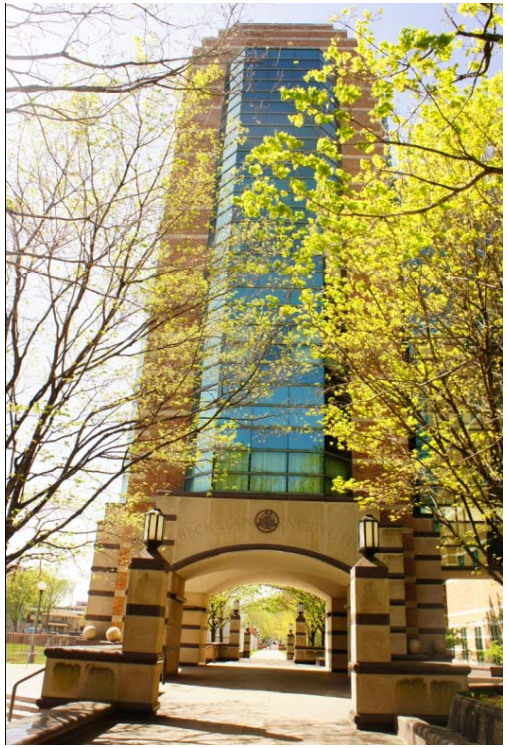
国際会議調査報告（1）

2012 IEEE Workshop on Silicon Errors in Logic-System Effects (SELSE VIII)

日立製作所横浜研究所生産技術センタ　伊部英史

イリノイ大学構内で見つけた人面木

パネル討論会場



イリノイ大学構内風景

SELSE VIII 概況

■SELSEは２００４年からIntel主催で論理回路のソフトエラーに特化して始まったWorkshopであるが、最近はサーバ、ルータ、車載MCU、スパコンなど電子機器のソフトエラー起因の障害が主対象となっている。特に、アメリカ、ヨーロッパの業界の大きな動きに関連する発表が多く、会場での議論が非常に活発なのが特徴。国内からは、日立のほか、九州大学からCRESTの成果発表があった。 尚、今年からGeneral Chair（Alan Wood氏、Oracle)の要請を受けて伊部がSELSEのプログラム委員に就任。

■車載機器の機能安全に関し、昨年１１月１４日Part10を除いて発行され、自動車業界に大きなインパクトとなると見られている。SELSE８でも冒頭のKeynote speechがISO26262向けのサービスを展開しているYogitechの共同経営者Marianiから”Designing Safe and Available Integrated Circuits According to Functional Safety Standard"と題する発表があった。

■日時：2012年3月27,28日

■場所：イリノイ大学Champaign-Urbana　ｷｬﾝﾊﾞｽ

SELSE VIII セッション概況(Day 1)

番号	セッション名称	トピックス（紹介）
I	Keynote	・ISO26262
II	Fault Analysis （伊部）chair	・GPUへのFault Injection（IBM） ・車載ブレーキシステムへの照射実験(iRoc) ・ネットワークプロセッサのSEU（Cisco）
III	Technology	・22nm Tri ゲートデバイスのSEU(Intel） ・FPGAのSEU（） ・RTN（Random Telegraph Noise) ・ミュー中間子、電子、低エネルギー中性子によるフォールトベースの上限設計（日立）
IV	Panel Discussion	Reliability Requirements of Large Scale Data Centers Panelists: Dr. Sarita Adve (UIUC) Dr. Al Geist (Oak Ridge National Laboratory) Dr. Ravi Iyer (UIUC) Dr. Thomas Wenisch (University of Michigan)
V	Keynote（Dr. Eugene Normand)	Single Event Effects in Avionics, Implications for SEE on the Ground

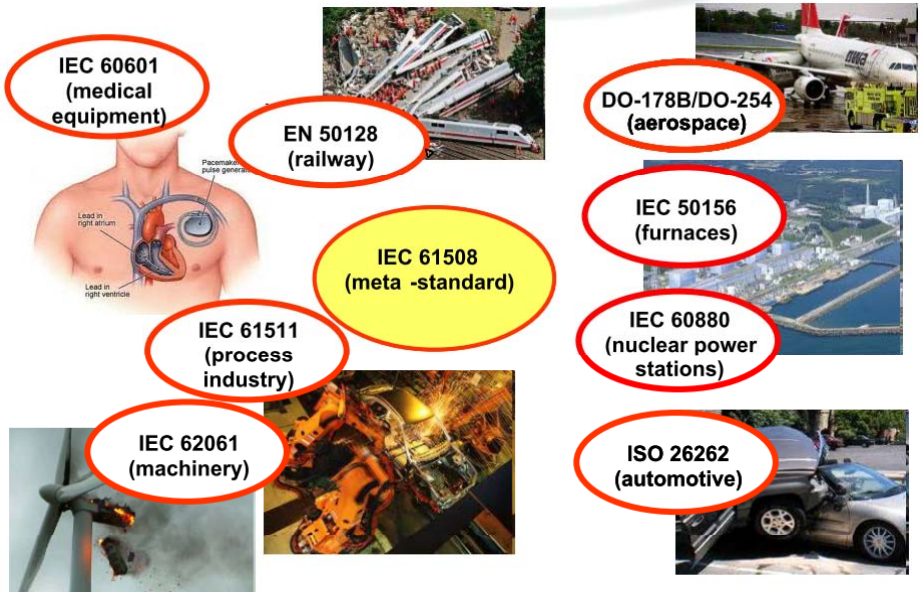
SELSE VIII セッション概況(Day 1)

