahagi, F. Kataoka, Y. Saito, A. Eto, and M. Sato, "A Self-Consistent Integrated System for Terrestrial-Neutron Induced Single Event Upset of Semiconductor Devices at the Ground," *2002 ICITA, Bathurst, Australia, November 25–28, 2002*, No.273–221 (2002).
41. Y. Yahagi, E. Ibe, Y. Saito, A. Eto, and M. Sato, "Self-Consistent Integrated System for Susceptibility to Terrestrial-Neutron Induced Soft-Error of Sub-quarter Micron Memory Devices," *2002 International Integrated Reliability Workshop, Stanford Sierra Camp, S. Lake Tahoe, CA,* pp. 143–143 (2002).
42. E. Ibe, S. Chung, S. Wen, Y. Yahagi, H. Kameyama, S. Yamamoto, T. Akioka, and H. Yamaguchi, "Valid and Prompt Track-Down Algorithms for Multiple Error Mechanisms in Neutron-Induced Single Event Effects of Memory Devices," *RADECS, Athens, Greece, September 27–29, 2006,* No. D-2 (2006).
43. K. Johansson, P. Dyreklev, B. Granbom, N. Olsson, J. Blomgren, and P-U. Renberg, "Energy-Resolved Neutron SEU Measurements from 22 to 13.0 MeV," *Trans. Nucl. Sci.,* Vol. 45, No. 6, pp. 2519–2526 (1998).
44. A.V. Prokofiev, O. Bystrom, C. Ekstrom, V. Ziemann, J. Blomgren, U.S. Pomp, S., M. Osterlund, and U. Tippawan, "The TSL Neutron Beam Facility," *10th Symposium on Neutron Dosimetry, Uppsala, Sweden, June 12–13, 200*3, Lecture A1–4 (2006).
45. M. Baba, H. Okamura, M. Hagiwara, T. Itoga, S. Kamada, Y. Yahagi, and E. Ibe, "Installation and Application of An Intense ^{7}Li(p,n) Neutron Source for 20–90 MeV Region," *Radiat. Prot. Dosimetry,* Vol. 123, No. 1–4, pp. 13–17 (2007).
46. H.W. Bertini, A.H. Culkowski, O.W. Hermann, N.B. Gove, and M.P. Guthrie, "High Nnergy (E < 100 GeV) Intranuclear Cascade Model for Nucleons and Pions Incident on Nuclei and Comparisons with Experimental Data," *Phys. Rev. C,* Vol. 17, No. 4, pp. 1382–1394 (1978).
47. I. Dostrovsky, Z. Fraenkel, and G. Friedlander, "Monte Carlo Calculations of Nuclear Evaporation Process. III. Applications to Low-Energy Reactions," *Phys. Rev.*, Vol. 113, No. 3, pp. 3.83–702 (1959).
48. E. Ibe, Y. Yahagi, H. Kameyama, and Y. Takahashi, "Single Event Effects of Semiconductor Devices at the Ground," *Ionizing Radiat,* Vol. 30, No. 7, pp. 263–281 (2004).
49. S. Furihata, "Parameters Used in GEM", Thesis for PhD, Tohoku University, pp. 18–20 (2002)
50. F. Bertland, and R. Peele, "Complete Hydrogen and Herium Particle Spectra from 30- to 60-MeV Proton Bombardment of Nuclei with A=12 to 209 and Comparison with the Intranuclear Cascade Model," *Phys. Rev. C,* Vol. 8, No. 3, pp. 1045–1064 (1973).
51. K.M. Warren, J.D. Wilkinson, R.A. Weller, B.D. Sierawski, R.A. Reed, M.E. Porter, M.H. Mendenhall, and R.D. Schrimpf, L.W. Massengill, "Predicting Neutron Induced Soft Error Rates: Evaluation of Accelerated Ground Based Test Methods," *IRPS 2008, Phoenix, AZ, April 27–May 1,* No.5A.2, pp. 473–477 (2008)
52. P.W. Lisowski, "The Los Alamos National Laboratory Spallation Neutron Sources," *Nucl. Sci. Eng.,* Vol. 103, pp. 208–218 (1990).
53. M. Baba, M. Takada, T. Iwasaki, S. Matsuyama, T. Nakamura, H. Ohguchi, T. Nakao, T. Sanami and N. Hirakawa, "Development of Monoenergetic Neutron Calibration Fields

Between 8 keV and 15 MeV," *Nucl. Instrum. Methods Phys. Res. A*, Vol. 376, pp. 115–123 (1996).
54. A. Dixit, R. Heald, and A. Wood, "Trends from Ten Years of Soft Error Experimentation," *SELSE 5, Stanford University, Stanford, CA, March 24, 25* (2009).
55. S. Wen, "Systematical Method of Quantifying SEU FIT," *IOLTS 2008, Greece, July 6–9, 2008,* pp. 109–116 (2008).
56. G. Schindlbeck, and C. Slayman, "Neutron-Induced Logic Soft Errors in DRAM Technology and Their Impact on Reliable Server Memory," *SELSE3, Austin, TX, April 3, 4, 2007* (2007).
57. R.C. Baumann, and E.B. Smith, "Neutron-Induced Boron Fission as a Major Source of Soft Errors in Deep Submicron SRAM Devices," *2000 IEEE Int'l Reliability Physics Symposium Proceedings, San Jose, CA, April 10–13*, pp. 152–157 (2000).
58. E.W. Blackmore, "Development of a Large Area Neutron Beam for System Testing at TRIUMF," *2009 IEEE Radiation Effects Data Workshop, Quebec City, Canada, July 20–24*, pp. 157–160 (2009).
59. A.V. Prokofiev, J. Blomgren, R. Nolte, S. Rottger, S.P. Platt, and A.N. Smirnov, "Characterization of the ANITA Neutron Source for Accelerated SEE Testing at The Svedberg Laboratory," *Idem.*, pp. 166–173 (2009).
60. H. Sakai, H. Okamura, H. Otus, T. Wakasa, S. Ishida, N. Sakamoto, T. Uesaka, Y. Satou, S. Fujita, and K. Hatanaka, "Facility for the (p,n) polarization transfer measurement," *Nucl. Instrum. Methods Phys. Res.. Section A,* Vol. 369, pp. 120–134 (1996).
61. S.P. Platt, and Z. Torok, "Charge-Collection and Single-Event Upset Measurements at the Isis Neutron Source," *2007 RADECS, Deauville, France, September 10–14, 2007*, No.F-2 (2007).
62. H. Kobayashi, H. Usuki, K. Shiraishi, H. Tsuchiya, N. Kawamoto, G. Kase, and J. Merchant, "Comparison Between Neutron-Induced System-SER and Accelerated-SER in SRAMs," *2004 IRPS, April 25–29, Phoenix, AZ,* pp. 288–293 (2004).
63. A. Lesea, and J. Fabula, "Continuing Experiments on Atmospheric Neutron Effects on Deep Sub-micron Integrated Circuits," *RADECS, Athens, Greece, September 27–29, 2006,* No.D-4 (2006).
64. J-L. Autran, P. Roche, J. Borel, C. Sudre, C., Castellani-Coulie, D. Muntean, T. Parrassin, G. Gasiot, and J.-P. Schoellkop, "Altitude SEE Test European Platform (ASTEP): Project Overview, First Results in CMOS 130 nm and Perspectives," *Idem.,* No.D-5 (2003).
65. J.L. Autran, P. Roche, S. Sauze, G. Gasiot, D. Munteanu, P. Loaiza, M. Zampaolo, J. Borel, S. Rozov, and E. Yakushev, "Combined Altitude and Underground Real-Time SER Characterization of CMOS Technologies on the ASTEP-LSM Platform," *ICICDT2007, Austin, TX, May 18–20*, pp. 113–120 (2009).
66. Y. Tosaka, R. Takasu, T. Uemura, H. Ehara, H. Matsuyama, S. Satoh, A. Kawai, and M. Hayashi, "Simultaneous Measurement of Soft Error Rate of 90 nm CMOS SRAM and Cosmic Ray Neutron Spectra at the Summit of Mauna Kea," *IRPS 2008, Phoenix, AZ, April 27–May 1, 2008,* No.SE01, pp. 727–728 (2008).
67. B.D. Sierawski, J.A. Pellish, R.A. Reed, R.D. Schrimpf, K.M. Warren, R.A. Weller, M.H. Mendenhal, A.D. Tipton, M.A. Xapsos, R.C. Baumann, X. Deng, M.J. Campola, M.R. Friendlich, H.S. Kim, A.M. Phan, and C.M. Seidleck, "Impact of Low-Energy Proton Induced Upsets on Test Methods and Rate Predictions," *Trans. Nucl. Sci.,* Vol. 56, No. 6, pp. 3085–3092 (2009).
68. B.D. Sierawski, K.M. Warren, R.A. Reed, R.A. Weller, M.M. Mendenhall, R.D. Schrimpf, and R.C. Baumann, "Contribution of Low-Energy Neutrons to Upset Rate in a 65 nm SRAM," *IRPS, Anaheim, CA, USA, May 2–6, 2010,* No.197 (2010).
69. D.F. Heidel, P.W. Marshall, J.A. Pellish, K.P. Rodbell, K.A. LaBe, J.R. Schwank, S.E. Rauch, M.C. Hakey, M.D. Berg, C.M. Castaneda, P.E. Dodd, M.R. Friendlich, A.D. Phan, C.M. Seidleck, M.R. Shaneyfelt, and M.A. Xapsos, "Single-Event Upsets and Multiple-Bit Upsets on a 45 nm SOI SRAM," *Trans. Nucl. Sci.,* Vol. 56, No. 6, pp. 3499–3504 (2009).
70. R.K. Lawrence, J.F. Ross, N. Haddad, D. Albrect, R.A. Reed, and M.A. McMahan-Norris, "Soft Error Sensitivities in 90 nm Bulk CMOS SRAMs," *2009 IEEE Radiation Effects Data Workshop, July 20–24, Quebec, Canada,* pp. 123–126 (2009).

71. C. Slayman, “Accuracy of Various Broad Spectrum Neutron Sources for Accelerated Soft Error Testing,” *SELSE6, Stanford University, Stanford, CA, March 23, 24* (2010).
72. H. Chapman, E. Landman, A. MargalitIlovich, Y.-P. Fang, A.S. Oates, D. Alexandrescu, and O. Lauzeral, “A Multi-Partner Soft Error Rate Analysis of an Infini Band Host Channel Adapter,” *SELSE6, Stanford University, Stanford, CA, March 23, 24* (2010).
73. H. Ando, and S. Hatanaka, “Accelerated Testing of a 90 nm SPARC3.4 V Microprocessor for Neutron SER,” *SELSE3, Austin, TX, April 3, 4* (2007).
74. A.L. Silburt, A. Evans, I. Perryman, S.-J. Wen, and D. Alexandrescu, “Design for Soft Error Resiliency in Internet Core Routers,” *Trans. Nucl. Sci.*, Vol. 56, No. 6, pp. 3551–3555 (2009).
75. L. Borucki, G. Schindlbeck, and C. Slayman, “Comparison of Accelerated DRAM Soft Error Rates Measured at Component and System Level,” *IRPS 2008, Phoenix, AZ, April 27–May 1,* No.5A.4 (2008).
76. K. Shimbo, T. Toba, E. Ibe, and K. Nishi, “Correlation of Mitigation of Soft-Error Rate of Routers Between Neutron Irradiation Test and Field Soft-Error Data,” *IEICE Tech. Rep.*, Vol. 109, No. 317, 318, pp. 51–55 (2009) (In Japanese).
77. E. Ibe, H. Kameyama, Y. Yahagi, and H. Yamaguchi, “Single Event Effects as a Reliability Issue of IT Infrastructure,” *ICITA, July 3–7, 2005, Sydney*, Vol. I, pp. 555–53.0 (2005).
78. N. Carter, “Cross-Layer Reliability,” *SELSE6, Stanford University, Stanford, CA, March 23, 24* (2010).
79. A. Sanyal, S. Alam, and S. Kundu, “A Built-In Self-Test Scheme for Soft Error Rate Characterization,” *IOLTS 2008, Greece, July 6–9, 2008*, No.3.3, pp. 65–72 (2008).
80. S. Prejean, “Neutron Soft Error Rate Testing of AMD Microprocessors,” *SELSE6, Stanford University, Stanford, CA, March 23, 24, 2010* (2010).
81. A. Balasubramanian, B.L. Bhuva, L.W. Massengill, B. Narasimham, R.L. Shuler, T.D. Loveless, and W. T. Holman, “A Built-In Self-Test (BIST) Technique for Single-Event Testing in Digital Circuits,” *Trans. Nucl. Sci.,* Vol. 55, No. 6, pp. 3130–3135 (2009).
82. T. Wang, Z. Zhang, L. Chen, A. Dinh, and R. Shuler, “A Novel Bulk Built-In Current Sensor for Single-Event Transient Detection,” *SELSE6, Stanford University, Stanford, CA, March 23, 24* (2010).

Chapter 3
Electromagnetic Compatibility

3.1 Introduction

Electromagnetic interference (EMI) causes malfunctions in electronic devices or components, resulting in hazardous consequences as soft and hard errors do. Electromagnetic compatibility (EMC) is defined as the ability of a device, equipment, or system to function satisfactorily in its electromagnetic environment without introducing intolerable electromagnetic disturbances to anything in that environment [1].

EMC problems are generally approached from two kinds of viewpoints: sources and receivers. In this chapter, the authors focus on the sources, in particular, printed circuit boards (PCBs) and their surrounding parts including chassis.

As illustrated in Fig. 3.1, typical PCBs consist of multi-layer conductive sheets with isolation layers in between [2]. Current in the layers or chassis connected with PCB with screws can be sources of electromagnetic disturbances.

A considerable number of concepts to improve EMC have been proposed and investigated for a long term, and also so many measurement techniques have been developed to investigate in more detail about those concepts, such as magnetic

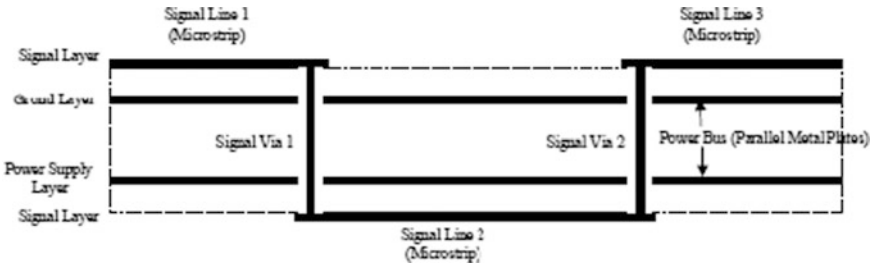


Fig. 3.1 Typical configuration of printed board circuit with ground, power supply, and signal lines [2]

Takashi Suga

N. Kanekawa et al., *Dependability in Electronic Systems*,
DOI 10.1007/978-1-4419-6715-2_3, © Springer Science+Business Media, LLC 2011

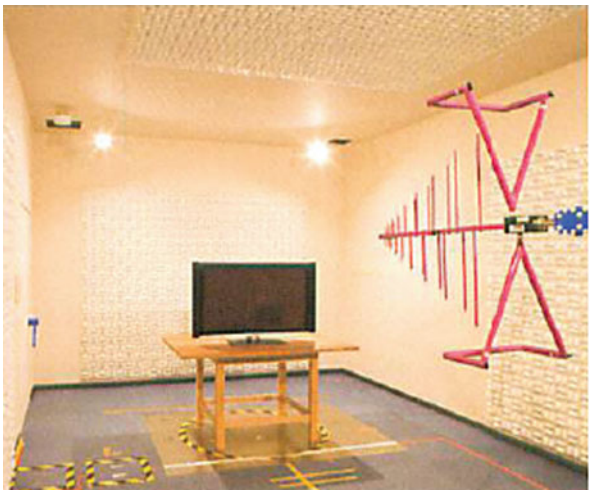


Fig. 3.2 Semi-anechoic chamber

near-field scanning which has been applied to various sorts of studies [3–5]. The higher operating speed of the latest electronics devices makes it more difficult to meet EMI regulations, leading to a long-term development time of a new product. The unintentional electromagnetic radiation from an electric device is commonly measured by using an anechoic chamber (see Fig. 3.2). That method measures the total EMI radiation and no analytic information is derived on the contribution of each part of the product to the total radiation. When the product fails to meet the EMI regulation, one needs to know which parts are the sources and how much each source should be reduced [6].

Following the enforcement of regulations on the electromagnetic radiation from electronic equipment, researchers are studying techniques for identifying radiation factors. Although radiation sources are identified in various ways, two main techniques have been investigated. One involves identification of the radiation efficiency of a printed circuit board, frame, or radiating element that functions as an antenna, and the other identifies the noise source current of an LSI or similar element that feeds power to a radiating element. These techniques are appropriately based on simulation or non-contact measurements that do not affect the current distribution or electromagnetic field environment, thereby allowing measurements without external influences.

We developed a new EMI measurement and analysis method to correctly identify the EMI source locations and to give quantitative description. The EMI-related development period of a new electronics product is drastically shortened with this technology. The principle of this method is as follows:

1. The near-field magnetic distribution of the operating circuit board is measured with a magnetic sensor.

2. The electric current distribution on the surface of the circuit board is calculated from the measurement result.
3. The radiated far-field EMI is calculated from the electric current distribution. The calculated electric field is equivalent to the result obtained by the EMI measurement using an anechoic chamber.

As this method first establishes the electric current distribution on the circuit board in operation and then calculates the resulting radiated EMI, the derived advantage is the analytic information on the contribution of each current segment to the total EMI radiation. This gives essential information directly useful for circuit designers when discussing EMI improvements of the product under development.

However, even if these EMC concepts are implemented in the design of PCB and it achieves exquisite EMC performance for just a PCB level, assembly with other components such as chassis, enclosure, or harness sometimes generates new EMC issues because generally the EMC design is optimized for each component level and each component is developed by different supplier/designer. These issues can become possible critical problems for product mostly at the stage of system integration, which cause significant time delay or extra developmental cost especially for the large-scale or complex systems consisting of a number of devices such as PCs, servers, or automotive application. Against this kind of issue, so many experimental and theoretical works have been ongoing not only for each component level such as cable, chassis, or enclosure with consideration of the total system, but also for the assembled components. The chassis or enclosure for PCB is one of the important components for EMC in integrated system, because it is mostly connected with circuit ground using connection parts such as screws, which means it can be the source of radiated emission excited by PCB ground bouncing besides the function as shielding. These design techniques of enclosure, which have been studied regarding the emission from chassis or the deterioration of shielding due to slots or holes [7–10], help to improve the system EMC but it can be more important for PCB to control and suppress the current flowing out through the chassis or enclosure by design of PCB. The effect of chassis with PCB on the electromagnetic emission has been investigated and reported [2, 11–14]. However, more investigation would be necessary to achieve general design concept which can be applied for PCB design in various configurations and systems.

Our study also focuses on the correlation between PCB design and radiated emissions from the chassis by investigating the current contributing to the emission, which would be junction current between chassis and PCB, to determine appropriate design guidelines for reduction of the radiated emission. The measurement technique of junction current and basic study has been reported [15]. In this chapter, the effect due to assembling with chassis and the correlation between junction current and radiated emission were investigated, including plural screws configuration. Then the junction current as source of the emission flowing through the screw was calculated using PSPICE model of PCB and chassis, which showed good correlation with the measurement result for junction current between PCB ground and chassis. Based on the investigation with SPICE calculation, a new concept to

reduce electromagnetic radiation from chassis with PCB was proposed and verified by actual measurement.

In the following, Section 3.2 describes the basic principle of EMI measurement, Section 3.3 describes the non-contact current distribution measurement technique for LSI packaging on PCBs, Section 3.4 describes the reduction technique of radiated emission from chassis with PCB, and Section 3.5 summarizes this chapter.

3.2 Quantitative Estimation of the EMI Radiation Based on the Measured Near-Field Magnetic Distribution

3.2.1 Measurement of the Magnetic Field Distribution Near the Circuit Board

The direction, magnitude, and phase of the magnetic field are measured near the surface of the board, as schematically shown in Fig. 3.3. Three tiny loop antennas assembled orthogonal to each other make a three-dimensional magnetic field sensor, as shown in Fig. 3.4. With this sensor, the magnetic field distribution on a plane in a constant short distance from the circuit board is measured in each orthogonal x–y–z direction. The output of the sensor is fed into a vector voltmeter to obtain the magnitude and phase of the magnetic field. The reference clock for the vector voltmeter is derived from the target circuit board.

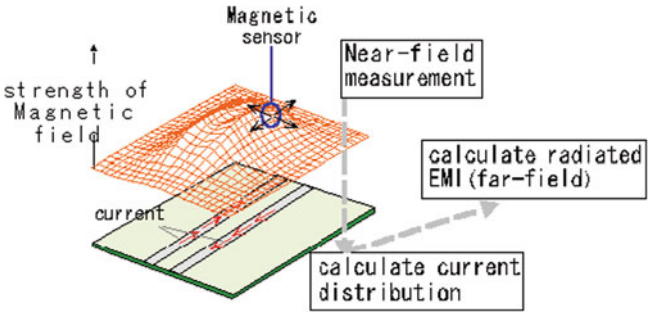


Fig. 3.3 Basic setup and procedures for EMI evaluation

3.2.2 Calculation of the Electric Current Distribution on the Circuit Board

The electric current distribution on the circuit board is calculated from the measured magnetic field distribution. The general calculation steps are explained below

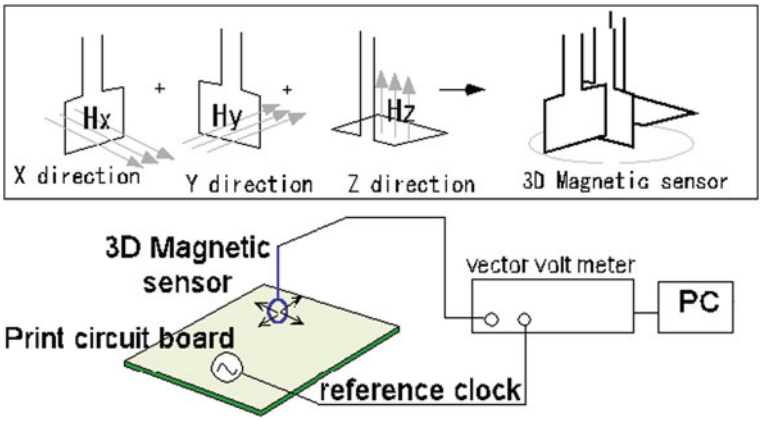


Fig. 3.4 Principle of the near-field measurement

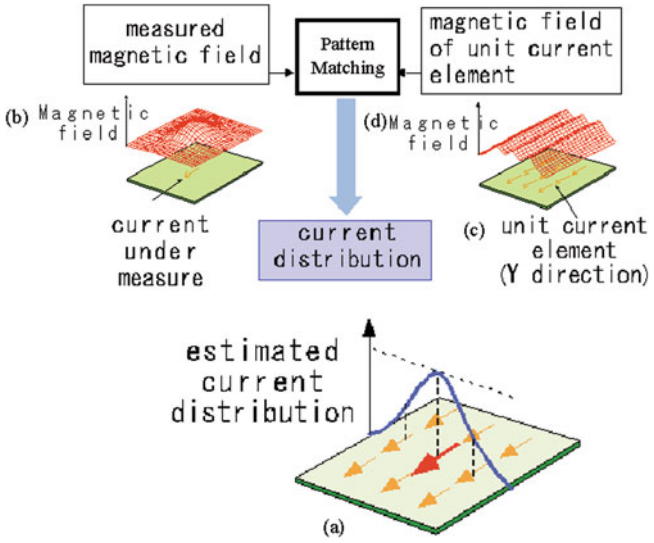


Fig. 3.5 Iterative procedure for calculation of current distribution

using the example shown in Fig. 3.5. With the existence of the electric current shown as (a), the magnetic field distribution on the board should be observed as shown in (b). Assuming unit current element uniformly distributed on the board as in (c), the resulting magnetic field distribution is calculated (Fig. 3.5d). Doing the pattern matching between the measured magnetic field and the calculated magnetic field from the uniformly distributed unit current elements derives the electric current existence probability. The distribution of the probability is displayed as the current

distribution. The advantage of this method over directly solving electromagnetic equations is the shorter calculation of CPU time and the process always finds results without being trapped in a diversified solution.

3.2.3 Calculation of the Far-Field Radiated EMI

With the calculated data on the direction, magnitude, and phase of the electric current distribution on the circuit board, the electric field in an arbitrary distance is obtained using Eq. (3.1):

$$E = \sum_{n=1}^{N} \frac{60\pi \cdot I_n \cdot dl}{\lambda \cdot r_n} \sin\phi_n \cdot e^{-jkr_n} \tag{3.1}$$

where I_n: magnitude of current element; r_n: distance; k: propagation constant; dl: length of current element; λ: wavelength.

The following are the results of the EMI measurement and analysis of a CPU circuit board using our proposed method:

(1) Figure 3.6 shows the estimated electric current distribution on the surface of the circuit board.
(2) Figure 3.7 shows the estimated far-field EMI under the same condition as the measurement in an anechoic chamber.
(3) The radiation from the front and backside of the board shows the highest value.

With this example, the following are made clear:

(1) The EMI of 65 dB μV/m is radiated from the board, which is exceeding the limit of EMI regulation.

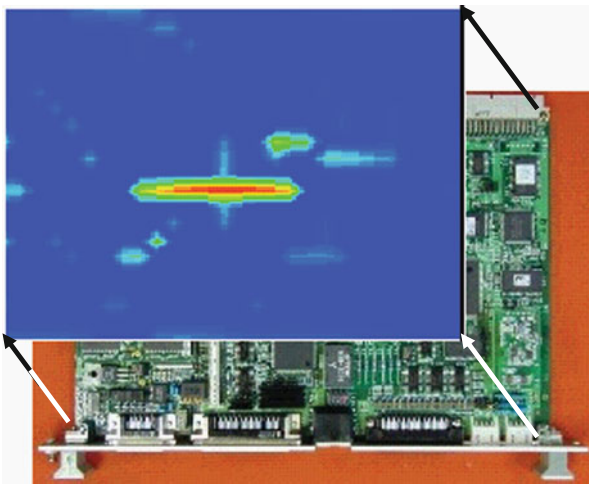


Fig. 3.6 Estimated current distribution of CPU board

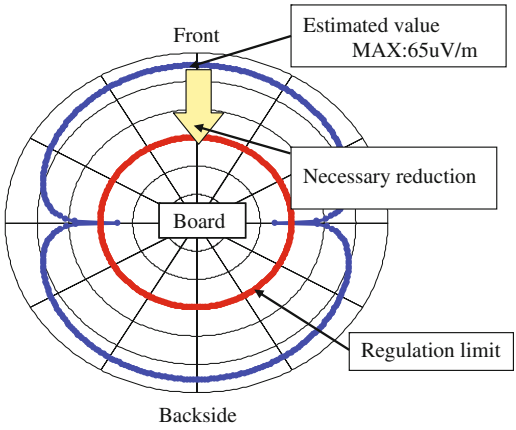


Fig. 3.7 Estimated EMI radiated from the CPU board

(2) The radiation source is the electric current shown as the red part in the right figure.
(3) The necessary reduction is 25 dB for satisfying the regulation limit.

The advantages of our proposed method are

(1) the quick and low-cost EMI measurement without using a costly anechoic chamber and
(2) analytic information on the EMI radiation source location for the prescription on EMI improvement.

3.3 Development of a Non-contact Current Distribution Measurement Technique for LSI Packaging on PCBs

3.3.1 Electric Current Distribution Detection

3.3.1.1 Target Specification

A current distribution detecting technique for identifying the noise source current of an LSI or similar element that feeds power to a radiating element requires a probing resolution of about 0.5 mm, corresponding to the pin pitch of an LSI package. In addition, the probing frequency range should be 30–1,000 MHz to satisfy the regulations on electromagnetic radiation.

3.3.1.2 Conventional and Proposed Technique for Obtaining Current Distribution

Electromagnetic field can be expressed with the simultaneous equations (3.2). This formula means that the magnetic field distribution $[H_m]$ is expressed with the product of the unit current $[I_n]$ and the function $[H_{mn}]$ based on the positional relation of the current and the assumed point of the magnetic field:

$$\begin{bmatrix} H_{mx} \\ H_{my} \\ H_{mz} \end{bmatrix} = \begin{bmatrix} 0 & Hx_y & Hx_z \\ Hy_z & 0 & Hy_z \\ Hz_x & Hz_y & 0 \end{bmatrix} \begin{bmatrix} I_{nx} \\ I_{ny} \\ I_{nz} \end{bmatrix} \tag{3.2}$$

Electromagnetic analysis is classified into forward analysis and inverse analysis. In forward analysis, the electromagnetic field distribution is directly calculated from a known current distribution. In inverse analysis, the current distribution is inversely calculated from a known electromagnetic field distribution. The current distribution can be obtained by solving the inverse matrix from Eq. (3.2) with a measured magnetic field distribution.

Although this technique produces an exact solution, doing so requires the solution of simultaneous equations. Furthermore, a number of magnetic field measuring points equal to the number of assumed current points are required, and the calculation time increases in proportion to the cube of the number of points. If the number of assumed current points is reduced, currents at extraneous points will cause the simultaneous equations to have no solution or diverge.

A technique for obtaining a current distribution, based on pattern matching, was therefore devised as a means of overcoming these disadvantages. The proposed method involves calculating mth magnetic field distributions $H_{mn}(x, y, z)$ with respect to the magnetic field measuring points based on a unit current element $I_n(x,y,z)$ assumed at the nth position (x,y,z) on the target. The current existence probability α_n can then be acquired from the degree of pattern matching with the measured magnetic field distribution $H_m(x,y,z)$:

$$\alpha_n = \frac{H_{mn} \cdot H_m}{|H_{mn}| \times |H_m|} \tag{3.3}$$

The near magnetic field distribution of the sample board shown in Fig. 3.8 was measured using the system shown in Fig. 3.9 under the conditions listed in Table 3.1. Figure 3.10 shows the results of measurement, and Fig. 3.11 shows the result of the current distribution obtained through this pattern matching.

When detecting a current distribution by pattern matching, setting more magnetic field measuring points than assumed current points is preferable for improving the current precision and positional resolution. As this pattern matching technique is a simple inner product operation (Eq. (3.3)), the calculation time is proportional to the square of the number of assumed current points. Even when the assumed current points differ from the actual current positions, this technique gives an outline of the current distribution, although the current and positional accuracy may decrease.

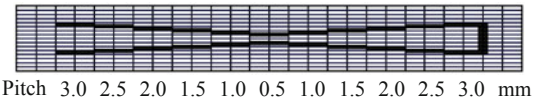


Fig. 3.8 Sample board

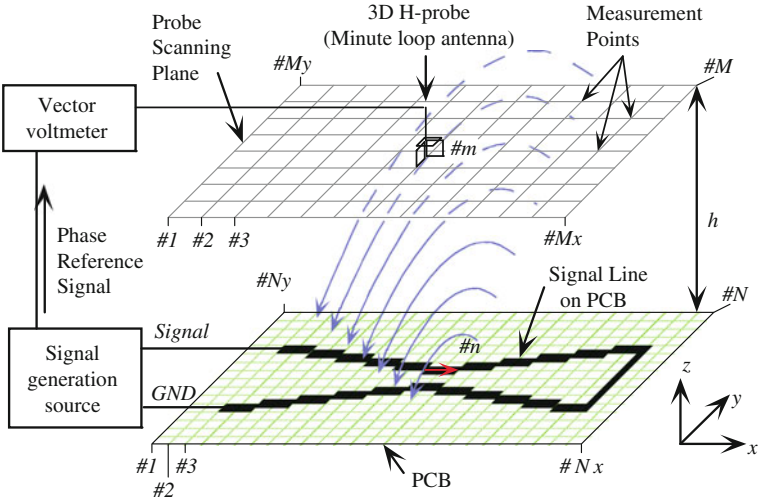


Fig. 3.9 Measurement system for near magnetic field distribution

Table 3.1 Measuring and detecting parameters

	X-axis pitch	*Y*-axis pitch	Total
Measuring area	3.5 mm 31 pts	0.25 mm 41 pts	1,271 pts
Probing area	3.5 mm 31 pts	0.25 mm 41 pts	1,271 pts
Probe	0.5 mm, Height: 1 mm		
Frequency	80 MHz		

However, the accuracy of this current detecting technique decreases when anti-phase currents are present, because the magnetic fields from narrow-pitch currents cancel as shown in Fig. 3.11. According to these results, the resolution of current distribution by this pattern matching is 3 mm or more, which is not sufficient for probing LSI pin current.

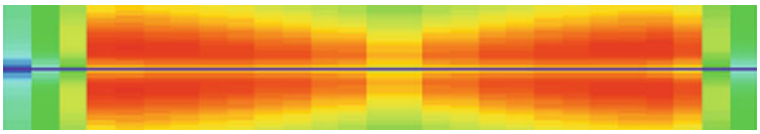


Fig. 3.10 Result of near magnetic field distribution measurement

Fig. 3.11 Result of detecting current (I_x) by pattern matching

3.3.1.3 High-Resolution Current Detecting Technique

To realize higher resolution using the pattern matching technique, the authors devised a filtering method using layout data of wiring. Filtering is repeated to minimize discrepancies between the measured magnetic field distribution and the calculated magnetic field from detected current distribution.

The layout data LD(n) is set to 1 when wiring is present and 0 when there is no wiring. This data is multiplied by the pattern matching result, and the first-level current distribution I_{n1} is calculated. Next, the resultant magnetic field distribution from the calculated first-level current distribution is obtained by the equation $I_{n1} \cdot H_{mn}$, the product of the assumed current $I_{n1}(x, y, z)$ and the function H_{mn} based on the position of current and magnetic field. Then the difference between this result and the measured magnetic field distribution $H_m(x,y,z)$ is calculated. The pattern matching technique is then applied again to give the additional second-level current distribution. The obtained additional current is defined as $I_{n2}(x,y,z)$ and gives more accurate distribution when summed up with the first-level current. This process is repeated, adding each calculated current successively as expressed in the following equation:

$$I_n = \sum_k \frac{H_{mn} \cdot (H_m - I_{nk} \cdot H_{mn})}{|H_{mn}| \times |H_m - I_{nk} \cdot H_{mn}|} \times LD(n) \tag{3.4}$$

The current detecting precision can be improved by repeating the above operation until the residual of the magnetic field distribution becomes smaller than the accuracy ratio β in the following equation:

$$\frac{|H_m - I_{nk} \cdot H_{mn}|}{|H_m|} \leq \beta \tag{3.5}$$

3.3.2 The Current Detection Result and Its Verification

Figure 3.12 shows the process and results of current detection from the magnetic field distribution measurement results, with the results of a direct current probe for comparison. Here, the accuracy ratio β according to the residual of the magnetic field distribution (Eq. (3.5)) was set to 5%. Figure 3.13 shows the remaining magnetic field with respect to the number of operation iterations along with the current accuracy per pitch.

This technique provides a detecting position resolution of 0.5 mm in 19 times of iterations even for anti-phase current. The current error accuracy was also within 10%.

Figure 3.14 shows the results of current detecting accuracy from 30 MHz to 1,000 MHz. The average current flowing on the wiring was resolved with an accuracy of ±1%. Even at a wiring pitch of 0.5 mm, the detected current was accurate to within 13%, which is considered sufficient.

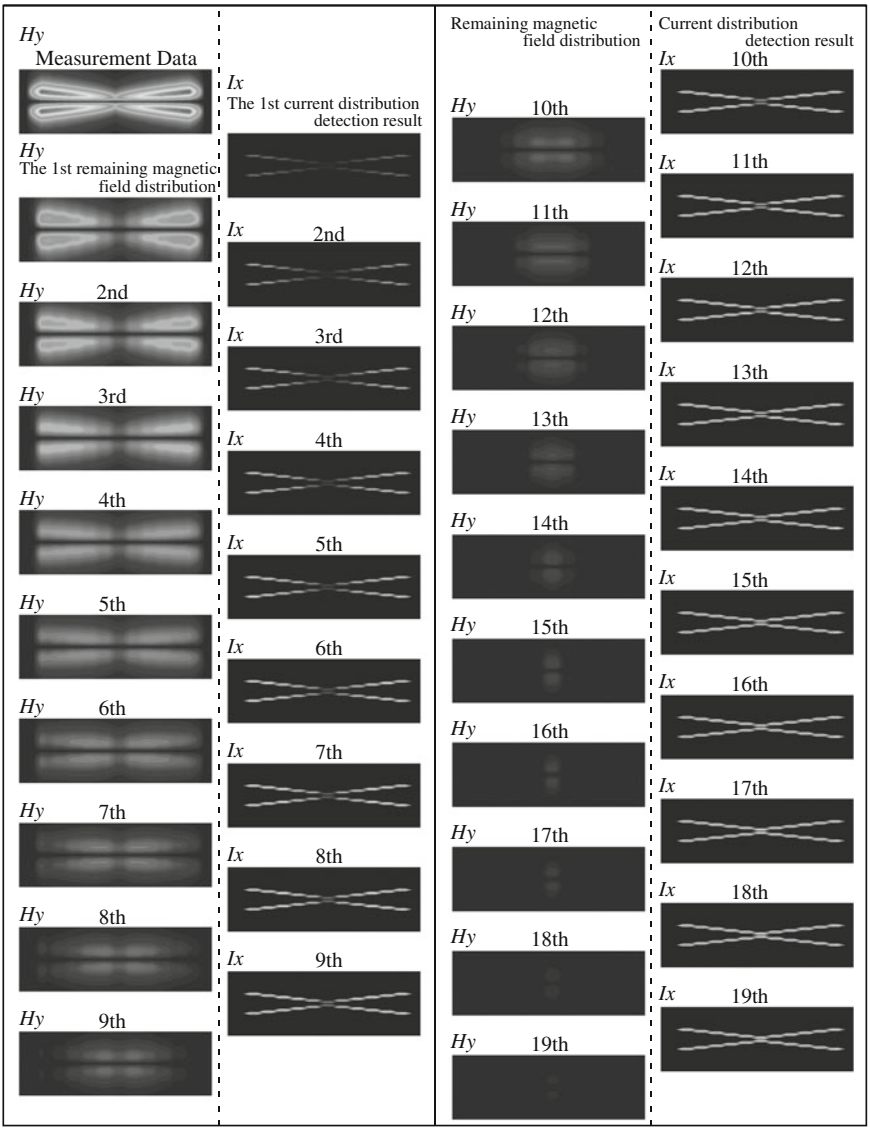
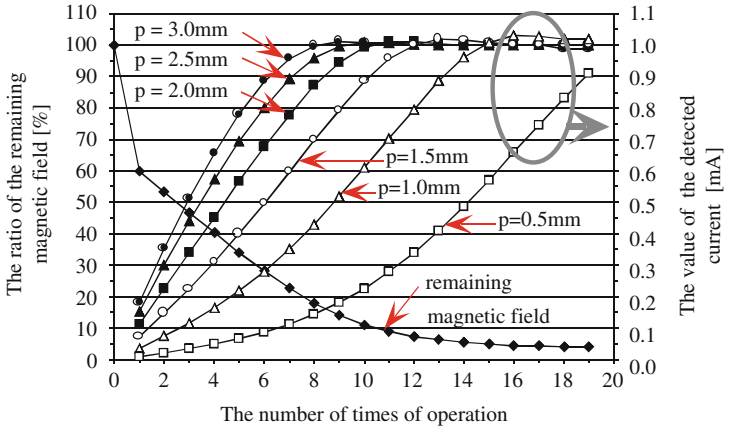


Fig. 3.12 Magnetic field distribution, anti-phase current probing process, and probing result

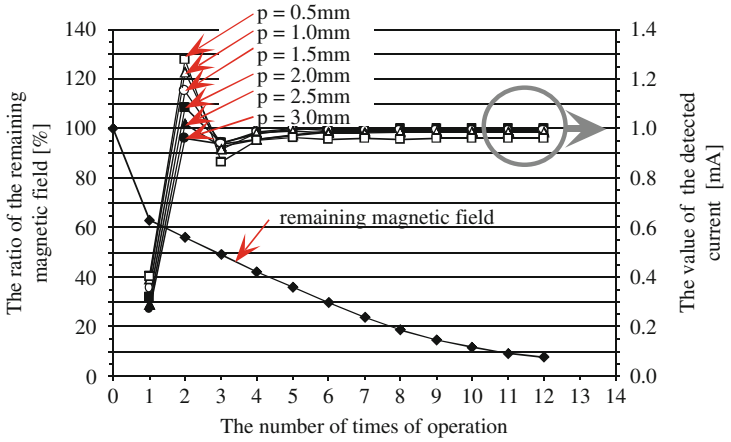
3.4 Reduction Technique of Radiated Emission from Chassis with PCB

3.4.1 Far-Field Measurement of Chassis with PCB

The effects f radiated emissions from a chassis with PCB were measured using the 3.5-inch hard disk drive shown in Fig. 3.15a, which is common type for PCs and



(a) Anti-phase current probing result



(b) Equi-phase current probing result

Fig. 3.13 Probing accuracy with respect to the number of iterations. (**a**) Anti-phase current probing result. (**b**) Equi-phase current probing result

servers. The chassis is 147 mm in length, 102 mm in width, and 26 mm in depth. The PCB and circuit on it were designed specifically for this experiment. The circuit consists of 10 MHz crystal oscillator, 74AC541 high-speed buffers with 1 μF bypass capacitors near the IC, and 10 pF load capacitors to GND and Vcc to simulate noise sources on the PCB. Figure 3.15b gives the schematic diagram of the circuit. The external battery pack supplies 5 V power through a 90 mm length of wire twisted with the GND wire to the PCB. The PCB consists of four layers: a top layer for parts mounting, a GND layer, a Vcc layer, and a bottom. The spacing between GND and Vcc layer is 0.15 mm, between top and GND is 0.22 mm, and between Vcc and bottom is 0.22 mm as well. The size of via is 0.3/0.5 mm and of anti-pads is

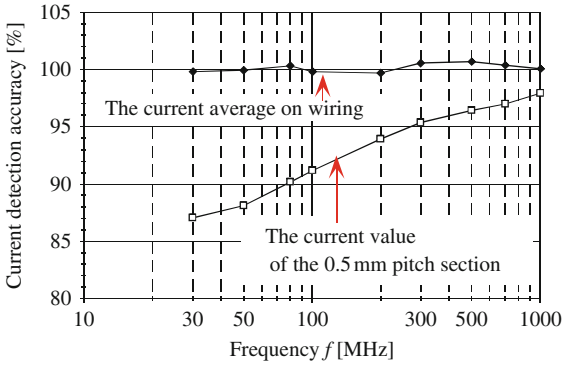
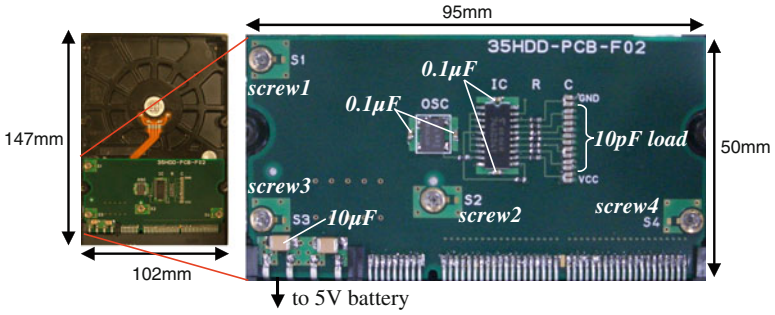
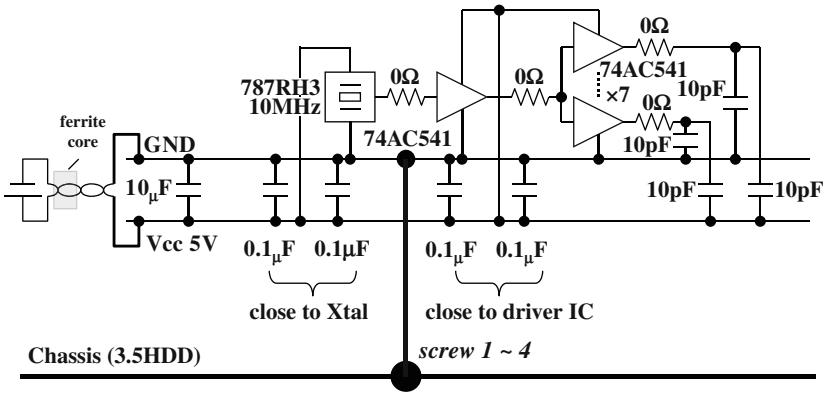


Fig. 3.14 Current probing accuracy with respect to current frequency



a) 3.5-inch hard disk drive chassis and PCB as DUT



b) Schematic circuit diagram for evaluation board

Fig. 3.15 Configuration of fabricated PCB. (**a**) 3.5-Inch hard disk drive chassis and PCB as DUT. (**b**) Schematic circuit diagram for evaluation board

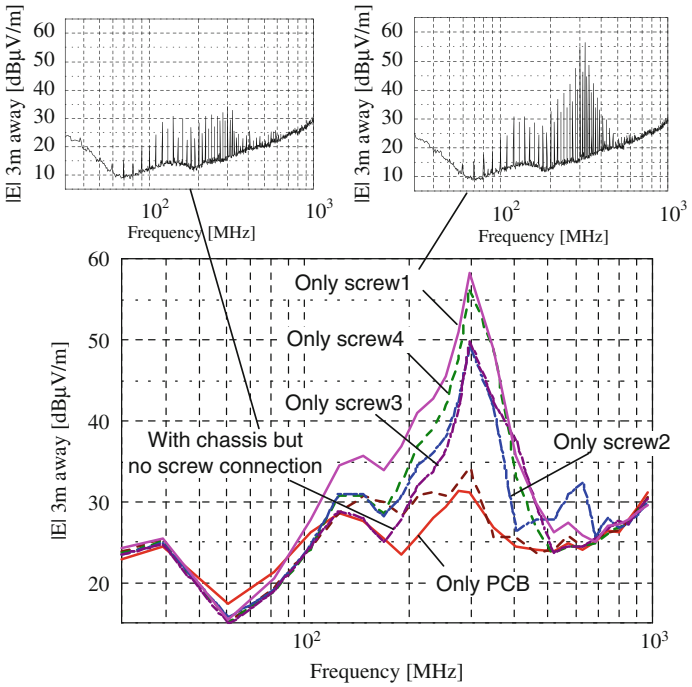


Fig. 3.16 The location of GND connection dependence of electric field 3 m away. Screws 1–4 indicate the result with only each connection individually

1.3/1.5 mm. The board has four screws (screws 1–4) for connections with the chassis GND, as shown in Fig. 3.15a. The height of screws is around 5 mm. The chassis is electrically connected with the PCB GND plane by those screws and no other portions of PCB were connected to the chassis. Figure 3.16 shows measurement results in anechoic chamber for the horizontal electric field at a distance of 3 m away with antenna height of 1.4 m for just a PCB (without chassis) or for PCB with chassis electrically connected by a screw. In the measurements, the device was placed on the center of a table flatly and peak values of electric field detected by antenna were collected by turning the table from 0? to 360?. Also in the measurement setup, plastic screws were used to fix the points which are not electrically connected to the chassis GND to improve the repeatability of the measurements. Figure 3.16 shows the results as envelop curvatures for all of radiated emission measurement results to make it easy to compare with the other results as well as original measurement result for no screw connections with chassis and for connection of only screw 1.

