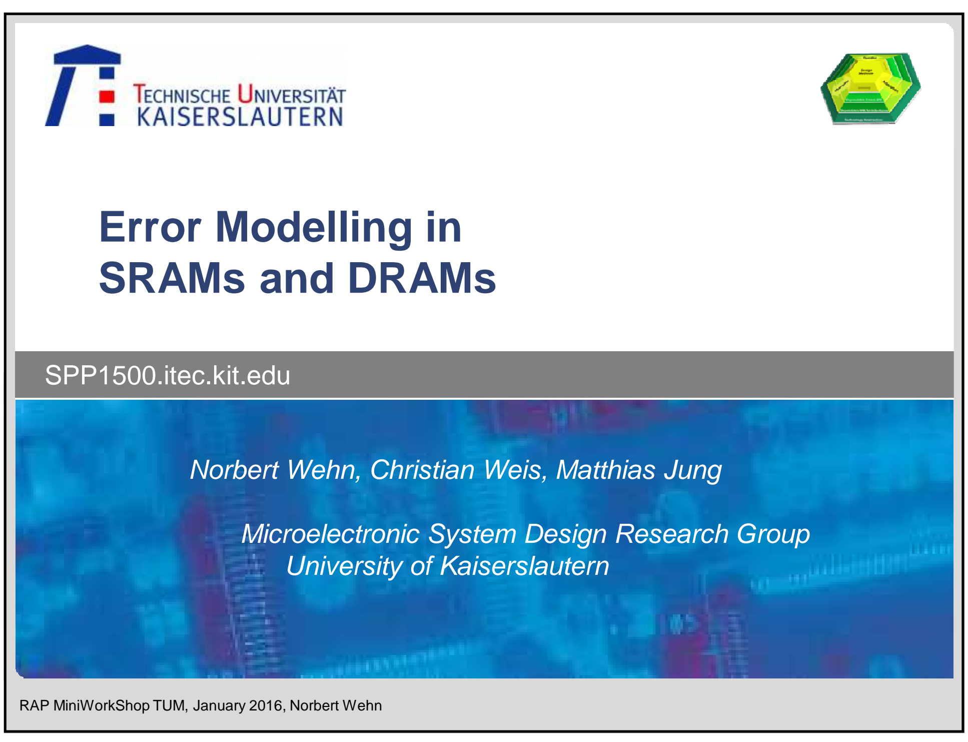
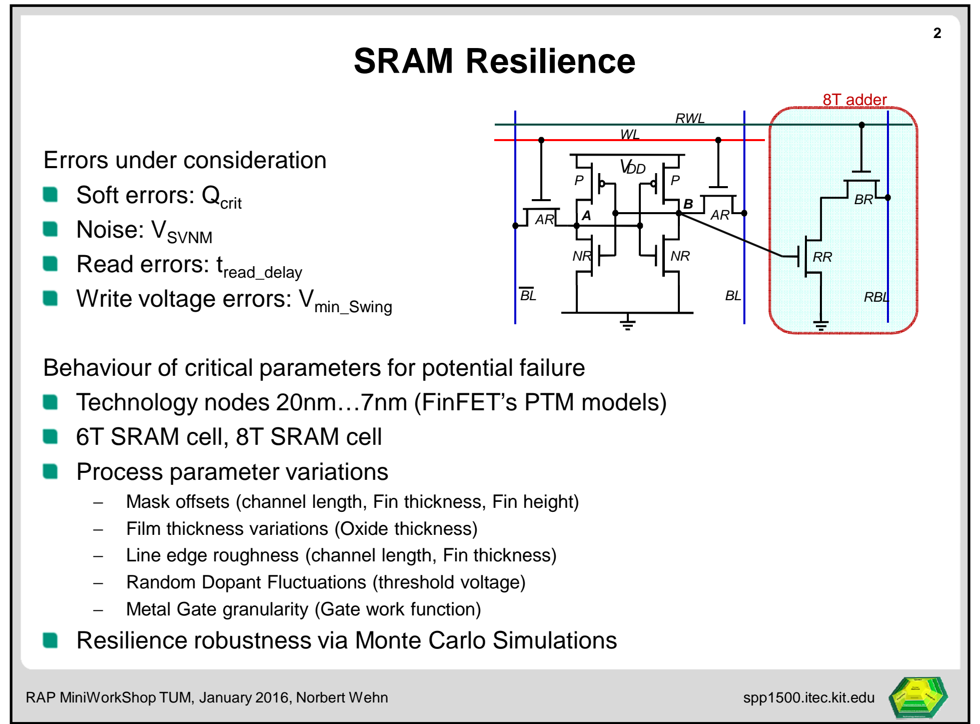
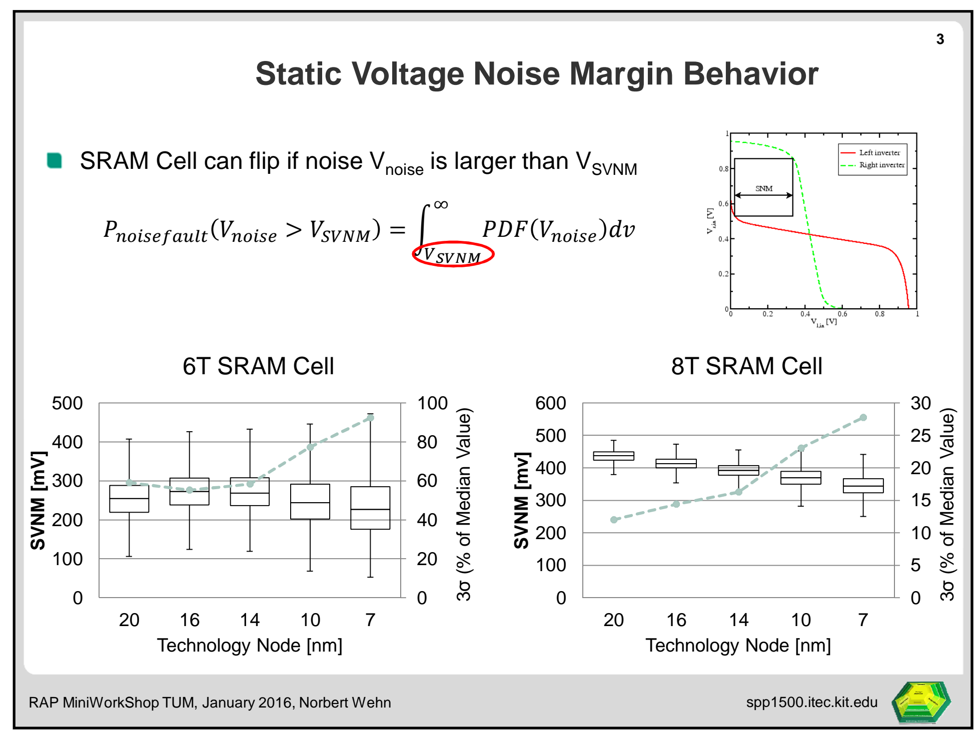
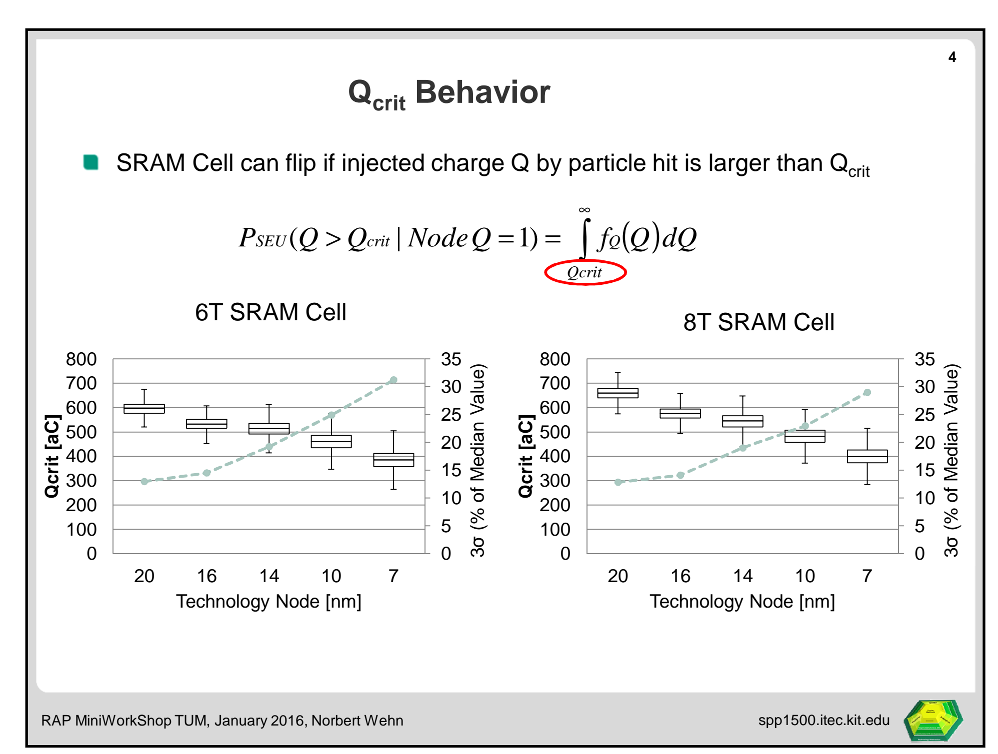
Technische Universität
Kaiserslautern

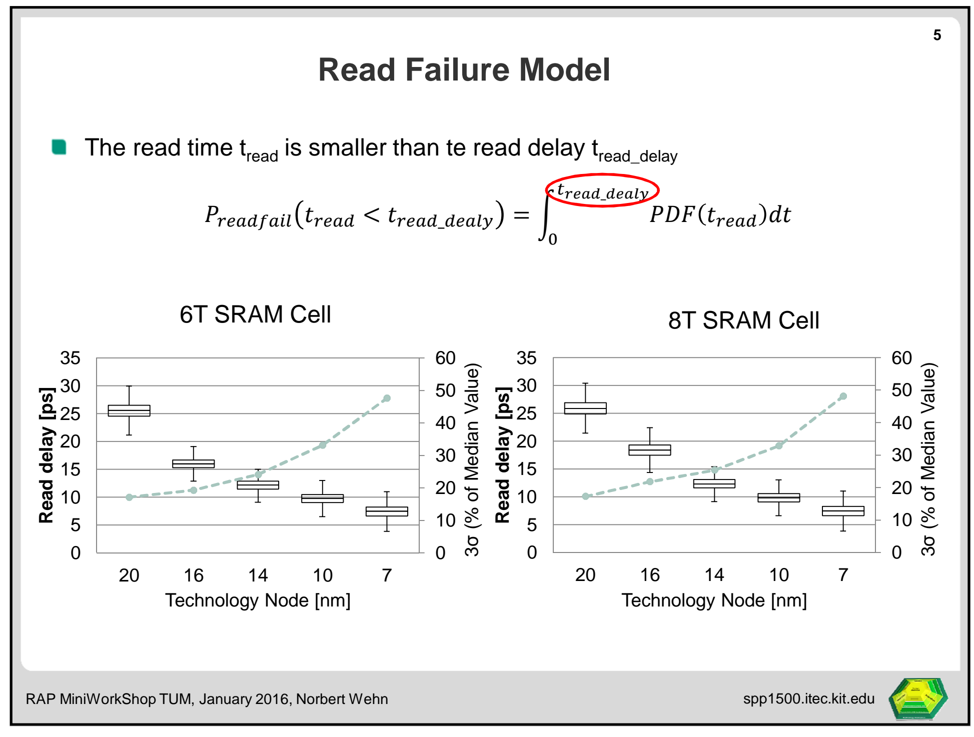

Technische Universität
Kaiserslautern
Error Modelling in
SRAMs and DRAMs