番号	セッション名称	トピックス（紹介）
VI	Keynote（ Dr. Al Geist (Oak Ridge National Laboratory) ）	Exascale Monster in the Closet
VII	Tools and Mitigation Techniques	・自動di/dtストレスマーク生成 ・ECC
VIII	Large Scale Case Studies	・DRAMのフィールドエラー
IX	Poster Session	・順序回路のソフトエラー伝搬解析（九州大学） ・レジスターの障害率予測法　他
X	Software Based Mitigation	・間欠エラー診断法 ・並列演算のエラー検出 ・ソフトエラー対策のコスト低減

Session I （Keynote).Designing Safe and Available Integrated Circuits According to Functional Safety Standard（1）

発表者	発表組織
R. Mariani	Yogitech
要旨	車載機器の機能安全に関し、昨年１１月１４日Part10を除いて発行され、自動車業界に大きなインパクトとなると見られており、国内でもJasperなど関連した動きがある。SELSE８でも冒頭のKeynote speechがISO26262向けのサービスを展開しているYogitechの共同経営者Marianiから発表があった。

Functional safety standards



About safety integrity levels....

Higher safety level

IEC 61508	ISO 26262	Application examples
SIL 4	-	Railway signal control
SIL 3	ASIL D	Brake-by-wire, EPS, Motor control, etc.…
	ASIL C	Battery management for hybrid vehicle cars
SIL 2	ASIL B	Automotive dashboard Industrial robots
SIL 1	ASIL A	Rear lights

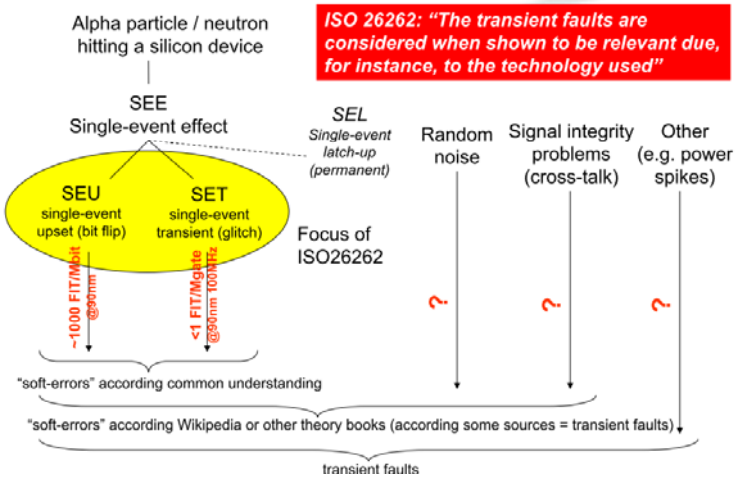
For example, ASILD means ≥ 99% faults must be detected and the probability of violation of safety goal due to HW random failures shall be less than 10 FIT (1 FIT = 1 failure in 1 billion of hours)

Session I.Designing Safe and Available Integrated Circuits According to Functional Safety Standard（2）

Fault models in ISO 26262 (excerpt)

Element	Analyzed failure modes for 60/90/99% DC		
	Low (60 %)	Medium (90 %)	High (99 %)
ALU - Data Path	Stuck-at	Stuck-at at gate level	d.c. fault model Soft error model (for sequential parts)
Registers (general purpose registers bank, DMA transfer registers…), internal RAM	Stuck at	Stuck-at at gate level Soft error model	d.c. fault model including no, wrong or multiple addressing of registers Soft error model
Address calculation (LSU, DMA addressing logic, memory and bus interfaces)	Stuck-at	Stuck-at at gate level Soft error model model (for sequential parts)	d.c. fault model including no, wrong or multiple addressing Soft error model (for sequential parts)
Interrupt handling	Omission of or continuous interrupts	Omission of or continuous interrupts Incorrect interrupt executed	Omission of or continuous interrupts Incorrect interrupt executed Wrong priority Slow or interfered interrupt handling causing missed or delayed interrupts service
Control logic (Sequencer, coding and execution logic including flag registers and stack control)	No code execution Execution too slow Stack overflow/underflow	Wrong coding or no execution Execution too slow Stack overflow/underflow	Wrong coding, wrong or no execution Execution out of order Execution too fast or too slow Stack overflow/underflow
Configuration Registers	-	Stuck-at wrong value	Corruption of registers (soft errors) Stuck at fault model
Other sub-elements not belonging to previous classes	Stuck-at	Stuck-at at gate level	d.c. fault model Soft error model (for sequential part)