In Fig. 3.16, the measurement result with all plastic screws (no electrical connections between PCB GND plane and chassis GND) was less than any other results using metal screws to connect PCB GND with chassis GND, which suggests that the chassis is excited by GND bouncing and is contributing the radiated emission when it's electrically connected with PCB GND. The results also give no difference

between the one for only PCB without chassis and the one for PCB with chassis but no electrical connection, which means that capacitive or inductive coupling between PCB and chassis has little effect on chassis current and the emission in this particular case. Also, the result in Fig. 3.16 shows the differences depending on GND locations up to 8 dB around at peak of 300 MHz. The result for grounding at the screw position 4 shows the greatest level for peak value, second is position 1, third is position 2, and the lowest is position 3. These differences seem not to depend on the resonance due to the size of the chassis, because the peak frequency did not change with or without the chassis. Additionally, the location dependence of radiated emission is assumed not to be attributable to resonances related to screws, since the envelope and peak frequency at around 300 MHz of the spectrum did not change with different configuration of screw from 1 to 4 in Fig. 3.16.

3.4.2 Measurements of Junction Current

The junction current which means the current flowing through the screw connecting PCB GND with chassis GND was measured using extremely thin current probe which we proposed to investigate this kind of issue. The junction current was measured using spectrum analyzer E4448A with coaxial cable less than 1 m long during devices on PCB working. The current probe which was used for measurement is 12 mm in diameter, 1.5 mm thick, and 9-turn coil type. The measurement power of spectrum analyzer was converted to the level of junction current using the calibration factor of the current probe which has been reported [14, 15].

Figure 3.17 shows the frequency spectra of the junction current changing the screw which connects PCB GND with chassis GND. Each plot in the figure shows the result with only each connection individually. The measurement performed using a thin current probe as described eliminates the effect due to the shifting of gap between PCB and chassis. Also, the plastic screws were used to fix the PCB with chassis for the screws which do not electrically connect with chassis GND to improve the measurement accuracy and repeatability. In Fig. 3.17, the peak level at

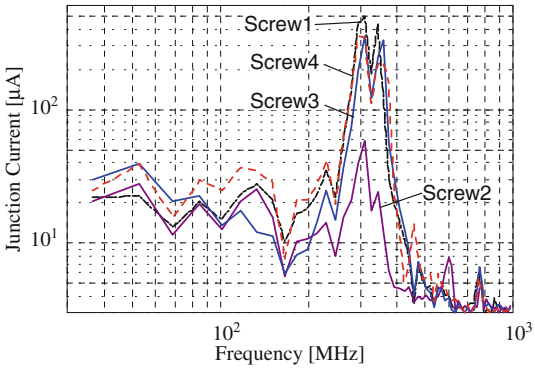


Fig. 3.17 Frequency spectra of junction current. Each plot shows the result with only each connection of screw (e.g., screw 1 indicates the current of screw 1 with only connection of screw 1)

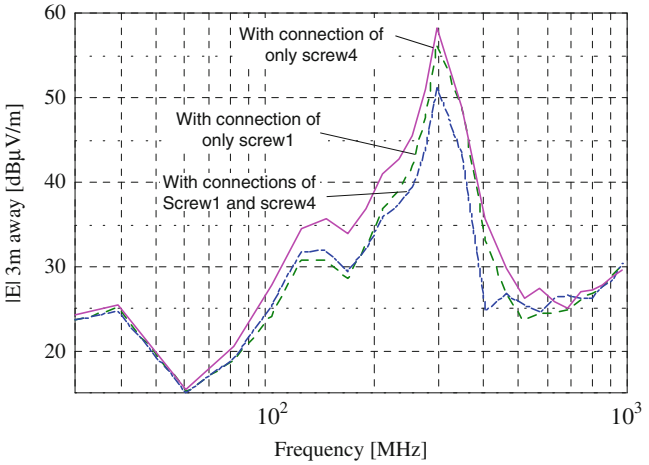


Fig. 3.18 Far-field electric field measurement result with connections of only screw 1, only screw 4, and both of screws 1 and 4

around 300 MHz is highest for the position of screw 1, and the lowest is for position 2. The results for screws 3 and 4 show similar peak level in this junction current spectrum. The order of the peak level and the envelope shape of the spectrum have a strong correlation, with far-field measurement results changing the location of screw as shown above, which means the current flowing through the screw has a big contribution to the radiated emission from this combined system. In terms of chassis design, further investigation including antenna factor of chassis, input impedance, or current distribution would be necessary toward an improvement. Meanwhile, lowering down the junction current can be one of the ways to reduce radiated emission from chassis without change of chassis design and it can be achieved by the design of PCB.

Figure 3.18 shows the measurement result of radiated emission with connections of only 1, only 4, and of both 1 and 4. The results show a difference of up to 6 dB at around 300 MHz. Figure 3.19 shows the frequency spectra for junction current measurements, which suggest a difference of up to 12 dB of junction current is much bigger than the difference of the emission. But it is reasonable that the result of plural connections is lower than the result of single connection, because it is considered that the cause of chassis current is related to the voltage bouncing of PCB GND and plural connections lowered the impedance and the bouncing of GND.

3.4.3 PSPICE Modeling

The location of GND connection with chassis GND on PCB could be crucial for system EMC, especially radiated emission. Generally, most products and PCBs implement GND connections with other components through wire harnesses or cables, which function as return current paths. Furthermore apart from those, the

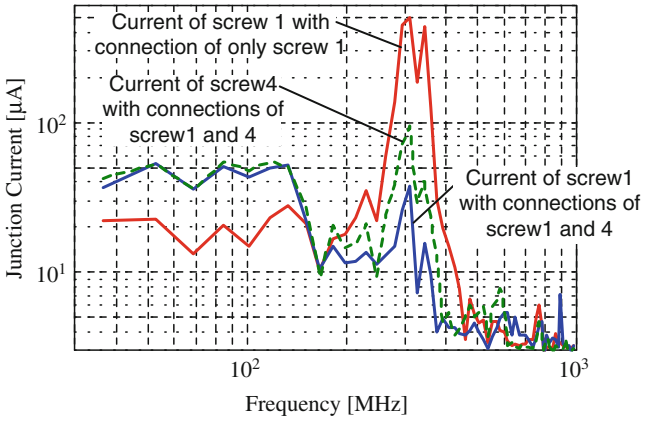


Fig. 3.19 Frequency spectra of junction current for screw 1 with only connection of 1 and with connections of 1 and 4, and for screw 4 with connections of 1 and 4

PCBs sometimes need GND points on board by connecting with chassis GND to suppress voltage bounce of the GND plane, to achieve stable GND, and to get good performance for ESD. Ideally, to improve EMC of PCBs, GND connections to the chassis are said to be located near interface connectors for other components and prevent discharged ESD current to propagate into the entire PCB. However, regarding emission from the chassis, it is less clear which screw locations and techniques can reduce excitation levels of chassis.

Our previous report proposed a simple concept to explain the cause of junction current and the reason for difference depending on the location of screw from the viewpoint of PCB design. Based on the mechanism we proposed, the junction current can be caused by the voltage bouncing between power plane and ground plane of PCB due to the switching current by IC and parasitic inductance of the plane. To investigate the way to reduce the junction current, PSPICE equivalent circuit model calculation was performed. A 4×9 LCR meshed network was used for each plane of PCB and chassis as shown in Fig. 3.20, in which the size of a mesh is smaller than one-tenth of the wavelength for 1 GHz; therefore it is considered small enough for the calculation with frequency up to 1 GHz. These LCRs represent the parasitic inductance and stray capacitance of/between planes, which were calculated using MoM-based simulation software, and Table 3.2 shows the result for the parameters.

Figure 3.21 shows simulation results of junction current in SPICE model. In the SPICE simulation, the screw was represented as 1 $\mu\Omega$ resistor and measured with current probe which is in series to the resistor. No model of plastic screw was implemented. The peak frequency is at around 320 MHz and it is similar to the far-field measurement result, which means the LCR modeling and calculation of parameters are reasonable. The order of the peak level starts from highest 4, second 1, third 2, and lowest 3, which is the same as the order of far-field measurement

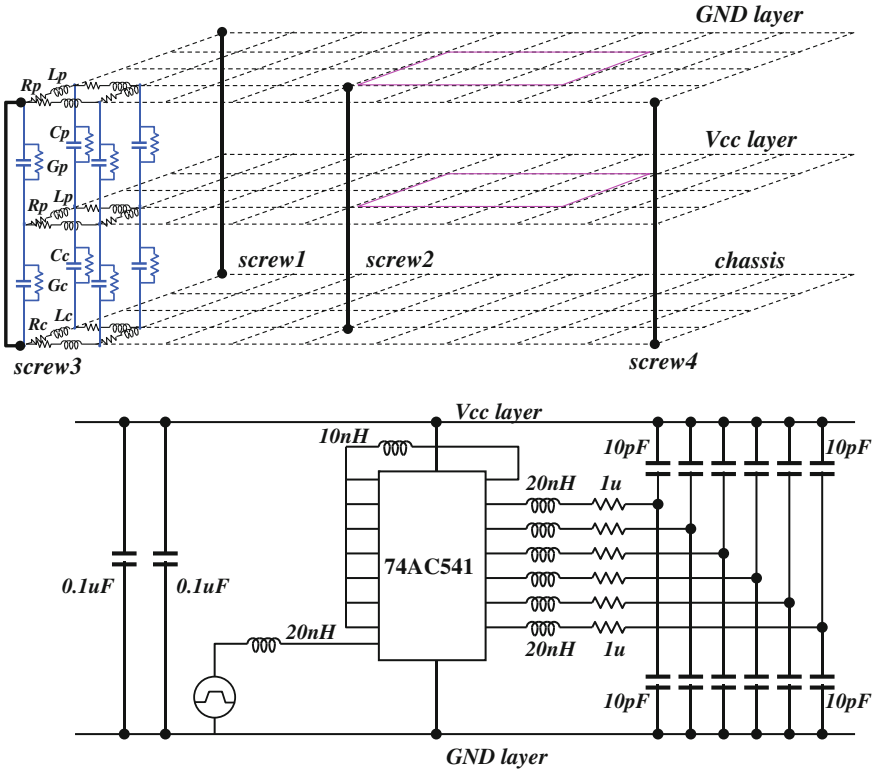


Fig. 3.20 LCR meshed network model of PCB and chassis in SPICE simulation

Table 3.2 Derived parameters for model

Rp	0.05 ohm	Rc	0.02 ohm
Lp	0.18 nH	Lc	6 nH
Cp	24 pF	Cc	0.3 pF
Gp	66 kohm	Gc	10 Mohm

results. The level of the peak in frequency spectrum is also close to the measurement results of the junction current.

Figure 3.22 also shows the junction current results for PSPICE simulation with plural screws configuration. The current for both screws is much smaller than the current with only screw 1, which is indicated with broken red line. The level of current for screw 1 with connection of screw 4 is lowered down to 150 μA which is half of only screw 1 and the current of screw 4 is much smaller than the level of screw 1. These trends can be considered same as measurement result. The difference in peak level between measurement result and simulation result is due to the accuracy of measurement and modeling. Eliminating the effect of capacitive coupling between

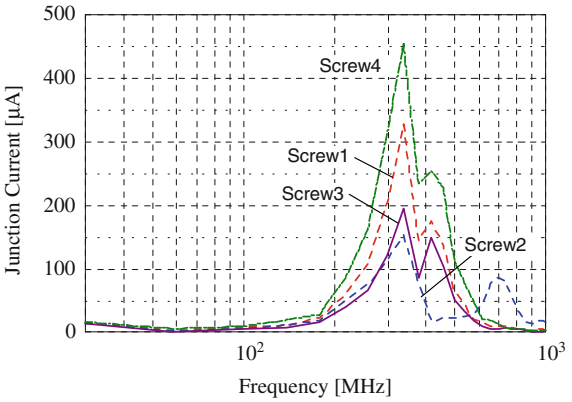


Fig. 3.21 Calculation results of junction current. Each plot shows the result with only each connection (e.g., screw 1 indicates the current of screw 1 with only connection of screw 1)

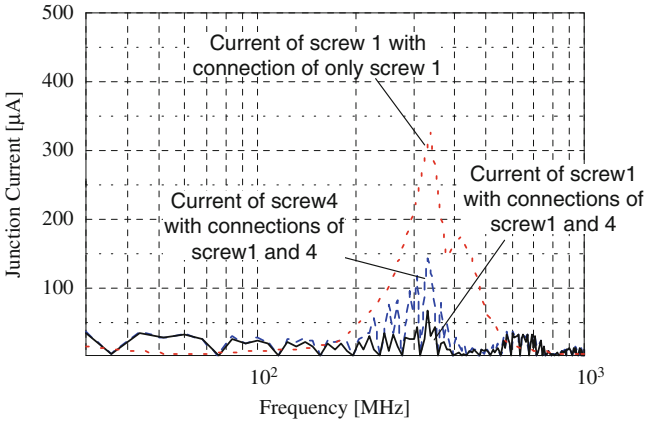
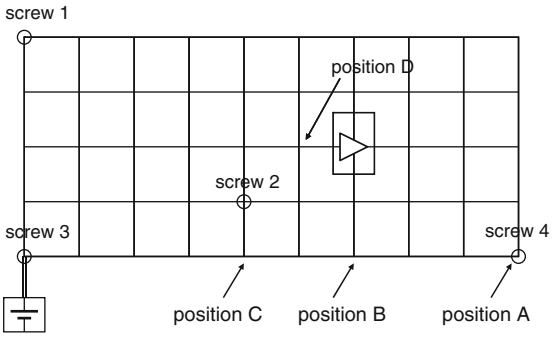


Fig. 3.22 Calculation results of junction current for screw 1 with only connection of 1 and with connections of 1 and 4, and for screw 4 with connections of 1 and 4

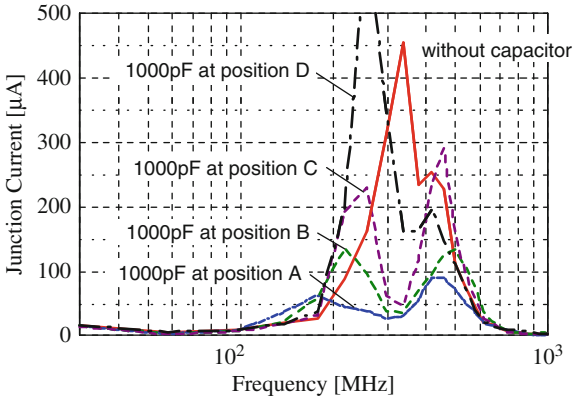
the probe for junction current and PCB tracing could improve the accuracy, and finer mesh network analysis can also improve the results if necessary.

Based on the results as described, the correlation between junction current and radiated emission from chassis with PCB is strong, which means reduction of junction current can be assumed to reduce also the emission from chassis with PCB. One of the ways to reduce the junction current is by placing a bypass capacitor between the power plane and GND plane much close to the screw which connects PCB GND with chassis GND, because the junction current representing chassis current would be caused by voltage bouncing between GND and power plane. It can be assumed that the location of capacitor between planes is very important to reduce the junction current.

The difference in junction current due to the location of capacitor was simulated using the SPICE model for the configuration that only screw 4 is connected to



a) Location of additional bypass capacitor on meshed model



b) Calculation results of junction current at screw 4 with only connection of screw 4 changing the location of additional bypass capacitor

Fig. 3.23 Dependence of junction current on the location of additional bypass capacitor. (**a**) Location of additional bypass capacitor on meshed model. (**b**) Calculation results of junction current at screw 4 with only connection of screw 4 changing the location of additional bypass capacitor

chassis GND which gave highest level for both junction current and far-field result. Figure 3.23b shows the frequency spectrum of junction current at screw 4 for the original configuration, with 1,000 pF at position C as shown in Fig. 3.23a, with 1,000 pF at position B, and with 1,000 pF at position A which means the same location as screw 4. The result shows that the peak value of junction current can be lowered by placing the capacitor, and the closer the capacitor is located to the screw, the lower the junction current. The results also suggest that there are two peaks close to 300 MHz which can also be seen in the measurement results of junction current, as shown in Figs. 3.17 and 3.19.

One of the factors that decide the frequency of peak is considered as the size of planes for PCB with components. Generally, the location of capacitor is very important to suppress or to change the resonant mode which is caused due to the

dimension of the PCB. However, the more complicated the PCB becomes, the more difficult it is to estimate and design the resonance of the PCB. For example, it would be difficult to control the resonance for the PCB which has complicated shape like polygonal GND or power planes with many slits, holes, and cutouts. Also, the actual PCB normally has so many components like capacitors or inductors, which should affect the resonant mode of the PCB. These factors make the design of PCB difficult to adjust and to control resonant frequency. However, placing the capacitor close to the connection between PCB GND and chassis can lower down the junction current which is caused by the voltage bouncing between GND and power plane regardless of the reason for the voltage bouncing.

Figure 3.23b also shows the result of frequency spectrum with 1,000 pF capacitor close to the IC actually at position D in Fig. 3.23a to compare with the result of capacitor close to the junction using SPICE simulation. There's almost no effect due to the additional 1,000 pF capacitor at position D because it can be assumed that the IC already has 0.1 μF bypass capacitors close to itself.

3.4.4 Experimental Validation

The effect of additional capacitor which is located close to the screw was verified in actual measurement using the PCB which has special pads for that capacitor as shown in Fig. 3.24, for example, of screw 1. The size of via for this special pattern is 0.3 mm diameter and of anti-pad is 1.3 mm. All other configurations for measurement were same as the original described. The 1,000 pF chip capacitor is the same as that used for calculation in the experiment. The impedance specification of the capacitor has resonant frequency at around 160 MHz due to the parasitic inductance which is about 1 nH but it can be the cause for lowering down the impedance between Vcc and GND because the impedance at peak frequency 300 MHz is less than 1.5 Ω and it is considered lower than the original impedance between Vcc and GND. But it would be necessary to reduce the parasitic inductance of tracing for additional capacitor to make it more effective.

Figure 3.25 shows the envelope of measurement results for far-field electric field with 1,000 pF capacitor close to the screw. The results give the frequency spectrum for only screw 1 and for only screw 4 with/without 1,000 pF capacitor each. The

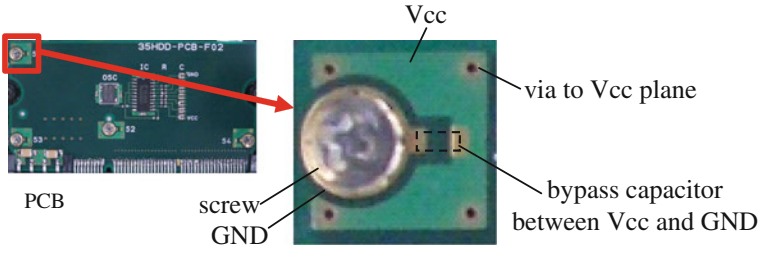


Fig. 3.24 Additional bypass capacitor located close to the screw for experiment

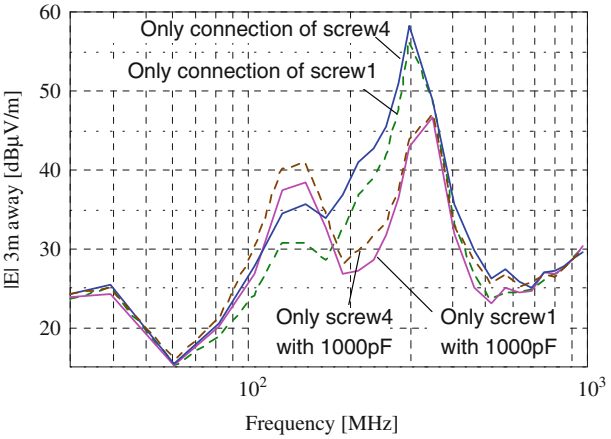


Fig. 3.25 Frequency spectra of far-field electric field with/without additional bypass capacitor

peak level at around 300 MHz is lowered down by additional 1,000 pF capacitor up to 10 dB in the emission for each configuration, screw 1 and screw 4. The results show the same trend as the SPICE simulation result. Another peak at around 130 MHz was pushed up around 7 dB in the emission results, which is considered to be related with the resonance due to additional capacitor. Further investigation will be necessary for this point.

Figure 3.26 gives original data for frequency spectrum of radiated emission measurement results with connections of screws 1 and 4 with/without 1,000 pF capacitor each. The result with 1,000 pF capacitor is almost 19 dB lower than without capacitors at peak frequency 320 MHz. The peak around 130 MHz was also changed to 6 dB higher than original, which is the same as for only screw 1 or 4. Frequency spectra of junction current for the condition with 1,000 pF were measured as shown in Fig. 3.27, which shows good correlation with the emission result. Based on these results, it is confirmed that the peak level at around 320 MHz can be lowered down in junction current and radiated emission of chassis with PCB by placing additional capacitor close to the screw which connects the PCB GND with chassis GND.

3.5 Chapter Summary

A new method for estimating the EMI radiation was proposed. The practical EMI measurement without using a costly anechoic chamber is achieved. The analytic information on the radiation source is fully obtained to identify the location on the board that needs some improvements for satisfying the EMI regulation.

As a technique for measuring high-frequency currents flowing through LSI pins, a non-contact detecting method for current distribution based on measurements of the near magnetic field distribution is investigated. The proposed technique

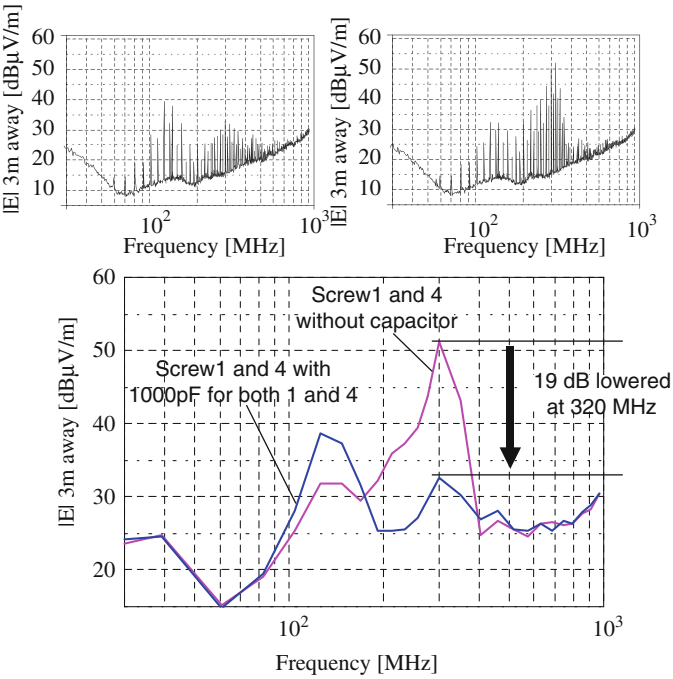


Fig. 3.26 Improvement of radiated emission with additional capacitors

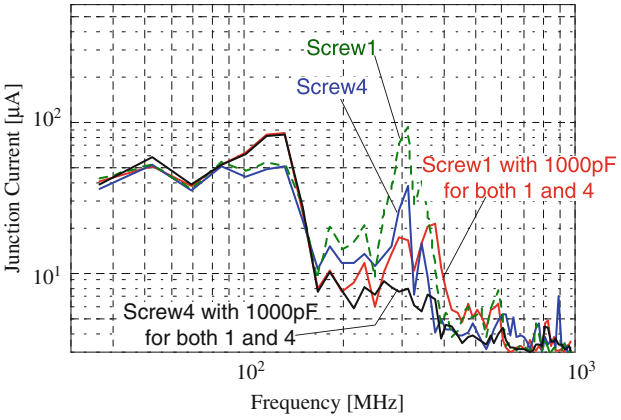


Fig. 3.27 Measurement results of junction current for screws 1 and 4 with connections of both screws 1 and 4 with/without 1,000 pF capacitors

draws the current distribution through iterative pattern matching between a measured near magnetic field distribution and the calculated one from the assumed currents. By filtering out the layout data and iteratively converging on a solution, discrepancy between the magnetic field distribution by the obtained current and

the measured magnetic field distribution becomes minimal. The proposed technique has a positional resolution of 0.5 mm and realizes non-contact measurement of LSI pin currents. Current accuracy of ±20% was verified in the frequency range from 30 MHz to 1,000 MHz.

The effect due to assembling with chassis and the correlation between junction current and radiated emission were investigated including plural screws configuration. SPICE model to investigate better location of additional bypass capacitor was created including chassis layer and it gave good correlation with measurement results for frequency spectra of junction current. Both SPICE calculation and measurement results suggest that plural connections by screws lower the junction current. Based on the SPICE investigation, a new technique by placing additional bypass capacitor close to the screw to reduce junction current was proposed and verified. The SPICE calculation results showed that the closer the additional bypass capacitor is located to the screw, the lower the junction current it gives, which gave better result than placing it close to the IC driver. The difference depending on the location of additional capacitor was up to 13 dB. Moreover, the effect of additional capacitor located close to the screw was confirmed in actual measurement. The result with the additional capacitor using special pads close to screws showed 10 dB improvement for single-screw connection and 19 dB improvement for plural screws connection at around original peak frequency of 320 MHz.

These studies showed that placing bypass capacitor can be one of the ways to reduce the radiated emission from chassis, which connects the GND with PCB GND. Further work will be performed including the emission source current distribution in chassis depending on the screw location.

References

1. IEEE Editorial Policy Statement, "*IEEE Transactions on Electromagnetic Compatibility*," EMC-29, pp. 202–206 (1987).
2. N. Kobayashi, K. Morishita, M. Kusumoto, T. Harada, and T. Hubing, "Coupling Analysis of PCB-Chassis Systems with Signal Lines and Via Structures using SPICE," *Proceedings of the 2006 International Symposium on EMC, Portland, OR, USA, August 2006* (2006).
3. D. Baudly, F. Bicrel, L. Bouchelouk, A. Louis, B. Mazari, and P. Eudeline, "Near-Field Techniques for Detecting EMI Sources", *Proceedings of the 2004 International Symposium on EMC, Sendai, Japan*, Vol. 1, pp. 11–13 (2004).
4. J. Shi, M. A. Cracraft, J. Zhang, R. E. DuBroff, K. Slattery, and M. Yamaguchi, "Using Near-Field Scanning to Predict Radiated FIELDS", *Proceedings of the 2004 International Symposium on EMC, Sendai, Japan*, Vol. 1, pp. 14–18 (2004).
5. X. Dong, S. Deng, T. Hubing, and D. Beetner, "Analysis of Chip-Level EMI Using Near-Field Magnetic Scanning", *Proceedings of the 2004 International Symposium on EMC, Sendai, Japan*, Vol. 1, pp. 174–177 (2004).
6. V.P. Kodali, "Engineering Electromagnetic Compatibility," *IEEE Press*, (1996).
7. J. Galejs, "Admittance of a Rectangular Slot Which is Backed by a Rectangular Cavity," *IEEE Trans. Antennas Propag.*, Vol. AP–11, pp. 119–126 (1963).
8. H.A. Mendez, "Shielding Theory of Enclosures with Apertures," *IEEE Trans. Electromagn. Compat.*, Vol. EMC-20, pp. 296–305 (1978).

9. G. Cerri, R.D. Leo, and V.M. Primiani, "Theoretical and Experimental Evaluation of the Electromagnetic Radiation from Apertures in Shielded Enclosure," *IEEE Trans. Electromagn. Compat.*, Vol. 34, pp. 423–432 (November 1992).
10. M. Li, J.L. Drewniak, S. Radu, J. Nuebel, T.H. Hubing, R.E. DuBroff, and T.P. Van Doren, "An EMI Estimate for Shielding-Enclosure Evaluation," *IEEE Trans. Electromagn. Compat*., Vol. 43, No. 3, pp. 295–304 (2001).
11. S. Daijavad, and B.J. Rubin, "Modeling Common-Mode Radiation of 3-D Structures", *IEEE Trans. Electromagn. Compat.*, Vol. 34, pp. 57–61 (1992).
12. M. Li, J. Nuebel, J.L. Drewniak, R.E. DuBroff, T.H. Hubing, and T.P. VanDoren, "EMI from Cavity Modes of Shielding Enclosures-FDTD Modeling and Measurements," *IEEE Trans. Electromagn. Compat.*, Vol. 42, pp. 29–38 (2000).
13. M. Leone, and G. Mönich, "Coupling of Apertures in Enclosures to External Cabling Structures," *IEEE Trans. Electromagn. Compat.*, Vol. 46, pp. 107–110 (2004).
14. N. Kobayashi, T. Harada, A. Shaik, and T. Hubing, "An investigation of the effect of chassis connections on radiated EMI from PCBs," *Proceedings of the 2006 IEEE International Symposium on Electromagnetic Compatibility, Portland, OR, USA*, August 2006, WEAM-2-1 (2006).
15. H. Funato, and T. Suga, "A Study on Correlation between the PCB Layout and EMI from Chassis", *Proceedings of the 2007 International Symposium on EMC, Qingdao, China, July 2007* (2007).

Chapter 4
Power Integrity

4.1 Introduction

Electronic systems consist of a lot of semiconductor devices, such as digital processor, memory, and RF IC. These active devices require a stable DC supply voltage, to within a certain percentage of ideal supply voltage, to ensure proper operation of logic and input/output (I/O) interface circuits. The power distribution system (PDS) must provide this steady voltage in the presence of very large DC and AC current demands. The resistive nature of on-chip wires and the inductance inherent in most packaging elements make this a difficult problem. Power integrity design is to design a power distribution system of electronic system to provide a small voltage fluctuation, power supply noise, in order to make an electronic system operation stable.

A typical power distribution system is a hierarchy. Small local elements, like on-chip bypass capacitors and on-chip voltage regulators, provide small amounts of energy to local regions and handle the high-frequency components of transients. Larger elements supply larger regions and handle lower frequency components of the transients. For example, bypass ceramic capacitors near LSI have a responsibility at middle frequency range, while large balk capacitors, such as tantalum solid electrolytic capacitor, distantly-positioned from LSI have a responsibility at low frequency range. Because of their physical distance from the point of use, and the inductance that implies, they are not able to manage the high-frequency transients. At higher levels of the hierarchy, the supply voltage is usually raised to allow distribution to be performed with lower currents and hence smaller and less expensive bus-bars and cables. Thus, power integrity requires hierarchical design concept with respect to each frequency.

In this chapter, we discuss the power integrity (PI) design of the information technology equipments, such as router, server, PC, and some parts are also available on mobile electronic systems.

Yutaka Uematsu

N. Kanekawa et al., *Dependability in Electronic Systems*,
DOI 10.1007/978-1-4419-6715-2_4, © Springer Science+Business Media, LLC 2011

4.2 Detrimental Effect and Technical Trends of Power Integrity Design of Electronic Systems and Devices

4.2.1 Detrimental Effect by Power Supply Noise on Semiconducting Devices

Power supply noise prevents semiconducting devices from operating with their primary performances as shown in Fig. 4.1. Among them, we show five detrimental effects of power supply noise: (a) voltage noise margin degradation, (b) clock timing, (c) signal timing uncertainty, (d) jitter in single-ended signaling, and (e) jitter in differential signaling [1, 2].

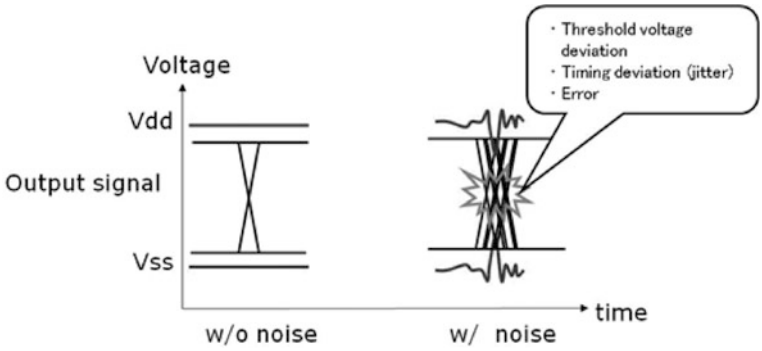


Fig. 4.1 Influence of power supply noise

4.2.1.1 Noise Margin Degradation

In digital logic systems using single-ended signal, the power and ground distribution network is also used as voltage reference for the on-chip signal. Let us consider the situation to convey to the receiver transmitter logic. When transmitter communicates the status of low logic state, e.g., low voltage, the output of the transmitter is connected to the local ground network. At a receiver side, by comparing signals transmitted from the transmitter to the voltage level of power and ground to determine the logic state. Away from the location of the transmitter and receiver, a mismatch between supply and ground voltage levels across the communications line transmitter and receiver occurs. In a system with supply voltage fluctuation, the greater the voltage level mismatch in the transmitter and receiver, the smaller the on-chip signal transmission noise margin, which increases the instability of the system. As the operating speed of LSI is faster, sufficient noise margin is becoming increasingly important to protect the stability of the system from a variety of other noise, such as crosstalk, intra-electromagnetic interference.

4.2.1.2 On-Chip Clock Timing

Power supply noise can significantly affect the timing of on-chip clock. In a most digital LSI, a phase-locked loop (PLL) is used to generate the chip clock signal. PLL is an electronic circuit that generates phase-synchronized signal from another oscillator, in addition to feedback control based on the periodic input signal. The periodic input signal is provided from the system that is usually produced by a crystal oscillator. The PLL due to external environment, such as power supply noise, affects the phase of on-chip clock signal. In the PLL feedback loop, PLL controls the output phase and aligns the phase of output signal with the system clock phase. Ideally, on-chip clock signal edge is determined by the system clock signal and should be precisely spaced intervals. The disturbance that period is shorter than the PLL response time, which is typically hundreds of nanoseconds, results in a shift of the on-chip clock timing from the timing should be. The time shift of the clock from the ideal timing is called as clock jitter [3]. For high-speed digital system, the clock jitter should be controlled precisely in order of picoseconds. The clock jitter can be classified into two types by their nature. One is cycle-to-cycle jitter and the other is peak-to-peak jitter (Fig. 4.2).

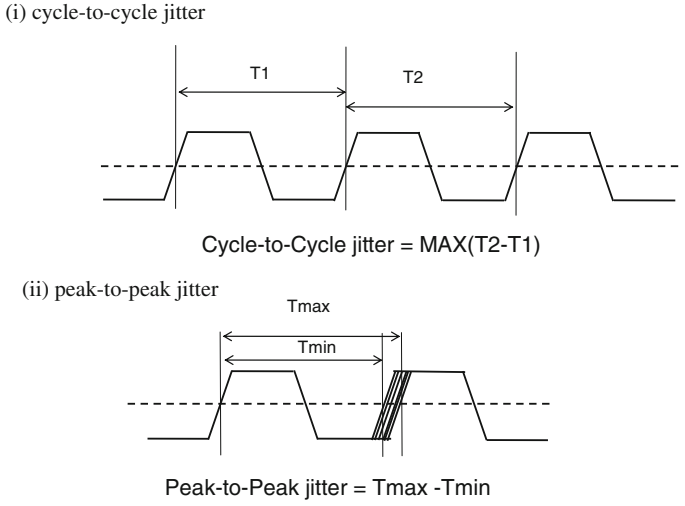


Fig. 4.2 Two types of clock jitter: (i) cycle-to-cycle jitter, (ii) peak-to-peak jitter

As shown in Fig. 4.2i, cycle-to-cycle jitter is determined as a maximum deference between adjacent two clock periods. This jitter refers to random deviations of the clock timing from the ideal. In this case, deviation from the ideal phase of the clock signal at either end is independent of other edges. As the cause of this cycle-to-cycle jitter, noise whose period is less than or equal to the period of the clock frequency is dominant, including high-frequency power supply noise and crosstalk, for example.

For a second type of jitter, we need to consider a peak-to-peak jitter that represents the maximum deviation of the clock periods as shown in Fig. 4.2ii. This

peak-to-peak jitter refers to systematic variations of on-chip clock phase as compared to the system clock. For timing requirements of on-chip circuitry, a violation does not occur while cycle-to-cycle jitter is sufficiently small. However, the phase difference between the system and the on-chip clock will continue to accumulate over time. PLL feedback adjustment to become effective requires a period of tens to hundreds of clock, the duration of fault is not resolved, which can lead to on-chip clock deviation to the system clock. This phase difference may reduce the synchronization between two clock domains. Clock domain synchronization is very important to maintain the reliability of communication between these domains.

The power supply noise highly affects the feedback response time of PLL [4]. Here, we show an example designed for IBM S/390 microprocessor. The PLL of it exhibits a response time of approximately 50 clock cycles when operating at 2.5 V power supply and disturbed by a 100 mV drop in supply voltage. By reducing the power supply voltage to 2.3 V and below, which is not so far from typical value, the recovery time from the same disturbance increases manyfold [4].

4.2.1.3 Signal Timing Uncertainty

In a signal transfer using NMOS/PMOS/CMOS logic circuit, the propagation delay strongly depends on the power supply voltage level. The CMOS consists of the PMOS and the NMOS transistors. The source of the PMOS transistors in pull-up networks within logic gates is connected to power supply voltage directly or through other transistors or resistor. In the same way, the source of the NMOS transistors in pull-down networks within logic gates is connected to the ground voltage network. In both cases, the drain current of MOS transistors increases when a voltage difference between gate and source of the transistor increases. Moreover, if a voltage difference between gate and source decreases, the drain current of the MOS transistor decreases. Since the drain current is output current of each MOS, increase and decrease of the drain current imply change of output timing. When the power supply voltage and ground voltage level are deviated due to power supply noise, the output current of NMOS/PMOS/CMOS is also affected. The signal propagation delay increases when the output current decreases, e.g., the voltage difference decreases. Conversely, if the voltage difference increases, the signal propagation delay decreases. The net effect of power supply noise on clock and data signal transmission, therefore, increases both the delay of the data path and the delay uncertainty. Consequently, power supply noise limits the maximum operating frequency of LSI [5].

4.2.1.4 Jitter in Single-Ended Signaling

The single-ended signaling is the interconnect that includes transmitters and receivers on a bus connected with single dedicated transmission line for each bit as shown in (Fig. 4.3). Data (DQ) signal of DRAM interface represents a typical

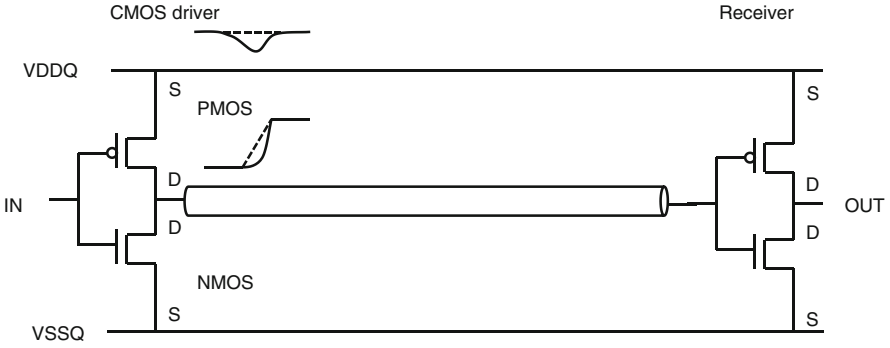


Fig. 4.3 Single-ended transmission line

single-ended transmission. As contrasted with single-ended transmission, there is a differential signal transmission. The single-ended signaling generally works at lower speed than the differential signaling and works well up to approximately a few Giga bits per second (Gbps). In single-ended signals due to poor resistance to external noise, such as crosstalk and power supply noise, the increase in data rates will be increasingly difficult to maintain sufficient signal integrity. Simultaneous switching noise (SSN), which is discussed in Section 4.5, is also one of the highest impacts on signal integrity of the single-ended signaling and is the power supply noise on I/O power supply network caused by the simultaneous switching of large arrays of I/O circuits with the same transition.

The single-ended transmission is transmitted to a single transmission line data latched at the receiver with the bus clock. In order to be latched as the correct logic at the receiver, the signal must finish the transition of the logic meeting the specification of the receiver. The transition timing, however, is affected by many kinds of noise in the transmission path. At a transmitter side, simultaneous switching output (SSO) noise, PLL/DLL jitter due to power supply noise, and crosstalk in the chip cause the transition timing deviation, e.g., jitter, of the transmitted data waveform. At the traces in the LSI package and PCB, crosstalk noise, reflection noise, and power plane noise increase the jitter. At a receiver side, simultaneous switching input (SSI) noise also affects the jitter. Thus, power supply noise, including SSN, provides a significant impact on single-ended jitter.

Additionally, in the case of DRAM interface, the decision of the logic, "0" or "1," is determined using the reference voltage V_{REF} (Fig. 4.4). If the received waveform has a voltage level greater than V_{REF}, the signal is latched in as "1," and if it is below V_{REF}, it is latched in as logic "0." In single-ended interface using V_{REF}, we must care the relationship among power supply voltage at transmitter and at receiver and V_{REF} at receiver. Figure 4.4 shows how noise can make the determination of logic "0" or "1" uncertain. The variation of V_{REF} causes not only voltage margin degradation but also timing margin reduction due to cross point variation between signal and V_{REF}.

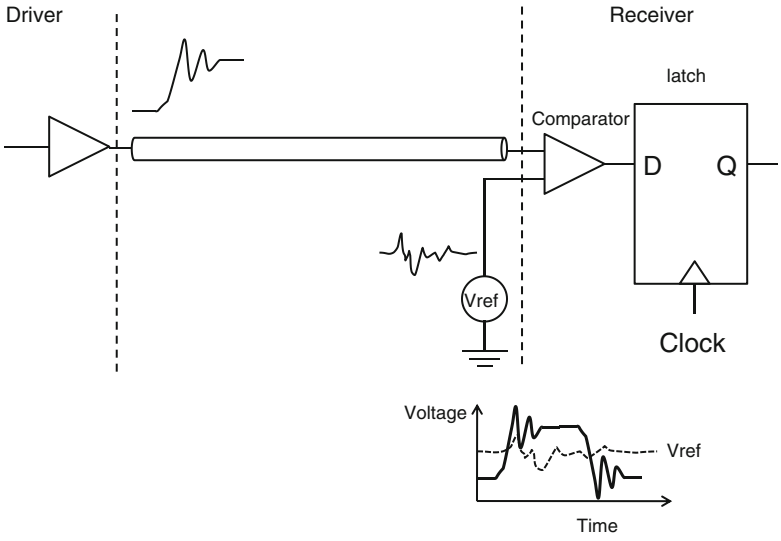


Fig. 4.4 Single-ended signaling with reference voltage

4.2.1.5 Jitter in Differential Signaling

As described in previous section, single-ended signaling is sensitive to the system noise generated by the switching of the circuits. A better solution to reduce dramatically the impact of system noise is to provide a pair of transmission lines for each bit on the bus. This technique using paired transmission lines is called differential signaling. The schematic of differential signaling is shown in Fig. 4.5. In this signaling, two transmission lines are driven 180° out of phase by the differential driver.

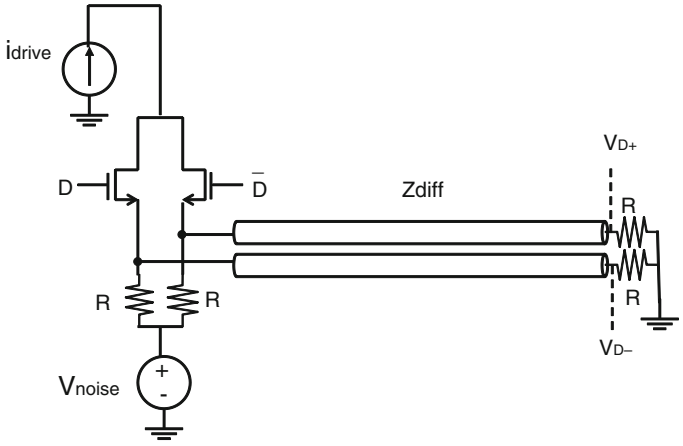


Fig. 4.5 Differential signaling scheme

This drive mode is called as the odd mode. The odd mode signal is transferred to differential receivers which have a differential amplifier to recover the signal to usual digital signal. The differential signaling is very effective for removing common-mode noise, which is represented by the SSN and crosstalk noise. If the differential bus is designed properly, the differential pairs, D^+ and D^-, are in close proximity to each other for each section, transmitter, transmission line, and receiver. In this configuration, the noise on D^+ will be approximately equal to the noise on D^-. Since the differential receiver senses the voltage difference between D^+ and D^-, the common-mode noise is eliminated. The common-mode noise elimination performance of the receiver is defined by common-mode rejection ratio (CMRR). By assuming a receiver circuit with reasonable CMRR and a bus designed properly, the output of a differential amplifier with unity gain is

$$V_{\text{diff}} = (v_{\text{D}^+} + v_{\text{noise}}) - (v_{\text{D}^-} + v_{\text{noise}}) = v_{\text{D}^+} - v_{\text{D}^-} \tag{4.1}$$

which removes the common-mode noise, with the amplitude of v_{noise}, coupled equally onto both traces of a differential pair. An example of differential pairs with the noise (v_{noise}) on the ground network is shown in Fig. 4.6. In this case, noise is common to both legs of the driver. As mentioned earlier, in the single-ended transmission, we must notice that the v_{D}^+ and v_{D}^- cannot be confirmed if the noise is very large. In the differential transmission, however, the bit stream can be recovered when the signals are subtracted by a differential amplifier ($v_{\text{D}}^+ - v_{\text{D}}^-$) even if the amplitude of the noise is so large because the noise is common mode, as shown in Fig. 4.6. If the phase relationship between v_{D}^+ and v_{D}^- deviates from 180° as the signals propagates toward the receiver, some of the energy will be converted from odd mode to even mode, e.g., differential mode to common mode. This phenomenon

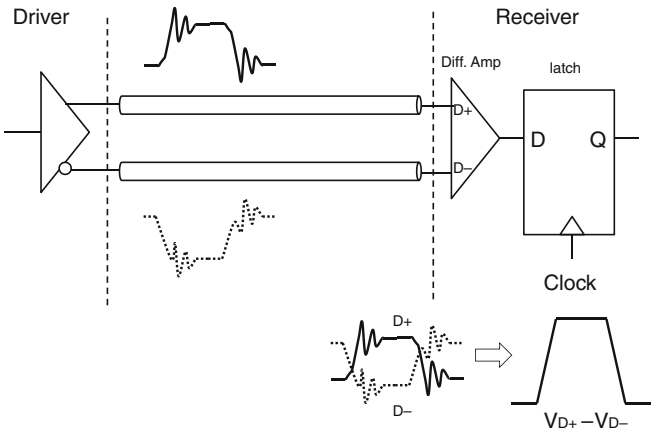


Fig. 4.6 Single-ended signaling with reference voltage

has many names, including mode conversion, differential-to-common-mode conversion, and AC common-mode conversion (ACCM conversion). In this text, we use the term ACCM conversion.

Although a differential transmission system is said to be a strong system against a common-mode noise, such as power supply noise, there is a frequency range that is weak against common-mode noise such as power supply fluctuation. Figure. 4.7 shows the example of these phenomena. In this circuit, although the circuit has high immunity performance in lower frequency range due to PLL and in higher frequency range due to clock data recovery (CDR) circuit, it has a low immunity performance in a mid-frequency range. In this case, mid-frequency range power supply noise could be an origin of jitter even for a differential signaling. Thus, it is very important to know the frequency dependence of immunity performance against a common-mode noise, especially for differential I/O circuits.

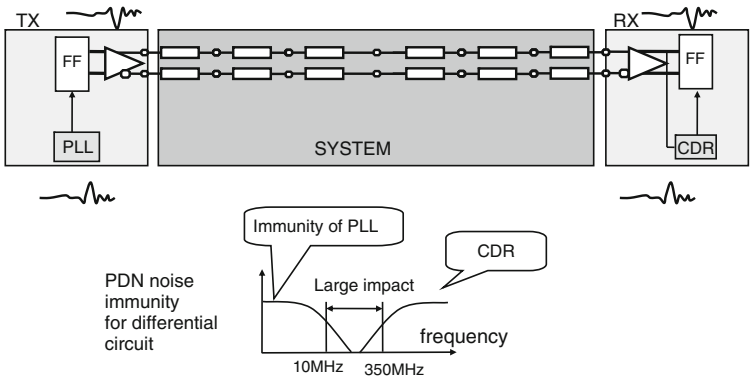


Fig. 4.7 Influence of the power supply noise for differential transmission line

4.2.2 Trends of Power Supply Voltage and Power Supply Current for CMOS Semiconducting Devices

Figure 4.8 shows trends of CMOS process technology and power supply voltage of semiconductor devices based on ITRS [6]. Accompanying by the process technology scale down, power supply voltage has become lower and lower. Comparing the values in 2000 and 2010, the power supply voltage scaled down to 1/3. Since voltage noise margin of semiconductor devices is defined by a certain percentage of power supply voltage, voltage noise margin becomes 1/3 of 2000, in 2010. The voltage noise margin, V_{margin}, can be expressed as follows:

$$V_{\text{maring}} = k \cdot V_{\text{dd}} \tag{4.2}$$

where k is a ratio of noise margin, whose value is typically 0.05 (5%).

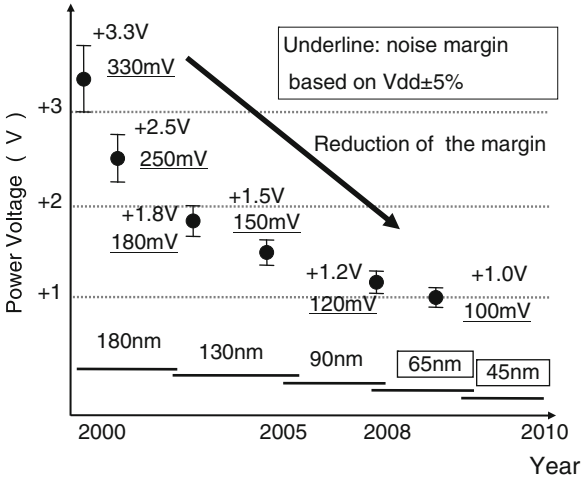


Fig. 4.8 Trend of power supply voltage for CMOS circuits. Voltage noise margin and process technology are also plotted

Maximum power supply voltage noise, $\Delta V_{\max}$, is determined by the product of maximum power supply current, $I_{\max}$, and power supply impedance, Z_{ps}, as described below:

$$\Delta V_{\max} = I_{\max} Z_{\mathrm{ps}} \tag{4.3}$$

This power supply noise is characterized by two kinds of noise. One is DC noise, which is determined by resistance and DC power supply current, the so-called IR drop. Another is AC noise, which is determined by high-frequency impedance and AC power supply current.

To describe voltage noise waveform, $\Delta v(t)$, with simple equation, we represent AC noise by inductive noise. Then the noise voltage waveform can be described as follows:

$$\Delta v(t) = R \cdot i_{\mathrm{ps}}(t) + L \frac{di_{\mathrm{ps}}(t)}{\mathrm{d}t} \tag{4.4}$$

where $i_{\mathrm{ps}}(t)$ is a power supply current waveform, R is a power supply resistance, and L is a power supply inductance. The current in contemporary microprocessors has exceeded 130 A and will further increase with technology scaling. Forecasted demands in the power supply current of high performance microprocessors are illustrated in Fig. 4.9. The rate of increase in the transient current, di/dt, is expected to be more than double the rate of increase in the average current, as indicated by the slope of the trend line depicted in Fig. 4.9.

Trends of power supply voltage and power supply current indicate that power supply system should consist of quite low resistance and low inductance in order to achieve a target voltage noise margin.

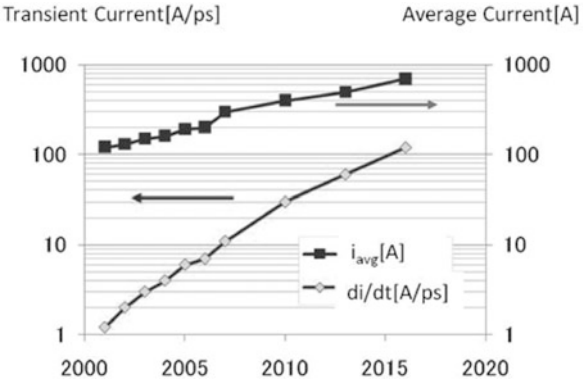


Fig. 4.9 Trends of power supply current and transient current of high performance microprocessors

4.2.3 Trend of Power Distribution Network Design for Electronic Systems

From the viewpoint of power distribution network design for electronic systems, there are some trends that make the design difficult. Here we show three examples: (a) demands of small factor, (b) multiple power supply voltage, and (c) functional power supply management for ecology.

First, while there is a demand of increasing of performance for electronic devices, the requirements of small factor of the components also exist. This is due to an appearance of many kinds of mobile application devices, such as smart phone, mobile game products, digital book reader. The small factor makes it difficult to achieve low inductive power supply networks because it requires small size and few layers of printed circuit board (PCB) that cause a thin and long power supply wiring. Figure 4.10 shows the changes of the computing products and the size of

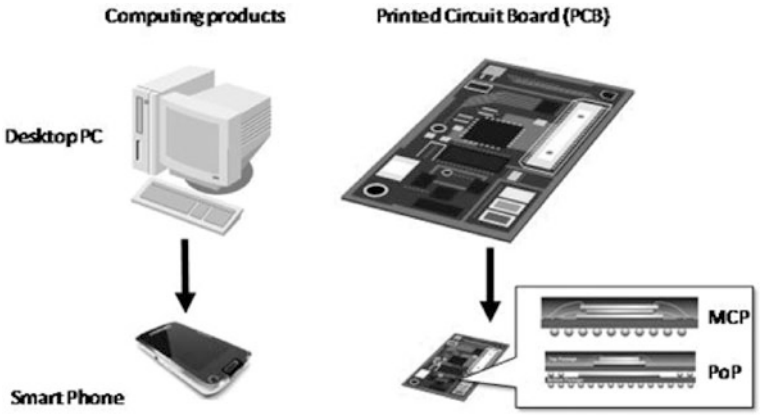


Fig. 4.10 Demands of small factor for semiconducting products

printed circuit board. In recent years, a small size electronic device, such as smart phone, has same or greater performances than old desktop, but just 5 years old, personal computer (PC), while the size of it is less than 1/20 of old desktop PC. In case of PC, PCB has an area of about 30 cm × 20 cm, while that of smart phone has only about 5 cm × 5 cm, or less. Due to a limit of thickness, numbers of PCB layers are also few. Moreover, LSI package in a smart phone forms a multi-chip packaging style, such as multi-chip package (MCP) and package on package (PoP) in order to reduce an LSI mounting area of PCB. These LSI packages have large parasitic inductance because of high density and high pin counts in a very small size package with stacked multiple LSIs. Thus, PI problems have become significant for small-sized products.

Second, in recent electronic system, there are many kinds of power supply voltages in one system. This strongly relates to the third topic, functional power supply management. In recent years, ecology is the most important proposition, so that electric power saving technology is proposed and adopted with high priority. One of the best ways to reduce power consumption is turning off the power supply for nonuse LSI or circuit blocks. In order to fine-tune power on/off for various functions, the power supply lines are broken down into individual voltages. In one system, it sometimes requires 10 or more kinds of voltages. Since the area for power supply wiring in PCB and LSI package is limited, increasing number of power supply voltage directly increases effective inductance in the power distribution networks.

Third, functional power supply management is used to maintain the power consumption as small as possible for ecology. For example, some of the INTEL processors have a function called OS power management (OSPM) [7–9]. Figures 4.11 and 4.12 show the explanation of OSPM. This kind of function can be realized by an integrated power gates that can stop power supply for each core by a gating switch as shown in Fig. 4.11 [9]. This power gating is controlled by a power control unit, which integrated proprietary microcontroller. In Fig. 4.12, we will show the example of power gating of internal section in the LSI [7]. By the island power gating, power supply current is reduced as small as 1/3 of full active in this case. It

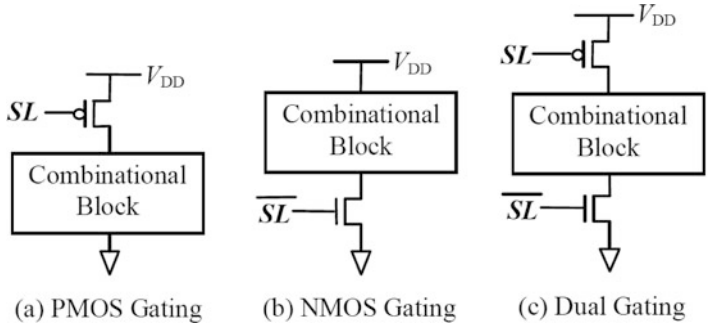


Fig. 4.11 Power Gating Technique using (**a**) PMOS Gating, (**b**) NMOS Gating, and (**c**) Dual Gating (© IEEE)

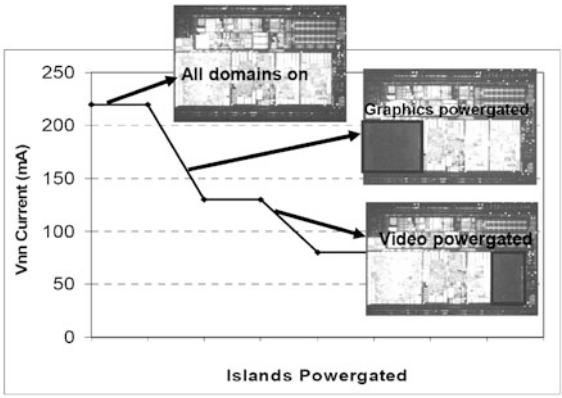


Fig. 4.12 Selective powering down of Lincroft power domains with power gates (© IEEE)

also shifts control from hardware to embedded firmware. In this system, real-time sensors for voltage, current/power, and temperature are used in order to control a power supply. From the viewpoint of power integrity, this power management function probably causes large voltage fluctuation due to large current profile (on/off) with high frequency.

Consequently, these trends affect power integrity design by increasing parasitic inductance of power supply network and increasing transient current.

4.3 Design Methodology of Power Integrity

4.3.1 Definition of Power Supply Noise in Electric System

The target of power integrity design is to reduce voltage variation inside an LSI chip under an allowed value. The allowance of the noise voltage is normally +/– 5% of power supply voltage, V_{dd}. It is very reasonable that we define an allowable voltage fluctuation level at nodes (voltage and ground) inside the LSI chip because the power integrity problem occurs when ideal voltage cannot be supplied for operating circuits as shown in Fig. 4.13a. However, we cannot measure a voltage noise inside the chip in the electric system without special circuits in the LSI as described in Section 4.6.1, because we cannot probe inside the LSI chip using commercial digital oscilloscope.

For convenience, the voltage waveform, which is discussed between LSI chip vendor and system developer for an operational voltage specification, is usually defined by the value observed at the BGA ball (or pins) of the LSI package placed on the printed circuit board (PCB) as shown in Fig. 4.13b. This approximation is based on the small effect of transfer function between LSI and PCB. However, over a mid-frequency range (tens MHz to hundreds MHz), this is not true in most cases.

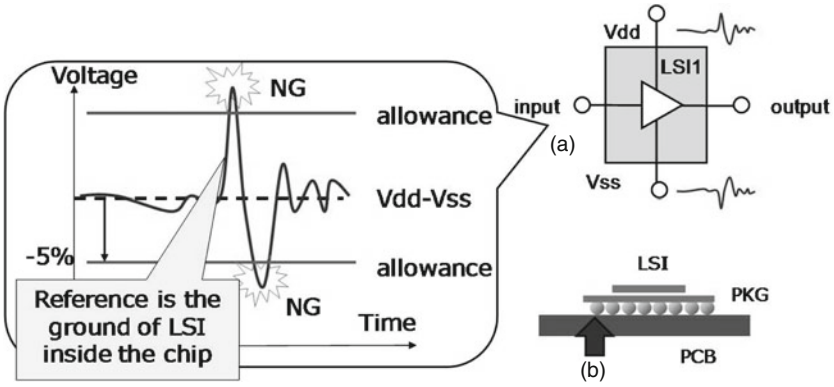


Fig. 4.13 Definition of the voltage noise variation

We also mention that the allowable voltage noise specification is not defined by the waveform, which includes information of time and voltage, but simply by the amplitude of noise in most cases. Although this definition extends facilities in the measurement, there are some imperfections for power integrity design. The imperfections come from (i) frequency dependence of transfer function between LSI and PCB, and (ii) different noise sensitivity in each frequency of the circuits in LSI. We may also need to consider that several waves overlap with certain phase difference as shown in Fig. 4.14. Although the possibility may be small, this kind of noise overlap sometimes causes poorly reproducible error in the system.

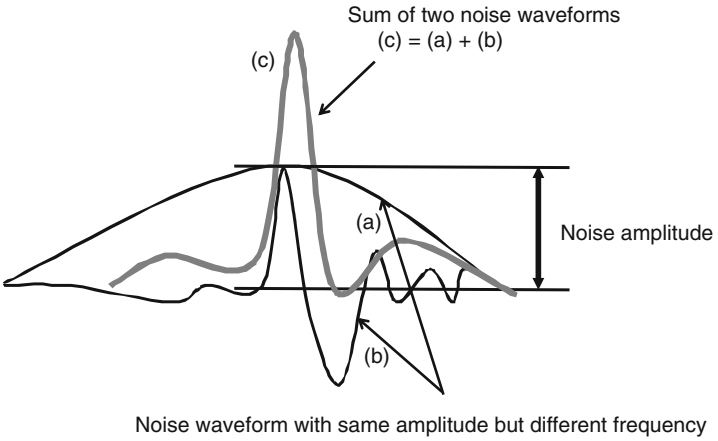


Fig. 4.14 A possibility of appearance of quite large noise when several waves overlap with certain phase

4.3.2 Time-Domain and Frequency-Domain Design Methodology

For power integrity design, we have two design domains, time and frequency. Let us consider the equation of power supply noise waveform as a response of the PDN system. Here we define three parameters relating to this system as shown in Fig. 4.15.

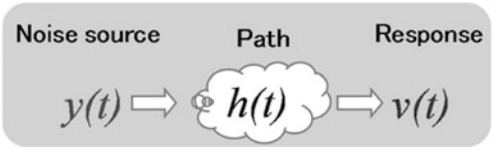


Fig. 4.15 Relationship between noise source and response

Based on a basic circuit theory, the relationships among three parameters can be described as follows:

$$\begin{aligned} v(t) &= h(t) \otimes y(t) \\ &\Updownarrow \\ V(\omega) &= H(\omega) \cdot Y(\omega) \end{aligned} \tag{4.5}$$

where $v(t)$: noise voltage waveform; $y(t)$: noise source waveform; and $H(\omega)$: path of noise propagation (mainly printed circuit board).

The first equation of Eq. (4.5) represents the "time-domain (TD) design," while the second equation represents the "frequency-domain (FD) design."

In the power integrity design, we use current waveform, $i(t)$, as a noise source and impedance, $Z(f)$, as a transfer function; therefore, the equation can be rewritten as the following relationship:

$$\begin{aligned} v(t) &= z(t) \otimes i(t) \\ &\Updownarrow \\ V(f) &= Z(f) \cdot I(f) \\ &\Downarrow \\ |V(f)| &= |Z(f)| \cdot |I(f)| \end{aligned} \tag{4.6}$$

The third equation of Eq. (4.6) represents an often-used concept of PDN design. In this equation, magnitude of each parameter is only discussed. Although this concept makes it easy to express a target specification of design, some assumptions must be considered. For example, we cannot express overlaps of noise waveform with different phase by this equation as described in Fig. 4.14. For a power integrity design, both time-domain and frequency-domain analyses are very important. Therefore, as described in Eqs. (4.5) and (4.6), it is important to convert time-domain characteristic into frequency-domain characteristic, or convert frequency-domain characteristic into time-domain characteristic. This is performed by utilizing a Fourier transform.

As proposed by Jean Baptiste Joseph Fourier, who was French mathematician and physicist and best known for initiating the investigation of Fourier series, any kinds of waveform, $f(t)$, can be expressed by a sum of sine wave and cosine wave.

$$f(t) = \sum_{K=-\infty}^{\infty} F_K \cdot e^{j2\pi Kf_0 t} \tag{4.7}$$

where

$$e^{j2\pi Kf_0 t} = \cos(2\pi Kf_0 t) + j\sin(2\pi Kf_0 t) \tag{4.8}$$

and

$$F_K = \frac{1}{T_0}\int_{-T_0/2}^{T_0/2} f(t) \cdot e^{-j2\pi Kf_0 t} dt \tag{4.9}$$

F_k is a coefficient of Fourier series expansion and it expresses magnitude of each frequency component.

4.3.2.1 Time-Domain (TD) Analysis

Time domain analysis is a good method to confirm electronic system dependability by a noise voltage waveform, because stable operations of LSI circuits are defined by time-domain characteristic of electrical current and voltage for each circuit power supply node. Therefore, most LSI vendors supply power integrity specification by time-domain characteristics.

For example, we will show a specification of V_{REF} tolerances for DDR3 SDRAM [10]. The DC-tolerance limits and AC-noise limits for the reference voltages V_{REFCA} and V_{REFDQ} are shown in Fig. 4.16 [5]. It shows a valid reference

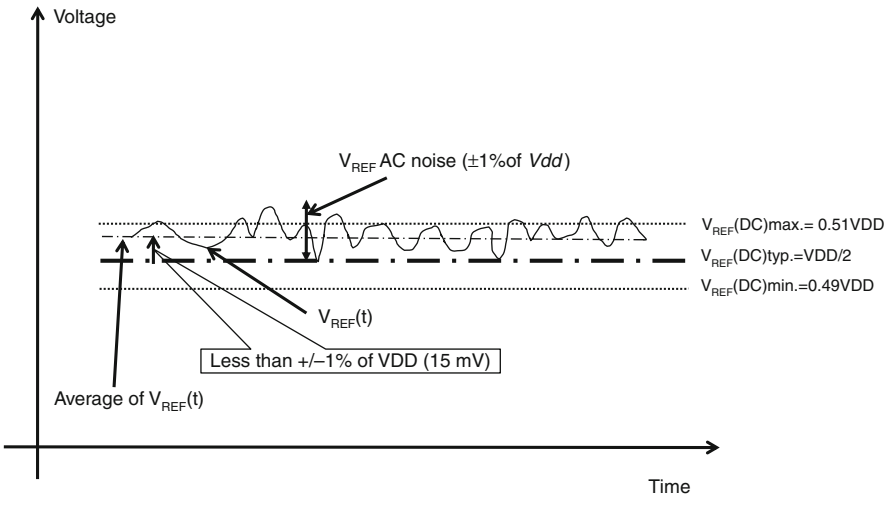


Fig. 4.16 Specification of V_{REF} voltage noise margin for DDR3 SDRAM

voltage $V_{REF}(t)$ as a function of time. (V_{REF} stands for V_{REFCA} and V_{REFDQ} likewise.). V_{REF}(DC) is the linear average of $V_{REF}(t)$ over a very long period of time (e.g., 1 s). This average has to meet the min/max requirements. Furthermore, $V_{REF}(t)$ may temporarily deviate from V_{REF}(DC) by no more than $\pm 1\%\ V_{dd}$. This clarifies that DC-variations of V_{REF} affect the absolute voltage that a signal has to reach to achieve a valid high or low level and, therefore, the time to which setup/hold is measured. System timing and voltage budgets need to account for V_{REF}(DC) deviations from the optimum position within the data-eye of the input signals. This also clarifies that the DRAM setup/hold specification and derating values need to include time and voltage associated with V_{REF} AC-noise. Timing and voltage effects due to AC-noise on V_{REF} up to the specified limit ($\pm 1\%$ of V_{dd}) are included in DRAM timings and their associated deratings.

Time-domain analysis is often called as "transient analysis" in circuit theory and often performed using simulation program with integrated circuit emphasis (SPICE) simulator. Transient analysis requires circuit models of all components building PDS in electronic system. The models consist of LSI (load, current source), LSI package (PKG), printed circuit board (PCB), and sometimes voltage regulator modules (VRM).

Active components, such as LSI current source and VRM, are described by MOS transistor model, time-variant resistor model, and piecewise linear (PWL) current or voltage source in SPICE simulator. While passive components, such as on-chip power supply wiring, LSI package, PCB, and decoupling capacitors, are described commonly by electrical circuit model, resistance R, inductance L, and capacitance C. Example of power supply noise simulation model in the time-domain is expressed in Fig. 4.17.

As we can see from Fig. 4.18a, it is easy to confirm the specification. However, analysis time is usually very long because power integrity simulation requires very long transient analysis time period (in the example of V_{REF} of DDR3 SDRAM, analysis time period of 1 s may be required to obtain V_{REF}(DC) by averaging $V_{REF}(t)$ for 1 s). One reason of the long analysis time period is the existence of power supply noise in a very wide frequency range of DC to over GHz. This is the difficulty in PI design.

4.3.2.2 Frequency-Domain Analysis

Frequency-domain analysis is a good method to specify problems in PDS and to determine how we reduce the power supply noise. In a frequency-domain design, we utilize an impedance, $Z(f)$, as a design parameter.

Figure 4.18b shows an example of frequency-domain analysis. Although the model is almost the same, we calculate an impedance profile inside an LSI chip in this method. The goal of this method is to meet target impedance across frequency range of interest. A merit of this method is ease of specifying problems in PDS and of determining how we overcome it. In this example, we can easily find that impedance peak around 100 MHz is a problem. To reduce impedance of this frequency range, it is effective to reduce PKG inductance or increase on-chip

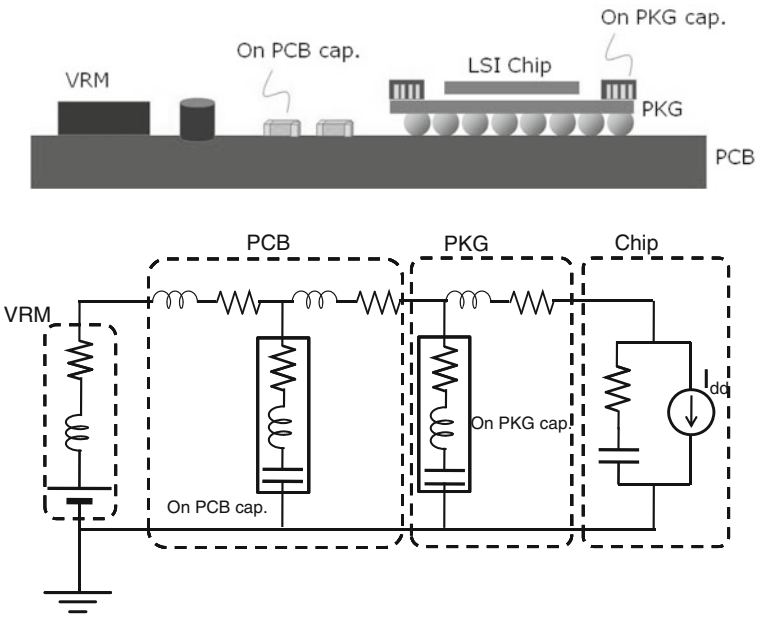


Fig. 4.17 Time-domain simulation model that consist of all components in the PDS

capacitance. By reducing PKG inductance, the impedance profile is improved and meets the target impedance.

Details about the concept of target impedance will be discussed in next section.

4.3.2.3 Target Impedance

In the frequency-domain design, we need certain target impedance. The target impedance was proposed by Larry Smith and defined as follows:

$$\begin{aligned} Z_{\text{target}} &= k \cdot \left(\frac{V_{\text{dd}}^2}{P_{\text{max}}} \right) \\ &= \frac{V_{\text{allow}}}{I_{\text{dd,max}}} = \frac{k \cdot V_{\text{dd}}}{I_{\text{dd,max}}} \end{aligned} \tag{4.10}$$

where $I_{\text{dd,max}}$: maximum power supply transient current [A]; V_{allow}: maximum allowable drop voltage [V]; V_{dd}: power supply voltage [V]; k: allowable power supply voltage drop ratio (usually in the range of 0.05–0.10); and P_{max}: maximum power consume [W].

For example, if we consider a case of $V_{\text{dd}} = 1.0\,[\text{V}]$, $k = 0.05$, and $I_{\text{dd,max}} = 50\,[\text{A}]$, target impedance is calculated as $Z_{\text{target}} = 0.05 \times 1/50 = 0.001\,[\Omega] = 1\,[\text{m}\Omega]$.

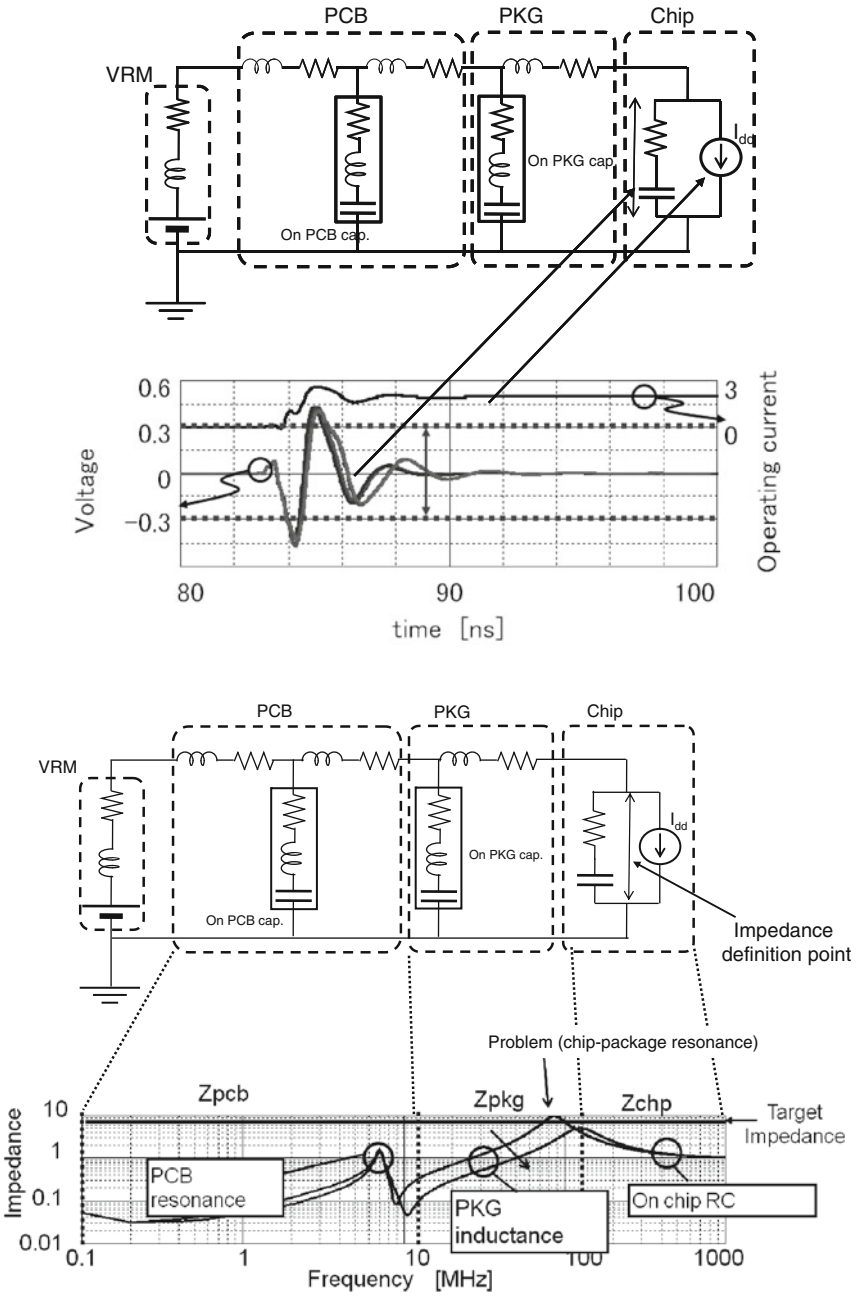


Fig. 4.18 (**a**) Transient simulation results of the PDS. (**b**) Frequency domain analysis for the circuit model

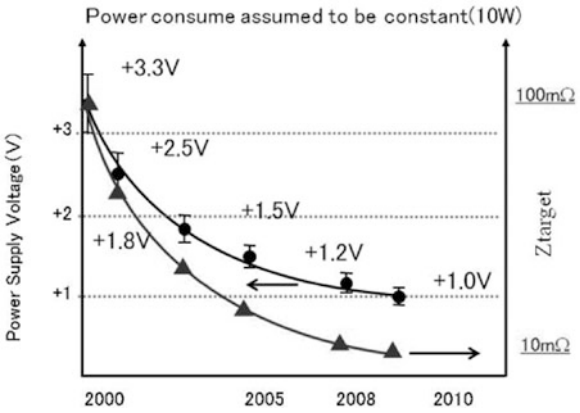


Fig. 4.19 Trend of power supply voltage and target impedance

A trend of target impedance is plotted in Figure 4.19. In these 10 years, the target impedance has become just one-tenth of that in 2000. Consequently, the impedance control to meet target impedance becomes quite difficult.

The design method using this target impedance is called as frequency-domain target impedance method (FDTIM) [11]. In this method, we can (1) calculate target impedance, (2) determine corner frequency, and (3) select components (VRM, bulk capacitors, high-frequency ceramic capacitors, and power planes) to meet target impedance. Corner frequency is a maximum frequency of interest. This is determined by rise time of the load and limited by package or PCB inductance.

A difficulty in FDTIM is to determine reasonable target impedance, which is not too low and not too high. If the target impedance is set to lower value, the system cost will be high because we need extra components for reducing impedance. If the target impedance is set to higher value, the system dependability will be worse and may cause some error due to poor power integrity. The difficulty in setting reasonable target value is mainly due to effect of phase of noise, circuit sensitivity, and current profile, $I(f)$. We will discuss two problems: (a) effect of phase and (b) circuit sensitivity.

Effect of Phase.

If PDS is just expressed by resistive components, we don't need to consider effects of noise phase. However, the existence of parasitic inductance and capacitance cause a phase changing of response against some input. Figure 4.20 shows an example of phase changing of the step response for Big-V PDN [12]. Big-V PDN has a sharp impedance drop around MHz region by adding lots of ceramic capacitors with same resonant frequency as seen in left of Fig. 4.20. As shown in right of Fig. 4.20, step response of it has different polarity in voltage. This will cause inter-symbol interference (ISI) of power supply noise, and the magnitude of the noise will be

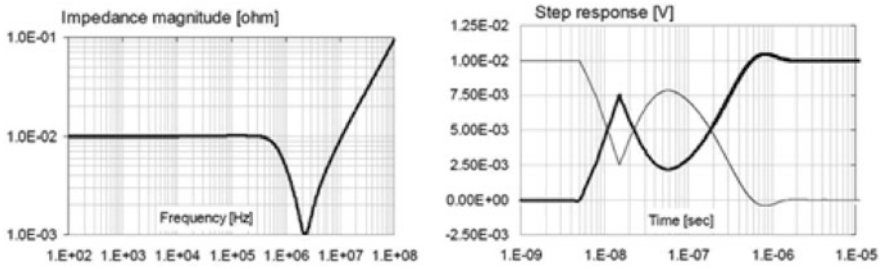


Fig. 4.20 Impedance profile and step response of a 10-milliohm Big-V PDN with AVP (© IEEE)

very large when the maximum peak of same polarity by different input overlaps at the same time.

Circuit Sensitivity.

Since allowable voltage variation should have frequency dependence, target impedance also should be a function of frequency. For example, for multi-gigabit I/O systems, many of the circuits are more sensitive to supply noise in one frequency range and less sensitive to supply noise in other frequency ranges. Therefore, supply induced jitter in an interface system is the result of the interaction of two separate and largely independent parameters. The first parameter is the amplitude and spectrum of the supply noise generated in the system. The second parameter is the sensitivity of the interface circuits to noise at different frequencies. Understanding both parameters independently as well as the interaction of these parameters provides us with insight necessary to predict and optimize supply noise induced jitter in the system [13–16].

R. Schmitt et al. demonstrated circuit sensitivity for analog power rail, V_{DDA}, which controls all internal timings of the system. They define the jitter sensitivity of an interface system as the ratio between the jitter generated by a single-frequency supply noise signal divided by the amplitude of this noise signal. The unit of jitter sensitivity is [ps/mV] and it is a function of the noise frequency.

$$\text{Sensitivity} = \frac{\text{Jitter}(f_{\text{sample}})}{\text{Noise}(f_{\text{sample}})} \left[{}^{\text{ps}}/_{\text{mV}}\right] \tag{4.11}$$

In order to measure the noise sensitivity at one frequency, supply noise is generated at this frequency and the resulting jitter at this frequency is measured. Sweeping the noise frequency provides the sensitivity profile over the frequency range of interest. They can estimate the jitter spectrum induced by supply noise in the interface by multiplying the simulated supply noise spectrum with the measured jitter sensitivity. The relationship among power supply noise, noise sensitivity, and jitter is displayed in Fig. 4.21. The "jitter impact" on the system is calculated by following equation.

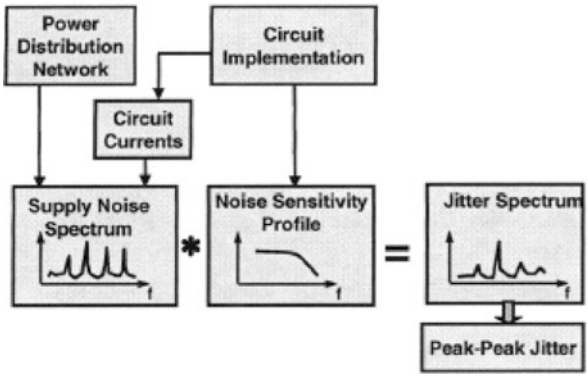


Fig. 4.21 Schematic of jitter generation due to supply noise (© IEEE)

$$(\text{Jitterimpact})(f) = \text{Sensitivity}(f) \cdot V_{\text{noise}}(f) \tag{4.12}$$

From the above equation, the jitter sensitivity profile is shown in Fig. 4.22. The shape of the cumulative jitter profile confirms the prediction of the supply noise spectrum and sensitivity profile that medium-frequency noise contributes significantly to the total jitter in the interface despite the fact that these frequencies are hardly excited by the current spectrum. This means that independent of the data rate in the interface system, special attention has to be paid to medium-frequency supply noise as well as the noise sensitivity profile of the interface circuits in this frequency range in this case.

Similar study was performed for DDR2-SDRAM on V_{REF} noise tolerance measurement [17]. To measure the V_{REF} noise tolerance, we developed a dedicated test

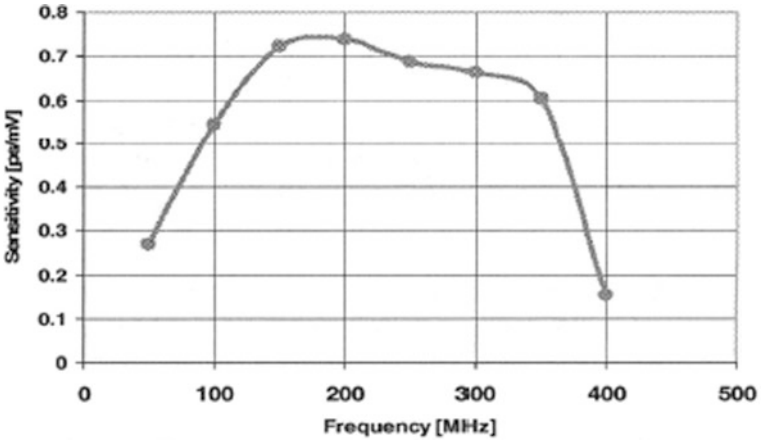


Fig. 4.22 V_{DDQ} supply noise sensitivity profile (© IEEE)

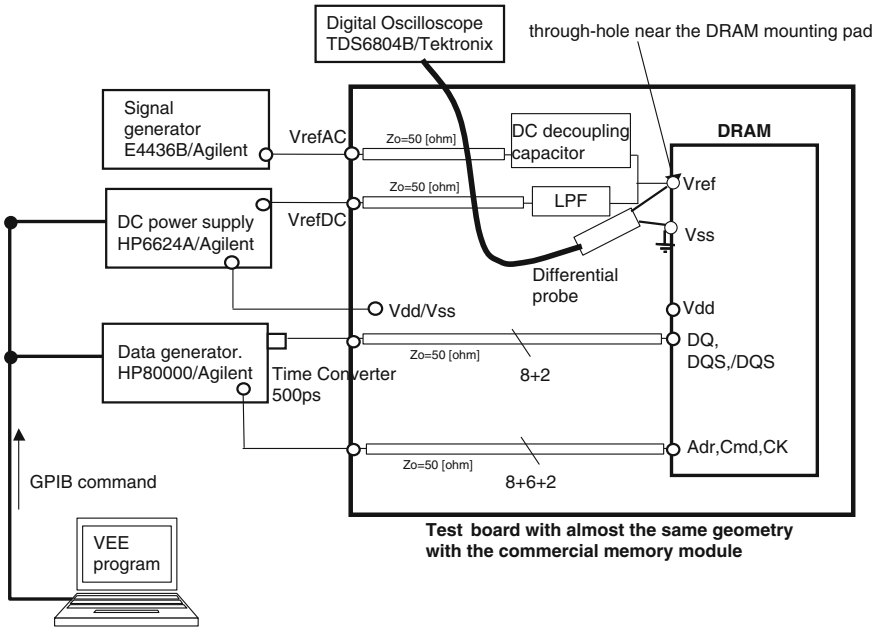


Fig. 4.23 Measurement setup of V_{REF} noise tolerance (© IEEE)

board that can be mounted with single DRAM. Figure 4.23 illustrates the measurement setup of the V_{REF} noise tolerance experiment. As shown in the figure, there are two voltage supply lines to the DRAM on this board. One is for the power supply voltage V_{dd} which is provided via a socket. The other voltage supply line is for V_{REF}. The V_{REF} supply line consists of two input lines on the board: one for DC-level input (V_{REF} DC in Fig. 4.23) and one for AC fluctuation input (V_{REF} AC in Fig. 4.23). The AC input line includes a DC blocking capacitor between the connector to the signal generator (acting as an AC noise source) and the V_{REF} pad of DRAM. The signal generator can generate a sinusoidal voltage waveform of a single frequency from 500 kHz to 1 GHz and changeable peak-to-peak voltage, maximum of 2 V.