About transient faults



■ISO26262は電子機器の総合機能安全規格IEC61508が母体となっており、自動車独自の安全指標をASIL A-Dまで規定しているが、IEC61508の最高の安全対策が要求されるレベルSIL4（1FIT/機器）に該当するランクはなく、ASIL D（10FIT/台）が最高である。但し、近年車載CPUは100個/台を超えるケースもあるので、IEC61508に比べ緩い規格とは言えない。

2.1 Statistical Fault Injection-Based Analysis of a GPU Architecture

発表者	発表組織
N. Farazmand,	NorthEastern University
要旨	最近では、高速並列演算機能に着目し、本来の画像処理でなく、スパコンのシミュレーションにGPU（Graphic Processing Unit）を採用するケースが増えているが、これがソフトエラーに弱いことも問題視されており、一般講演（Ujiv. of British Columbia, Canada)でもGPUへのFault Injectionに関する報告があった。

■グラフィックプロセシングユニット（GPU）が画像処理以外の目的で広く使われるようになってきている（GPGPU)。信頼性の低いGPUを使って高信頼性の計算をすることもこれに該当する。性能や、ハードウェアのサイズなどにインパクト無くGPUの信頼性を担保するにはGPUのハードウェアの慎重な解析が不可欠である。本論文では、CPUに無かった、GPUハードウェア構造のArchitectural Vulnerability Factor（AVF）の新しい側面を提示する。 レジスタファイル（REG)、アクテイブマスクスタック（AMS）やローカルメモリ（MEM)への統計的フォールトインジェクションにより、GPUに特有のAMSが40% AVF-utilのフォールト耐性要求を持ち、特に脆弱であることが分かった。その一方でREGとMEMのAVF/AVF-utilは、それぞれ6%/15%、1%/3%で通常のCPUよりも低いことが分かった。

・AVFは注入されたフォールトがFailure(装置障害）に到る比率。CPUではREGで15%、キャッシュメモリで25%が普通。

・AVF-utilはbenchmarkによって実際に使用されている領域を分母にとったもの。

・実験にはAMDのEvergreen ファミリのGPU（Radeon HD 5870 GPU)を使用。フォールトインジェクションのシミュレータとしてMulti2Simを用いた。

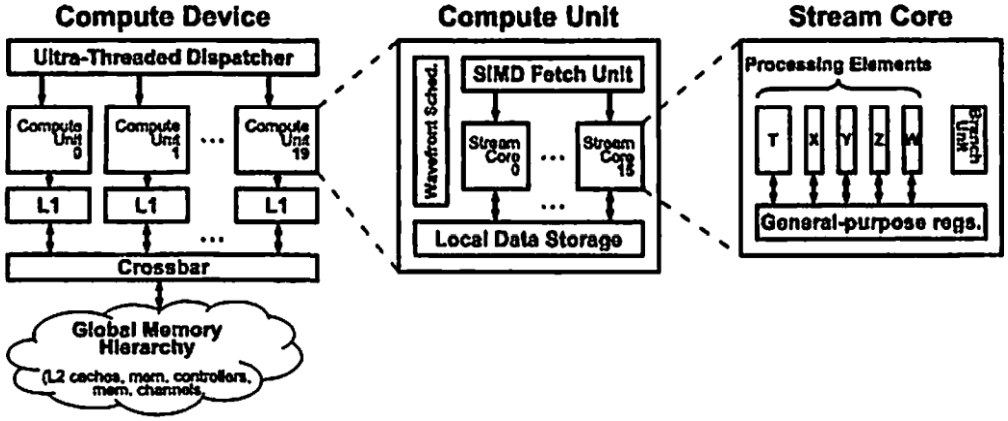


図1 Radeon HD 5870 GPUのブロック図

表1 AVFの実験結果(utilは使用された部位のみの結果）

罫線がずれている

	REG(%)		AMS(%)		MEM(%)		MAX occupancy (%)		
Benchmark	AVF	AVF-util	AVF	AVF-util	AVF	AVF-util	REG	MEM	AMS
BitonicSort	0.04	25.00	0.00	0.00	N/A	N/A	0	0	3
DwtHaar1D	1.13	10.17	0.00	0.00	0.50	4.17	50	50	9
RecursiveGaussian	2.08	5.81	0.36	16.98	0.00	0.00	78	25	9
ScanLargeArrays	3.91	14.50	0.02	33.33	0.48	4.23	63	25	9
MatrixMultiplication	20.30	32.59	0.10	71.43	3.75	3.84	63	100	13
SobelFilter	19.36	22.50	2.86	24.78	N/A	N/A	75	0	9
DCT	3.68	9.01	0.72	53.73	0.10	1.74	44	6	6
URNG	0.18	0.88	0.00	0.00	N/A	N/A	19	0	3
Average	6.34	15.06	0.58	40.05	0.97	2.80	49	23	8