In the experiment, the input waveform of the V_{REF} of DRAM is as shown in Fig. 4.24. The voltage waveform is a single-frequency sinusoidal wave with an offset of $V_{REF,typ} = 0.9$ V, which is supplied from the DC power supply. The single-frequency sinusoidal wave is induced from the signal generator. The applied AC voltage peak-to-peak value, V_{AMP}, was measured at the through-hole of the V_{REF} pad on the backside of the test board under the mounted DRAM. The V_{REF} noise tolerance at f_{noise} is obtained using the following procedure: (i) apply the V_{REF} AC noise, V_{AMP}, at f_{noise} and perform the WRITE command, (ii) stop the V_{REF} AC noise and replace the DQ line connections to the data generator system with the connection to the digital oscilloscope to show the read data waveform, and perform READ command, and confirm whether the READ data corresponds to the WRITE data; (iii) if identical, increase the voltage V_{AMP} by the value of $\Delta V = 20$ mV,

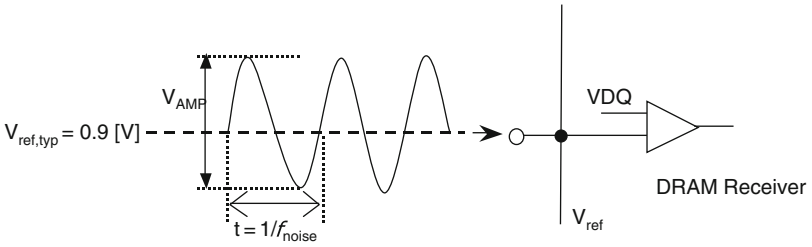


Fig. 4.24 Voltage waveform induced to V_{REF} (© IEEE)

and repeat the steps (i) and (ii); (iv) if the READ data is not equal, then the value V_{AMP} of the previous experiment is the V_{REF} noise tolerance V_{tol} at f_{noise}. Thus, by changing the noise frequency, we can obtain the V_{REF} noise tolerance frequency profiles.

Figure 4.25 plots the results of measuring the relationship between V_{REF} noise tolerance and induced noise frequency for the DDR2 SDRAM test chip. This leads to a revision of the idea that the target impedance is constant at all frequencies, i.e., the target impedance at high frequency need not be low. We can therefore design PCB patterns to satisfy the V_{REF} noise tolerance, leading to a low cost and more effective design technique than conventional methods. A particular advantage is non-necessity of high-frequency range for impedance design on board.

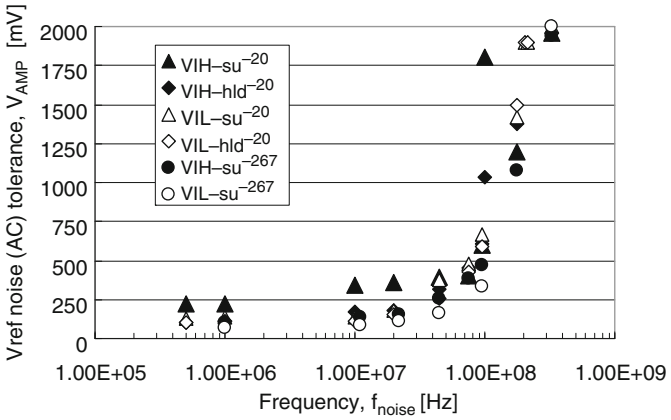


Fig. 4.25 Measured V_{REF} noise tolerance (shmoo plot) of DDR2-SDRAM test chip (© IEEE)

These kinds of results will lead practical setting of target impedance as shown in Fig. 4.26. Indeed, to obtain a practical target impedance, we require (i) noise sensitivity of the objective circuit, (ii) maximum current profile of the objective circuits, and (iii) transfer voltage noise profile from other LSIs. For (iii), high frequency noise (> few hundreds MHz) are very few in case of different packaged LSIs. In recent years, however, the distance between different LSIs are closing because of

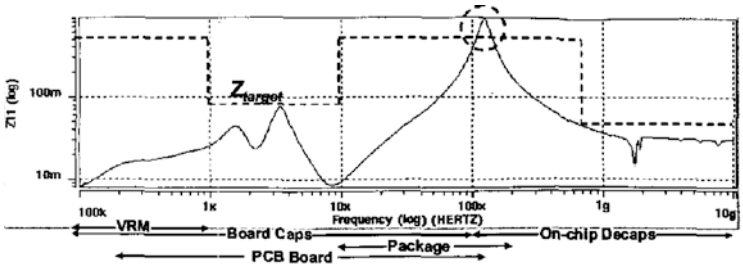


Fig. 4.26 Practical setting of target impedance (© IEEE)

demands of small factor as described in Section 4.2.3. For example, stacked LSI utilizing Through Silicon VIA (TSV) allows locating 2 LSI chips as close as less than 0.1 mm. In this case, we need more attention to GHz range noise transfer between adjacent LSIs. This kind of noise separation for wide frequency range will be an important technical issue for future LSIs.

4.3.2.4 Comparison Between TD and FD Analyses

We summarize the advantage and disadvantage of time-domain and frequency-domain analyses. Table 4.1 shows merit and demerit of both the analysis methods. Although frequency-domain analysis is a good method to specify problems in PDS, setting adequate target still includes a difficulty, as described in the previous section. While time-domain analysis is a good method to confirm target specification,

Table 4.1 Comparison of each design methodology with different domain

#	Design domain	Specify problem areas	Ease of setting target specification	Modeling (active device, noise source)	Computing time	Modeling (passive)
1	Frequency	Very good (discriminate by frequency component)	Not good (difficulty in setting effective target impedance)	Not good (difficulty in preparing noise spectrum)	Good (fast)	Good (ease of modeling of Z(f))
2	Time and frequency		Very good (both waveform and impedance)	Good (prepare current waveform for each operation mode)		
3	Time	Not good (Complex)	Good (time domain waveform)		Not good (slow)	Not good (specify an electrical circuit model)

it requires long simulation time and has difficulty in finding problems and how to solve the problem.

Figure 4.27 shows an example of combination method of time-domain and frequency-domain analyses. As you can see from this flowchart, design optimization is performed by frequency-domain analysis. After this matter, time-domain analysis is performed in order to confirm the specification meeting by waveform. By utilizing this kind of process, the period of analyzing and deciding design becomes shorter.

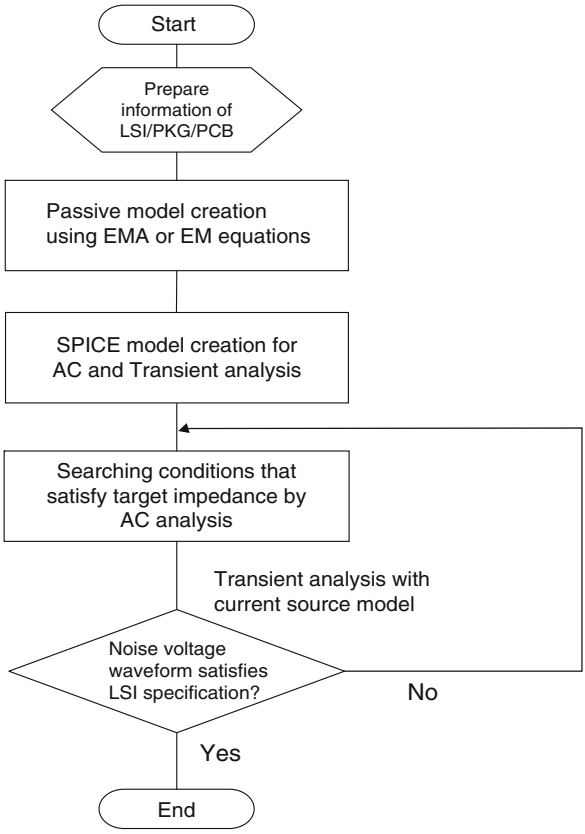


Fig. 4.27 Combination of frequency and time-domain approach

4.4 Modeling and Design Methodologies of PDS

In this section, modeling methodology for PDS design is discussed. There are three main approaches to model passive components for supply distribution inside PCB boards and packages: (1) equivalent lumped circuit models, (2) traditional numerical full-wave electromagnetic field solvers to analyze the power distribution system, and (3) divide the power planes into an array of small unit cells. This book focuses

on approach (1) because no one need expensive electromagnetic field solver and can use SPICE. Both frequency-domain analysis and time-domain analysis can be performed by a SPICE simulator.

This approach (i) calculates circuit parameter by a physical size (no CAD data required), (ii) is a small-scale equivalent model, (iii) with low cost and stable for simulation, and (iv) is based on the physical dimension by considering electrical current path.

4.4.1 Modeling of Electrical Circuit Parameters

Figure 4.28 shows components of PDS and typical equivalent circuit. Modeling method of each component will be discussed in the following.

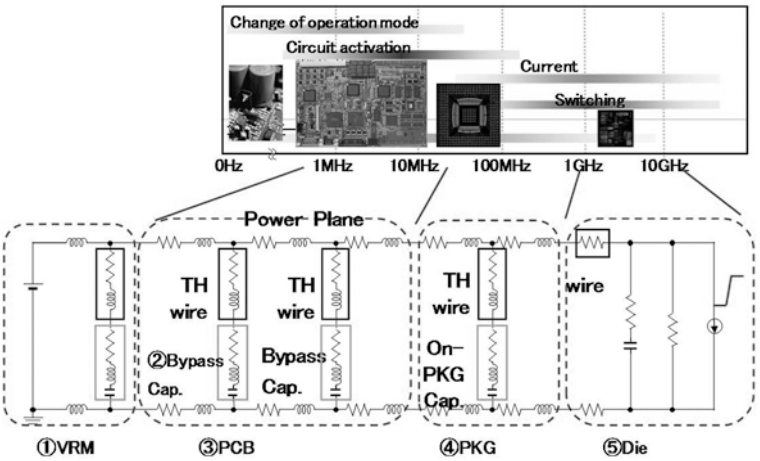


Fig. 4.28 Power distribution network description

4.4.1.1 Voltage Regulator Module (VRM)

Voltage regulator module (VRM) is a power supply stabilization circuit for CPU. A typical characterization test for a regulator module is shown in Fig. 4.29 and is explained in "http://www.sigcon.com/Pubs/edn/VoltageRegModel.htm" in detail. The module has an 8 A step load with a maximum di/dt of 2.5 V/μs and a period of about 320 μs. The plot in Fig. 4.29 shows the voltage regulator response to this current. For a modeling of this voltage regulator, we do not need additional information about the internals of the regulator. The only required information for the modeling is a step response waveform. From this waveform, we can determine a simple electrical circuit model for VRM as shown in Fig. 4.30. The circuit model assumes a perfect voltage source, V_1, connected through components R_1 and L_1 to

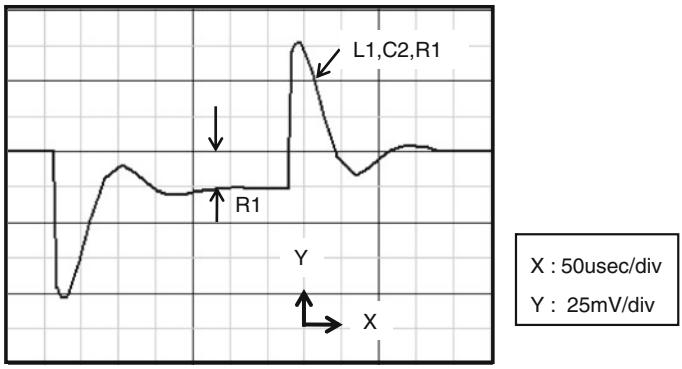


Fig. 4.29 Circuit parameters control the low-frequency step response

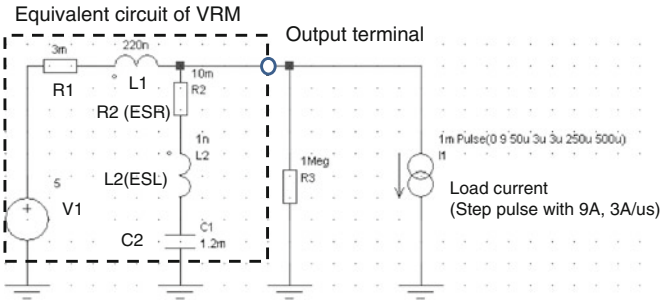


Fig. 4.30 Most voltage regulators behave like this simple circuit

the output terminal. Electrical components R_1 and L_1 represent the action of the regulator. Electrical component C_2, along with R_2 and L_2, represents the bulk capacitor in the VRM application. If you can find the R_1 and L_1 data values from the data sheet of VRM, you can build the equivalent circuit model as shown in Fig. 4.30. In this circuit, the simplest parameter to determine is R_1. As shown in Fig. 4.29, step response shows a damping oscillating waveform and the decay period is about 100 μs, so that over a time period of more than 100 μs, the circuit comes to stable DC operating condition. In the DC operating condition, the current paths due to the bulk capacitor can be almost open, while L_1 can be replaced by a zero ohm resistance. Consequently, from a DC drop voltage and the DC load current, we can easily determine the value R_1. For a next step of the modeling, we need to focus on a damping waveform region. For the shape of the damped sinusoidal response, components C_2 and L_1 come into play. The width of the glitch of the damping sinusoidal waveform is determined by C_2 and L_1. So if you can find a parameter value of C_2 in the application note of this component, you can find a reasonable value of L_1 by adjusting to match the glitch width. Finally R_2 can be determined from damping factor of each sinusoidal pulse. Although the value of L_2 is not decided, it is not so

important for the modeling of VRM. This is because the VRM usually covers the frequency range from DC to approximately 100 kHz, and in this frequency range inductance of nH order is almost negligible. Thus we can determine the electrical circuit model for VRM.

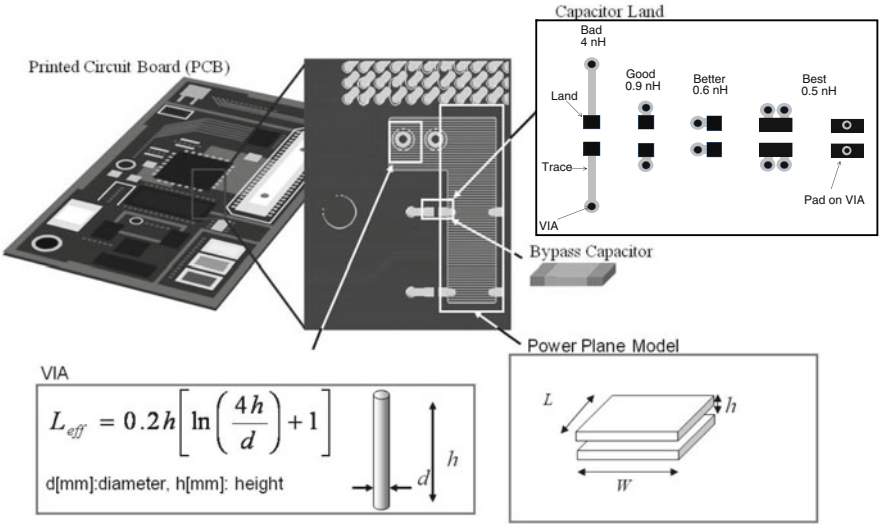


Fig. 4.31 Passive components of PDS included in PCB and LSI package

4.4.1.2 Bypass Capacitor

Figure 4.31 shows passive components of PDS included in PCB and package. First, we model a bypass capacitor. Bypass capacitor components consists of equivalent series resistance (ESR) and equivalent series inductance (ESL) in addition to capacitance.

Simple equation of this impedance is described as below.

$$Z(\omega) = R + j\omega L + {}^{1}/_{j\omega C} \tag{4.13}$$

Figure 4.32 shows impedance profile of bypass capacitor. V-shape impedance profile is seen. The minimum impedance is determined by a resonant frequency of LCR series circuit. The resonant frequency is described as,

$$f_{res} = \frac{1}{2\pi\sqrt{LC}} \tag{4.14}$$

By reducing ESL, the impedance profile of higher frequency part is reduced and resonant frequency moves to higher frequency. For wide-frequency-band impedance reduction, low-ESL capacitor component is important.

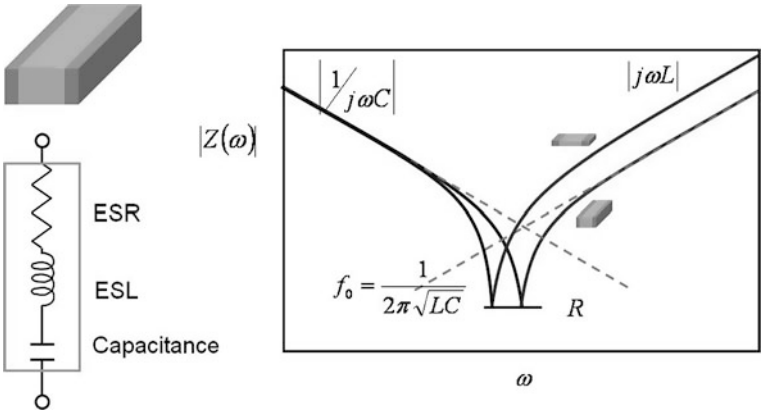


Fig. 4.32 Equivalent circuit model and impedance profile of bypass capacitor

4.4.1.3 Land of Bypass Capacitor

Bypass capacitor is mounted on land of PCB. Even if we use same components, mounting inductance are quite different with different land and mounting geometries. Figure 4.33 shows examples of mounting inductance for each geometry (http://www.xilinx.com/support/documentation/application_notes/xapp623.pdf). Long trance and distance between VIAs cause large mounting inductance. As you can see from this figure, the mounting inductance is 10 times different by only a difference

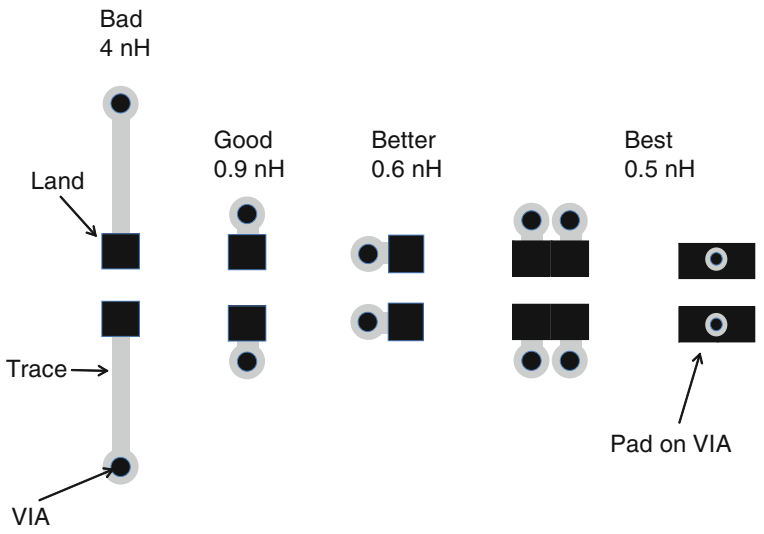


Fig. 4.33 Example of capacitor land and mounting geometry

of land pattern. For lowering impedance over mid-frequency, land pattern of bypass capacitor is one of the important design issue.

4.4.1.4 Power and Ground Planes

In usual PCB, most part of PDS consists of power and ground plane, which is a parallel metal plate of power plane and ground plane (see inset of Fig. 4.31). The inductance and resistance are calculated by

$$\begin{aligned} L_e &= \frac{\mu_0 L h}{W} \\ R_e &= 1.69 \times 10^{-8} \times L/(t \times W) \times 2 \end{aligned} \tag{4.15}$$

where μ_0 is permeability, L is the length of plane, W is the width of plane, h is the spacing between power plane and ground plane, and t is the thickness of metal plate. The resistance is calculated based on copper resistivity, which material is used in most PCB. The calculation of plane inductance is based on assuming thin dielectric layer and relatively wide trace. To maintain low plane inductance, wide and short trace with thin dielectric layer is necessary.

4.4.1.5 VIA

VIA is used for vertical electrical connection in PCB and LSI package (see inset of Fig. 4.31). The shape of VIA is a cylinder-like, and the effective inductance is calculated as

$$L_{\text{eff}} = 0.2\,h\left[\ln\left(\frac{4\,h}{d}\right) + 1\right] \tag{4.16}$$

where d [mm] is the diameter of VIA and h [mm] is the length of VIA. To lowering inductance of VIA, via height is much important than the via diameter as described in Eq. (4.16). It is also noted that pair of power and ground VIA should be close each other, because mutual inductance between power and ground VIA cause the lowering of loop inductance of VIA.

4.4.1.6 BGA

In recent LSI package, ball grid array (BGA) is often used for connecting LSI package and PCB, in order to fine pitch with large amount of pins. The inductance of BGA ball is calculated by the following equation by assuming the geometry is quite similar to cylinder (see inset of Fig. 4.34).

$$L_{\text{eff}} = \frac{\mu}{2\pi}\left\{h\log\left(\frac{h+\sqrt{a^2+h^2}}{a}\right) - \sqrt{a^2+h^2} + a\right\} \tag{4.17}$$

where a is the radius of BGA ball and h is the height of BGA ball.

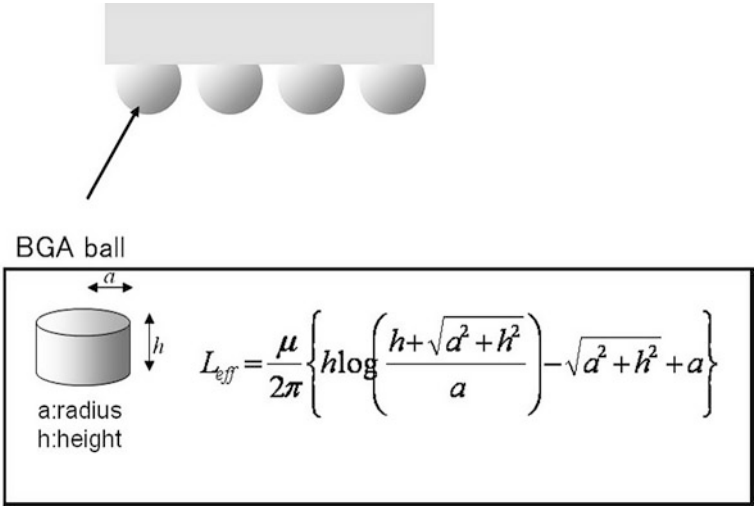


Fig. 4.34 BGA balls for LSI package

4.4.1.7 On-Chip Bypass Capacitors

On-chip bypass capacitors reduce the peak current demand on the distribution network. Deciding suitable on-chip bypass capacitor value is not only important to reduce high frequency noise but also important to make the LSI cost low. Extra on-chip bypass capacitor requires extra chip area on LSI that cause LSI cost higher.

Thin-oxide MOS capacitors are most often used for on-chip bypass because they give the highest capacitance per unit area. Well and diffusion junction capacitors and metal and polycrystalline silicon parallel plate capacitors can also be used for this purpose. A thin-oxide capacitor is essentially an MOS transistor with its source and drain tied together. As long as the voltage across the capacitor is greater than the threshold voltage, its capacitance is well approximated by

$$C_{\text{ox}} = \frac{\varepsilon_r \varepsilon_0 WL}{t_{\text{ox}}} = \frac{3.45 \times 10^{-13} WL}{t_{\text{ox}}} \tag{4.18}$$

where W and L are the width and length of the capacitor, respectively, in μm and t_{ox} is the oxide thickness in angstroms. For example, a 0.35 μm process with $t_{\text{ox}} = 70$ angstroms has a C_{ox} of about 5 fF/μm^2 [18].

4.4.2 Design Strategies of PDS

In this section, we show one of the design methodology based on frequency-domain method. In this method, impedance control for certain frequency range is a strategy to meet target specification. In a frequency-domain design, first we decide target

impedance from Eq. (4.7). The target impedance guarantees that supply will not exceed specified tolerance with given transient current. In this case, definition of transient current is important.

When the impedance of the PDS is flat in frequency domain, acceptable regulation in time domain is obtained. The example of simulation is displayed in Fig. 4.35. As a second case, we consider the case that impedance of the PDS has a dips and peaks in frequency domain. This is a usual case in the design. As shown in Fig. 4.36, excessive noise in the time domain appears. The noise becomes worse when the operating frequency and resonant frequency are equal. Thus, the resonant peaks

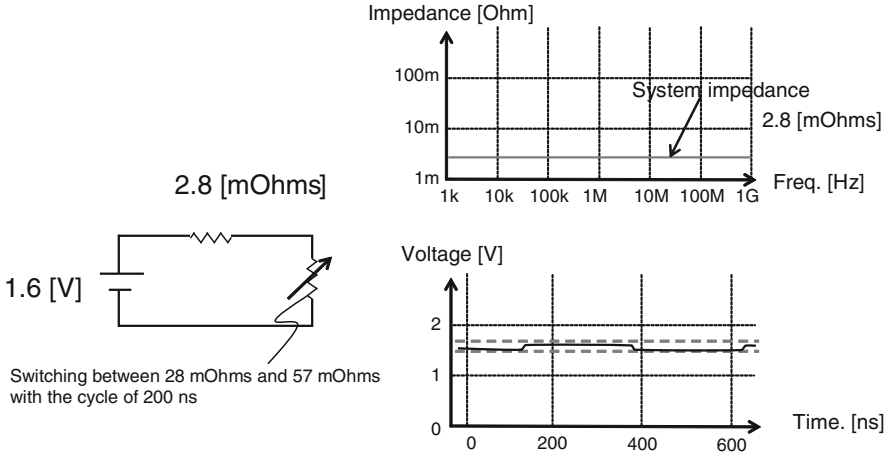


Fig. 4.35 The PDS which has flat impedance profile for all frequency range (© IEEE)

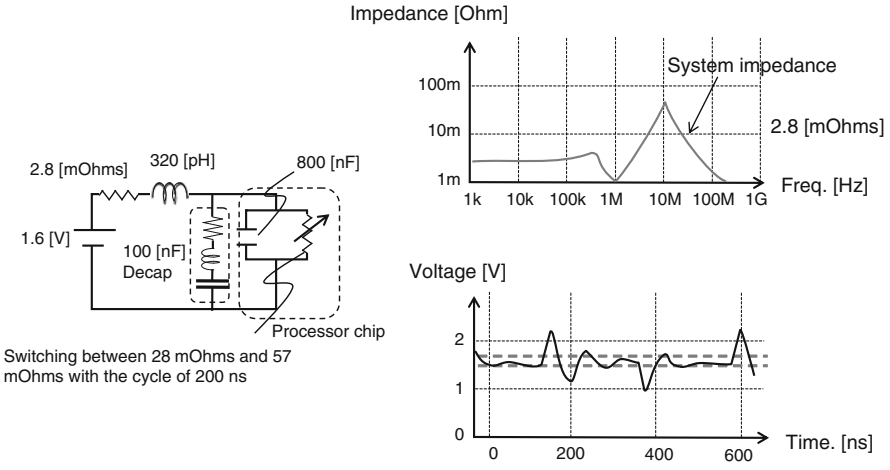


Fig. 4.36 The PDS which has dips and peaks in impedance profile (© IEEE)

must be avoided by controlling the resonant frequency which occur impedance peak no to match the operating frequency. To reduce impedance, bypass capacitor optimization is one of the most effective strategies for design of PDS in PCB.

Optimization of bypass capacitor selecting is to select combination of (a) type, (b) mounting position, and (c) number of bypass capacitors to meet target impedance in the least expensive BOM, the least board area. Here we will see some strategies for selecting bypass capacitors.

4.4.2.1 Usage of Different Capacitors

To reduce wide frequency range, it is better to use different kinds of bypass capacitor with different size. In principle, large component has large capacitor and large inductance, while small component has small capacitor and small inductance. To cover wide frequency range with small number of components, combinations of these capacitors are very important. Figure 4.37 shows the example of combination. Type A represents low ESL and small capacitor component, while Type B represents large capacitor and large ESL. Due to large value of capacitance and ESL for type B, the resonant frequency is lower than the type A and covers low frequency region for lowering impedance. While type A covers high frequency region to maintain impedance lower.

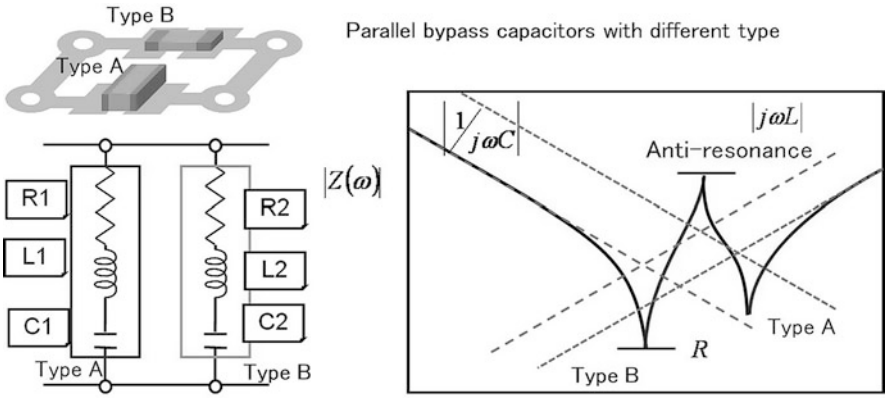


Fig. 4.37 Impedance profile for parallel bypass capacitors with different types

When using different types of capacitor, we should be careful about the existence of anti-resonance. Due to LC parallel circuit, large impedance peak appears between each resonant frequency.

4.4.2.2 Usage of a Capacitor with Large BQF

When we select a bypass capacitor itself, we have to select a low ESL one with large bypass quality factor (BQF) [20]. BQF is an index of bypass capacitor how it can cover wide frequency range. BQF is calculated as follows:

$$\mathrm{BQF} = \mathrm{C/ESL} \tag{4.19}$$

From Eq. (4.19), one can imagine low ESL and large capacitance are important for obtaining large BQF. If there are some bypass capacitor components with same ESL and different capacitance, you had better to choose large capacitance one. If there are some bypass capacitor components with same capacitance and different ESL, you'd better choose small ESL one.

Figure 4.38 shows an example of two kinds of BQF capacitor.

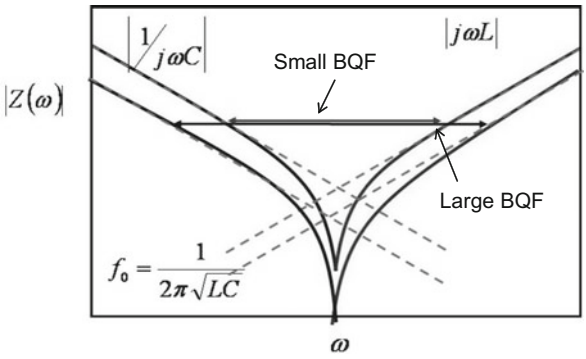


Fig. 4.38 Bypass capacitor with different BQF

4.4.2.3 Usage of a Large ESR

As described in Section 4.4.2.1, if we use different kinds of bypass capacitor, there appears anti-resonant peak in impedance profile. The parallel resonant impedance peak is inversely proportional to sum of each component as shown in the following equation.

$$Z_{\mathrm{peak}} \sim \frac{\mathrm{L_1}}{\mathrm{C_2}}\left(\frac{1}{\mathrm{R_1} + \mathrm{R_2}}\right) \tag{4.20}$$

By selecting large ESR component, the effect of anti-resonance is considerably small [19].

4.4.2.4 Usage of Multiple Terminal Components

Recently, there are many kinds of capacitor with low inductance. Figure 4.39 shows an example of low ESL capacitor. This component has geometry of short length and large width compared to normal component. Additionally, there are multi-terminal components, as shown in Fig. 4.40. The merit of using multi-terminal component is not only small ESL component, but also very small mounting inductance. Total inductance of multi-terminal capacitors sometimes become as low as 1/10 of normal components with same size.

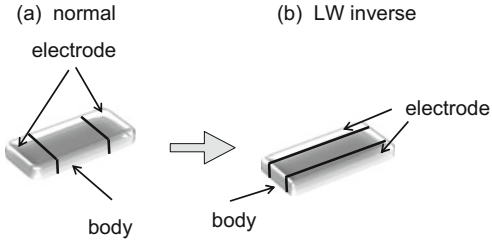


Fig. 4.39 LW inverse bypass capacitors

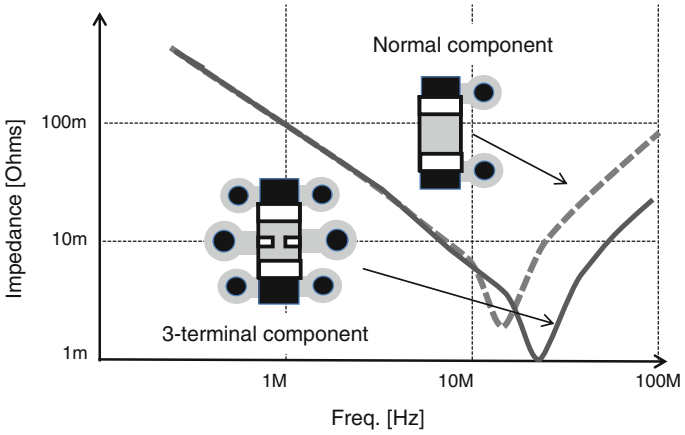


Fig. 4.40 Comparison of impedance profiles of normal and multi-terminal caps

4.4.2.5 Place Components as Close as Possible

The effective inductance from inside the chip is calculated as

$$L_{\text{eff}} = L_{\text{pkg}} + L_{\text{pln}} + \frac{L_{\text{dec}}}{N_{\text{dec}}} \tag{4.21}$$

where L_{eff} is the effective inductance from inside the chip, L_{pkg} is a loop inductance of LSI package, L_{pln} is a loop inductance of power and ground planes, L_{dec} is ESL of bypass capacitor with mounting inductance, and N_{dec} is the number of bypass capacitors. Even if we increase the number of bypass capacitors, L_{eff} cannot be less than $L_{\text{pkg}} + L_{\text{pln}}$. To minimize the number of components to meet target impedance and to minimize L_{pln}, placing the components as close as LSI package is very important. The example based on Eq. (4.21) is shown in Fig. 4.41.

4.5 Simultaneous Switching Noise (SSN)

In recent years, the speed and the integrated density of the LSI are increasing. In high-speed operation, there appears I/O supply noise that occurs when all drivers

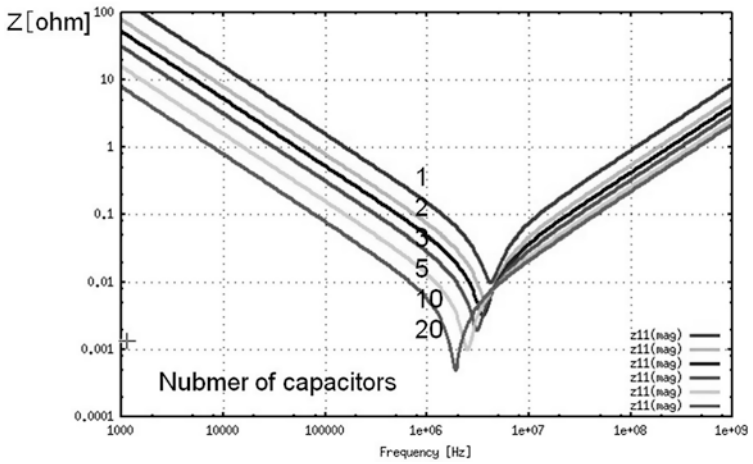


Fig. 4.41 Impedance profile dependence of PDS with different number of capacitors

switch simultaneously. In this section, we focused on a power supply noise for I/O circuit.

4.5.1 Principle of SSN

Simultaneous switching noise (SSN) refers to the noise generated in a digital system due to rapid changes in voltage and current caused by many circuits switching at the same time. We will show the example of SSN generation by using low to high transition case. Figure 4.42 shows a system consisting of a chip with *N* drives that connect to the system through a package. For low to high transitions,

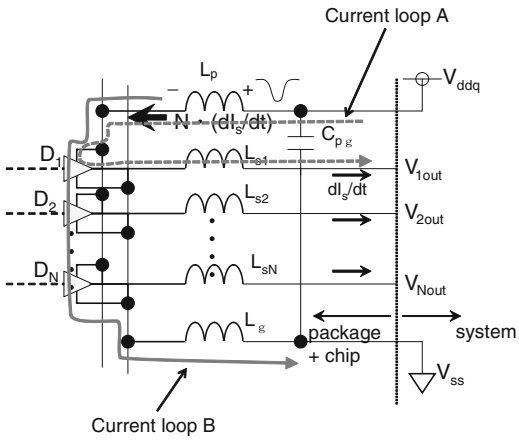


Fig. 4.42 Simultaneous low to high transition

the current paths are shown in the figure. We have two kinds of current loop, A and B.

For a current loop A, as the large number of drivers switches, large switching current flows from power line to signal line through package, and due to the presence of package inductance, voltage of $L\mathrm{d}i/\mathrm{d}t$ generated for package inductance L. Thus this voltage move down the reference high-voltage level at the switching time and the voltage fluctuation behaves as noise. For the case of high-to-low transition, same thing happens and the ground voltage level move up by that noise at the switching time. Hereinafter, we call this SSN as Signal-Ground loop SSN (S–G loop SSN).

For a current loop B, due to an existence of crossover current, power supply current from power line to ground line occur. This electrical current strongly depends on an equivalent electrical circuit of power ground loop of I/O power supply network. In usual case, the circuit is expressed by simple series and parallel RLC circuit. Hereinafter, we call this SSN as Power-Ground loop SSN (P-G loop SSN).

4.5.2 S–G loop SSN

Let us consider the noise voltage for S–G loop SSN. The noise voltage is determined by slew rate of the current flowing in the power or ground traces of the package and effective inductance of the package. For example, if the effective inductance equals to 3 nH and the slew rate equals to 200 mA/ns, the noise voltage achieve as large as 600 mV. To reduce this noise, one method is to reduce effective inductance and the other is to control $\mathrm{d}i/\mathrm{d}t$ term, such as modified asymmetrical slew rate (MASR) method. In this book, we focused on the efficiency of LSI package effective inductance to reduce SSN.

$$V_{\mathrm{SSN,SG}} = L_{\mathrm{eff}} \frac{di_{\mathrm{s}}}{dt} \quad \ldots \tag{4.22}$$

Here we define two kinds of SSN, Quiet low (QL) noise and Quiet high (QH) noise:

QL noise: Objective DQ pin is fixed to low (S–G loop SSN for ground (V_{ss}) line)
QH noise: Objective DQ pin is fixed to high (S–G loop SSN for power (V_{ddq}) line).

Next, we will show an example of active bit number dependency of SSO noise. We show the results for two kinds of LSI package (type A and type B) in Fig. 4.43. Effective inductance of LSI package of type A is about 1/4 to 1/2 of that of type B. By increasing the active bit number, the SSN are linearly increased until 8 bits. Over 8 bits, the SSN was saturated for both type A and type B. Over the 8 bits, clearly type A's noise are smaller than that of type B. The SSN saturations at 8 bits is due to the reduction of effective inductance over 8 bits.

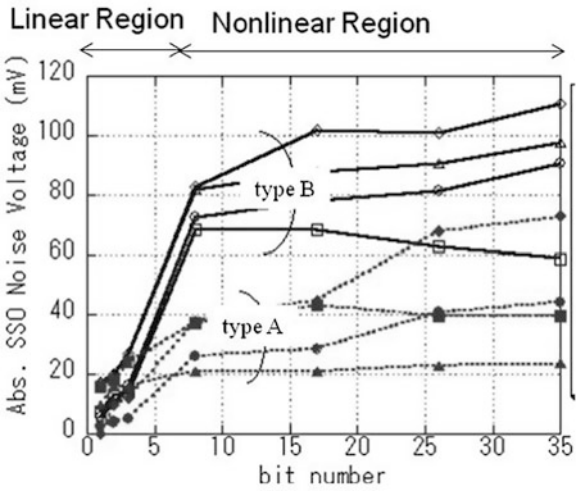


Fig. 4.43 Bit number dependence of simultaneous switching noise for two kinds of LSI package

The saturation of SSN can be simply explained by the current flowing of return path. In Fig. 4.44, we show the case of two signal lines and one ground line. In this case, if we increase switching inverter, the SSN will increase because the current flowing to ground path becomes twice. However, if we consider the case as shown in Fig. 4.45, four signal lines and two ground lines, SSN will not be four times the case of only one driver switching case. This is due to a parallel L_{eff}, as shown in Fig. 4.46.

$$\begin{aligned} \frac{1}{L_{\text{eff}}} &= \sum_{i=1}^{n} \frac{1}{L_{gi}^{e}} \\ L_{gi}^{e} &= \sum_{j=1}^{n} L_{gij} \frac{i_{gi}}{I_{gi}} - \sum_{j=1}^{m} L_{gisj} \frac{i_{sj}}{I_{gi}} \end{aligned} \tag{4.23}$$

where L_{eff}: effective inductance; L_{gi}^{e}: equivalent partial inductance of ground conductor i; I_{g}: slew rate in ground conductor; I_{s}: slew rate in signal conductor; n: number of ground conductor; and m: number of signal conductor.

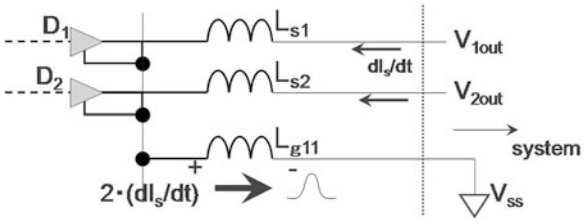


Fig. 4.44 Simplified model of SSN (2-bit case)

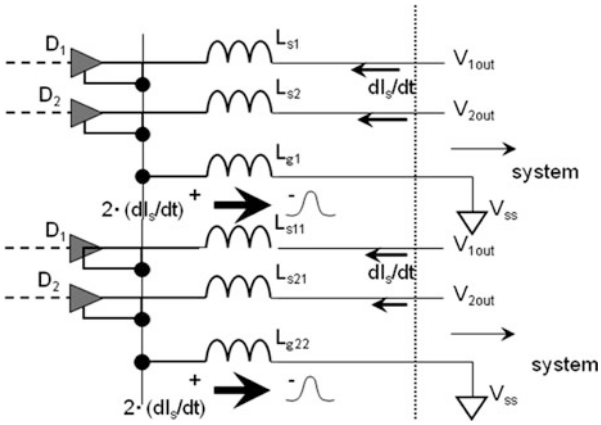
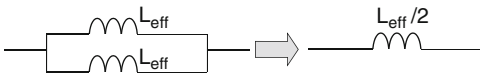


Fig. 4.45 Simplified model of SSN (4-bit case)

Fig. 4.46 Parallel *L*eff



If there is no mutual term, independent two effective inductances can be treated as just two parallel connected inductances.

$$L_{g1} = L_{g11}\frac{2\dot{I}_s}{2\dot{I}_s} - L_{g1s1}\frac{\dot{I}_s}{2\dot{I}_s} - L_{g1s2}\frac{\dot{I}_s}{2\dot{I}_s}$$
$$L_{g2} = L_{g22}\frac{2\dot{I}_s}{2\dot{I}_s} - L_{g2s3}\frac{\dot{I}_s}{2\dot{I}_s} - L_{g2s4}\frac{\dot{I}_s}{2\dot{I}_s} \quad (4.24)$$

The above Eq. (4.24) express the ground inductance calculation for the case of Fig. 4.45. As you can see from this equation and Fig. 4.46, electromagnetically independent ground lines do not increase the SSN linearly by increasing the bit numbers. As seen from this feature, in order to reduce SSN effectively, it is also important to optimize the ground wiring in conjunction with the layout of signal lines, in addition to increase the number of ground wires.