2.2 Evaluation of Device-Level Irradiation Effects in a 32-bit Safety Micro Controller for Automotive Braking Applications

発表者	発表組織
D. Baumeister	Continental AG, Freescale
要旨	自動車のブレーキングシステム（アンチロックや姿勢制御）の障害が個別の機器のソフトエラー率の積み重ねでは実態に即さない高い障害率になることから、二重系でオンチップモニタで異常を検知しながら、ロックステップで動作するブレーキングシステムにタイヤからの回転速度の模擬信号を入れながら、α線（Th232)や中性子線（ロスアラモス国立研）での照射実験を行った結果。

■種々のモードを観測し、障害発生率の評価値は市場に近い結果が得られた。
■また、車載機器にはオンチップモニタを標準装備すべきというメッセージの発信もあった。
■中性子線に対する結果はProceedings中になし。当日発表の有無は記憶なし。

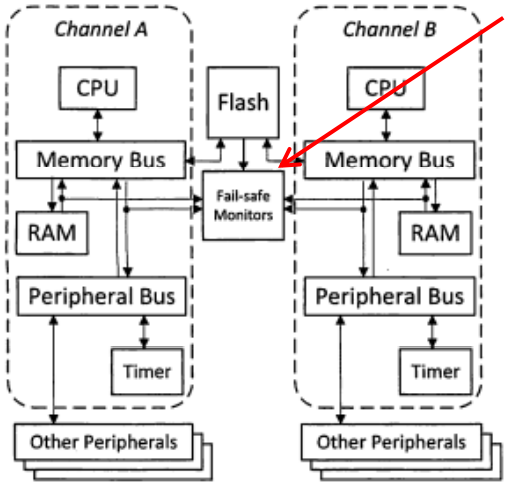


図1 Dual チャネル ロックステップMCUの基本構成(90nmプロセス)

＊CAN：Controller Area Network、Boschの車載LAN規格

オンチップモニタで以下を検知
- dual-channel synchronicity error for RAM access
- dual-channel synchronicity error for peripheral access
- Flash ECC error

表1 α線による障害モード別発生率
（１１FITに相当）

	Run1	Run2	Run3	Sum
EEPROM Dumps	31	47	53	
Red. Timebase Violation	2	40	43	85
Reset Source Violation	20	30	36	86
Dual-channel Error	5	11	12	28
Flash ECC Error	0	2	1	3
Wheel-Speed Processing Error	0	0	1	1
Flash CRC Error	0	1	0	1
CAN Message Plausibility Error	0	2	0	2
No Error recorded	4	0	1	5
Total	**31**	**86**	**94**	**211**

2.3 Case Study of SEU Effects in a Network Processor（1）

発表者	発表組織
A. Evans	Cisco Systems,　TIMA Laboratory
要旨	フリップフロップのソフトエラーの制御は高信頼性のシステム設計に本質的に重要。産業規模でのタイミング、論理、機能的マスキング効果の正確な評価はチャレンジングである。本論文では、40nmネットワークプロセス用ASICから抽出した3つの設計ブロック（epsilon、gamma、omega）50万個のフリップフロップのSEU効果の詳細解析結果を紹介する。機能的テストベンチを効率的なフォールトインジェクションシミュレーション環境に変換するための加速技術を紹介する。Derating係数を計算し、統計解析により、信頼性区間を検証する。フリップフロップのSEUがある中で、マスキング効果を統合し、特定の設計のシステムの挙動を予測する。提案手法は普遍的に使用でき、マイクロプロセッサのような特定のアプリケーションに限定されるものではない。

表1　設計ブロック

Name	Function	Number Flops
epsilon	Output data-path	102 559
gamma	On-chip packet storage	341 615
omega	Packets re-assembly from DRAM	184 552

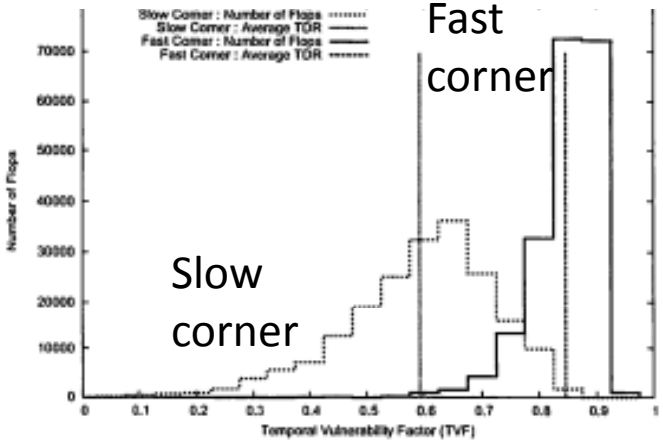


図1　FFのTiming Vulnerability Factor(TVF)の分布計算値（Omega）

表2　SEU効果の分類

Category	Sub-Category	System Outage	Description
Masked	Logically	None	Upset state is overwritten after one or more clocks.
	Functionally	None	Upset state remains but has no functional effect.
Corrected		None	Error is corrected (e.g. ECC).
Detected	Explicitly	Medium	Explicit mechanism detected the error (e.g. parity).
	Indirectly	High	Error detected due to a side-effect. (e.g. FIFO overflow).
Silent	Minor	Low	Operation is silently affected, but impact is contained (e.g. single corrupted packet).
	Major	Unknown	Internal state is affected causing unpredictable effects (e.g. linked list corruption).
	Lockup	Unknown	Packet traffic ceases to flow.

2.3 Case Study of SEU Effects in a Network Processor（2）

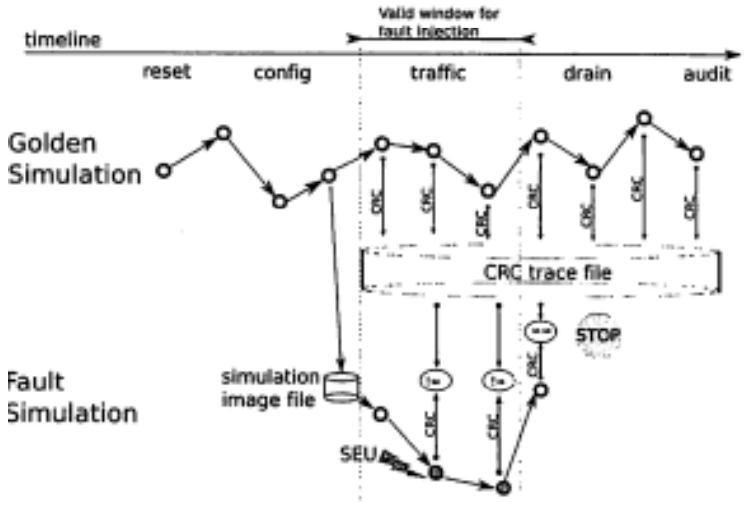


図2　チェックポイントとCRCマッチングを有したテストベンチ

表3　シミュレーション中のCPU使用率

Category		Epsilon		Gamma		Omega	
		Runs	CPU %	Runs	CPU %	Runs	CPU %
Fail		2102	26.5	1536	32.4	3312	33.8
Pass	Matched	7148	32.6	7439	25.0	4858	10.8
	No Match	750	40.9	1025	42.6	1427	55.4

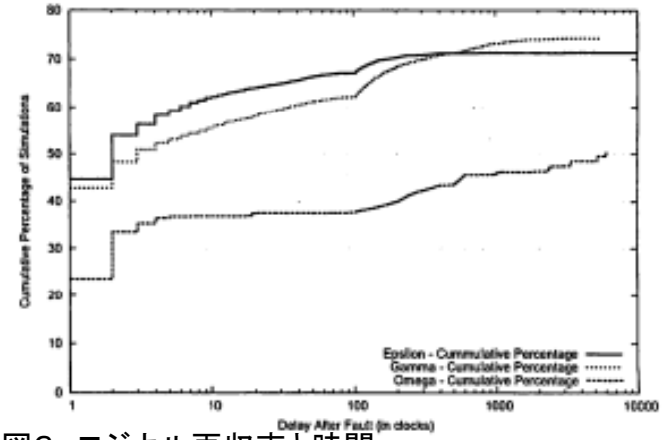


図3　ロジカル再収束と時間

表4　SEU効果の結果

Category	Sub-Category	Epsilon	Gamma	Omega
Masked	Logically	71.5 ± 0.8	74.4 ± 0.9	60.7 ± 3.2
	Functionally	7.5 ± 0.5	10.3 ± 0.6	13.9 ± 2.2
Corrected		0.9 ± 0.2	0.6 ± 0.2	0.8 ± 0.6
Detected	Explicitly	0.1 ± 0.1	6.1 ± 0.5	6.7 ± 1.6
	Indirectly	13.1 ± 0.6	1.0 ± 0.2	0.3 ± 0.4
Silent	Minor	5.6 ± 0.4	3.0 ± 0.3	11.6 ± 2.1
	Major	1.3 ± 0.2	4.7 ± 0.4	4.1 ± 1.3
	Lockup	0.0 ± 0.0	0.0 ± 0.0	2.0 ± 0.9

表5　重大な停止時間を招いた割合

Name	Percentage SEUs Producing a Serious Impact
epsilon	1.2 %
gamma	6.5 %
omega	5.2 %

<結論>

■膨大な数のフリップフロップを使用している設計ブロックへのフォールトインジェクションの有効性を検証。

■加速手法の導入により、適正な時間範囲内でシミュレーション実行可。

■ある信頼性レベルに対してより計算時間や、計算のケース数を低減できるより強力な手法の開発、クリテイカルなフリップフロップの同定法の本手法への導入を進める。

3.1 Soft Error Susceptibilites of 22nm Tri-Gate Devices

発表者	発表組織
N. Seifert	Intel
要旨	22nm　high-kメタルゲートのバルクとTri-ゲートメモリと論理回路についての陽子照射によるSEU断面積(CS)の測定結果を報告する。