4.5.3 P–G loop SSN

P–G loop SSN is the noise produced by current flowing in I/O power supply networks; the noise waveform depends strongly on the power supply network impedance defined at the power and ground nodes of I/O circuit. In most cases, the impedance profile of the I/P power supply network has a peak due to an anti-resonance of LC parallel circuit, which is originated from on-chip capacitor and loop inductance of power traces of LSI package. This resonance is called as chip-package resonance. If this resonance frequency is low enough compared to the pulse width of the crossover current, the noise waveform of P–G

loop SSN can be assumed as an impulse response against the I/O power supply network. The chip-package resonant frequency is typically in the range of 10 MHz–1GHz, which has a period of 1–100 ns cycle. If the pulse width of the crossover current is much smaller than this period, the current can be assumed as an impulse response for the PDNs, as shown in Fig. 4.47 [21]. The coefficient of the impulse response is the area of the switching current, e.g., charge amount Q. In Fig. 4.47, the PDN impedance Z_{in} can be represented in the Laplace domain description as

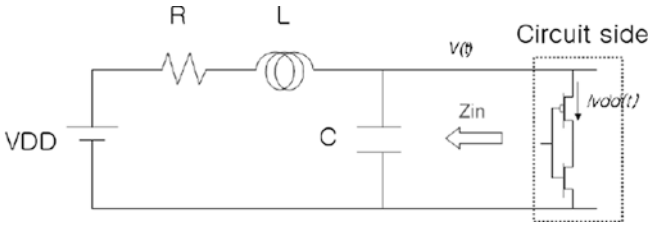


Fig. 4.47 An example of single-resonance PDNs (© IEEE)

$$Z\text{in}(S) = \frac{R + S \cdot L}{S^2 \cdot L \cdot C + S \cdot C \cdot R + 1} \tag{4.25}$$

Then, the impulse response of $Z_{\text{in}}(S)$ in the time domain can be found by the inverse Laplace transform as

$$\begin{aligned} Z\text{in}(t) &= \tfrac{1}{C} \cdot \exp(-\tfrac{1}{2} \cdot \tfrac{R}{L} \cdot t) \\ &\cdot \left[\cos(t\sqrt{\tfrac{1}{L \cdot C} - (\tfrac{1}{2} \cdot \tfrac{R}{L})^2}) + \frac{R \cdot \sqrt{C}}{\sqrt{4 \cdot L - R^2 \cdot C}} \cdot \sin(t \cdot \sqrt{\tfrac{1}{L \cdot C} - (\tfrac{1}{2} \cdot \tfrac{R}{L})^2}) \right] \\ &\text{for } t \geq 0 = 0 \text{ for } t < 0 \end{aligned} \tag{4.26}$$

The time-domain impulse response $Z_{\text{in}}(t)$ has the waveform as shown in Fig. 4.48. The initial value of $Z_{\text{in}}(t \to 0)$ is $1/C$, and $Z_{\text{in}}(t)$ resonates within the envelop of exponential term in the equation. From the interest for power integrity design, both peak-to-peak amplitude of the noise and damping oscillating factor are the design parameters. From Eq. (4.26), the impact of R, L, and C of the PDN on the power supply noise waveform can be understood. To reduce peak-to-peak amplitude, C should be large, because C is inversely proportional to the amplitude of the impulse response. To maintain the damping oscillating factor, R and L are also related. To control the oscillating frequency, C and L are the key parameters. As the operating speed increases, damping factor becomes a very important issue since the PDN impulse response can be overlapped. To increase the damping factor, large R is desirable.

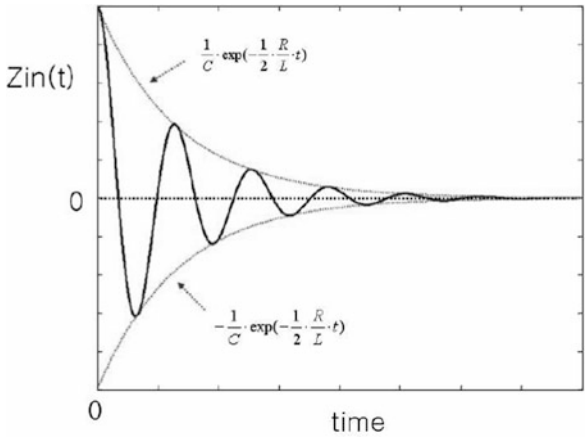


Fig. 4.48 Time-domain impulse response of PDNs (© IEEE)

4.6 Measurement of Power Distribution System Performance

As described in earlier section, on-chip PDN characterization is the most important for PI design. In this section, we will introduce some measurement techniques concerning on-chip voltage waveform and on-chip power supply impedance measurement.

4.6.1 On-Chip Voltage Waveform Measurement

Here we introduce three types of measurement circuits, based on DA converter (DAC), ring oscillator, and delay fluctuation of inverter chain circuits. Each measurement technique has trade-off for design cost and measurement performance. It is important to select the measurement circuit according to the purpose.

4.6.1.1 DAC

Figure 4.49 shows a block diagram of the sampling oscilloscope, which consists of one timing generator block and multiple sampling heads for measuring voltage fluctuation [22]. For this circuit, 10 mV voltage resolutions and 1 ps timing resolutions are achieved, although several digital I/O and analog input are needed to be added. In this circuit configuration, the sampling oscilloscope block generates excitation timing, sampling enable timing (SE), and reference voltage (V_{REF}), which are connected to each sampling head. A master clock (CK) generates all timings in this system. Since all circuit operations are reset and restarted with every master clock edge, neither clock jitter issue nor jitter accumulation issue should be considered. A repetitive waveform (V_{DUT}) is incident to the sampling comparator in the sampling

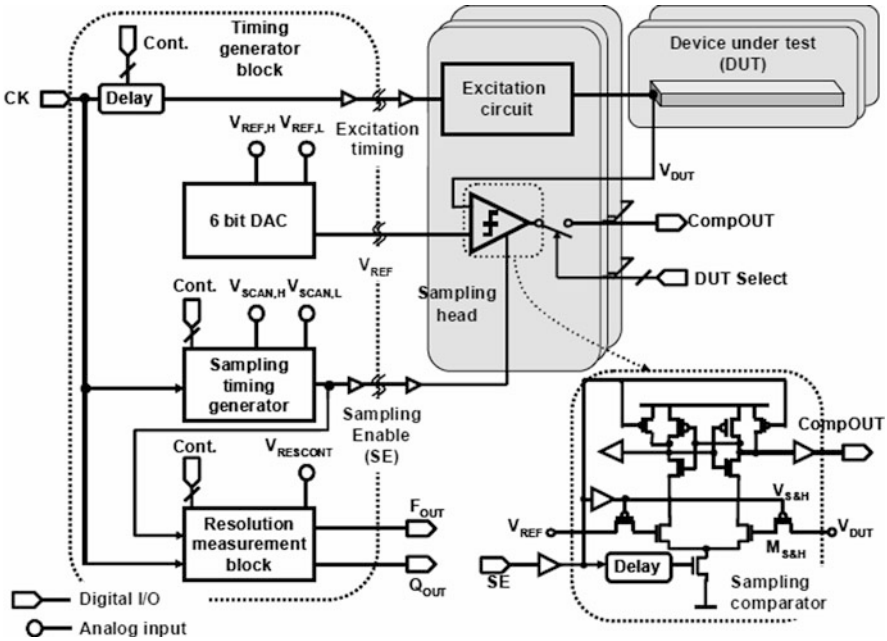


Fig. 4.49 Overall block diagram of on-chip sampling oscilloscope (© IEEE)

head, and V_{DUT} is compared with the V_{REF} at SE edge. V_{DUT} can be reconstructed by scanning V_{REF} and SE and by monitoring "1" and "0" of the CompOUT which is a digital signal. Although DUT is driven by an excitation circuit in Fig. 4.49, excitation circuit is eliminated if the noise on a chip is to be measured. In this case, CK is generated from the main clock of the circuit block under test. In this circuit, 128 levels of V_{REF} are produced by a resistor ladder to achieve 10 mV voltage resolutions.

By measuring a known DC voltage and observing the difference between the known voltage and the measured voltage, the offset voltage of the sampling comparator can be fully compensated. Figure 4.50 shows measured and simulated waveforms of a line by changing the location of a capacitor of 1.9 pF, which represents a decoupling capacitor at the far end, center, and near end. As shown in Fig. 4.50, both are in good agreement.

4.6.1.2 Ring Oscillator

Ring oscillator is an oscillator with a ring structure attached to the plurality of delay elements as a whole with a negative gain. It typically consists of an odd number of NOT gates. From an oscillating frequency of the ring oscillator, voltage level inside the chip is measured in this circuit configuration. Figure 4.51 shows the whole

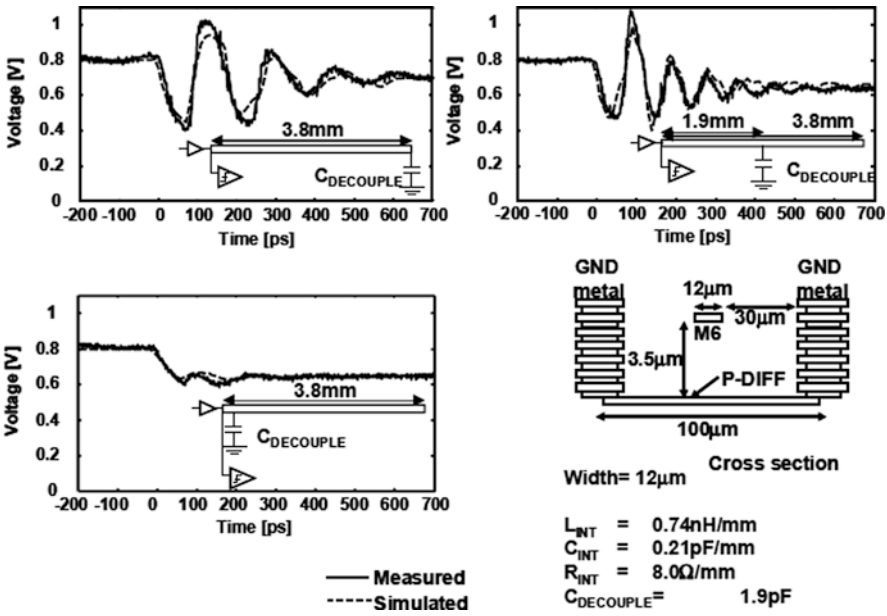


Fig. 4.50 Measured and simulated waveforms of power supply line with varying decoupling capacitor location (© IEEE)

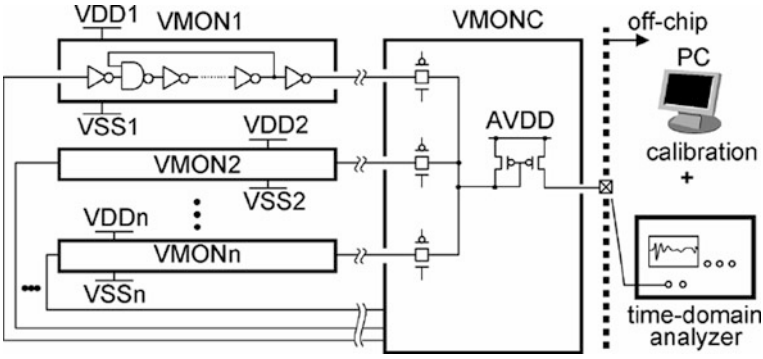


Fig. 4.51 In situ supply-noise-map measurement scheme (© IEEE)

configuration of the measurement system based on a ring oscillator [23]. The key features of this measurement circuit are minimal size of on-chip measurement circuits and support of off-chip high-resolution digital signal processing with frequent calibration, resulting in the non-need of sampling and hold circuit in the chip. In this configuration, few additional digital I/O and no analog input are required. The on-chip circuits have several voltage monitors (VMONs) and the controller (VMONC) of VMONs. The VMON is a ring oscillator that acts as a supply voltage-controlled

oscillator, so that the local power supply difference can be translated to a frequency-modulated signal. The VMONC activates only one of the VMONs and outputs the selected frequency-modulated signal to the external path of the chip. The output signal from the chip is then demodulated in conjunction with time-domain analysis by an oscilloscope and calibrations by a PC. The frequency-modulated signal has high noise immunity for long distance and wired signal transmission, because the important information exists in the oscillating frequency. The dynamic range of the measuring voltage is not limited, despite requiring no additional dedicated supply voltage, because this system requires a measurement of a frequency fluctuation as a voltage fluctuation, which is based on the fact that the oscillation frequency of a ring oscillator is a simple monotonic increasing function of the power supply voltage.

The voltage measurement mechanism of the ring oscillator and definition of measured voltage utilizing this circuit are shown in Fig. 4.52 in the simple case of a five-stage ring oscillator. In the ring oscillator, since only one inverter in the ring is activated at one time, each inverter converts the local power supply voltages into delays one after the other. In this scheme, the local power supply distribution is calculated from a measured period or from a measured frequency. It is noticed that the measured one is therefore an average value. Since the voltage fluctuation is integrated through the period, time resolution of the circuit is determined by the period. The higher the frequency of the ring oscillator is, the higher the time resolution. The signal transmission at higher frequency, however, limits the length of the transmission line between the VMONs and the VMONC due to the bandwidth limitation of the transmission line. Therefore, there is a trade-off between time resolution and transmission length.

Figure 4.53 shows measurement voltage waveform of local supply noise by VMON embedded in the LSI. The voltage drop during the Dhrystone execution is clearly observed. The voltage resolution is as small as 1 mV, and the time resolution is 5 ns in this case.

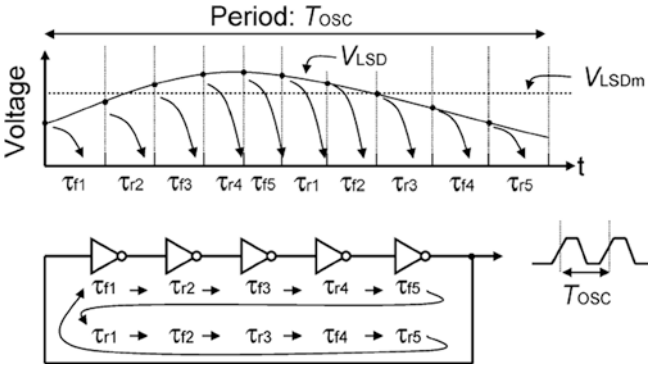


Fig. 4.52 Sampling of a ring oscillator (© IEEE)

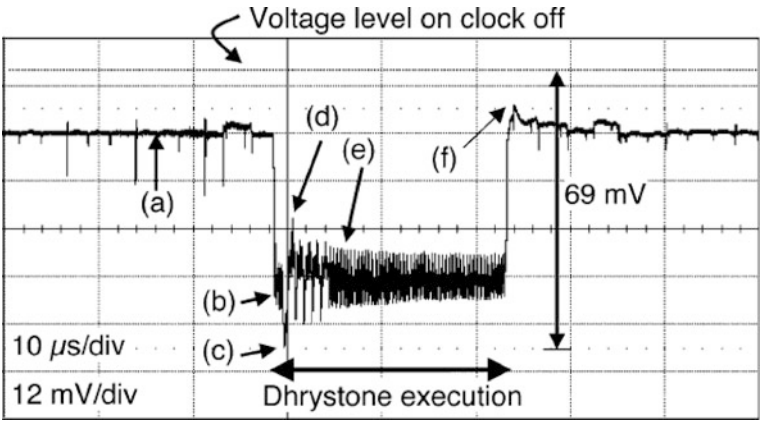


Fig. 4.53 Measured local supply noise by VMON1 (© IEEE)

4.6.1.3 Delay Observation

The CMOS inverter is a circuit that reverses the input signal and transfers the output signal to the next steps [24]. A constant delay is required for the charge/discharge of the load capacity, as shown in Fig. 4.54a. The amount of delay relates to the applied voltage difference. If the voltage fluctuation, ΔV_{dd}, from the reference voltage, V_{dd}, is small (<10% of V_{dd}), the amount of delay fluctuation, Δt, can be written as

$$\Delta t = \alpha(V_{dd'} - V_{dd}) = \alpha \Delta V_{dd} \tag{4.27}$$

where α is the voltage-delay conversion coefficient for a single inverter. When we know α, we can determine voltage fluctuations on the chip by observing delay fluctuations offchip. However, we need to solve the two following problems to apply this method: (i) Δt is generally too small to measure and (ii) detecting local delays is very difficult due to many buffer inverters between the target inverter, whose delay fluctuations we want to grasp, and I/O or delay detect circuits.

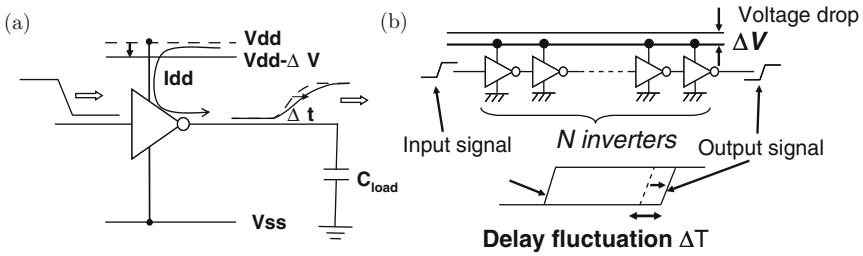


Fig. 4.54 Single and *N*-inverter chain output delay by a voltage drop (© IEEE)

To solve the problem (i), we configured numerous inverters connected in series, as shown in Fig. 4.54b. In this case, delay fluctuation ΔT becomes

$$\Delta T = \alpha \cdot N(V_{\mathrm{dd}}, - V_{\mathrm{dd}}) = \alpha \cdot N\Delta V_{\mathrm{dd}} = \alpha_N \Delta V_{\mathrm{dd}} \tag{4.28}$$

where α_N is a voltage-delay convert coefficient for N-series inverters. Here, we should mention that the waveform reproducibility for series inverters has a trade-off involving the number, N. If N increases, the voltage resolution increases, as described in Eq. (4.28), while measurable maximum noise frequency, $f_{\max}$, decreases because the total inverter delay T_{total} increases ($f_{\max}$ is proportional to $1/T_{\mathrm{total}}$). We added the function that switches N to 50, 250, 1,250, or 2,500 via selector A–D as shown in Fig. 4.55. For example, an N of 50 is for high-frequency noise (>100 MHz) of approximately 1 mV resolution. An N of 2,500 is for low-frequency noise (<1 MHz) of approximately 20 μV resolution.

To solve problem (ii), we prepared a calibration path to eliminate delay fluctuations caused by the unnecessary buffers of the inverter chain circuits (buffers X and Y in the inset of Fig. 5.53). To eliminate the effects of buffer X, we created a rectangle pulse using the exclusive-OR (ExOR) operator between the through path and the inverter chain path. To eliminate the effects of buffer Y, we prepared a zero-inverter chain path, shown as path (a) in Fig. 4.55. For example, for 50 inverters (gate-chain A), by subtracting the pulse width of path (a) from path (b), we obtain the delay fluctuations of gate-chain A alone.

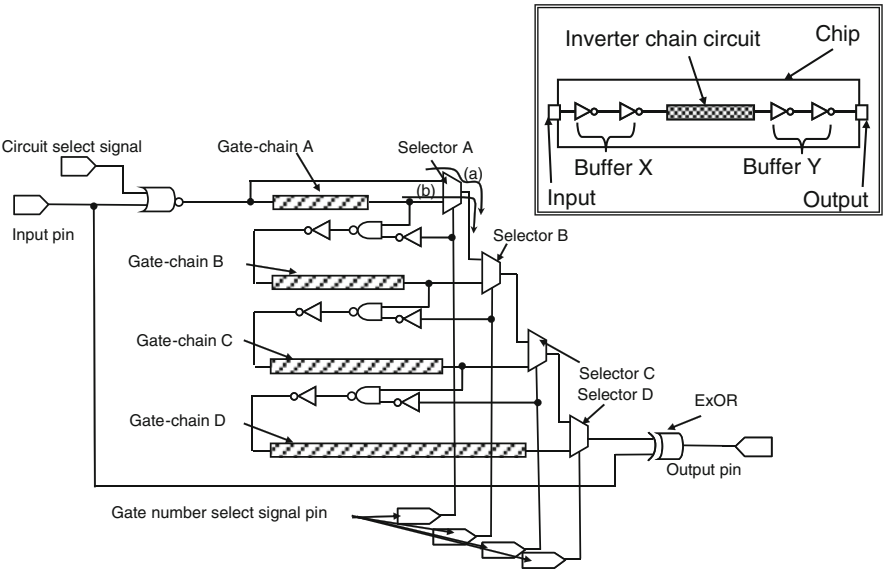


Fig. 4.55 Inverter chain circuit for on-chip voltage measurement (© IEEE)

As shown in Fig. 4.55, our circuit is a simple configuration capable of satisfying requirement (II), as discussed in the introduction. This circuit can be also as small ($320\,\mu m^2$) if only 50 inverters are used, permitting application for various types of LSI, including those used for consumer products such as for mobile phone, TVs, and other products.

We evaluated the voltage-delay convert coefficient of the test chip by measuring the output pulse width dependencies on applied DC voltage. The experimental result of the coefficient was about 1.6 ps/mV for the circuit with 50 inverters. Since the trigger jitter of the oscilloscope is 1.5 ps (rms), a voltage resolution of 1 mV can be expected.

Using the 50-inverter circuit, we measured on-chip noise waveforms when all noise source circuit switches operated simultaneously. The dashed line in Fig. 4.56 indicates the measured waveform using the inverter-chain circuit. In this figure, a dumping waveform is clearly visible. This measured waveform is in a very good agreement with the simulated waveform.

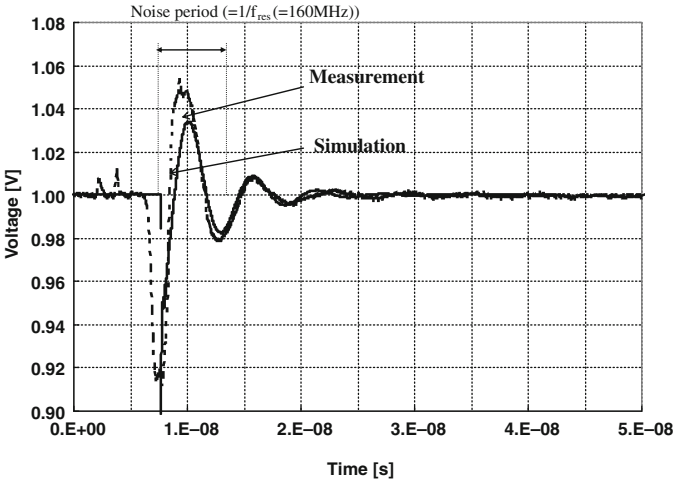


Fig. 4.56 Comparison of measurement (dashed) and simulation (solid) results (© IEEE)

4.6.2 On-Chip Power Supply Impedance Measurement

Here we introduce two types of measurement circuits for on-chip power supply impedance, IFDIM and impulse response method.

4.6.2.1 Integrated Power Supply Frequency Domain Impedance Meter (IFDIM)

Integrated power supply frequency domain impedance meter (IFDIM) is a unique measurement method of on-chip power supply impedance utilizing rectangular current waveform. Figure 4.57 illustrates a concept of IFDIM [25]. For this

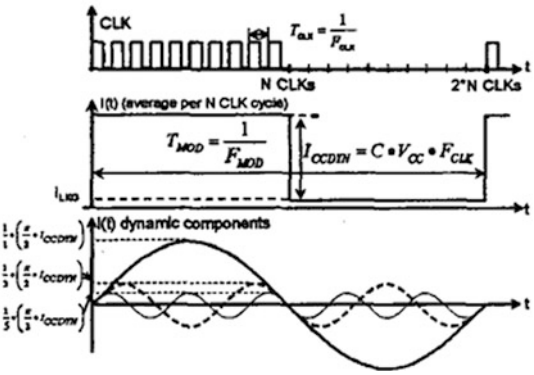


Fig. 4.57 The concept of IFDIM measurement (© IEEE)

measurement, the current waveform of the LSI is controlled to be a rectangular shape with certain cycle time, T_{MOD}. The rectangular current waveform is generated by a clock (CLK) activation which has cycle time, T_{CLK}, much smaller than T_{MOD}. The amplitude of the rectangular current is calculated by a multiple of load capacitance, C, and supply voltage, V_{CC}, and the clock frequency, F_{CLK}. In the case of rectangular waveform, the main spectrum consists of odd number of the base frequency. Especially, first, third, and fifth spectra of the base frequency can reproduce almost original waveform. By measuring the voltage waveform near the chip (as shown in Fig. 4.58) and the current waveform which is of a rectangle shape with cycle time, T_{MOD}, the on-chip impedance plot of $1/T_{MOD}$, $3/T_{MOD}$, and $5/T_{MOD}$ is obtained by a calculation of $V(f)/I(f)$ using FFT. By changing T_{MOD} using special operation set of processor, the impedance profile at wide frequency range can be obtained as shown in Figure 4.59. The plotted measurement data has almost same profile shape with the power SI simulation result.

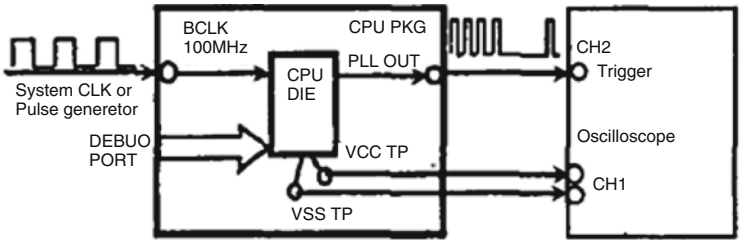


Fig. 4.58 IFDIM measurement setup (© IEEE)

4.6.2.2 Impulse Response Method

Circuit response to both an input and an initial condition is called the complete response and consists of zero-input response (ZIR) and zero-state response (ZSR)

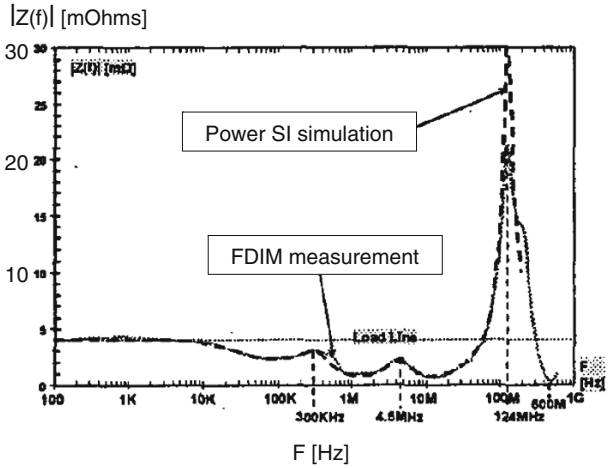


Fig. 4.59 Correlation between IFDIM measurement and power SI simulation (© IEEE)

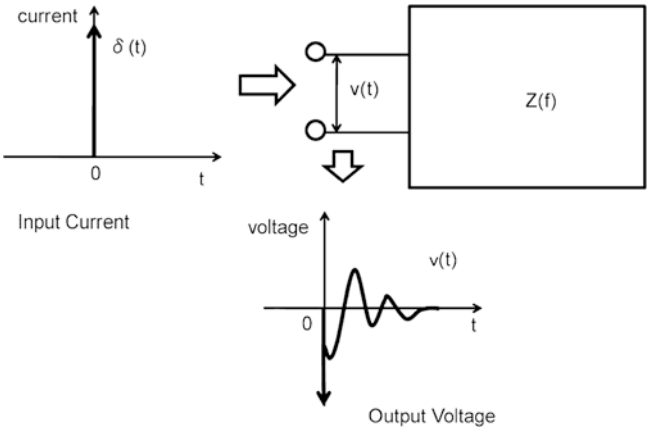


Fig. 4.60 Concept of impulse response method (© IEEE)

[26]. Since ZSR depends simply on initial conditions and circuit properties, measuring ZSR is an excellent way to characterize a black box circuit. ZSR measurements can be performed by applying an impulse to the circuit as shown in Fig. 4.60. Since the impulse response waveform expresses the transfer function of the black box circuit, we can determine the equivalent circuit from the shape of the response. There are several ways to obtain the equivalent circuit from the impulse response. If we know the form of the equivalent circuit of the target, we can determine the values of the electrical circuit parameters by solving the circuit equation. An example of this method is discussed in Section 4.5.3.

For modeling of chip-package resonance of the test chip, we have measured the impulse response waveform using on-chip measurement circuit, inverter chain circuit, described in Section 4.6.1.3. The impulse current is produced by numerous parallel switching inverter circuits. Figure 4.61 shows the measured voltage waveform using our test chip. The voltage waveforms are offset over the DC level. As we can see from this figure, clear damping waveform was observed. To express this waveform we assume the equivalent circuit of a parallel RL–RC circuit as shown in the inset of Fig. 4.61. We compared the voltage waveform obtained by experiment to simulated data from the equivalent circuit consisting of parallel RL–RC circuits having the electrical parameters obtained from impulse response. The current source model of this simulation circuit expresses the current waveform of the test chip. Experimental and simulation results are in very good agreement.

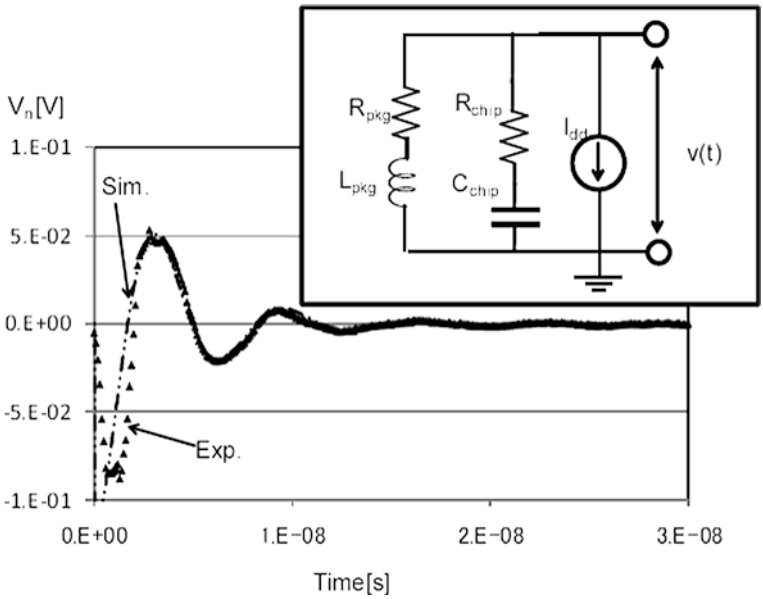


Fig. 4.61 Comparison of voltage waveforms between experiment (Exp.) and simulation (Sim.) (© IEEE)

4.7 Summary

In this chapter, trends in power integrity (PI) design are reviewed and the problems are discussed. As we described here, there are several conditions that make PI design more difficult. For a design methodology, frequency domain target impedance meter (FDTIM) is well used in recent design. However, we still have technical challenges for setting reasonable target impedance as discussed in Section 4.3.2.3. Several methods for measuring on-chip PI performance (noise voltage waveforms and impedance) are also introduced.

References

1. M. Popovich, A.V. Mezhiba, and E.G. Friedman, "Power Distribution Networks with On-Chip Decoupling Capacitors," Springer (2008).
2. S.H. Hall, and H.L. Heck, "Advanced Signal Integrity for High-Speed Digital Designs," WILEY (2009).
3. E.G. Friedman, "Clock Distribution Design in VLSI Circuits—An Overview," *ISCAS 1993, Chicago, Illinois, USA*, Vol. 3, pp. 1475–1478 (1993).
4. J.P. Eckhardt, and K.A. Jenkins, "PLL Phase Error and Power Supply Noise [microprocessors]," *Electrical Performance of Electronic Packaging, 1998, West Point, NY, USA*, pp. 73–76 (1998).
5. M. Saint-Laurent, and M. Swaminathan, "Impact of Power-Supply Noise on Timing in High-Frequency Microprocessors," *Electrical Performance of Electronic Packaging, 2002, Monterey, CA, USA*, pp. 261–264 (2002).
6. International Technology Roadmap for Semiconductors, 2001 Edition, Semiconductor Industry Association, http://public.itrs.net (2001), accessed on Oct 1, 2006.
7. R. Islam, A. Sabbavarapu, and R. Patel, "Power reduction schemes in next generation Intel(R) ATOM(TM) processor based sOc for handheld applications," *Proc. of VLSIC 2010, Honolulu, Hawaii, USA*, pp.173–174 (2010).
8. "Intel and Core i7 (Nehalem) Dynamic Power Management", http://cs466.andersonje.com/public/pm.pdf, accessed on Oct 11, 2010.
9. T. Lin, K.-S. Chong, B.-H. Gwee, and J.S. Chang, "Fine-grained power gating for leakage and short-circuit power reduction by using asynchronous-logic," *ISCAS 2009, Taipei, Taiwan*, pp. 3162–3165 (2009).
10. Data Sheet of 1 GB DDR3 SDRAM, E1494E60 (Version 6.0), Elpida, December 2009 (K) Japan (2009).
11. L. Smith, "Frequency Domain Target Impedance Method for Bypass Capacitor Selection for Power Distribution Systems," *DesignCon 2006*, *Santa Clara, California, USA*, http://si-list.net/files/designcon_2006/DC06_PDN-design_panel-slides.pdf, accessed on Oct 10, 2010 (2006).
12. I. Novak, L.M. Noujeim, V. St Cyr, N. Biunno, A. Patel, G. Korony, and A. Ritter, "Distributed Matched Bypassing for Board-Level Power Distribution Networks," *IEEE Trans. Adv. Packaging,* Vol. 25 , No. 2, pp. 230–243 (2002).
13. R. Schmitt, H. Xuejue, Y. Ling, and Y. Xingchao, "Modeling and Hardware Correlation of Power Distribution Networks for Multi-gigabit Designs," *Proceedings of 54th Electronic Components and Technology Conference, 2004.* Vol. 2, pp. 1759–1765 (2004).
14. R. Schmitt, L. Hai, C. Madden, and Y. Chuck, "Investigating the Impact of Supply Noise on the Jitter in Gigabit I/O Interfaces," *Electrical Performance of Electronic Packaging, 2007, Atlanta, Georgia, USA*, pp. 189–192 (2007).
15. R. Schmitt, K. Joong-Ho, and Y. Chuck, "Frequency-Domain Figures-of-Merit for the Design of Interface Supply Networks," *IEEE International Symposium on Electromagnetic Compatibility 2006*, Vol. 2, pp. 383–388 (2006).
16. R. Schmitt, K. Joong-Ho, D. Oh, and C. Yuan, "Power Delivery Design for 800 MHz DDR2 Memory Systems in Low-Cost Wire-Bond Packages," *Proceedings of Electronic Components and Technology Conference, 2006, San Diego, CA, USA*, (2006).
17. Y. Uematsu, H. Osaka, Y. Nishio, and S. Hatano, "A Method for Measuring V_{ref} Noise Tolerance of DDR2-SDRAM on Test Board Simulating Actual Memory Module," *Electrical Performance of Electronic Packaging, 2007, Atlanta, Georgia, USA*, pp. 11–14 (2007).
18. W.J. Dally, and J.W. Poulton, "Digital Systems Engineering," Cambridge (1998).
19. I. Novak, S. Pannala, and J.R. Miller, "Overview of Some Options to Create Low-Q Controlled-ESR Bypass Capacitors," *IEEE 13th Topical Meeting on Electrical Performance of Electronic Packaging, 2004, Portland, Oregon, USA*, pp. 55–58 (2004).
20. I. Novak, "Power Distribution Network Design Methodologies," *International Engineering Consortium* (2008).

21. W. Kim, and P. Harper, "Estimation of Simultaneous Switching Noise from the Power Distribution Network Impedance in LPDDR2 Systems," *DesignCon 2010, Santa Clara, California, USA*, http://www.designcon.com/2010/DCPDFs/10-TA1_Woopoung_Kim.pdf, accessed on Oct 10, 2010 (2010).
22. K. Inagaki, D.D. Antono, M. Takamiya, S. Kumashiro, and T. Sakurai, "A 1-ps Resolution On-Chip Sampling Oscilloscope with 64:1 Tunable Sampling Range Based on Ramp Waveform Division Scheme," *Digest of Technical Papers of 2006 Symposium on VLSI Circuits 2006, Honolulu, Hawaii, USA*, pp. 61–62 (2006).
23. Y. Kanno, Y. Kondoh, T. Irita, K. Hirose, R. Mori, Y. Yasu, S. Komatsu, and H. Mizuno, "In-Situ Measurement of Supply-Noise Maps With Millivolt Accuracy and Nanosecond-Order Time Resolution," *IEEE J. Solid-State Circuits*, Vol. 42, No. 4, pp. 784–789 (2007).
24. Y. Uematsu, H. Osaka, E. Suzuki, M. Yagyu, and T. Saito, "Measurement Techniques for On-Chip Power Supply Noise Waveforms Based on Fluctuated Sampling Delays in Inverter Chain Circuits," *Proceedings of Electrical Performance of Electronic Packaging 2008, San Jose, California, USA*, pp. 69–72 (2008).
25. A. Waizman, M. Livshitz, and M. Sotman, "Integrated Power Supply Frequency Domain Impedance Meter (IFDIM)," *Proceedings of IEEE 13th Topical Meeting on Electrical Performance of Electronic Packaging, Portland, Oregon, USA*, pp. 217–220 (2004).
26. Y. Uematsu, H. Osaka, M. Yagyu, and T. Saito, "Modeling of Chip-Package Resonance in Power Distribution Networks by an Impulse Response," *Proceedings of IEEE 14th Workshop on Signal Propagation on Interconnects (SPI) 2010, Hildesheim, Germany*, pp. 15–18 (2010).

Chapter 5
Fault-Tolerant System Technology

5.1 Introduction

Dependability of electronic systems is indispensable for our contemporary society and used for a range of application fields as shown in Table 5.1. Transportation systems, such as aerospace, automotive, train, elevator, are life-critical applications and require dependability from old days. The signal system in use at the time of the rail-road commencement was simple, just hanging a ball with a rope by a pulley. If the rope is broken, the ball falls by the gravitation of the Earth. This is the first inherent fail-safe system with asymmetric failure feature utilizing gravitation of the Earth. As the time passed by, the signaling system came to be implemented by electricity (relays) and electronics (solid-state devices), and then computerized and became the current form, succeeding to the fail-safe characteristics by asymmetric failure feature. Here, the signaling system includes railway switches, blockade, and interlocking systems in addition to traffic lights. It is still new in our memory that the computer systems for spaceship Apollo played a very important role in order to bring human being to the moon for the first time in history.

Table 5.1 Necessity for Dependability

-Transportation systems
(aerospace, automotive, train, elevator, etc.)
-Infrastructure
(bank, stock exchange, electric power)
-Production systems
(steel manufacturing, chemical manufacturing)

Infrastructure systems such as bank, stock exchange, electric power also require dependability to ensure social stability. Computer systems play a very important role in contemporary society, especially in financial system. Therefore, failure of a computer system may cause very serious problem like Black Monday. Furthermore,

Nobuyasu Kanekawa

N. Kanekawa et al., *Dependability in Electronic Systems*,
DOI 10.1007/978-1-4419-6715-2_5, © Springer Science+Business Media, LLC 2011

dependability on 24 h, 365 days availability of video-on-demand systems, database systems, and search engines is required for convenience.

Production systems, such as steel manufacturing and chemical industry, require dependability because failure in computer system directly causes loss of production and profit. Each application requires different aspect of dependability to the system, and employs different techniques to attain dependability.

First of all, this chapter discusses metrics for dependability in Section 5.2 and explains with an example of paradox caused by misunderstanding on tricky aspect of the metrics in Section 5.3. Also, this chapter surveys fault-tolerant techniques in Section 5.4, summarizes technical issues on fault tolerance in Section 5.5, and introduces author's industrial approaches in Sections 5.6, 5.7, 5.8, 5.9, 5.10, 5.11, and 5.12. Section 5.6 introduces overview of the author's approach to realize dependability, and Sections 5.7, 5.8, and 5.9 describe complementary approaches, misdetection tolerant data selection scheme, stepwise negotiating voting (SNV), and self-checking technologies to improve fault-detection coverage. Furthermore, Section 5.8 describes redundancy management for balanced graceful degradation, as an extension of SNV.

Section 5.10 introduces an approach of on-chip redundancy that implements self-checking technologies stated in Section 5.9 within a single large-scale integrated (LSI) circuit chip. Section 5.11 introduces fault-tolerance techniques employed by commercial fault-tolerant computer as examples of techniques to realize high performance and transparency, in addition to dependability. Finally, Section 5.12 introduces X-by-Wire as a current application field and prospects of cost reduction by scale merit of mass production with LSI technology.

5.2 Metrics for Dependability

First of all, let us summarize metrics and related topics for dependability here, to comprehend a variety of dependability aspects required by a wide variety of applications.

5.2.1 Reliability

Reliability is defined as the probability that the item performs its required functions under stated conditions for a specified period of time. Reliability is a widely used metric for systems without repair.

If the item is a single (non-redundant) system, the reliability R is represented as

$$R(t) = \exp(-\lambda t) \tag{5.1}$$

where λ: failure rate of the item and t: period of time.

Here, fit (failure unit 10^{-9} [h^{-1}]) is widely used as a unit of failure rate λ in order to adjust numeric value into practically convenient range because the value of λ is generally extremely small. For example, it is widely said that λ of LSIs is estimated

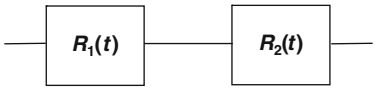


Fig. 5.1 Series system

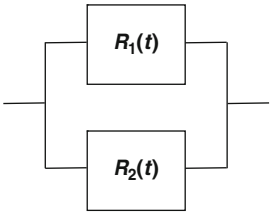


Fig. 5.2 Parallel system

in a range from 50 to several hundred [fits]. The data of failure rate λ are generally estimated based on MIL-HDBK-217, IEC62380, and various field data.

The reliability of more complex systems such as redundant systems without repair is explained by combinational model. For example, the reliability of series system as shown in Fig. 5.1 is derived from probability of the event that both the subsystems are normal; therefore, it is expressed as

$$R(t) = R_1(t) \times R_2(t) \tag{5.2}$$

And the reliability of parallel systems as shown in Fig. 5.2 is probability of the event that both the subsystems are normal and one of the subsystems is normal and another is faulty; therefore, it is expressed as

$$\begin{aligned} R(t) =& R_1(t)R_2(t) + R_1(t)(1 - R_2(t)) + R_2(t)(1 - R_1(t)) \\ =& R_1(t) + R_2(t) - R_1(t)R_2(t) \end{aligned} \tag{5.3}$$

5.2.2 Availability

Availability is defined as the ratio of time the item operates normally to its entire mission time. Availability is a widely used metric for systems with repair.

If the item is a simple system and mean-time between failures (MTBF) and mean-time to repair or mean-time to restoration (MTTR) are known, the availability A is expressed as

$$A = \mathrm{MTBF}/(\mathrm{MTBF} + \mathrm{MTTR}) \tag{5.4}$$

By the way, some specialists and textbooks define MTBF as one which includes mean-time to repair (MTTR) or

$$\mathrm{MTBF} = \mathrm{MTTF} + \mathrm{MTTR} \tag{5.5}$$

where MTTF: mean-time to failure.

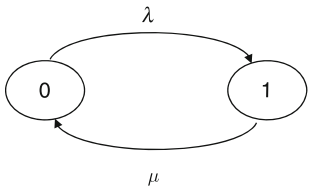


Fig. 5.3 Markov model

According to this definition, the availability A is expressed as

$$A = \mathrm{MTTF}/\mathrm{MTBF} \tag{5.6}$$

Here, note that it is generally said that MTBF is used for systems with repair and MTTF is used for systems without repair. More generally, A is expressed as

$$A = \mathrm{UT}/(\mathrm{UT} + \mathrm{DT}) \tag{5.7}$$

where UT: up time and DT: down time.

As for more complex systems with repair, the reliability is expressed by Markov model. For example, the system which has normal state 0 and faulty state 1 and which is transiting between these states in failure rate λ and repair rate μ is represented in Fig. 5.3. Here, we illustrated with a relatively simple example for easier explanation, but in reality, actual systems will be more complex.

Let the probabilities that the system is in the state 0 and 1 are $P_0(t)$ and $P_1(t)$, respectively, then we obtain the following differential equations

$$\begin{aligned} P_0{}'(t) &= -\lambda P_0(t) + \mu P_1(t) \\ P_1{}'(t) &= \lambda P_0(t) - \mu P_1(t) \\ P_0(t) + P_1(t) &= 1 \end{aligned} \tag{5.8}$$

Solving them with initial conditions, $P_0(t) = 1$, $(t) = 0$, we obtain

$$P_0(t) = \{\lambda + \mu \exp[-(\lambda + \mu)t]\}/(\lambda + \mu) \tag{5.9}$$

Here, $P_0(t)$ stands for the availability at time t or instantaneous availability. Let $\mu = 0$, $P_0(t)$ is equal to the reliability, which is a dependability metric for systems without repair.