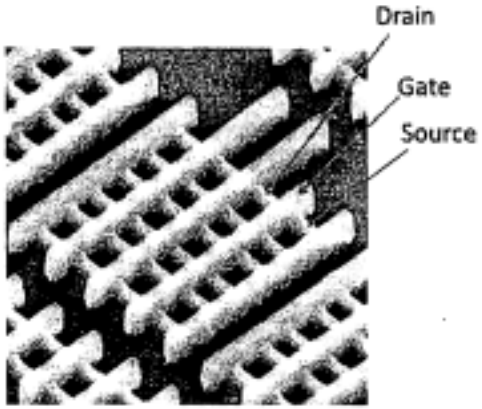


図1　Intelの22nmTri-ゲートトランジスタ(寸法明記なし。ドレイン、ゲート、ソースとも幅数nmと推測。チャネル6本(それぞれがFinFET構造)で駆動力と動作安定性確保)

■陽子線はIndian University Ctclotron Facilty (IUCF)利用。陽子線の試験結果から地上の中性子環境のエラー率を求める手法を開発(別途詳細報告)
■フリップチップ6T　SRAMが供試体・
■　順序回路はチェーンを形成して試験
■　組み合わせ論理回路は50MHz～2GHzの動作条件で試験(結果の表示なし)

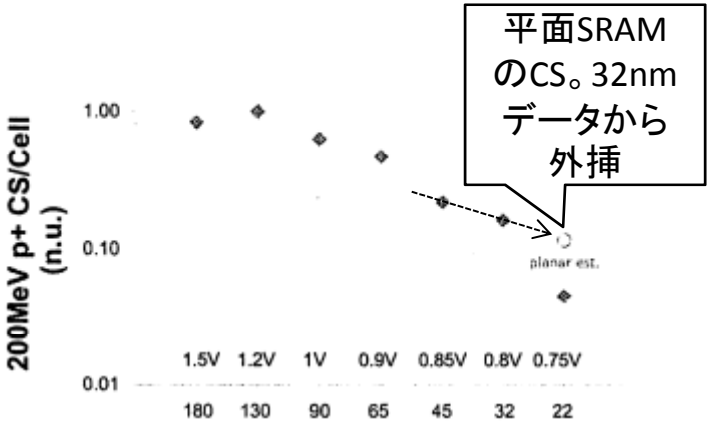


図2　6T SRAMの結果。 22nmの下のデータがTrigate。平面構造よりx3.5耐性が良いとしている。

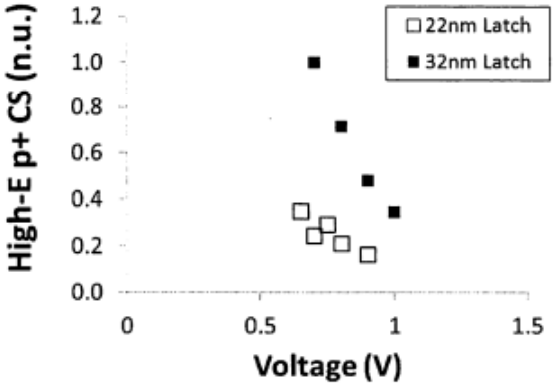


図3　32nm(平面構造)と22nmラッチ(Trigate)のCSの電圧依存性

3.2 A Tale of Two Test Chips : 28nm Configuration RAM and Dual-Port RAM

発表者	発表組織
A. Lesea	Xilinx
要旨	略

■TSMCの28nmHPL（High Performace, Low power)プロセスを用いたCRAMとBRAMのソフトエラー耐性をα線（Th233　フォイル、LANSCE中性子線、UC　Davis　Crocker　68MeV陽子線照射により評価した。 CRAMは2.83Mbitで、2fF~6fFの静電容量を与している。BRAMは1.187Mbit。

■ α線の試験ではCRAMのSEU断面積は$4.46\times10^{-11}cm^2$/bit。BRAMは$6.46\times10^{-11}cm^2$/bit。ULA材料を想定してα線によるエラー率は、CRAMで40FIT/Mb、BRAMで100FIT/Mbと推測。フランスのRustrel地下施設での測定結果はこの推測値よりはるかに低い。
■陽子の照射試験では、CRAMは$7.12\times10^{-15}cm^2$/bit、（中性子12.9n/cm^2/hで置き換えられるとすると、92FIT/Mb）、BRAMは$8.42\times10^{-15}cm^2$/bit（109FIT/Mb)。
■中性子の照射試験では、CRAMが$7.89\times10^{-15}cm^2$/bit（102FIT/Mb）、BRAMが$8.12\times10^{-15}cm^2$/bit（105FIT/Mb)。