In addition, let $t \to \infty$, the differential equations become ordinary simultaneous equations; we obtain stationary solution without solving differential equations as

$$P_0(\infty) = \mu/(\lambda + \mu) \tag{5.10}$$

$P_0(\infty)$ is terminal value of instantaneous availability and called steady-state availability.

Table 5.2 SIL (Safety Integrity Level): Low demand mode of operation

Safety integrity level (SIL)	Average probability of a dangerous failure on demand of the safety function
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{3}$
4	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Table 5.3 SIL (Safety Integrity Level): High demand mode of operation or continuous mode of operation

Safety integrity level (SIL)	Average frequency of a dangerous failure of the safety function [h^{-1}]
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
4	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

5.2.3 Safety

Safety is defined by safety integrity level (SIL) based on probability or frequency of a dangerous failure as shown in Tables 5.2 and 5.3 in the international functional safety standard IEC 61508 "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems." Required SIL is to be determined based on criticality of the application. For ultimate safety layer, the probability of a dangerous failure is basically represented by

$$(1 - R)^*(1 - C) \tag{5.11}$$

or more precisely

$$\sum_i \text{Prob}(f_i)(1 - C_i) \tag{5.12}$$

otherwise, the frequency of a dangerous failure is represented by

$$(1 - A)^*(1 - C) \tag{5.13}$$

where R: reliability, f: fault, i: index of faults, A: availability, and C: coverage.

It is necessary to improve the coverage besides the reliability or availability for safety improvement.

Functional safety is a concept supplement for a concept of inherent safety. The inherent safety originally means safety that an item is endowed by nature or definite safety in the field of human health and safety at work. The functional safety means

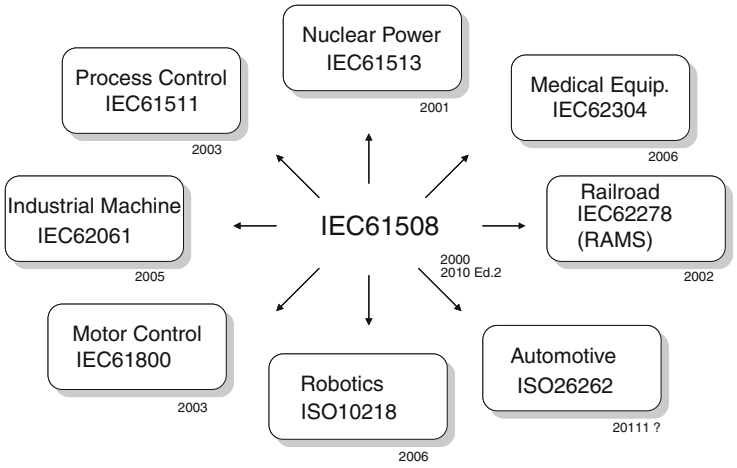


Fig. 5.4 Functional safety standards

an approach to reduce risk artificially or to eliminate risks except tolerable risks based on as low as reasonably practicable (ALARP) principle.

After the establishment of IEC 61508 in 2000, functional safety standards in various fields are established derived by the IEC 61508 as shown in Fig. 5.4, and the IEC 61508 was revised to IEC 61508 Edition 2 in 2010.

5.3 Reliability Paradox

It is generally said that majority voting (TMR: triple modular redundancy systems, more generally NMR: N-tuple modular redundancy) systems sound more reliable than stand-by redundancy systems. Also, the TMR systems are widely used for life-critical applications. But reliability of the stand-by redundancy systems is supposed to be higher than the TMR systems, on the numerical formula as follows, at a glance.

R_s, the reliability of stand-by redundancy system with two redundant subsystems is generally expressed as

$$\begin{aligned} R_s &= R_1^2 + 2R_1(1 - R_1) \\ &= 2R_1 - R_1^2 \end{aligned} \tag{5.14}$$

where R_1: reliability of redundant subsystems.

Besides, R_{TMR} the reliability of TMR systems is expressed as

$$\begin{aligned} R_{TMR} &= R_1^3 + 3R_1^2(1 - R_1), \\ &= R_1^3 + 3R_1^2 - 3R_1^3 \\ &= 3R_1^2 - 2R_1^3 \end{aligned} \tag{5.15}$$

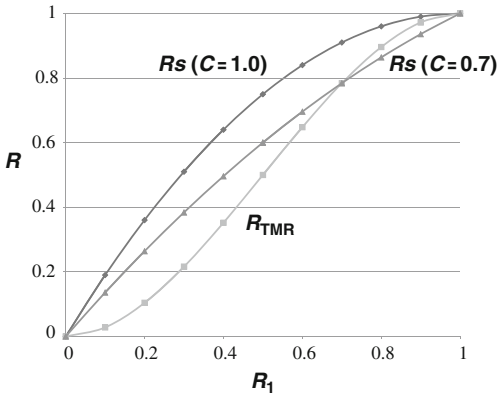


Fig. 5.5 Reliability comparison

Figure 5.5 depicts reliability comparison between stand-by redundancy system and TMR systems based on the Eqs. (5.14) and (5.15). Figure 5.5 also shows that the reliability of the stand-by redundancy system R_s is higher that the reliability of the TMR system R_{TMR} for all R_1.

But the expression above is based on assumption that fault-detection coverage is 100%. Let the coverage C, we denote

$$R_s = R_1^2 + 2CR_1(1 - R_1) \tag{5.16}$$

Therefore, R_s greatly depends upon C, and R_s becomes higher than R_{TMR} if the C is smaller. So fault-detection coverage is definitely important to realize ultimate safety. Also, the TMR systems have higher fault-detection coverage with the feature of data comparison by nature, and higher reliability especially for shorter t. Therefore, the TMR systems are widely used for ultimate safety systems for life-critical applications with relatively shorter mission time.

In addition to the reliability, the coverage C also has somewhat tricky aspect. The coverage C is defined as

$$C = [\#\,\text{of covered faults}]/[\#\,\text{of all faults}] \tag{5.17}$$

Here, note that, strictly speaking, [# of faults] should be weighted by probability of fault occurrences as

$$C = \sum_i \text{Prob}(f_i|\,\text{covered})/\sum_i \text{Prob}(f_i) \tag{5.18}$$

When we obtain the coverage by the fault injection, it will be simpler as

$$C = [\#\,\text{of covered faults}]/[\#\,\text{of injected faults}] \tag{5.19}$$

Correct Output is / Output	Available	Not Available
Execute	Normal Operation	*Error of Commission*
Stop	*Error of Omission*	Safe Shut-Down

Fig. 5.6 Error of commission and error of omission

But in reality, god knows the [# of all faults]; therefore, the coverage is practically defined as

$$C = [\#\,\text{of covered faults}]/[\#\,\text{of assumed faults}] \tag{5.20}$$

If we define a complete design as the design corresponding to all of the assumed faults, the coverage will be 100%. The most important thing here is not a value of coverage itself but the denominator, number or range of assumed faults. I think that you should interpret the value of coverage such as 60, 90, 99, . . ., as the representation of the number or range of assumed faults, for example, depending on whether it includes only stuck-at faults, or includes also other faults such as open, short, and parametric faults.

According to the author's opinion, there are two types of errors for dependable systems as shown in Fig. 5.6, error of omission and error of commission. The error of omission is an error to suspend output even if the correct output data is available. This error decreases system's reliability and availability. The error of commission is an error to continue output when the correct output data is not available and provide erroneous output as a result. This error degrades system's coverage or safety. Therefore, it is very important to reduce and balance probability or frequency of these types of errors for dependable systems.

5.4 Survey on Fault-Tolerant Systems

Fault tolerance is conventionally realized by redundancy in time domain and item or subsystem level. Recovery block, retry, essential recovery scheme, etc., are proposed as time redundancy. As for hardware-based redundancy, majority voting redundancy (TMR), stand-by redundancy, hybrid modular redundancy (HMR) [1], and self-purging redundancy [2] are proposed.

Stand-by redundancy selects output data of redundant subsystems based on diagnostic results as shown in Fig. 5.7. If the diagnostic function is not perfect, the system cannot select proper data as the system output and may cause the error of commission. Therefore, fault-detection coverage is essential for dependability of

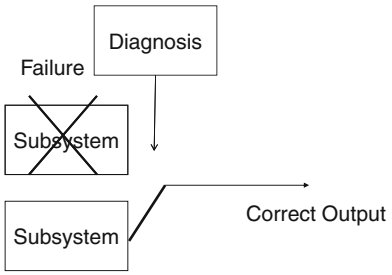


Fig. 5.7 Stand-by redundancy

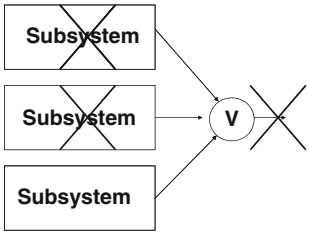


Fig. 5.8 Majority voting redundancy

stand-by redundancy. It is very difficult to detect transient faults perfectly because they should be detected by online checking. So, generally, the stand-by redundancy is good for multiple, permanent fault tolerance and reduces the errors of omission, but is not good for transient fault tolerance.

On the other hand, the majority voting redundancy has very high fault-detection coverage and reduces error of commission. The majority voting redundancy determines system's output among outputs from redundant subsystems by majority voting. But the majority voting redundancy cannot mask multiple faults as shown in Fig. 5.8 because the majority voting requires more than half redundant subsystem normal. Permanent fault may be accumulated and grows to multiple faults.

HMR combines features of the majority voting redundancy and the stand-by redundancy to enjoy their advantages and to compensate for their shortcomings. HMR is a method adding spare redundant subsystems to the majority redundancy to extend lifetime of the system as shown in Fig. 5.9. If fault occurred in any of the

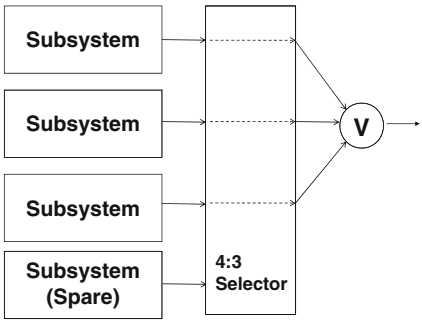


Fig. 5.9 HMR

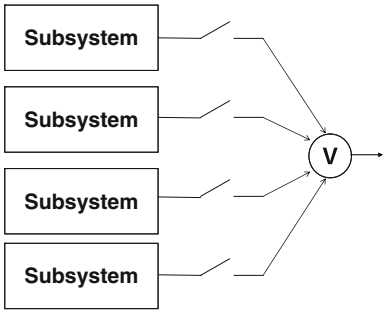


Fig. 5.10 Self-purging voting

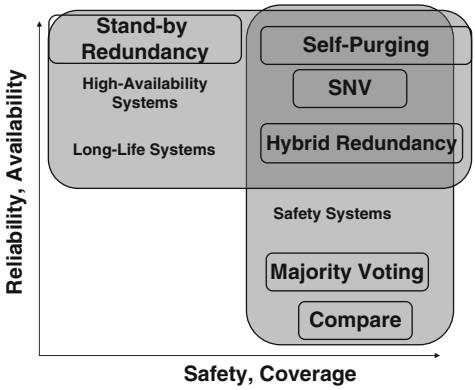


Fig. 5.11 Dependable system matrix

redundant subsystems participating in the majority voting, the faulty subsystem is replaced by the spare subsystem. The replacement compensate shortcoming of the majority voting redundancy, less good for multiple permanent fault tolerance.

In self-purging voting, only fault-free subsystems take part in the voting, and faulty subsystems are purged from voting as shown in Fig. 5.10. The number of subsystems that participate in the voting is flexible in this method, but constant in the HMR. Moreover, a voting mechanism for this method will be complex and has higher failure rate to realize the flexibility of voting participants number. So, the author proposed stepwise negotiating voting (SNV) [3] as stated in Section 5.8.

Figure 5.11 depicts mapping of dependable systems into matrix. The matrix has two axes, the vertical axis for reliability or availability and horizontal axis for safety or fault-detection and recovery coverage. In other words, the vertical axis stands for the index reflecting the probability, or ratio of normal operation, or how low the probability of error of omission is, whereas the horizontal axis stands for the index how low the probability or frequency of dangerous failure or error of commission is.

High-availability systems (systems with higher reliability or availability) and long-life systems generally employ stand-by redundancy as shown in the upper left

corner of the matrix. Most of high-availability-oriented OLTP employs the stand-by redundancy.

As for high availability systems, Tandem Computers Inc. started commercial production of tandem non-stop system (Tandem 16); the first commercial fault-tolerant system realized high availability and online repair and expansion in 1977 [4]. The tandem non-stop system has from at least 2, up to 16 processor modules. The processor modules are interconnected via Dynabus, and these modules are online replaceable during operation. Strarus Computer Inc. started production of STRATUS S/32 in 1982 [5]. The STRATUS S/32 has hardware-based fault-tolerance utilizing the latest LSI technologies, besides the tandem non-stop system has software-based fault-tolerance based on checkpointing techniques.

A typical well-known long-life system, STAR (self-testing and repairing), which was developed in the JPL (Jet Propulsion Laboratory) in the 1960s for planetary explorer mission, employs the stand-by redundancy [6]. The OLTP gains its availability by repair or maintenance, and the STAR gains its lifetime or reliability by massive spare modules.

Safety systems (system with higher safety or coverage) generally employ majority voting (TMR, more generally NMR) or dual and compare methods as shown in the lower right corner of the matrix. Software implemented fault tolerance (SIFT) [7] and fault-tolerant multi-processor (FTMP) [8] basically employ the majority voting. The voting is performed by data recipients among data provided by redundant subsystems which execute previous data processing via system bus, and the selection of participants through voting or by previous redundant subsystems is flexible because they are interconnected via system bus. Therefore, voting process is HMR-like behavior rather than the conventional voting, in both methods. But SIFT implements the voting function by software besides, the FTMP implements by hardware.

Moreover, systems with both reliability and safety employ combined approaches such as hybrid modular redundancy (HMR), self-purging voting, and stepwise negotiating voting (SNV), as shown in the upper right corner of the matrix. SIFT and FTMP have flexibility in choice of participants of voting process and have HMR-like features.

5.5 Technical Issues

Redundancy is widely used to realize fault detection and fault tolerance (fail-operative feature). Figure 5.12 depicts an example of redundant configuration for fault tolerance. The system has redundant subsystems, the primary and the secondary subsystems. The system operates with the primary subsystem if the system does not have failure. If failure occurs in the primary subsystem, the system selects output from the secondary subsystem and continues its operation. Basic principle of the fault-tolerant system is as stated above. Dependable systems are used for a wide range of applications and required a wide range of requirement such as high performance, transparency, and ultra dependability.

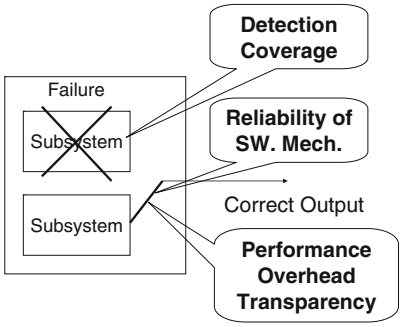


Fig. 5.12 Dependable system

5.5.1 High Performance

According to the Moore's Law, operation of microprocessor became faster and faster year by year. So fault-tolerant technology with higher performance is required to utilize state-of-the-art latest and fastest microprocessors. Fault-tolerance mechanisms cause performance overheads. Overhead for fault detection is unavoidable, and there is additional delay in switch mechanism. In addition, overhead for synchronization between redundant subsystems is also indispensable for seamless take-over between subsystems.

Methods of synchronization among redundant hardware are classified into two levels, message or task level and clock level.

Synchronization method in message or task level synchronizes the redundant hardware at each checkpoint as shown in Fig. 5.13. For online transaction processor (OLTP), the synchronization is necessary only at the start and the end of transaction. But for hard real-time controllers, overhead for synchronization at every control frame interval will be very tight bottleneck for speedup.

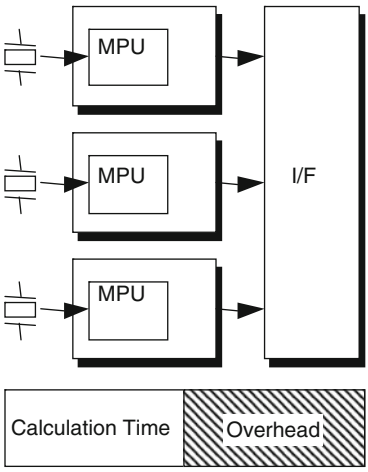


Fig. 5.13 Synchronization and overhead in task/message level

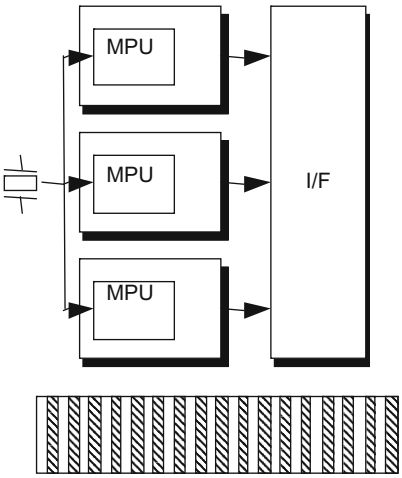


Fig. 5.14 Synchronization and overhead in clock level

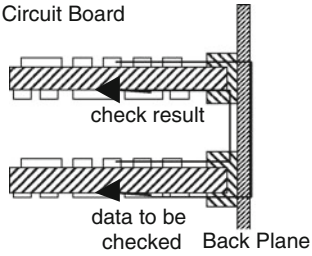


Fig. 5.15 Signal propagation delay

Synchronization method in clock level synchronizes the redundant subsystems at each clock cycle or bus cycle as shown in Fig. 5.14. Signal propagating delay on synchronization governs upper bound of operating clock frequency. Conventional commercial fault-tolerant computers implemented redundant subsystems into physically separated printed circuit boards in order to replace faulty subsystem easily on its failure. Therefore, the signal propagation delay was a major problem. As for clock distribution, the problem can be solved to some extent by design rule equal to length wiring, but the problem for signal exchange for inter-subsystem synchronization and data comparison cannot be solved. Assuming that the wire length between subsystems is 50 cm and that propagation delay is 7 ns/m, it takes 7 ns to arrive at the comparator for the data to be checked and again for the check result to return as shown in Fig. 5.15. Therefore, the overhead ratio by propagation delay in total delay becomes larger in higher clock frequency as shown in Fig. 5.16. Integration of redundancy such as intra-board or on-chip level will be a prospective approach to mitigate the redundant subsystem synchronization problem for higher clock frequency.

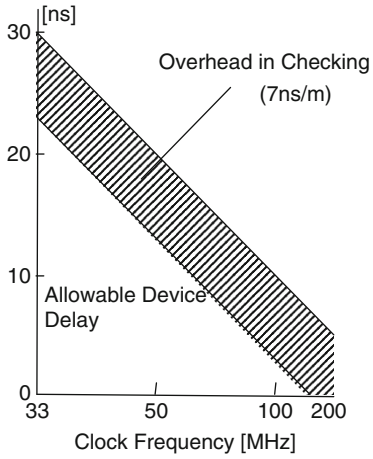


Fig. 5.16 Delay vs. frequency

5.5.2 Transparency

Dependable systems are used not only for control applications but also for information systems such as online transaction processors and database machines, and require globalization and standardization feature. So dependable systems with transparency, or with standard operating system and software developed without being conscious to fault tolerance, is necessary.

In the history of fault-tolerant computers, software-implemented fault tolerance (SIFT) and fault-tolerant multi-processor (FTMP) are developed. After the competition, the developing team of FTMP was employed for US Air Force standard fault-tolerant mini-computer systems. The major reason of choice was transparency of fault tolerance seen from software. Fault-tolerant systems based on hardware such as the FTMP has difficulty in performing complex output data selection control, but fault tolerance is transparent from software; in other words, the FTMP can use existing software and operating system. Transparency becomes more important with recent globalization and standardization of information systems.

By the way, fault-tolerant systems implemented by software can realize flexible and complex judgment and output data selection (voting) control without complex hardware. For example, confidence voting selects output data based on error correlation among software versions, while stepwise negotiating voting (SNV) selects output data based on estimated reliability of output data.

5.5.3 Physical Transparency

Dependability realization causes physical overhead to hardware such as dimension, weight, and power dissipation increase because of redundancy, and the dependability or durability realization requires special requirements for hardware, components,

and parts used for the system. Here, let us call the characteristics which do not need special physical requirements for dependability realization as physical transparency. The physical transparency or transparency seen from hardware for dependability is preferable, in addition to the (logical) transparency seen from software, as stated above.

An approach to use commercial off-the-shelf (COTS) components in space has been promoted recently, through Hiten (ISAS|Lunar Swing-by HITEN (MUSES-A)/Missions http://www.isas.jaxa.jp/e/enterp/missions/hiten.shtml], TSUBASA (Mission Demonstration Satellite-1 "TSUBASA" (MDS-1) http://www.jaxa.jp/projects/sat/mds1/index_e.html) and SERVIS (Space Environment Reliability Verification Integrated System) (PROJECT_SERVIS http://www.usef.or.jp/english/f3_project/servis/f3_servis.html) missions.

Details of the "Hiten" onboard computer are described in Section 5.8. As for an approach to utilize COTS component in space after the "Hiten" mission, the Mission Demonstration Test Satellite-1 (TSUBASA) of JAXA launched in 2002 and SERVIS 1 of USEF (Institute for Unmanned Space Experiment Free Flyer) launched in 2003 provided successful results in collecting field data of commercial off-the-shelf electronic devices. The results of these missions certified feasibility of approach to utilize COTS components to satellites. During writing this manuscript, SERVIS 2 was launched in June 2010.

The USEF released the COTS database mainly with irradiation test on ground. In addition, the USEF also released Equipment Design Guideline, the guideline to utilize COTS electronic devices such as microprocessor and memory (PROJECT_SERVIS http://www.usef.or.jp/english/f3_project/servis/f3_servis.html).

Cross-talk-tolerant self-checking techniques described in Section 5.9.1 relax design restriction in detailed wiring and routing to realize self-checking logics in LSI chips. Therefore, the detailed wiring and routing process will be automated and only rough floor plan should be manually done with designer's heuristics and knowledge.

On-chip redundancy which reduces dimensions and number of redundant components is also proposed to realize the physical transparency, utilizing the latest semiconductor integration technologies. Nowadays, safety microcontrollers which have internally duplicated cores became commercially available from most of major microprocessor manufacturers mainly for automotive applications [9–11]. Also, safety microcontroller which has single core with additional fault detection function is addressed [12]. Details of the on-chip redundancy are written in Section 5.10.

5.5.4 Fault Tolerance of Fault Tolerance for Ultimate Safety

Computer systems used for transportation, such as aerospace, automotive, train, elevator, require ultimate safety. These life-critical applications require fault-tolerance mechanism for fault-tolerance itself in addition to conventional techniques for fault-tolerance. Reliability of fault-tolerance mechanism greatly depends upon

fault-detection coverage and reliability of fault masking mechanism or switch mechanism.

The fault-detection coverage is an index to indicate how perfectly the system detects faults. The system can selects proper output from the secondary subsystem and can continue its operation when the failure occurs in the primary subsystem as shown in Fig. 5.12, only if the failure is detected. On the contrary, if failure is not detected when the primary subsystem is faulty, the system may continue to operate using erroneous output of the primary subsystem.

Self-checking logic is a very prospective approach to improve fault-detection coverage. Redundant codes [13–15] such as parity [16], two rail logic, and M-out-of-N code [17] are used to implement self-checking logic. There are two ways to realize self-checking logics:

(a) an approach to implement whole logic by ad hoc design using redundant codes, and
(b) an approach to duplicate functional blocks and compare their outputs.

The approach (a) requires to newly redesign all the circuits, and the approach (b) requires ad hoc design only in comparator for self-checking. In other words, the approach (b) can utilize existing design for functional block and make it self-checking with just duplication. Therefore, this approach can reduce development cost and time, and is well matched to state-of-the-art semiconductor technology. But fault-detection coverage in this approach greatly depends upon independence of fault occurrence or how to reduce common cause failures among duplicated functional block and coverage of comparator. The independence of fault occurrence or common cause failure reduction is a major issue.

The author developed self-checking comparator with cross-talk tolerance by orthogonal signals as stated in Section 5.9.1, and developed floor planning and the optimal time diversity with half or its odd multiple clock difference to reduce common cause failures as stated in Section 5.9.2. Recently, safety microprocessor with cores mirrored and rotated by 90° and with 1.5 cycle delay to reduce common cause failures are proposed (TMS570 floating-point MCUs http://ti.fleishman.de/electronica/) [18].

Reliability of the switch mechanism is also important in addition to the fault-detection coverage. The switch mechanism switches over output of the primary subsystem into the secondary subsystem incase of failure in the primary subsystem. If the switch mechanism fails, the system may not provide correct output from the primary subsystem due to absence of failure in the primary subsystem, nor from the secondary subsystem due to presence of failure in the primary subsystem.

FTMP employs duplicated Bus Guardian in bus interface of modules to protect system buses from erroneous bus access as shown in Fig. 5.17. The Bus Guardian shuts off the bus access in case of failure in the modules. And the bus access is also suppressed if any of the duplicated Bus Guardians is faulty. The concept of the Bus Guardian is also employed for time-triggered protocol (TTP) [19] and

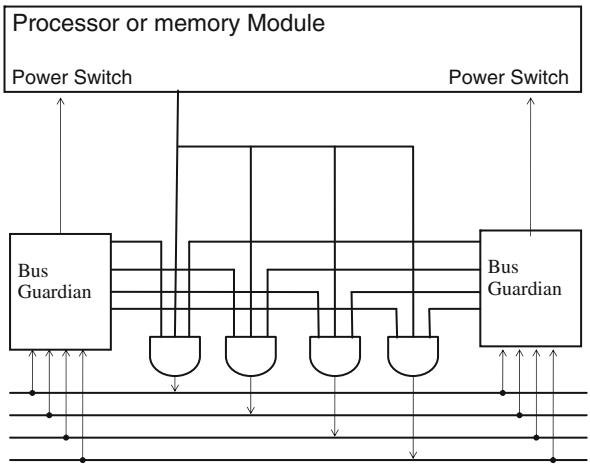
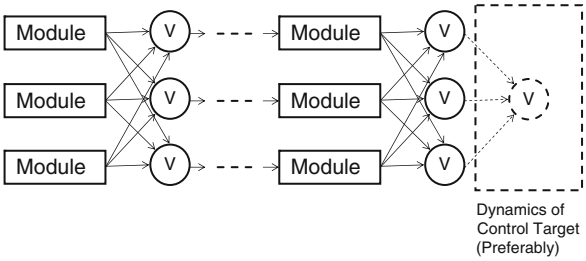


Fig. 5.17 Bus Guardian

Fig. 5.18 Cascade TMR



FlexRay (FlexRay Consortium http://www.flexray.com/) to allow nodes bus access in assigned time slot only and to ensure fail-silent behavior.

Final output stage, voter in case of majority redundancy (TMR) is a bottleneck of reliability of the whole system if the final output stage is single, not redundant. Cascade TMR, as shown in Fig. 5.18, is often used to solve the bottleneck problem. But the bottleneck problem in the final stage, an interface to real world, still remains in most of the cases. The problem can be solved if the final stage is realized by voting in dynamics of control target as shown in the figure.

Special fail-safe technique has been realized using asymmetrical failure devices in rail-road control field. The asymmetrical failure devices have asymmetric failure features, probability of the specific failure mode (hereinafter "probable failure mode") is higher than another failure mode (hereinafter "less-probable failure mode"). Preferably, reliability of the probable failure mode should be extremely higher than the less-probable failure mode. We can realize fail-safe systems if we assign an output signal pattern which the probable failure mode may cause to signal which stands for safety-side operation command and another output signal pattern, which the less-probable failure mode may cause to signal, and which stands for

non-safety-side operation command. For example, the safety-side operation command falls on brake command and the non-safety-side operation command falls on acceleration command. In case of the probable failure mode, the failure causes the safety-side operation command; therefore, the system's fail-safe state is secured. Unate circuits, relay logics, alternate logics, frequency logics, etc., are widely used as the asymmetrical failure devices to realize fail-safe system in rail-road control field.

5.5.5 Reliability of Software

Reliability of software is also essential technical issue for dependable systems. Although this book is focusing on hardware fault issues, let us survey software issues briefly here.

N-version programming [20, 21], recovery block scheme [22], and essential recovery scheme [23] are proposed to tolerate software design faults (bugs).

N-version programming is proposed to detect and mask errors caused by design faults (bugs) in software development. In this method, data processing is executed according to plural versions of software which are independently developed, and detect and mask the errors by voting or comparison among processing results, at the end of processing or checkpoints. This method can detect and masks most of transient faults, part of permanent hardware faults, in addition to software design faults. This method is based on the assumption that there are no fault correlations among independently developed software versions. But some reports [24] imply existence of fault correlation.

In the recovery block scheme, the system executes plural versions of software sequentially and verifies the processing result by acceptance test. If the first version passed the acceptance test, the system executes the next step of processing; otherwise the next version is executed sequentially until any of the prepared versions pass the acceptance test. Major differences of this method from the N-version programming are that processing is executed sequential in this method, but parallel in the N-version programming, and that result is verified by acceptance test in this method, but by data comparison or voting in the N-version programming. Therefore, coverage of the recovery block scheme greatly depends upon fault-detection coverage of the acceptance test.

In the essential recovery scheme, the system re-executes the same version of program with essential information which it took over from previous execution and which does not include cause of faults, in case of faults in the previous execution. This method is proposed based on difference between Bohr and Heisenberg Bug. The Bohr Bug is named after a famous physicist devised deterministic model, and the Heisenberg Bug is also named after a famous physicist devised probabilistic atomic model. The Bohr Bug means a bug which deterministically causes errors, while the Heisenberg Bug means a bug which probabilistically cause errors or depending upon conditions on execution. The Bohr Bug will appear tangibly and can be deleted perfectly during debug process. Therefore, the remaining bugs at the

time of shipment are the Heisenberg Bugs. If the system re-executes the processing under different conditions with essential data only, the error never recurs. The essential recovery scheme was employed SURE SYSTEM 2000.

Functional safety standard IEC61508 requires and recommends various techniques and measures for software design and development, for example, design diversity, automatic software code generation, structured methods, usage of certified tools and translators.

Reusability improvement is also a very prospective approach to reduce software design faults. Reusability improvement is generally granted as an issue on productivity improvement. Furthermore, if the software portion of newly developed is reduced, design faults caused by human factor will be reduced, and reliability of software will be improved.

Software framework and software product line [25] are proposed and practically used. Software framework is an approach to develop a new software product utilizing existing common software module assets having commonality adding ad hoc code for variability.

The software product line is a development methodology to build software assets, a set of software product line systematically through individual development based on analysis of commonality and variability. This approach is to challenge to develop codes for variability as software assets, which are developed as ad hoc code in the software framework.

5.6 Industrial Approach

Figure 5.19 shows the history of industrial approach to dependability by authors and their affiliation, Hitachi, Ltd. The starting point of the affiliation's dependability technology is in the railway and nuclear power generation field where absolute safety is demanded and it has been established by an original fail-safe and reliable technology.

Hitachi established an original concept of autonomous decentralized systems in the latter half of the 1970s [26–28], and applied it to a major ironworks in the beginning and it has been applied to a range of fields, including transporting systems, electric power systems, and industry systems in Japan. The autonomous decentralized systems and other technologies for dependability has been applied to computer-assisted traffic control system (ATOS: autonomous decentralized transport operation control system) [29], as shown in Fig. 5.20.

The application to consider reliability of the system especially in fields other than the railway and nuclear power started with the onboard computer loaded on "*Hiten*" launched in 1991, and was succeeded to the fault-tolerant computer HITAC FT-6100 and FT90/600, and embedded controllers and various servers that pursues high availability.

Authors concentrated to improve coverage to secure safety through a joint research concerning Fly-by-Wire with the avionics partners, in the middle of the 1990s. Coverage is a metric that shows how a reliable system can correspond to

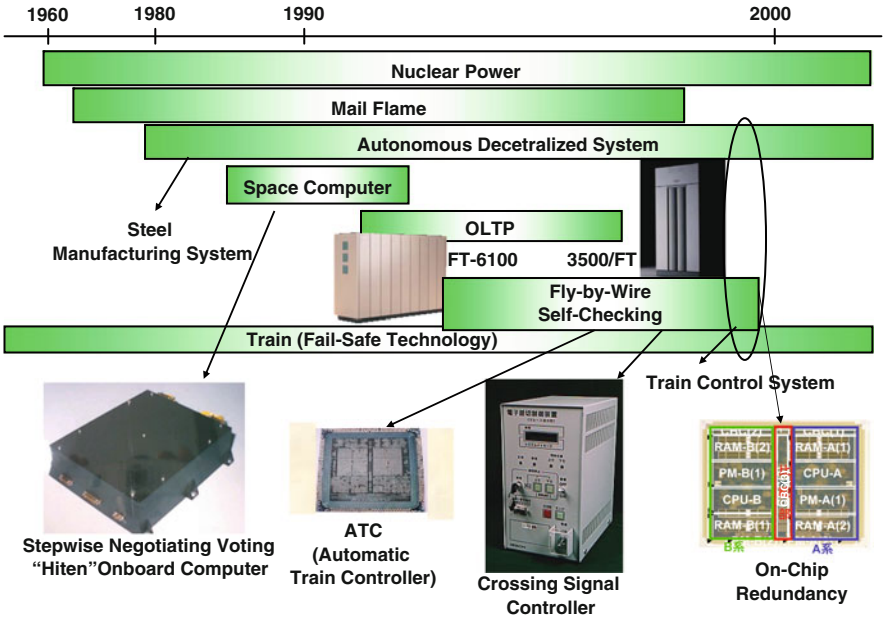


Fig. 5.19 Expertise in dependability

History

1977	Installed in Steel Manufacturing Factory
1993	Open Autonomous Decentralized System on Sale
1996	Disclose Open Network Spec.

Use Case

Field	Contents
Transportation Systems	Train Operation & Management, Road Management, X-by-Wire Systems
Electric Power System	Power Generation, Power Management, Nuclear Power Systems
Industry System	Automotive/Steel Manufacturing, Logistics/Newspaper Publishing,/Energy (Gas) Supply Management Systems
e.t.c.	Water Treatment System

Fig. 5.20 Autonomous decentralized system

failures. The reliability of "mechanism for high reliability" is required to realize ultimate reliability. The ultimate high-reliability technology thus established was applied to the railway control system such as electronic rail-road crossing controllers starting with LSI for automatic train protection (ATP). Although the concept

of coverage was not so general at that time, it is taken to functional safety standard IEC61508 and it became general now.

Such a technology leads to the development of the safety processor with on-chip redundancy that is combined with the synthesizable technology. Also, special requirements for on-chip redundancy are defined in IEC61508 Ed.2. Part2, Annex E and F in 2010.

5.6.1 Autonomous Decentralized Systems

Autonomous decentralization is the concept that the function of the node of the system was likened to the function of the cell of creature as shown in Fig. 5.21. The concept of autonomous decentralized system resembles to endocrine system rather than nervous system.

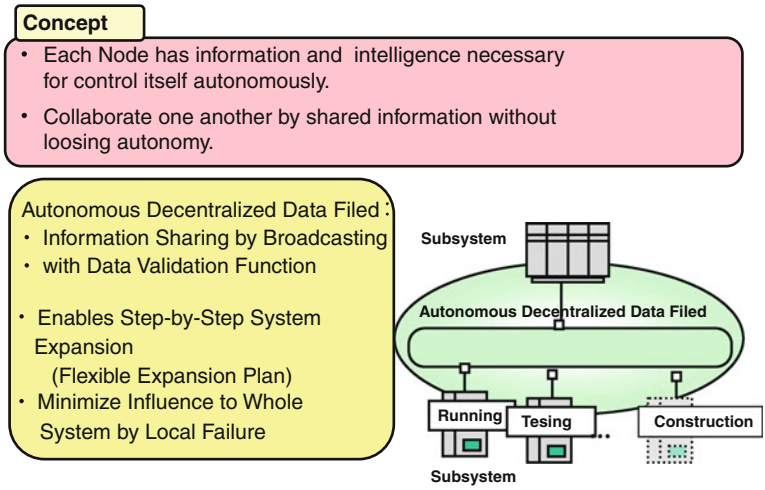


Fig. 5.21 Autonomous decentralized system

Autonomous decentralization is a technology that provides (1) necessary information and intelligent for each node to control itself, and (2) the function to cooperate each other by the information sharing without ruining autonomy. These nodes are connected by the autonomous distributed data field with information sharing function by the broadcast and the effectiveness verification function of information.

According to the above-mentioned organization, construction can be flexibly scheduled according to the possible investment plan, in the stepwise construction process of the subsystem. Moreover, the spread to a whole system due to local trouble can be minimized.

5.6.2 Space Application

Electronic equipment is exposed to severe environments such as temperatures and vibrations. Single-event upsets are mainly caused by the cosmic rays in space. Moreover, the repair is almost impossible after the launch. Therefore, dependability is definitely necessary for the electronic equipment used in space. It was a technical issue to improve reliability efficiently by using the limited tedious resource in this development.

The newly developed method, stepwise negotiating voting (SNV) [3] method enables to obtain higher reliability with the limited hardware. The method predicts the reliability of redundant subsystems based on check results, and selecting the output of the computer with the highest predicted reliability.

The onboard computer by this method was loaded on the satellite "Hiten" of the Institute of Space and Astronautical Science (ISAS, Currently Japan Aerospace Exploration Agency (JAXA) Space and Astronautical Science Research Headquarters) launched in 1991, and completed the duty continuing the normal performance for the period for three-and-a-half years [30].

The "Hiten" onboard computer was implemented using commercial off-the shelf (COTS) electronic devices to verify availability of them in space. If the approach is verified, utilization of COTS components will shorten development period and lower non-recurring and recurring costs and enables to improve performance using state-of-the-art LSI technology in space.

For details on the "Hiten" onboard computer, see Section 5.8.

5.6.3 Commercial Fault-Tolerant Systems

At the end of 1980s, specialized makers commercialized a no-stop-type computer in the USA [4, 5], and had a big success and the words "the fault-tolerant computer" became widely used, too. With the scale expansion and globalization of the computing system, 24 h, 365 days consecutive operation and also online expansion have been demanded in infrastructure fields such as the electricity in Japan.

In 1991, the authors developed triple processor check redundancy (TPR) architecture [31] to enable compact and fast system with consecutive operation and online expansion, and started a mass production as HITAC FT-6100 and HIDIC FT90/600. In this method, three processors are mounted with high density in a basic processing unit (BPU) board for miniaturization and high speed. The processors carry out the same processing and separate instantly if failure occurs to one of the processors and continue processing with the remaining two processors. With multiple BPU boards, the system enables to relocate the job of the failed BPU board to other BPU boards, and physically replaced a faulty BPU board by maintenance/exchange online.

In addition, the dependable technology cultivated here is succeeded to in HITAC 3500/FT and HIDIC RS90/FT which are fault-tolerant models of Hitachi creative server 3500 and HIDIC RS90/FT. For details on the TPR architecture, see Section 5.11.

5.6.4 Ultra-Safe System

The coverage is an index to show how perfect a dependable system can cope with failures as stated above. The ultimate dependable system which improved coverage applies to an electronic rail-road crossing control unit as shown in Fig. 5.22 and automatic train protection (ATP) – LSI.

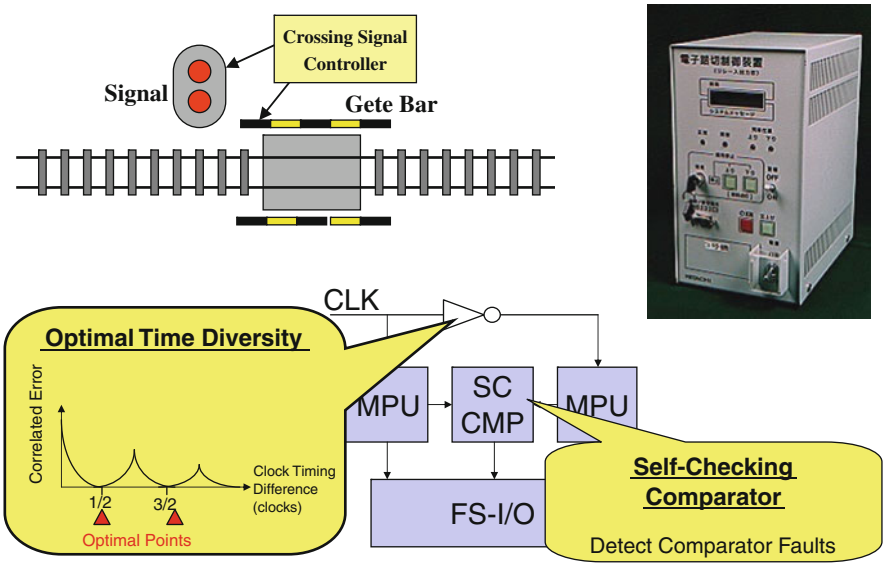


Fig. 5.22 Self-checking application

The electronic rail-road crossing control unit takes down a crossing gate surely and must operate a warning signal if you detect the approach of the train to the rail-road crossing till a train finishes passing by. When it broke down, it must take down a crossing gate for security and must operate a warning signal to maintain the fail-safe state. Therefore, it is demanded to detect failure surely. At first the authors make micro-processing unit (MPU) two folds as shown in Fig. 5.22. The system detects abnormality of MPU by comparing the output with a comparator. The fail-safe input/output (I/O) receives the comparator output and realize fail-safe state. Because the system cannot detect faults of MPU when a comparator broke down by any chance, the authors employ the self-checking comparator which can detect faults of comparator itself [32].

Furthermore, the authors propose to keep a difference in the operation timing of two folds of processors of the odd multiple of the half-clock to prevent the same errors in processors and to improve fault-detection coverage. For details on fault-detection coverage improvement, see Section 5.9.

5.7 Availability Improvement vs. Coverage Improvement

It is very challenging to improve both reliability or availability and coverage of the system to realize dependable systems mapped in the upper right corner of the matrix in Fig. 5.11. If one feature is improved, it becomes more difficult to improve another feature. To say more specifically, if we improve reliability by reducing error of omission, it becomes more difficult to improve coverage or safety by reducing error of commission [33]. The stand-by redundancy is good for multiple, permanent fault tolerance and reduces the errors of omission, but is less good for transient fault tolerance. On the other hand, the majority voting redundancy has very high fault-detection coverage and reduces error of commission. But the majority voting redundancy cannot mask multiple faults.

The authors made complementary approaches to realize both availability and coverage improvement. The authors proposed data selection scheme based on estimated reliability of data processing, SNV method, which tolerates imperfect detection coverage. This approach enables trade-off between error of commission reduction and error of omission reduction. Furthermore, the SNV can be extended to redundancy management for balanced graceful degradation. Also, the authors proposed self-checking comparator and optimal time diversity to improve fault-detection coverage. This approach reduces ambiguity on fault detection and reduces both error of commission and error of omission.

5.8 Trade-Off Between Availability and Coverage – Stepwise Negotiating Voting

5.8.1 Basic Concept

The authors proposed a new voting scheme, stepwise negotiating voting (SNV) [3]. In this method, output data are selected based on estimated reliability R_d of redundant subsystems. Data from a subsystem with the highest estimated reliability is selected as the output of the system. The reliability R_d, or probability of fault-free operation in each redundant subsystem, is estimated based on the probability of misdetection, as shown in Fig. 5.23, assuming that the system has only two checking functions, Check 1 (self-diagnosis) and Check 2 (data compare) for easier explanation. In reality, system has a combination of plural checking functions for higher detection coverage. In Fig. 5.23, P_e is the probability of fault occurrence, P_{de} is the probability of misdetection by Check 1 (self-diagnosis), and P_{ae} is the probability of misdetection by Check 2 (data compare). P_{de} generally ranges from 0.9 to 0.99 and P_{ae} is almost 1.0. Therefore, the order of R_d, the reliability of the subsystem, can be represented by Fig. 5.24. The data granted as good by Check 1 (self-diagnosis) and agreed with other data in Check 2 (data compare) have the highest reliability, and the data not granted as good by Check 1 (self-diagnosis) and agreed with other data in Check 2 (data compare) have the second highest reliability, and the data not

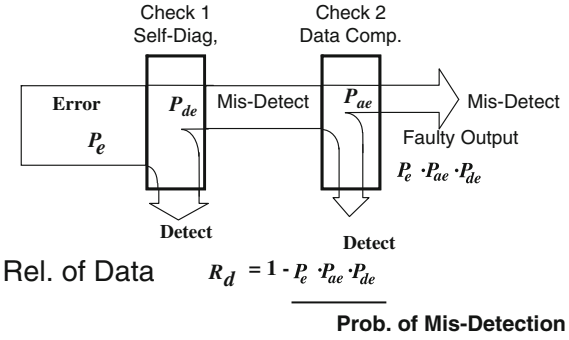


Fig. 5.23 Mechanism of misdetection

Self Diag.	Data Comp.	R_d
Good	Agree	$1 - P_e \cdot P_{ae} \cdot P_{de}$
Faulty	Agree	$1 - P_e \cdot P_{de}$
Good	Disagree	$1 - P_e \cdot P_{ae}$
Faulty	Disagree	———

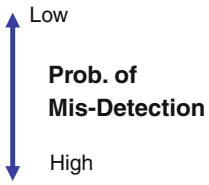


Fig. 5.24 Order of R_d

granted as good by Check 1 (self-diagnosis) and did not agree with other data in Check 2 (data compare) have the third highest reliability.

Figure 5.25 depicts system configuration for the SNV. Data processing is performed by each redundant subsystem. The redundant subsystems are called "cells" in analogy to living creatures according to the concept of autonomous decentralized system. Redundant subsystems have immunity rejecting harmful influences from other faulty subsystems or harmful communication accesses such as excessive communication request and illegal data transfer via inter-cell communication channels. The result of data processing and result of self-checking in each cell are exchanged among cells via the inter-cell communication channels. The exchanged data processing results are used for the Check 1 (data compare), and the reliability of data processing is estimated based on the results of checking and determined the data to be selected as the system output by judge function. The proper output data are preliminarily selected by select function of subsystems. During the final stage, modified voter (MV) selects final output from pre-selected output data from subsystems based on status which shows data to be selected. The MV consists of a switch matrix and a conventional voter as shown in Fig. 5.26. Figure 5.27 depicts an example of switch logic table for the switch matrix. Combination of the preliminary data selection by subsystems and the final MV enables complex data selection with less complex hardware or less hardware failure rate. In the figure, D_a, D_b, D_c, and D_d stands for output data, and S_a, S_b, S_c, and S_d stands for status signals from Cell A, B, C, and D, respectively. If the status signals show all the cells are good, the

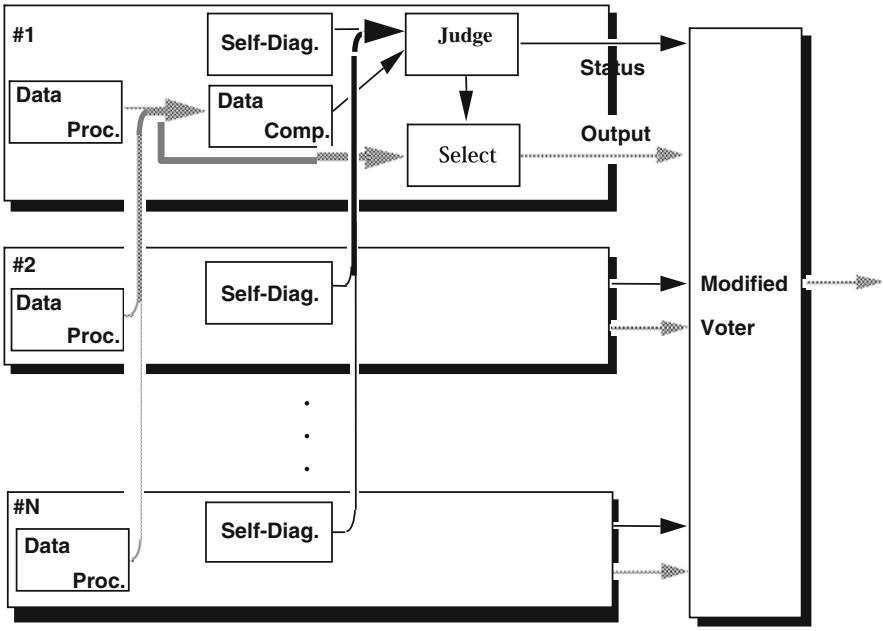
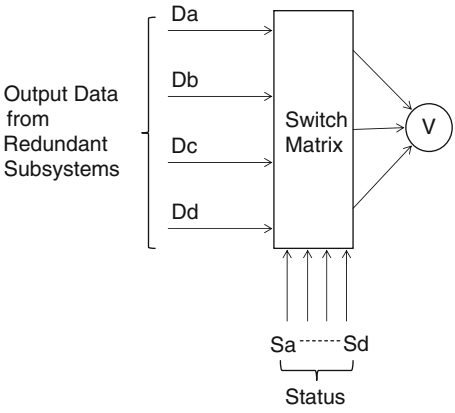


Fig. 5.25 System configuration for the SNV

Fig. 5.26 Configuration of MV



switch matrix selects D_a, D_b, and D_c for candidate data to be voted. If one of the cells is faulty, the switch matrix selects D_d instead of the data from faulty cell. If two of the cells are faulty, the switch matrix selects D_d instead of one of the faulty data, and fail-safe signal (all 1 or all 0) instead of another faulty data. If the status signals identify one good cell out of cells, the switch matrix selects the data from the identified cell.

Fig. 5.27 Switch logic of MV

Sa	Sb	Sc	Sd	Selected Data		
1	1	1	*	Da	Db	Dc
1	1	0	1	Da	Db	Dd
1	0	1	1	Da	Dd	Dc
0	1	1	1	Dd	Db	Dc
1	1	0	0	Da	Db	F.S.
1	0	1	0	Da	F.S.	Dc
1	0	0	1	Da	Dd	F.S.
0	1	1	0	F.S.	Db	Dc
0	1	0	1	Dd	Db	F.S.
0	0	1	1	Dd	F.S.	Dc
1	0	0	0	Da	Da	Da
0	1	0	0	Db	Db	Db
0	0	1	0	Dc	Dc	Dc
0	0	0	1	Dd	Dd	Dd
0	0	0	0	F.S.	F.S.	F.S.

*: Don't care F.S.: Fail-Safe Output

5.8.2 Hiten Onboard Computer

The SNV is employed for onboard computer (OBC) loaded on Hiten, scientific satellite of Institute of Space and Astronautical Science (ISAS, Currently Japan Aerospace Exploration Agency (JAXA) Space and Astronautical Science Research Headquarters), which was launched on January 24, 1990 [30]. Figure 5.28 depicts photograph of the OBC. The objectives of mission were

– experiments for fault-tolerance verification,
– experiments for verification on utilization of COTS electronic components in space, and
– high-efficiency packet telemetry transmission experiments.

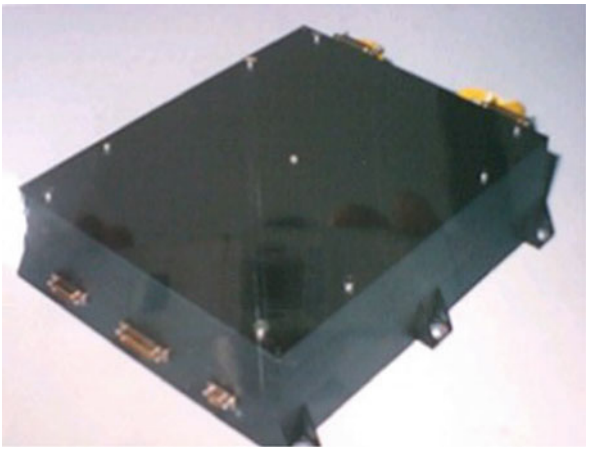


Fig. 5.28 Hiten OBC

Table 5.4 Specification of OBC

Fault-tolerance	SNV (Stepwise negotiating voting) method
MPU	HD68HC000 base (8 MHz Clock)
Operating system	HI68 K (TRON[a] Spec.)
Memory	64 K bytes + ECC
Degree of redundancy	3 (up to 4)
Dimensions	260 × 10 × 76 (mm)
Weight	2.6 kg
Power dissipation	1.8 W (5 V DC)

[a] The real-time operating system nucleus

Table 5.4 shows specification of the OBC. The OBC consists of COTS 16-bit microprocessor (HD68HC000), direct memory access controller (DMAC), read only memory (ROM), random access memory (RAM), and gate arrays implement peripheral interface circuitry and all the necessary facilities for fault tolerance. The system was designed to have up to four subsystems, but the flight model has three subsystems, cells A, B, and C because of restriction of weight and power dissipation.

Software for the fault tolerance was also realized using COTS operating system (HI68K) and additional handlers to assure dependable behavior of the user program (application program) or packet telemetry function.

In addition, the OBC has remote-loading function which enables to load program from an Earth station. This function was used for fault-tolerance verification experiments such as intentionally fault injection and filed data collection. In the original plan, the field data is supposed to be collected via the real-time telemetry data. But the authors used the field data collection function (fault record function and download function) installed by the remote-loading function, because it turned out that the field data collection via real-time telemetry data had two major problems after the launch. The first shortcoming was limitation of data collection period; the real-time telemetry data is received only if the satellite is visible from the Earth station. The visible period was approximately 4 h a day for Hiten and the actual period will be shortened by operation schedule of the Earth station. Therefore, the actual data collection period by the real-time telemetry will be limited to extremely small portion of the whole mission time. The second shortcoming was influence of data transmission error. The data transmission error occurs randomly and the transient fault occurs as the same. So, it is very difficult to distinguish transient fault from data transmission errors. The field data collection function enables to obtain the transmission error-free field data during the entire mission time.

5.8.3 Fault-Tolerance Experiments

5.8.3.1 Fault-Injection Experiments

Fault tolerance of the OBC was verified by fault-injection experiments in the orbit. The fault-injection function was installed by the remote-loading function, as

stated above. These experiments were executed after the launch, in addition to the functional test before the launch.

In the experiments, inter-cell communication errors and data processing errors were injected. The inter-cell communication was emulated by placing an illegal data specification code into inter-cell communication message. This experiment is to verify the immunity function of cells which detects and protects the cells from harmful communication access from other faulty cells. Recipients of the message successfully detected the injected faults and blocked the communication channel to the faulty cell.

The data processing errors were emulated by placing errors into packet telemetry data for processing at a particular cell. This experiment is to verify the function to detect and repot fault occurrence in the cell, the function of the MV, and the immunity function in the inter-cell communication. The fault-injected cell successfully detected and reported its faulty status to the MV and rebooted itself immediately. Other cells blocked the communication channel to the fault-injected cell.

5.8.3.2 Field Data

Figure 5.29 depicts the chronology chart of the Hiten OBC. The OBC started its mission on February 5, 1990 when it was powered on, and terminated on April 10, 1993 when the Hiten hard-landed to the Moon. The field data are collected during the period from July 5, 1990 when the field data collection function was installed at the end of the mission time.

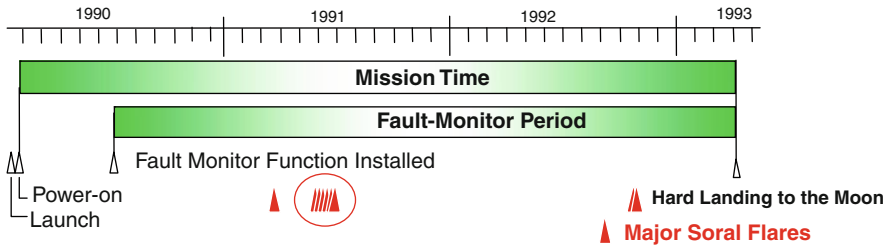


Fig. 5.29 Chronology chart of the Hiten OBC

During the mission time, the OBC has no permanent hardware faults or no latch-ups. The OBC encountered nine major solar flares with subsequent burst SEUs in March and June 1991, October and November 1992. Also, 655 SEUs were observed in the three cells during the fault monitoring period, including the burst SEUs after the solar flares. The OBC did not select the output data from the cell where the SEU observed, but selected the output data from other cells according to the data selection algorithm of the SNV method.

MPU were rebooted four times during the mission time. MPU is reset by watch dog timer or an exception handler process in case of MPU runaway. According to the field data, no malicious behavior such as erroneous data output and whole system down by the MPU runaway was not observed.

Figure 5.30 shows the proportion of SEUs in each portion of the OBC, in the MPU, inter-cell communication interfaces, and RAM. The number of SEU in RAM

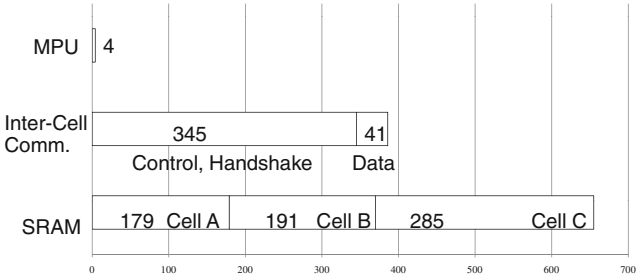
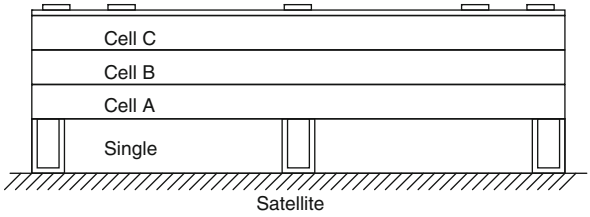


Fig. 5.30 SEUs in each portion of the OBC

Fig. 5.31 OBC structure



in each cell decreases in the order of cells A, B, and C. The order coincides with the order of exposure, and the cells are located outward in the order of C, B, and A, as shown in Fig. 5.31.

Figure 5.32 shows burst SEU occurrence after a series of solar flares in June, 1990. The graph shows number of SEUs in each cell in every half day. These flares

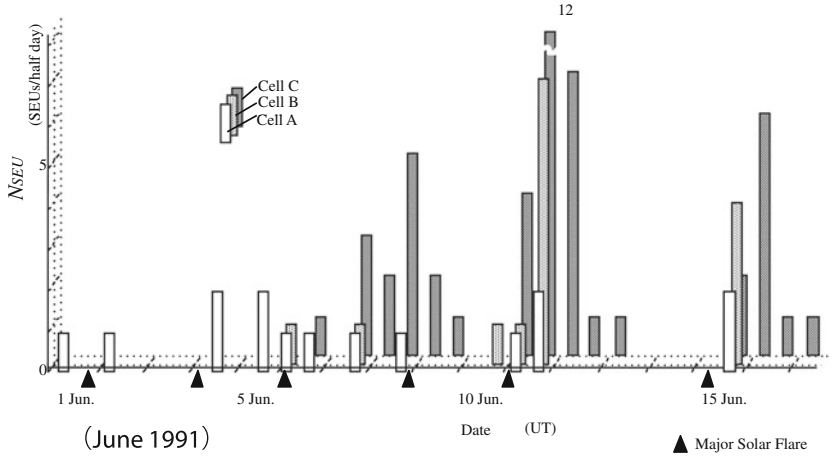


Fig. 5.32 SEU occurrence

were so energetic that their intensity exceeded the measuring limit, X12.0. Table 5.4 shows SEU rate in various environmental conditions. Memory size of contemporary computer systems is roughly more than 1,000 times larger than the OBC. Therefore, SEU occurrence in the whole system will be more than 1,000 times in frequency even if the SEU rate is unchanged. In reality, the SEU rate increased with finer process; therefore, we cannot ignore SEU occurrence also on the Earth.

5.8.4 Extension of SNV – Redundancy Management

Redundancy management such as saturation [34] to maximize reliability of tasks using redundancy effectively minimizing idleness of redundant resource in multi-task system is proposed. Reliability-based data selection such as SNV has prospects of extension to the redundancy management [35].

Figure 5.33 depicts reliability comparison of a system with redundancy management which shares redundant resources flexibly among tasks and a system without it. The horizontal axis stands for reliability of redundant subsystems which form the fault-tolerant system and the vertical axis stands for reliability of the fault-tolerant systems which performs two tasks using redundant subsystems, one fault-tolerant system performs two tasks using six subsystems flexibly, and another fault-tolerant system performs two tasks using three dedicated subsystems for each task, respectively. The figure shows that reliability of the system with redundancy management is higher than the system without it.

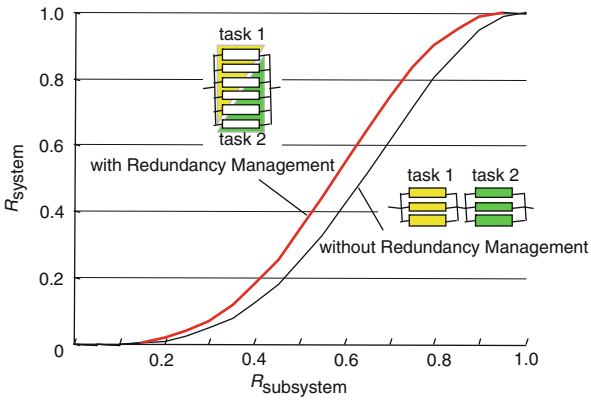


Fig. 5.33 Reliability with redundancy management

The saturation method assigns redundant resources fixedly for tasks at the beginning of task execution. In addition, the author proposed a redundancy management scheme based on the SNV, which reassigns redundant resources and rebalances reliability every output cycle or control frame. Figure 5.34 shows basic idea of the redundancy management based on SNV; if two subsystems for task 1 become faulty and reliability of data processing decreased, the system reassigns one subsystem

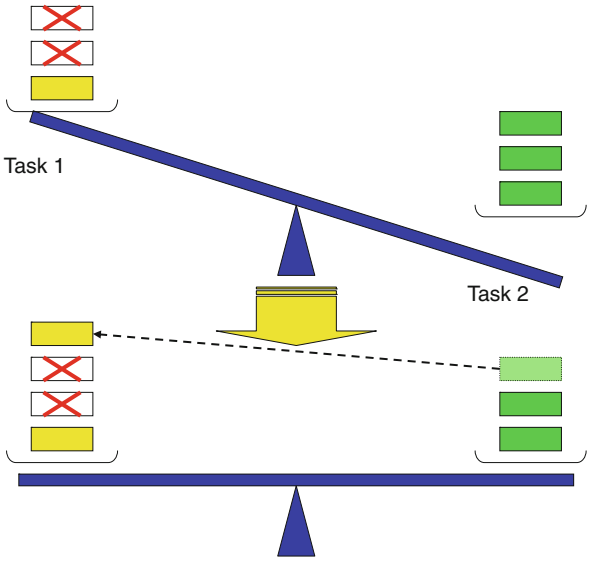


Fig. 5.34 Basic idea of redundancy management

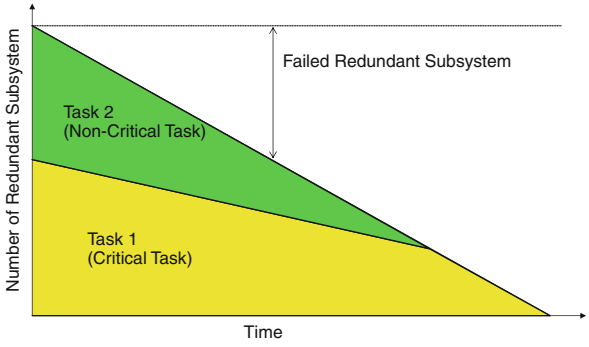


Fig. 5.35 Behavior of redundancy management

which has performed task 2 for task 1, here the reliability of data processing is estimated based on the SNV, as stated in Section 5.8.1. Therefore, reliability of endangered task 1 is recovered and reliabilities of both tasks are rebalanced. When number of faulty subsystems increased and number of good subsystems decreased as the time passed, the system realized balanced graceful degradation from the viewpoint of degree of redundancy or reliability for each task, as shown in Fig. 5.35. If there is difference between critical task and non-critical task, reliability or degree of redundancy of the critical task is kept higher than the non-critical task as shown in the figure.

Essential control task falls on the critical task and auxiliary functions, such as online regulator tuning for adaptive control system, planning system, control

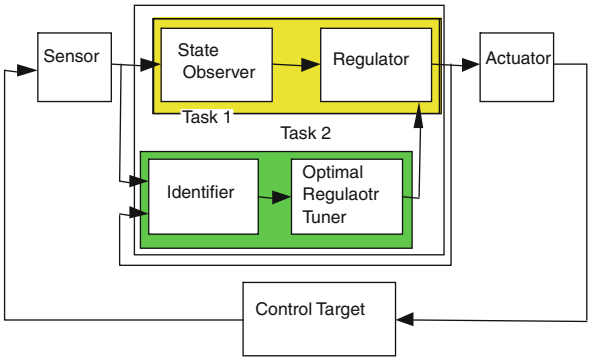


Fig. 5.36 Online regulator tuning

optimizing by simulation or speculative execution, and fall on the non-critical function.

Figure 5.36 shows diagram for adaptive control system by online regulator tuning. Online regulator tuning consists of identifier and optimal regulator tuner that are implemented as non-critical task or task 2, besides critical task or task 1, while essential control function consisting of state observer and regulator is critical task. The identifier identifies parameters of the control target and the optimal regulator tuner determines the optimal control parameters for the identified control target parameters. In case of failure in sensor, actuator, or control target, the on-line regulator tuning determines new control parameter adapting to the failed situation. Therefore, the adaptive control system with the online regulator tuning scheme realizes fault tolerance of control system. For example, failure in a control surface in aircraft control system can be handled by the adaptive control system using other healthy control surfaces.

To prevent single point of failure or bottleneck in reliability, it is better to realize the redundancy management function in a distributed autonomous manner by each subsystem than in a centralized manner. Hunting and overshoot are indispensable issue in realizing management function in autonomous manner, as shown in Fig. 5.37. The figure shows result of fault-injection simulation; fault is injected into one subsystem every 20 control frames. The horizontal axis stands for time in control frame and vertical axis stands for number of subsystems which are assigned to each task by the redundancy management. Figure 5.38 shows results of simulation with stabilization countermeasures such as moving average in reliability criteria and subsystem priority reassignment.

5.9 Coverage Improvement

The author employs an approach to duplicate functional block (MPU) and compare their outputs, because development cost and time can be reduced, utilizing existing MPU design and minimizing ad hoc design. Also, the authors developed

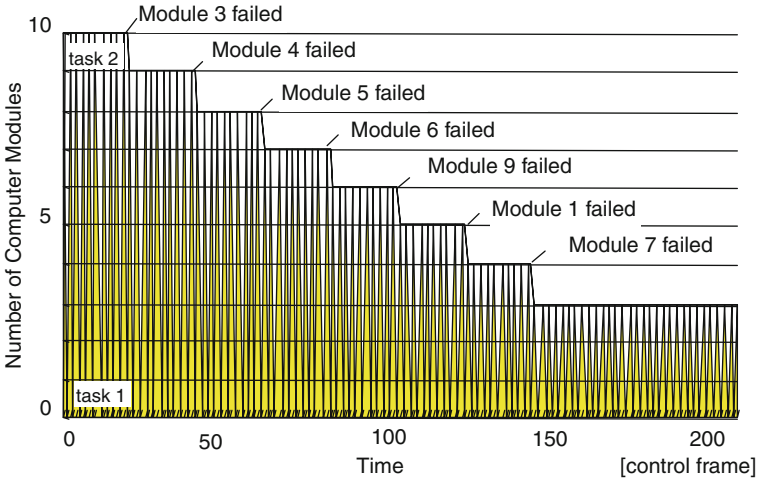


Fig. 5.37 Behavior of redundancy management

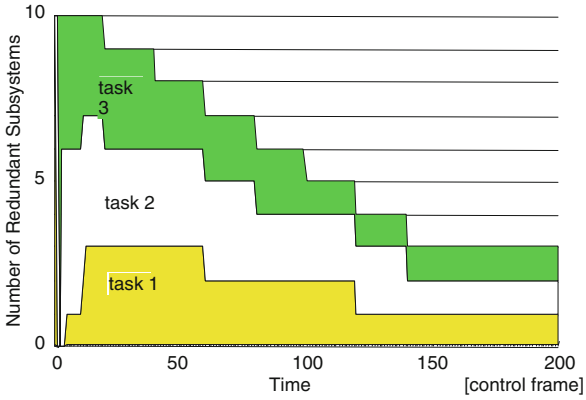


Fig. 5.38 Behavior of redundancy management

self-checking and cross-talk tolerant comparator to improve coverage of the comparator with relaxed design restrictions. In addition, the authors employed special diversity and time diversity, more specifically the optimal time diversity. In the following sections, the authors introduce the self-checking comparator and the optimal time diversity.

5.9.1 Self-Checking Comparator

Self-checking comparator can be realized by redundant code in order to detect any single fault occurring in the comparator itself. However, latency in detection

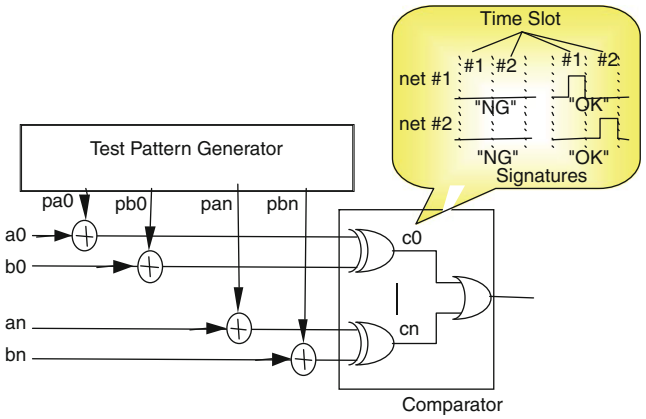


Fig. 5.39 Self-checking comparator

of certain specific faults is extremely large. Because fault occurrence in the functional blocks is very rare, the signal paths which represent disagreement of the functional blocks are seldom activated. The rareness of the disagreement implies fault latency, i.e., stuck-at fault in the signal path are seldom detected by the redundant code.

Fault injection to input data is widely employed in order to eliminate the fault latency by exercising the signal paths. Dynamic codes such as alternating codes and frequency logics are also effective to eliminate the latency.

The frequency logic is a widely accepted technology, especially in Japanese railroad control field to ensure fail-safe operation. The frequency logic has not only dynamic feature but also redundant feature. In the frequency logic, signals at a specified frequency are recognized as proper signals which fall on "code words" in redundant codes, and other signals are recognized as illegal signals which fall on "non-code words." Therefore the frequency logic is potentially well suited to realize fail-safe and self-checking circuits.

Figure 5.39 depicts self-checking comparator proposed by the authors [32]. Test pattern generator generates test pattern or intentional fault-injection pattern to the input data A and B to solve the fault-latency problem in conventional static code logic. Here, a_0–a_n and b_0–b_n are input data from duplicated functional blocks to compare, and pa_0–pa_n and pb_0–pb_n are test pattern generated by the test pattern generator, and c_0–c_n are bitwise compare results. The test pattern or fault-injection pattern for the comparator is specially designed so that the comparator provides a specific pattern of signal which is a signature, representing that the input data agree, the test pattern generator is good, and the comparator is good. Therefore, if the input data disagree, or any of the test pattern generator and the comparator is faulty, the comparator does not provide the signature with the specific waveform as shown in Fig. 5.40.

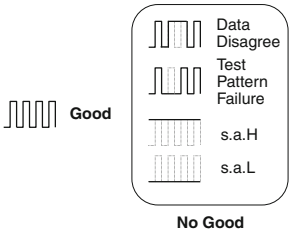


Fig. 5.40 Waveforms in the self-checking comparator

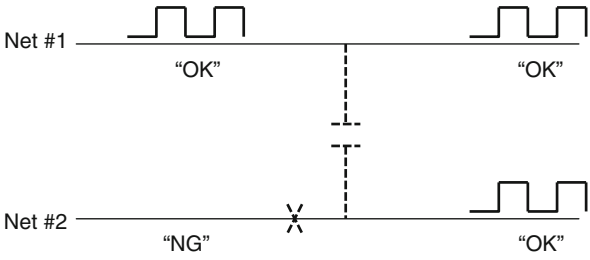


Fig. 5.41 Cross-talk among wiring nets

In addition, the test pattern is also specially designed using orthogonal signals in order to detect open failures in any of wiring nets within the self-checking comparator. If the open failures occur, the net is electrically floated and signal may be induced from adjacent net by cross-talk among wiring nets as shown in Fig. 5.41. If wiring nets has common signature pattern, the cross-talk may cause faked signature. Very strict wiring restrictions are required to avoid the signature faking in conventional method.

The proposed method dedicates peculiar signature pattern to each wiring net exclusively using orthogonal signals to avoid the signature faking caused by the cross-talk. Because each wiring net has exclusively dedicated signature pattern, the faked signature induced by the cross-talk will be easily distinguished from the regular signature. Orthogonal functions can be used as the peculiar signatures to identify regular signature from faked signatures. Sin functions in different frequency and random M series are widely known as orthogonal functions.

The authors employ pulse patterns which turn on their peculiar time slots as the signature as shown in Fig. 5.39. Therefore, the signal turns on at the time slot #*i* will be supposed to be signature for wiring net #*i*. On the contrary, signal turn on at the time slot #*i* is always assigned to wiring nets other than net #*i*. The signature patterns turn on at their peculiar time slots can be interpreted as dynamic redundant code represented by a series of digitized wavelets. The wavelets are orthogonal functions and have variety in both frequency domain as a scale parameter and time domain as a shift parameter. The author employed variety in time domain for easier

implementation, at the same frequency (scale parameter) with variety of time (shift parameter).

5.9.2 Optimal Time Diversity

The concept of time diversity, which diverses the operation timing of redundant processor to prevent the same error outbreak, is conventionally proposed, as shown in Fig. 5.42. In the macroscopic aspect of time diversity effect, two folds of MPUs carry out different operation at the time of an electric noise imposed, so different processing is affected in different ways by the noise and the time diversity is effective in preventing the same error outbreak, as shown in Fig. 5.43. The effect of time diversity will be higher so that time lag between two folds of MPUs is larger in macroscopic aspect.

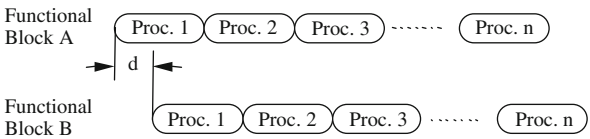


Fig. 5.42 Concept of time diversity

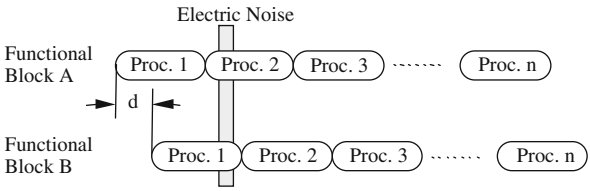


Fig. 5.43 Effect of time diversity (in macroscopic aspect)

In the microscopic aspect of time diversity effect, if a signal is not stable for a certain period of time before and after the rising or falling edge of the clock signal in the digital circuit which is synchronized to a clock, malfunction occurs. These periods are generally called setup time and hold time. Furthermore, the authors decide to call it a noise-sensitive window, because malfunction occurs if a noise is impressed within this period. Considering time distance between the noise-sensitive windows of two folds of MPUs, time distance A grows larger when the time lag grows as far as a half-clock. Furthermore, time distance B shrinks when time lag grows larger than a half-clock and approaches one clock. Therefore, time distance between the noise-sensitive windows becomes the largest when the time lag is a half-clock difference or its odd multiple as shown in Fig. 5.44 [36]. On the basis of the above-mentioned consideration, the overall effect is expected to be the greatest at the time of half-clock difference or its odd number multiple as shown in Fig. 5.45.

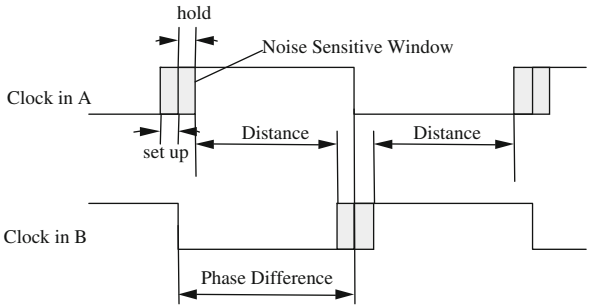


Fig. 5.44 Effect of time diversity (in microscopic aspect)

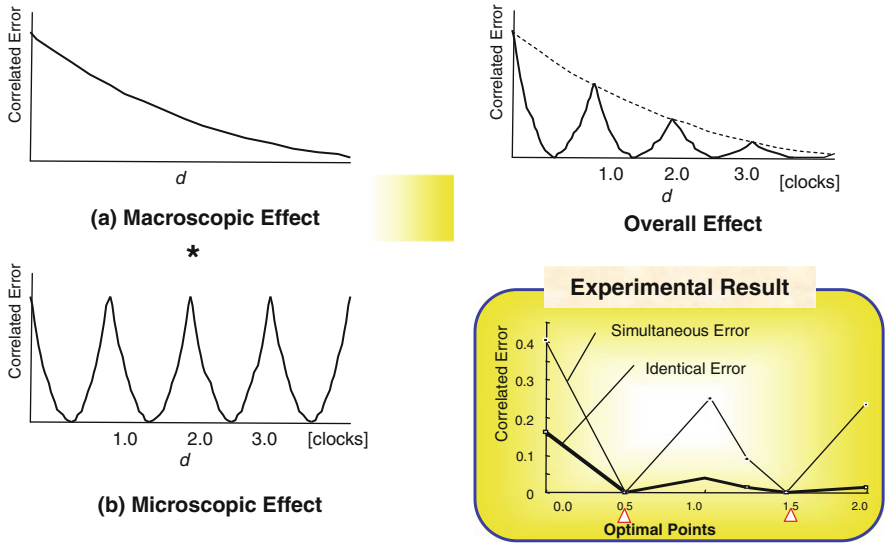


Fig. 5.45 Effect of time diversity

The actual experiment gives a result to affirm this expectation. The experimental result shows the optimal point of the clock phase difference at 1/2 and 3/2 clock cycles as shown in Fig. 5.45. No coincident errors or no simultaneous errors are observed for over 300,000 noise injections at these optimal points. It was certified that the time diversity with the time lag, a half clock, or its odd number multiple is the most effective by theory and experiment, therefore we call it "optimal time diversity method," and more particularly "optimal clock diversity method" because we can realize a diversity with the time lag of the clock. In addition, it is called "differential duplication method" in the field of rail-road control.

Furthermore, the time diversity gives us a fringe benefit. Simultaneous switching noise (SSN) caused by operation of logic circuit will be reduced and enhances noise margin by the time diversity. Logic circuit operation results in collateral electric noise in power supply and ground lines by impulse current for switching of logic

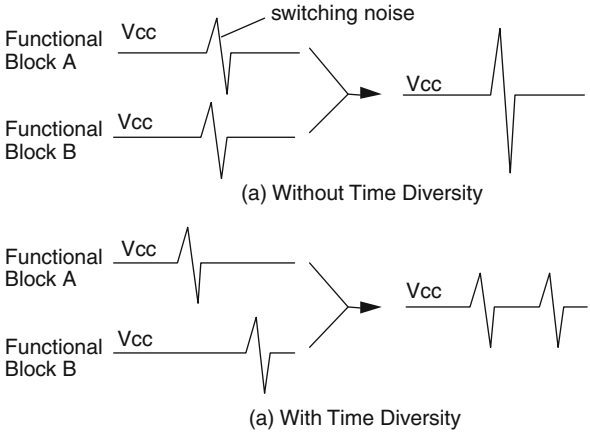


Fig. 5.46 Effect of time diversity (power supply noise reduction)

level. If duplicated subsystems operate at the same timing, both of them will generate the electric noise at the same timing. Therefore, the electric noises are added as simultaneous switching noise and grow larger in current and voltage. If we employ the time diversity for the operation of the duplicated subsystems, peek value of the electric noise will be reduced as shown in Fig. 5.46. See Section 4.5 for details of the SSN.

Furthermore, advantage of the optimal time diversity over the conventional clock synchronized system and conventional task-level synchronized system is verified by experiments. Figure 5.47 depicts the experimental result, runaway ratio of self-checking systems with (1) optimal time diversity, (2) conventional clock-level synchronization, and (3) task-level synchronization. The horizontal axis stands for runaway ratio, where lower runaway ratio means higher detection coverage. Also, the horizontal axis stands for noise intensity by capacitance for noise injection. Figure 5.48 shows retry coverage and the vertical axis stands for recovery coverage

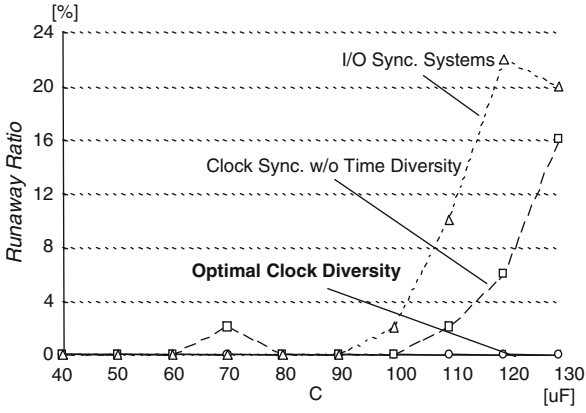


Fig. 5.47 Effect of time diversity (runaway ratio reduction)

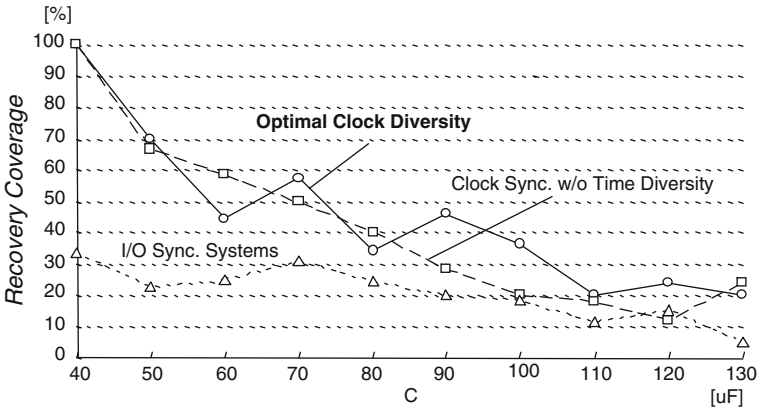


Fig. 5.48 Effect of time diversity (retry coverage improvement)

in percentage. The experimental results show higher recovery coverage of clock-level synchronized systems over task-level synchronized systems. The advantage of the optimal time diversity is not so remarkable in this graph, besides it is obvious in Fig. 5.47.

The experiment was performed by the experimental system as shown in Fig. 5.49 and self-checking processor prototype as shown in Fig. 5.50 was used as the system under the experiment. The experimental result shows better fault-detection coverage by the optimal time diversity over conventional methods, clock synchronized system without time diversity, and task-level synchronized system.

In the task-level synchronized system, redundant subsystems are synchronized and they compare their processing results on output to peripherals. Faults are seldom

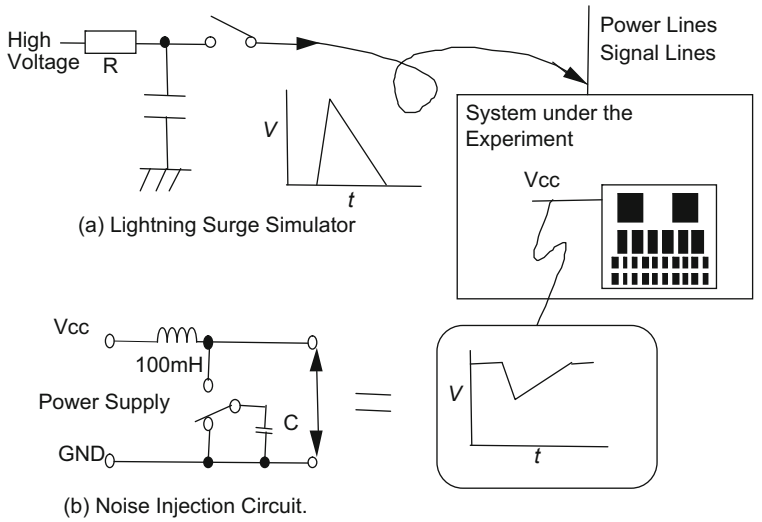


Fig. 5.49 Experimental system

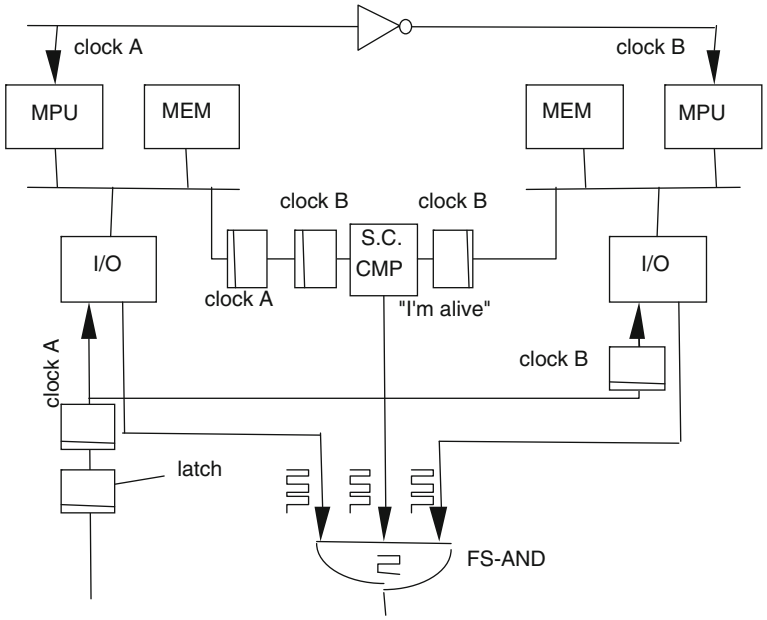


Fig. 5.50 Self-checking processor prototype

detected until output timing, as shown in Fig. 5.51. The peripheral output timing is the control frame for controller applications and varies from 1 to 100 ms. Therefore average latency, i.e., the period from fault occurrence to detection varies from 0.5 to 50 ms. A microprocessor will execute millions or billions of instructions during

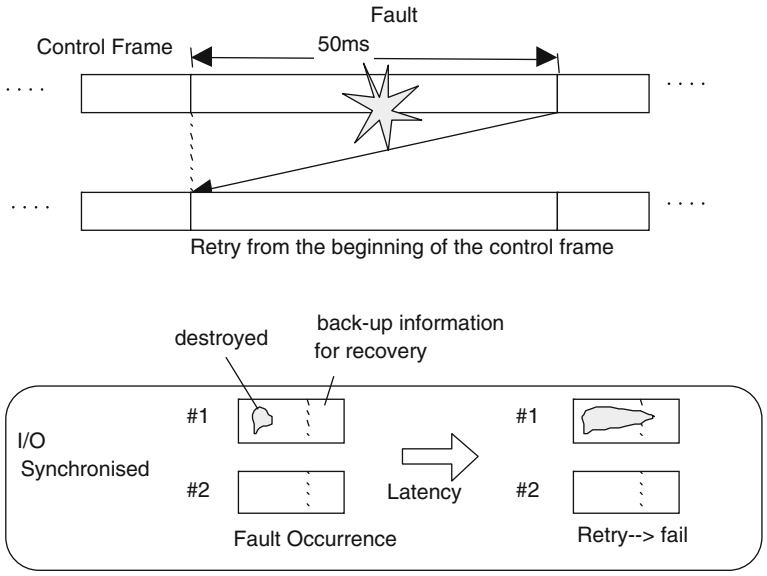


Fig. 5.51 Recovery process in task-level synchronized systems

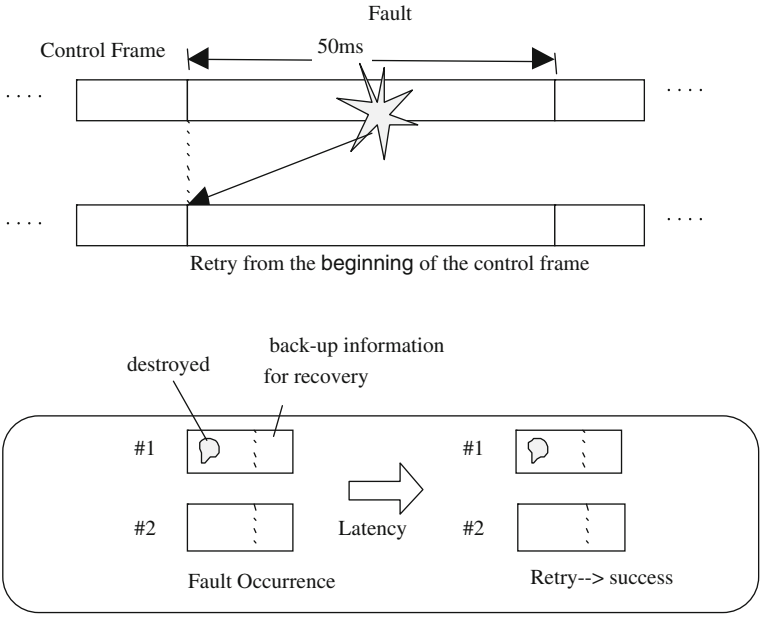


Fig. 5.52 Recovery process in clock-level synchronized systems

this period. Back-up information which is necessary for recovery may be destroyed during this period.