（（伊部）注：著者は単独で、単位の表記もいい加減。ちょっと信頼性に欠ける発表の印象。FPGAの陽子照射実験は宇宙関係で多くなされているので整合性チェック可。）

3.3 Fault-Based Reliable Design-On-Upper-Bound of Electronic Systems for Muons,Electrons and Low Energy Neutrons

発表者	発表組織
E. Ibe	日立製作所
要旨	これまで電子機器のエラー、障害は高エネルギー中性子が主因であったが、近年、配線加工工程で混入するB-10と低エネルギー中性子の反応や、地上のミュー中間子、福島事故の放射能などが、電子機器の障害になりうることが懸念されており、高エネルギー中性子含め、考えられる全ての地上の放射線を解析できるプラットフォームが必要であることを指摘、旧（生研）開発のソフトエラーシミュレータCORIMSを拡張し、Fault（収集電荷量）の分布について地上のスペクトルに基づいて結果を示した。 ミューオンは既に影響が出ている可能性があること、福島原発事故の放射能は現在の電子機器に対しては問題ないこと、低エネルギー中性子は高エネルギー中性子に比べて影響は小さいが十分の一程度には大きくなりうることなどを初めて定量的に示した。 低エネルギー中性子の影響評価に特に会場の関心が集中した。

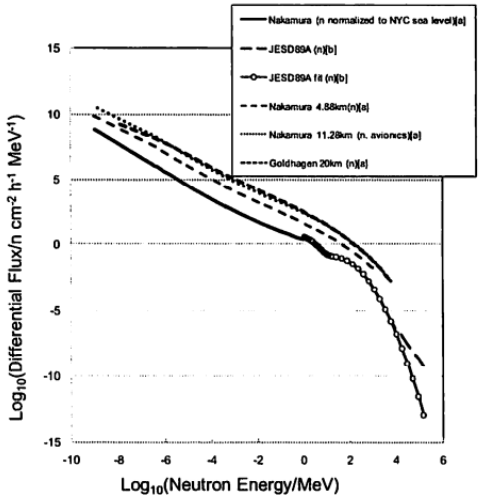


図1　全エネルギー範囲の中性子スペクトル

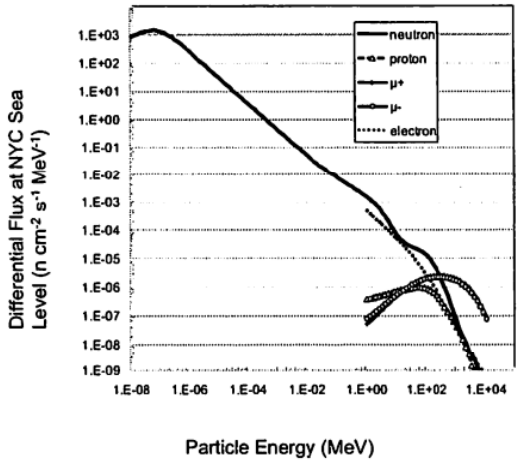


図2　地上の粒子線スペクトル（EXPACSによる）

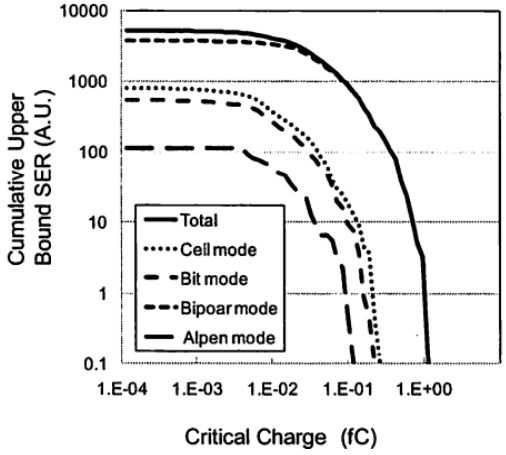


図3　地上のミューオンによる累積上限SER

4. Panel Discussion:

Reliability Requirements of Large Scale Data Centers

発表者	発表組織
Dr. Sarita Adve	UIUC
Dr. Al Geist	Oak Ridge National Laboratory
Dr. Ravi Iyer	UIUC
Dr. T. Wenisch	University of Michigan
要旨	Data CenterのHardwareの信頼性を如何に考えるか(”Reliability Requirements of Large Scale Data Centers“)についてパネル討論が実施された。イリノイ大学のAdve教授、Iyer教授、ORNLのGeist氏、ミシガン大学のWenisch教授がパネリストで、Googleのクラウドコンピュータの Outageが年々著しく増加していることや、1ビットのサーバ間の情報(communication)伝達エラーでAmazonのクラウドサーバが8時間停止した例や、大きなサーバシステムのMTBFが10時間以下であること、Bank of America(HPのnon-stop serverを3系統使用)のサーバシステムなどを例に挙げて議論を展開した。 全体としての結論が今一つ見えなかった。