In the clock-level synchronized system, redundant subsystems are synchronized and they compare their processing results in every clock cycle. This method can detect fault and retry almost immediately as shown in Fig. 5.52. The latency is within a few instructions at the most. Therefore, the probability of back-up information corruption is extremely low. In other words, coverage of the clock synchronized systems will be much higher than the task-level synchronized system, if the optimal time diversity prevents common cause failure.

5.10 On-Chip Redundancy

Nowadays, the whole system comes to be integrated within one chip as a result of development of high-density integration by the Moore's Law, as stated earlier. Moreover, plural systems can be placed within one chip. In the field of microprocessor, multi-core processors which constitute plural processor cores within one chip appear. In the field of dependable computing, the concept of self-checking logic by on-chip redundancy which has plural processors operating identical processes and detect fault by comparison is proposed [32].

The fault-detection coverage by on-chip redundancy greatly depends on the independence of fault occurrence among the redundant subsystems and the

fault-detection coverage of comparison mechanism. The self-checking comparator stated formerly can be employed in order to improve the fault-detection coverage of comparison mechanism. Furthermore, the optimal time diversity also stated formerly and spatial diversity can be employed in order to guarantee the independence of fault occurrence among the redundant subsystems. The spatial diversity is realized by design restriction floor planning, wiring and routing in the LSI chips. Corresponding portions of the redundant functional blocks can be placed at separate locations in the LSI chip.

Design rule or restrictions in detailed wiring and routing is relaxed by cross-talk-tolerant feature of the proposed self-checking comparator. A rough floor plan can be given by the designers based on human heuristics and expertise, and a detailed wiring routing can be determined by design automation system based on several kinds of routing algorithms in contemporary design process. Therefore, special diversity realized by the floor plan is quite well suited to contemporary design automation systems.

Figure 5.53 shows a photograph and a floor plan of the first prototype of the self-checking LSI. This prototype was experimentally fabricated using commercial off-the-shelf LSI process in these days (Hitachi's HG62S gate array) to validate fault-tolerance coverage of on-chip redundancy technology. The prototype has two sets of self-checking clusters. Each cluster has pseudo-CPU subset of SH1 microcontroller as the duplicated functional blocks and the self-checking comparators. As mentioned formerly, frequency logic has very good fail-safe features and is employed for train control systems in Japan. The authors can also employ the on-chip redundancy technologies to realize the fail-safe feature of the train control systems.

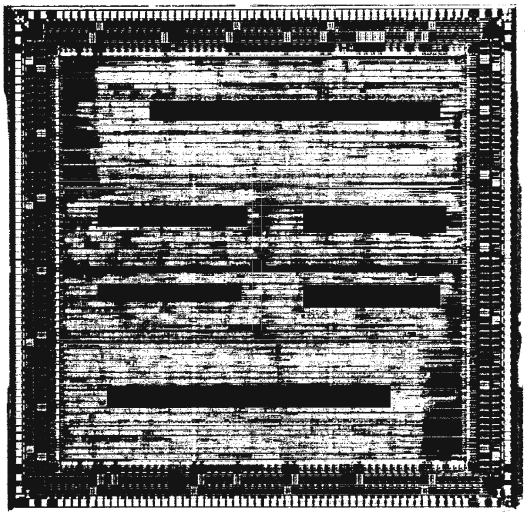


Fig. 5.53 Self-checking LSI prototype

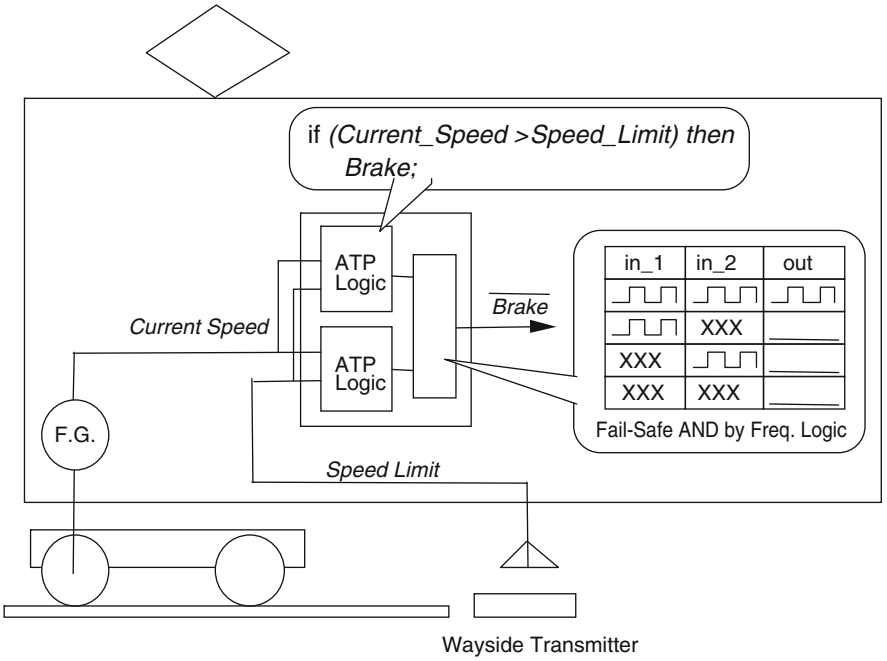


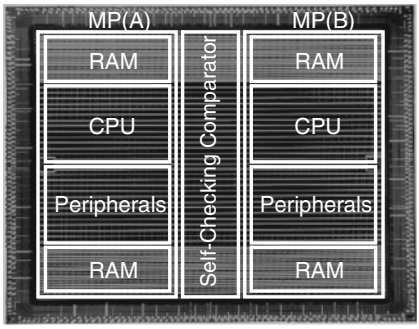
Fig. 5.54 ATP (automatic train protection) system

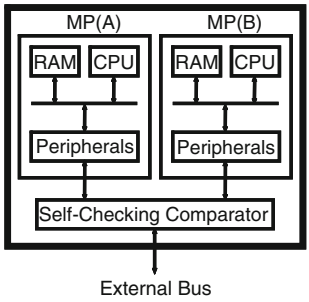
Figure 5.54 depicts a block diagram of automatic train protection (ATP) system employing on-chip redundancy. The duplicated functional blocks have the same function as conventional ATP logics. They compare the actual current train speed from frequency generator (FG) and the speed limit from ATP wayside transmitter. If the actual speed exceeds the speed limit, the ATP logics engage the brake command. Brake command outputs of the ATP logics are represented by active low in frequency logic, i.e., alternating signal at specified frequency stands for non-brake command and other signals stands for brake command.

Fail-safe AND logic by the frequency logic ensures brake command safety. The fail-safe AND logic outputs non-brake command only if the both of ATP logics output the non-brake commands. On the contrary, it outputs brake command and ensures fail-safe state of the train in other cases. The on-chip redundancy enables fail-safe features of LSI with design restriction such as layout and wiring rules in limited portion, the fail-safe AND, and can relax layout and wiring restriction for ATP logics.

At first, the authors established a synthesizable core (soft IP) technology to port the design assets of the processor for a different process, and experimentally produced self-checking processor FUJINE[1] which implemented two folds of processor,

[1] Named after the mountain where Hitachi Research Laboratory locates.

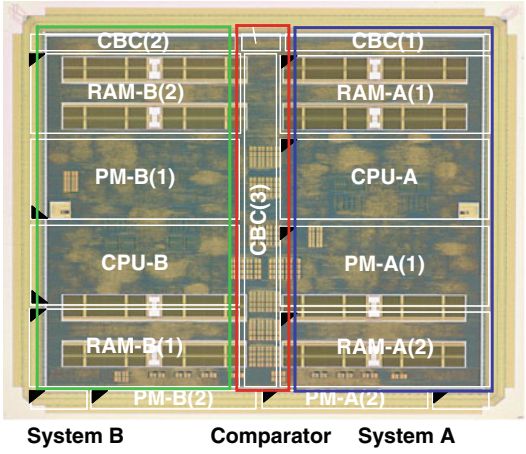




Process	0.35μm 5 Metal CMOS
Hard Macros	PLL x 2, RAM(40KB)
Random Logic	740k gates
Chip Size	14.75 mm^2
Operating Frequency	60 MHz
Power Dissipation	2.6W @ 60MHz
Package	479pin BGA

Fig. 5.55 Safety micro-controller prototype (FUJINE)

Fig. 5.56 Safety micro-controller



the comparator implemented on logic in 1999 (Fig. 5.55) [37]. Furthermore, the authors developed a fail-safe CPU (FS-CPU) which added the functions such as a floating point arithmetic function and a cache memory, with the parallel computation of two processors in 2006 (Fig. 5.56) [38] and are promoting an application to various kinds of products as a standard part of the railway signaling system.

5.11 High Performance (Commercial Fault-Tolerant Computer)

5.11.1 Basic Concepts of TPR Architecture

The TPR architecture achieved operation at 33 MHz, the highest frequency at that time [31]. Because the architecture is still good now, it is introduced here. Here are the basic concepts of TPR architecture.

5.11.1.1 System Reconfiguration by Collaboration of Hardware and Software

TPR architecture employs immediate reconfiguration and deferred reconfiguration to realize transparent, high-speed, and complex reconfiguration, as shown in Fig. 5.57. The immediate reconfiguration is a simple, first-aid system reconfiguration implemented by hardware with fine grained time scale, in each machine cycle. Synchronization among redundant subsystems and data selection just after fault occurrence are classified into the immediate reconfiguration. The deferred reconfiguration is a complex, thorough system reconfiguration implemented by software with coarse time scale, in task level.

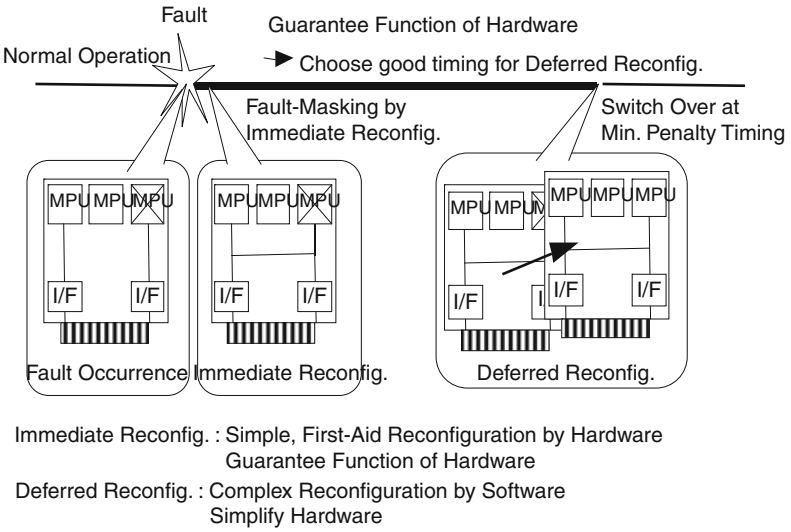


Fig. 5.57 Immediate/deferred reconfiguration

Just after the fault occurrence, the immediate reconfiguration masks influence of fault and guarantees function of hardware for a while. So the system can choose proper timing (e.g., context switch) for deferred reconfiguration in order to minimize penalty, and the guarantee of hardware function instantly means guarantee of

software function, especially operating system. Therefore, the deferred reconfiguration can be implemented by additional handler with support of existing operating system functions. In other words, fault tolerance can be realized based on standard operating systems and well matched to standardization and globalization trends.

5.11.1.2 Intra-board Fault-Masking

As stated in Section 5.5.1, synchronization overhead among redundant subsystems will be major cause of performance degradation by fault tolerance. TPR architecture implements all the necessary redundant processors for fault tolerance within a single printed circuit board, and synchronizes them in clock level, in order to reduce signal propagation delay and the synchronization overhead as shown in Fig. 5.58. Furthermore, all the redundant processors can be granted as logically single and the redundancy is transparent because they operate completely synchronized and completely in identical manner. Therefore software and operating systems already developed without considering fault tolerance can be used for the system, and existing technologies such as multi-processor technology indispensable for high-performance computing can be easily utilized. The TPR architecture has triplicate microprocessor, and the outputs of the processors are compared.

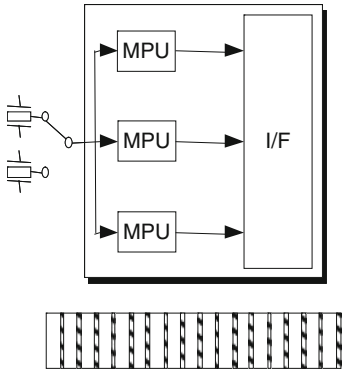


Fig. 5.58 Intra-board synchronization

Fault tolerance of clock generator is indispensable for clock synchronized systems because failure in clock generator influences all the redundant subsystems. TPR architecture has redundant clock generator with hot stand-by, clocks are monitored mutually by counters, and switched according to timing to which the phase is corresponding without glitch, in case of clock failure.

5.11.2 System Configuration

Figure 5.59 shows system configuration of fault-tolerant computer system by TPR architecture. Basic processing unit (BPU) has triple micro-processing units (MPUs),

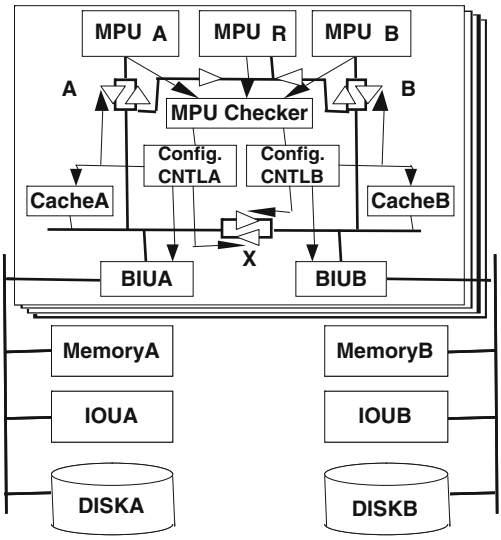


Fig. 5.59 TPR architecture

and other portions such as cache memories, bus interface units (BIUs) are duplicated. The BPU is connected to IOU, main memory and hard disk, etc., via system bus. The IOU, the main memory and the hard disk, etc., are also duplicated for fault-tolerance.

TPR architecture employs triplicate approach in order to realize fault-tolerant computer with high performance low cost utilizing commercially off-the-shelf state-of-the-art MPU. The triple MPUs operate with clock-level synchronization and their behaviors are checked and compared with each bus cycle to identify faulty MPU. Most of COTS MPUs are designed for high performance and cost effectiveness without considering fault detection.

Portions other than MPUs, such as cache memories, bus interface units (BIUs) are newly designed as self-checking to identify faulty part and duplicated for continuous operation with normal portion. MPU A and MPU B output data and address signals into cache memories and BIUs in systems A and B, respectively. Data and address outputs from MPU R is used for reference and fed to MPU checker to identify which of MPUs A and B is normal.

Check results from MPU checker and check functions in the system are collected from the reconfiguration controllers, Config. CNTLA and Config. CNTLB, in order to identify fault location and reconfiguration for fault-masking by controlling tri-state buffers. The reconfiguration controllers make outputs of cache memories and BIUs high-Z state, and make tri-state buffers A and B externally connected to MPUs A and B high-Z state in order to prevent propagation of faulty signal on failure. The tri-state buffer X connecting buses in A and B sides intakes signals from one side to another on fault occurrence.

5.11.3 System Reconfiguration on Fault Occurrence

Figure 5.60 shows signal flow after the immediate system reconfiguration on fault in MPU A. Fault in MPU A is detected by MPU checker and Reconfig. A lets tri-state buffer A high-Z state and enables tri-state buffer X from B to A direction to feed normal signal from MPU B instead of fault signal from MPU A. Table 5.5 shows system reconfiguration on fault occurrence by controlling buffers by immediate system reconfiguration. If fault occurred in the system bus, Config. CNTLA controls buffers in the same manner as faults in BIU. In this case, as contents of memory connected to the failed system bus are corrupted, contents of memory in another side should be copied into corrupted memory. BPU realize the memory copy reading data from normal side and writing into both sides of memories.

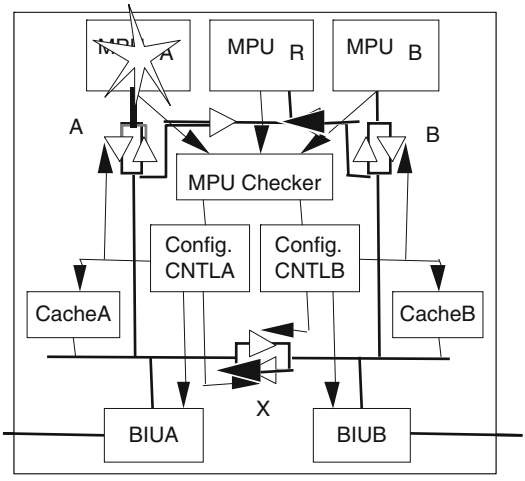


Fig. 5.60 Signal flow on fault in MPU A

Table 5.5 SEU rates

Environment	SEU rate [upset/bit/day]	SEU Interval (288 KB)
Ordinary (Solar-max.)	3.0×10^{-7}	2.3 days
Oedinary (Solar min.)	2.0×10^{-7}	2.1 days
After solar flare (ave. in 8)	7.2×10^{-5}	9 min.
After solar flare (peak)	2.0×10^{-4}	3 min.

5.11.4 Processing Take-Over on Fault Occurrence

TPR architecture has fault-tolerance function by the immediate system reconfiguration in BPU itself implemented by a single printed wiring board which is a replacement unit on maintenance. Therefore, data processing operation can be sustained until next “convenient timing” when fault occurred in any of BPUs.

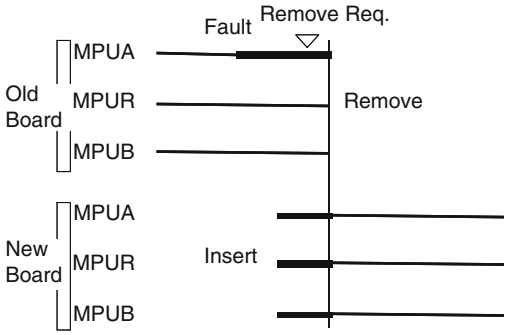


Fig. 5.61 Deferred reconfiguration

Figure 5.61 shows an example of data processing operation take-over by the deferred system reconfiguration on fault occurrence in MPU A. The BPU in failed board continues its data processing operation using normal MPU B and MPU R until the "convenient timing." Moreover, another BPU in new board takes over the data processing operation at the "convenient timing" by deferred system reconfiguration. The deferred system reconfiguration may be done in two ways:

(a) immediate after the fault occurred, and
(b) board replacement timing on maintenance.

In case (a), high reliability can be guaranteed because use of faulty BPU is limited during short period. But performance is degraded because the faulty BPU stop its data processing operation. In case (b), performance is not degraded, but there is possibility that the second and the third faults may occur during the period of the faulty BPU operation. As stated above, TPR architecture minimizes performance degradation on data processing take-over, and reduces overhead by checkpoint backup for checkpoint restart recovery.

5.11.5 Fault Tolerance of Fault Tolerance

5.11.5.1 Fault Tolerance of System Reconfiguration

TPR architecture has system reconfiguration control function for systems A and B independently and they control signal flow into systems A and B exclusively. As for buffer X, tying internal bus A and B, signal flow from B to A is controlled by Config. CNTL A and signal flow from A to B is controlled by Config. CNTL B, respectively. Therefore, the influence of fault in Config. CNTL A will be limited in system A only, as shown in Fig. 5.62 and never affects system B or both the systems.

5.11.5.2 Fault Tolerance of MPU Checker

The MPU checker is key component to compare signals from MPU A, B, and R to identify fault occurrence in MPUs. The MPU checker has redundant comparators,

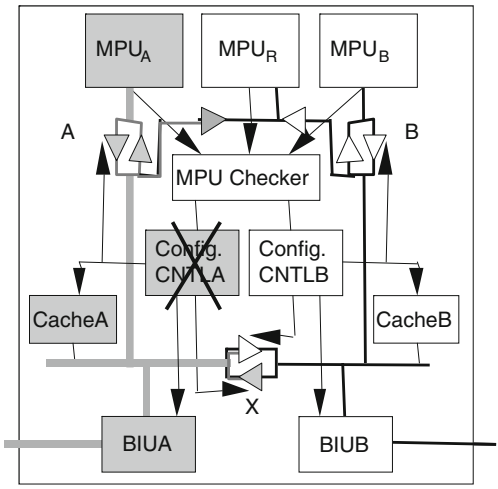


Fig. 5.62 FT of FT mechanism

Comp. AB, AR, and BR as shown in Fig. 5.63, where fault of MPUs can be identified by only two comparators. Faults in comparator such as false alert (faked report) and mis-alert (absence report) can be detected by checking compatibility and rationality of comparator outputs as shown by Table 5.6. If one of MPUs A, B, and R has fault, two of three comparators AB, AR, and BR will report disagreement. And if any of three comparators causes false alert (faked report) or mis-alert (absence report), one or three comparator(s) report(s) disagreement as shown by Table 5.7. Based on this regularity, if one comparator reports or three comparators report disagreement, rationality check function identifies the fault in comparator. The rationality check function guarantees that MPU is normal only if both MPU and comparator are normal (Table 5.8).

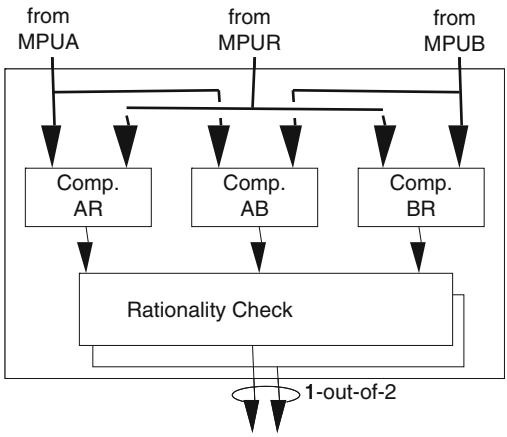


Fig. 5.63 MPU checker

Table 5.6 System reconfiguration on fault occurrence

	Buffers							
Fault location	A	B	CacheA	CacheB	BIUA	BIUB	X	MPU R reads from
All good	Open	Open	Open	Open	Open	Open	Hi-Z	A
MPUA	Hi-Z	Open	Open	Open	Open	Open	B->A	B
MPUB	Open	Hi-Z	Open	Open	Open	Open	A->B	A
MPUR	Open	Open	Open	Open	Open	Open	Hi-Z	A
CacheA	Open	Open	Hi-Z	Open	Open	Open	B->A	B
CacheB	Open	Open	Open	Hi-Z	Open	Open	A-B	A
BIUA	Open	Open	Open	Open	Hi-Z	Open	B->A	B
BIUB	Open	Open	Open	Open	Open	Hi-Z	A->B	A

Open: Output enabled Hi-Z: output disabled

Table 5.7 MPU checker (Fault location vs. Comp. report)

Fault location								
MPU			Comp.			Comp. report		
A	R	B	AR	AB	BR	AR	AB	BR
G	G	G	G	G	G	Agree	Agree	Agree
G	G	G	FR	G	F	Disagree	Agree	Agree
G	G	G	G	FR	G	Agree	Disagree	Agree
G	G	G	G	G	FR	Agree	Agree	Disagree
F	G	G	G	G	G	Disagree	Disagree	Agree
F	G	G	FR	G	G	Disagree	Disagree	Agree
F	G	G	G	FR	G	Disagree	Disagree	Disagree
F	G	G	G	G	FR	Disagree	Disagree	Disagree
F	G	G	AR	G	G	Agree	Disagree	Agree
F	G	G	G	AR	G	Disagree	Agree	Agree
F	G	G	G	G	AR	Disagree	Disagree	Agree

Table 5.8 MPU checker (Comp. result vs. rationality check result)

Comp. result			
A != B	B != R	R!= A	Rationality check result
F	F	F	All good
F	F	T	Comp_RA fault
F	T	F	Comp_BR fault
F	T	T	MPUR fault
T	F	F	Comp_AB fault
T	F	T	MPUA fault
T	T	F	MPUB fault
T	T	T	Multiple fault

G Good, *F* Faulty, *FR* Faked error report, *AR* Absence of report

A_good, B_good, and R_good, the event that MPUs A, B, and R are good, respectively, are expressed as follows:

A_good =	! AR & ! AB	| ! AR & BR & BA
		| AR & BR & ! BA
B_good =	! BR & ! AB	| AR & ! BR & BA
		| AR & BR & ! BA
R_good =	!BR & ! AR	| ! AR & BR & BA
		| AR & ! BR & BA

Where

AR: Comp AR reports agreement,
AB: Comp AB reports agreement,
BR: Comp BR reports agreement.

Furthermore, the rationality check circuit consists of complimentary logic circuits to detect fault in the rationality check circuit itself.

5.11.6 Commercial Product Model

The TPR architecture stated above was employed by commercial fault-tolerant server HITAC FT-6100 (Fig. 5.64) for information systems and HIDIC FT90/600 for control systems, and enabled both reliability and performance. These systems have MTBF of about one million hours, and realized operation at 33 MHz clock frequency with 68,040 processors in 1991. The system can have from one BPU at the minimum configuration, up to four BPUs for multi-processing for higher performance. Combination of immediate system reconfiguration realized by hardware and deferred system reconfiguration by software realizes transparent system with fault-tolerant operating system based on standard operating system, UNIX with handler for the deferred system reconfiguration.

Fig. 5.64 FT-6100

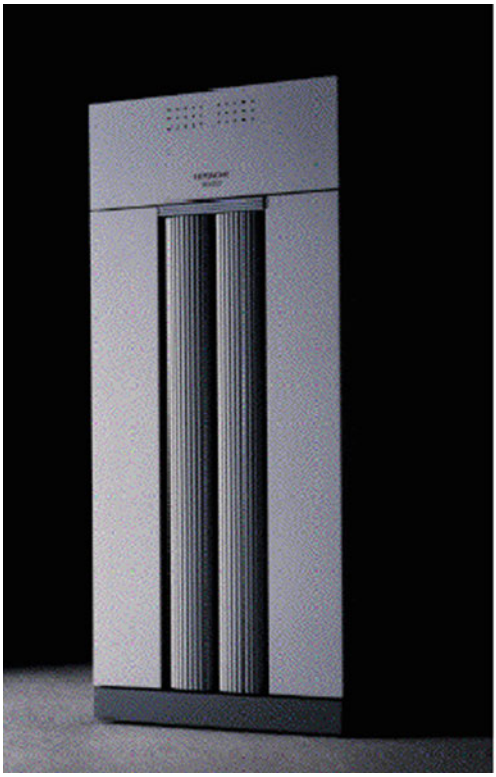


Fig. 5.65 3500/FT

In addition, the dependable technology cultivated here is succeeded to in HITAC 3500/FT (Fig. 5.65) and HIDIC RS90/FT, which employ quadruple processor redundancy (QPR) architecture for partitioning and modularity reasons. The QPR architecture has two lanes of self-checking BPUs and each BPU has duplicated microprocessors for fault detection. The QPR architecture is the most prospective solution to realize fault isolation between two lanes of self-checking BPUs, and tightly coupling between the duplicated microprocessors especially for on-chip redundancy.

5.12 Current Application Field: X-by-Wire

X-by-Wire is the technology to control automotive systems with computer aids, like Fly-by-Wire which controls airplanes with computer assistance. The technology computerizes the control of the automotives and aims to enable complex control such as vehicle stability control and improve safety and driving characteristic. Steer-by-Wire controls the steering and Brake-by-Wire controls brakes.

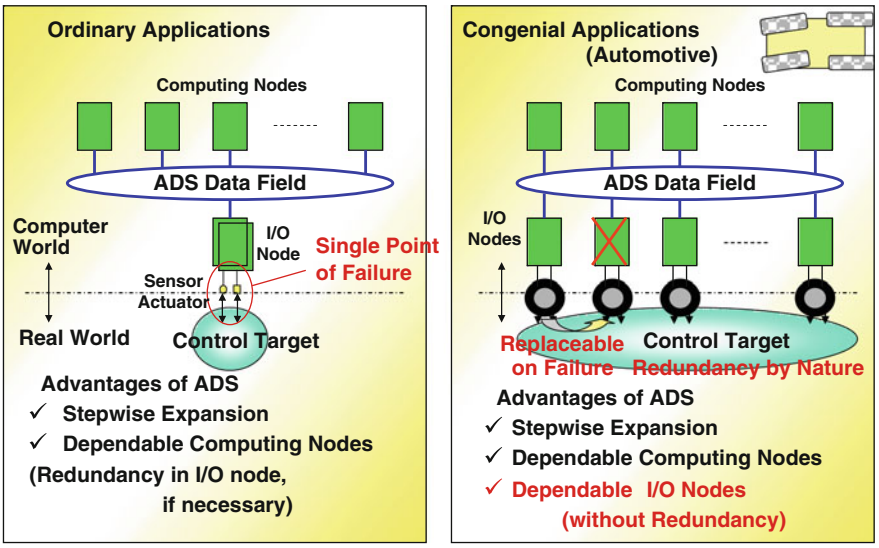


Fig. 5.66 Congenial applications for ADS

The authors produce electronic stability control system by X-by-Wire, which applied autonomous decentralized system experimentally and push forward on laboratory experiments. Applying to a range of industry field, autonomous decentralized system is used to enable replacement of computing nodes on their failure and improve their dependability. In addition, autonomous decentralized system is expected to enable replacement of input/output nodes closely tied to control objects on their failure and improve their dependability, if applied to congenial applications as shown in Fig. 5.66 [39, 40]. The control objects are distributed globally and having the redundancy by nature in the congenial applications such as automotive and

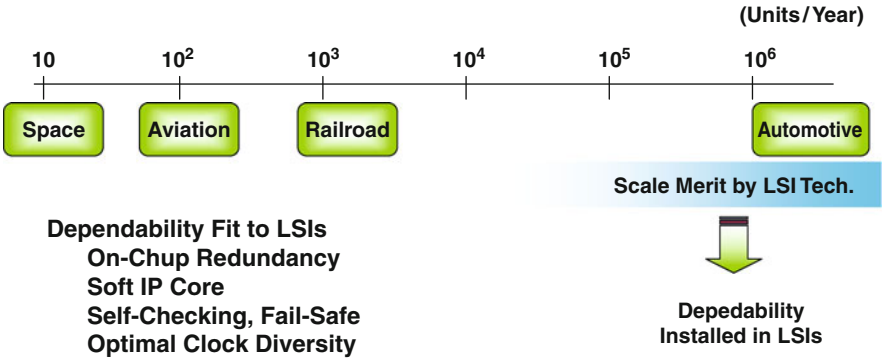


Fig. 5.67 Scale merit for X-by-Wire

aerospace control systems. For example, it is possible to control aircrafts with other control surfaces even if one of control surfaces fails. Also, it is possible to control vehicles with other three wheel brakes even if one of four wheels failed. If a braking force in the failed side is short, the braking force on both (right and left) sides is imbalanced, and the vehicle body tends to turn. But yaw rate sensor detects it and controller for electronic stability control system prevents it. In other words, dependability of input/output nodes can be improved without further explicit redundancy utilizing redundancy the control object possesses.

Cost is the most major problem for application to the automotive systems, but production scale of automotive systems is much larger than other application fields such as space, aviation, and rail-road fields as shown in Fig. 5.67. Therefore, we can expect cost reduction by a mass production effect with LSI technology in particular. So, the author has kept it in mind to develop dependable technologies that fit well to LSI technology, such as on-chip redundancy, self-checking/fail-safe logics, and optimal clock diversity.

References

1. F.P. Mathor, "On Reliability Modeling and Analysis of Ultrareliable Fault-Tolerant Digital systems," *IEEE Trans. Comput.*, Vol. C-20, pp. 1376–1382 (1971).
2. J. Losq, "A Highly Efficient Redundancy Scheme: Self-Purging Redundancy," *IEEE Trans. Comput.*, Vol. C-25, pp. 569–578 (1976).
3. N. Kanekawa et al., "Dependable Onboard Computer Systems with a New Method – Stepwise Negotiating Voting," *Proceedings of the 19th International Symposium on Fault-Tolerant Computing*, FTCS-19, pp. 13–19 (1989).
4. J.A. Katzman, "*A Fault-Tolerant Computing System*," Tandem Computers, Cupertino, CA, (1977). (Reprinted in D. P. Siewiorek, et al., "*The Theory and Practice of Reliable System Design,*" pp. 435–452, Digital Press, Bedford, MA, (1982).).
5. D. Taylor, et al., "Stratus" Chapter 10, "*Dependability of Resilient Computers*," BSP Professional Books, Oxford (1989).
6. A. Avizienis, et al., "The STAR (Self-Testing And Repairing) Computer: An Investigation of the Theory and Practice of Fault-Tolerant Computer Design," *IEEE Trans. Comput.*, Vol. C-20, No. 11, pp. 1312–1321 (1971).
7. J.H. Wensley, et al., "SIFT: Design and Analysis of a Fault-Tolerant Aircraft Control," *Proc IEEE*, Vol. 66, No. 10, pp. 1240–1254 (1978).
8. A.L. Hopkins, Jr. et al., "FTMP A Highly Reliable Fault-Tolerant Multiprocessor for Aircraft," *Proc IEEE*, Vol. 66, No. 10, pp. 1221–1239 (1978).
9. Freescale and Continental Collaborate on Multi-Core 32-bit Microcontroller for Electronic Braking Systems (16 October, 2007) http://media.freescale.com/phoenix.zhtml?c=196520&p=irol-newsArticle&ID=1063162.
10. First Automotive Dual Core, Floating Point MCUs from Texas Instruments Let Designers Innovate and Differentiate for Safety Critical Applications (3 November, 2008) http://focus.ti.com/pr/docs/preldetail.tsp?sectionId=594&prelId=sc08145.
11. Renesas Electronics, Providing the Car with Intelligence, http://www.renesas.com/applications/automotive/child_folder/inteview/i3car/intelligence.jsp.
12. Toshiba Announces Implementation of New Functional Safety Concept on MCU for SIL3 and ASILD Level Applications (18 January, 2010) http://www.toshiba-components.com/prpdf/5937E.pdf.
13. T.R.N. Rao, "*Error Coding for Arithmetic Processors*," Academic, New York, NY (1974).

14. T.R.N. Rao, et al., "*Error Control Coding for Computer Systems*," Prentice-Hall, Upper Saddle River, NJ (1989)
15. J. Wakerly, "*Error Detecting Codes, Self-Checking Circuits and Applications*," North Holland, Amsterdam (1978)
16. W.C. Carter, et al., "Design of Dynamically Checked Computers," *Inform. Process.*, Vol. 68, pp. 878–883 (1969).
17. D.A. Andeson, et al., "Design of Totally Self-Checking Circuits for m-out-of-n Codes," *IEEE Trans. Comput.*, Vol. 22, No. 3, pp. 236–269 (1973).
18. P. Tummeltshammer, et al., "Power Supply Induced Common Cause Faults – Experimental Assessment of Potential Countermeasures," *Proceedings of the 39th International Conference on Dependable Systems and Networks, Estoril, Lisbon, Portugal*, DSN2009, pp. 449–457 (2009).
19. H. Kopetz, et al., "TTP – A Time-Triggered Protocol for Fault-Tolerant Real-Time Systems," *Proceedings of the 23rd International Symposium on Fault-Tolerant Computing, Toulouse, France*, FTCS-23, pp. 524–533 (1993).
20. L. Chen, et al., "N-version Programming: A Fault-Tolerance Approach to Reliability of Software Operation," *Proceedings of the 8th International Symposium on Fault-Tolerant Computing*, FTCS-8, pp. 3–9 (1978).
21. A. Avizienis, "The N-version Approach to Fault-Tolerant Software," *IEEE Trans. Softw. Eng.*, Vol. SE-11, pp. 1491–1501 (1985).
22. B. Rendel, "System Structure for Software Fault-Tolerance," *IEEE Trans. Softw. Eng.,* Vol. SE-1, pp. 220–232 (1975).
23. N. Kurobane, "A Fault Tolerant Operating System using Essential Recovery Data (Japanese)," *Proceedings of ISPJ Congress, Sendai, Japan*, pp. 750–751 (1990).
24. J.C. Knight, et al., "A Large-Scale Experiment in N-version Programming," *Proceedings of the 16th International Symposium on Fault-Tolerant Computing, Vienna, Austria*, FTCS-16, pp. 165–170 (1986).
25. J.D. McGregor, et al., "Successful Software Product Line Practices," *IEEE Softw.*, Vol. 27, No. 3, pp. 16–21 (2010).
26. K. Mori, S. Miyamoto, and H. Ihara, "Proposition of Autonomous Decentralized Systems Concept (Japanese)," *Trans. IEE Jpn.,* Vol. 104-C, No. 12, pp. 303–310 (1984).
27. S. Miyamoto, K. Mori, and H. Ihara, "Autonomous Decentralized Control and Its Application to the Rapid Transit System," *Int. J. Comput. Ind.*, Vol. 5, No. 2, pp. 115–124 (1984).
28. H. Ihara, and K. Mori, "Autonomous Decentralized Computer Control Systems," *IEEE Comput.,* Vol. 7, No. 8, pp. 57–66 (1984).
29. F. Kitahara, et al., "The ATOS Tokyo Metropolitan Area Train Traffic Control System," *HITACHI Rev.*, Vol. 46, No. 2, pp. 67–72 (1997). http://www.hitachi.com/rev/1997/revapr97/rev205.htm.
30. T. Takano, et al., "In-orbit Experiment on the Fault-Tolerant Space Computer Aboard the Satellite "Hiten," *IEEE Trans. Reliab.*, Vol. 45, No. 4, pp. 624–631 (1996).
31. N. Kanekawa, et al., "High-Speed and Transparent Fault-Tolerance by Intra-Board Fault-Masking (in Japanese), *Trans. IEE Jpn.*, Vol. 114-D, No. 9, pp. 903–909 (1994).
32. N. Kanekawa, et al., "Self-Checking and Fail-Safe LSIs by Intra-Chip Redundancy," *Proceedings of the 26th International Symposium on Fault-Tolerant Computing, Sendai, Japan*, FTCS-26, pp. 426–430 (1996).
33. Jean Arlat, et al., "Dependability of Railway Control Systems" *Proceedings of the 26th International Symposium on Fault-Tolerant Computing, Sendai, Japan*, FTCS-26, pp. 150–155 (1996).
34. Jean Charles Fabre, et al., "Saturation: Reduced Idleness for Improved Fault-Tolerance," *Proceedings of the 18th International Symposium on Fault-Tolerant Computing, Tokyo, Japan*, FTCS-18, pp. 200–205 (1988).
35. N. Kanekawa, "Dynamic Autonomous Redundancy Management Strategy for Balanced Graceful Degradation," *Fault-Tolerant Parallel and Distributed Systems*, Dhiraj Pradhan and Dimiter Avresky ed. *IEEE, College Station, TX, USA*, pp. 18–23 (1994).

36. N. Kanekawa, et al., “Fault Detection and Recovery Coverage Improvement by Clock Synchronized Duplicated Systems with Optimal Time Diversity,” *Proceedings of the 28th International Symposium on Fault-Tolerant Computing, Munich, Germany*, FTCS-28, pp. 196–200 (1998).
37. K. Shimamura, et al., “*A Fail-Safe Microprocessor Using Dual Synthesizable Processor Cores*,” *Seoul, Korea*, AP-ASIC, pp. 46–49 (1999).
38. K. Shimamura, et al., “*A Single-Chip Fail-Safe Microprocessor with Memory Data Comparison Feature*,” *Riverside, CA, USA*, PRDC 2006, pp. 359–368 (2006).
39. K. Sakurai, et al., “Dependable and Cost-Effective Architecture for X-by-Wire Systems,” *FISITA 2008 World Automotive Congress September-08, Munich, Germany*, Paper No. F2008-05-04 (2008).
40. K. Sakurai, et al., “Membership Middleware for Dependable and Cost-Effective X-by-Wire Systems,” *SAE 2008 World Congress April-08* Technical Paper No. 2008-01-0478.

Chapter 6
Challenges in the Future

The three major factors, soft-error, electromagnetic compatibility, and power integrity, that govern dependability of the electronic systems in addition to conventional hardware failure are brought together in one hard-cover book, to the best of the authors' knowledge, for the first time in the history of silicon industry. Integration of these factors with high-level mitigation of failures to dependable electronic systems turned out to be very challenging efforts themselves.

Simultaneous interactions of these noise sources, for example, may deteriorate the single-ended mitigation techniques originated from these three independent fields. Such chaotic situation will be even worse by further scaling down, power-lowering, and speed-up of semiconductors and relevant components. To balance the mitigation technique or to make synergetic effects to develop, for example, common-mode or all-in-one mitigation techniques, very high level challenges are required in the future. The following may be a part of such challenges:

- Capture or detection faulty signals from very-noisy power supply line and diagnosis of the signal.
- Design techniques to minimize the adverse effects from the three major noise sources while maximizing system performance.
- Valid and effective fault recovery schemes with very low power, area, and cost penalties [1, 2].
- Fault aware-automatic logic circuit and layout synthesis technique
- Noise protection and isolation techniques from power supply and global control lines.
- Fault-tolerance of power supply.
- Mitigation of human factors such as human error and intentional attack or tampering.
- Discrimination between transient faults and intermittent faults; preventive maintenance will be possible if the discrimination between transient faults and intermittent faults is realized based on statistical analysis because intermittent fault may be a precursor of permanent fault or hardware failure. The occurrence of

---

By all

N. Kanekawa et al., *Dependability in Electronic Systems*,
DOI 10.1007/978-1-4419-6715-2_6, © Springer Science+Business Media, LLC 2011

transient faults follows a Poison Distribution besides the occurrence of transient faults does not.
- Mitigation technologies for dependability in currently emerging applications such as on-chip redundancy [3], x-by-wire [4, 5], cloud computing, surgical micro-robot, and many-core processor.
- Mitigation of device parameter variation and fluctuation mainly caused by spatial distribution variation of dopant atoms with finer process size [6].

References

1. E. Ibe, "Novel SER Standards: Backgrounds and Methodologies," *ICICDT, Grenoble, France, June 2–4, 2010,* pp. 203–207 (2010).
2. N. Carter, "Cross-Layer Reliability," "*SELSE6, Stanford University," Stanford, CA, March 23, 24* (2010).
3. N. Kanekawa, et al., "Self-Checking and Fail-Safe LSIs by Intra-Chip Redundancy," *Proceedings of the 26th International Symposium on Fault-Tolerant Computing, Sendai, Japan*, FTCS-26, pp. 426–430 (1996).
4. K. Sakurai, et al., "Dependable and Cost-Effective Architecture for X-by-Wire Systems," *FISITA 2008 World Automotive Congress September-08, Munich, Germany*, Paper No. F2008-05-048 (2008).
5. K. Sakurai, et al., "Membership Middleware for Dependable and Cost-Effective X-by-Wire Systems," *SAE 2008 World Congress April-08,* Technical Paper No. 2008-01-0478.
6. B. Becker, et al., "DFG-Projekt RealTest – Test und Zuverlässigkeit nanoelektronischer Systeme (DFG-Project – Test and Reliability of Nano-Electronic Systems)". *IT – Inform. Technol.,* Vol. 48, No. 5, pp. 304–306 (2006).

Index

N. Kanekawa et al., *Dependability in Electronic Systems*,
DOI 10.1007/978-1-4419-6715-2,