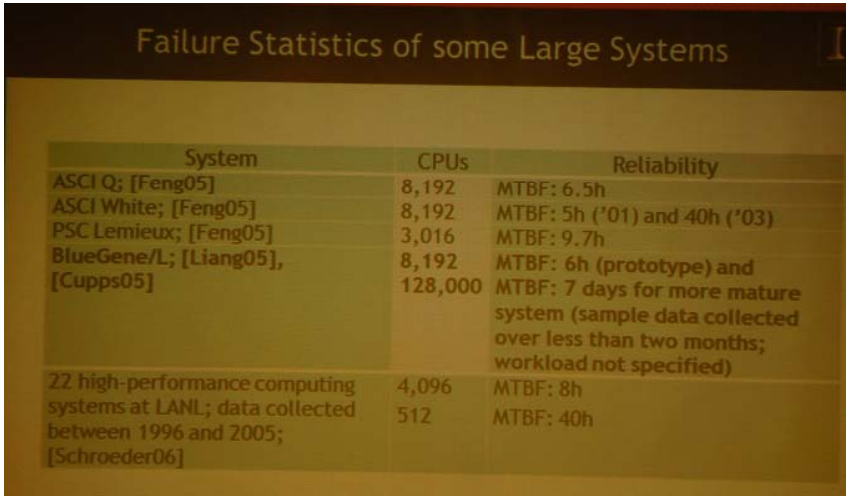


図1　大規模システムの障害事例

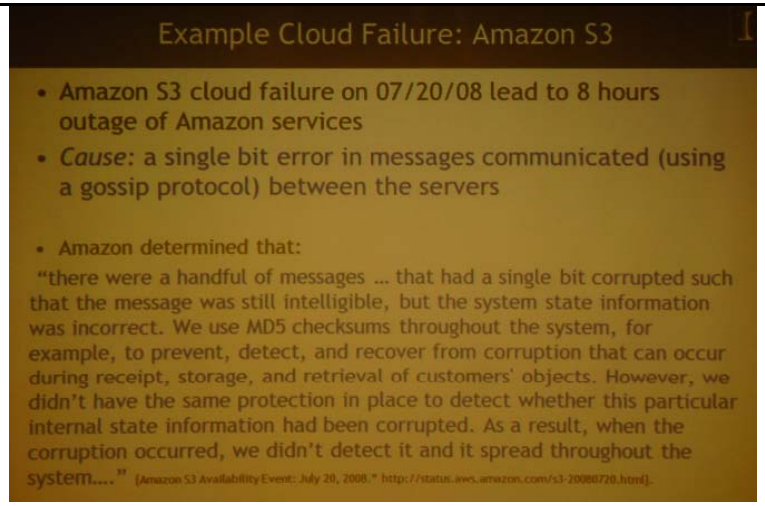


図2　Amazonのクラウドサーバの障害例

6.Exascale Monster in the Closet

発表者	発表組織
A. Geist	Oak Ridge National Laboratory（Key note）
要旨	米国では2008年からExaScale Initiativeという「京」より二桁高速の10の18乗FLOPS/sのスパコンを開発する国家プロジェクトが進行中であるが、今回SELSEとしては初めてExascale Projectに特化したKeynote Speech（"Exascale Monster in the Closet"）がORNLのGeist氏からあった。

■中国のスパコンに抜かれる前の世界最速のスパコンJaguarの実態を例に、128PBのメモリを持つExascaleではECCで対応できないダブルビットエラーが4分に一回でるため、IBMのchipkill（同一のワードビットをﾓｼﾞｭｰﾙ間に分散する）技術でも対応が難しい
■Jaguarで採用しているCheckpointing-Rollbackでも修復する時間よりエラーが発生する間隔の方が短くなるので、別な手法の開発が必要である
■検出できないエラー（Silent Data Corruption）の問題が一層深刻になること
■フォールトに耐えるソフトウェア（パラダイムシフト）の開発が必要と結論した。

SELSE VIII まとめ

- ISO26262の公開に伴い、車載機器関係の発表が増加傾向。
  ISO26262の上位規格であるIEC61508（機能安全全般）に比べ、ソフトエラーのウェイトが非常に大きくなっていることなど、相違が目立つ。
- データセンタなど、大規模システムの信頼性の実態や、今後の推移を懸念する議論が一層拡大。ソフトウェアのパラダイムシフトが必要であるという議論が発展。
- FinFET、TriGateなど、新デバイスへの展開も継続。
- FPGAのCRAMとBRAMのSEUの測定結果の報告あり。
- Fault-Injection法が試験法として定着の感あり。
- 日立から、提案中のInter-LAyer Built-In Reliability (LABIR)、DOUB（Design On Upper Bound)の発展形の一例として、収集電荷量に基づくUpper Bound SERの解析結果をミューオン、電子（ベータ線）について紹介。ベータ線の影響は当面心配ないが、原理的には否定できないと結論。