SPP1500.itec.kit.edu
Norbert Wehn, Christian Weis, Matthias Jung
Microelectronic System Design Research Group
University of Kaiserslautern
RAP MiniWorkShop TUM, January 2016, Norbert Wehn

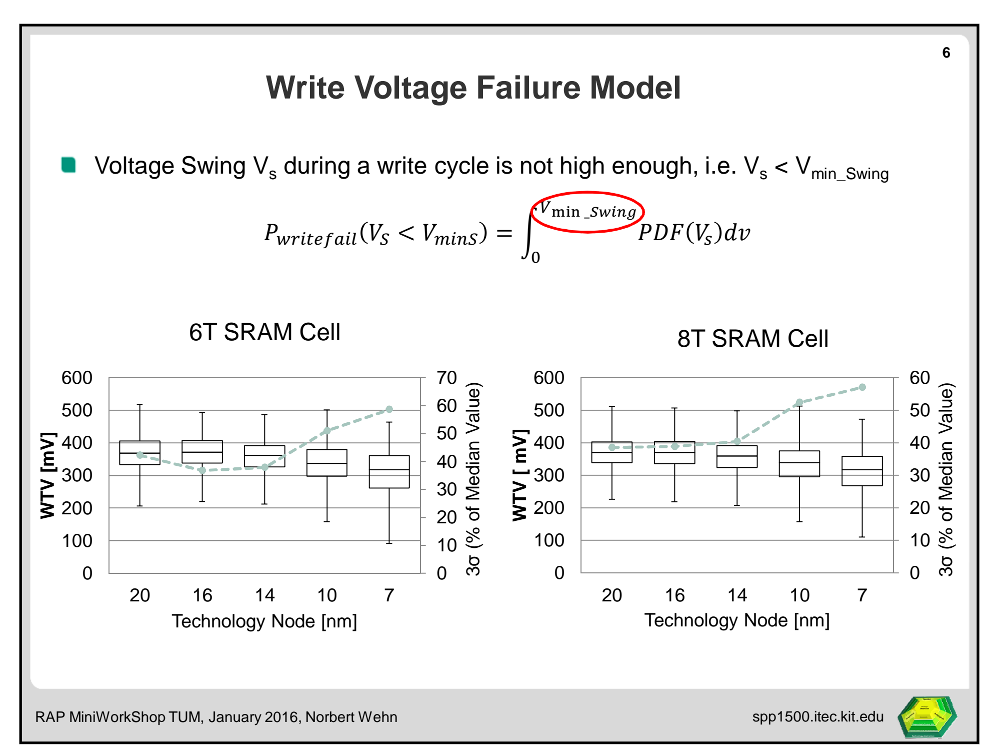

2
SRAM Resilience
Errors under consideration
Soft errors: Qcrit
Noise: VSVNM
Read errors: tread_delay
Write voltage errors: Vmin_Swing
8T adder
RWL
WL
VDD
P
P
AR
A
B
AR
NR
NR
BL
BL
BR
RR
RBL
Behaviour of critical parameters for potential failure
Technology nodes 20nm…7nm (FinFET's PTM models)
6T SRAM cell, 8T SRAM cell
Process parameter variations
– Mask offsets (channel length, Fin thickness, Fin height)
– Film thickness variations (Oxide thickness)
– Line edge roughness (channel length, Fin thickness)
– Random Dopant Fluctuations (threshold voltage)
– Metal Gate granularity (Gate work function)
Resilience robustness via Monte Carlo Simulations
RAP MiniWorkShop TUM, January 2016, Norbert Wehn
spp1500.itec.kit.edu

Technische Universität
Kaiserslautern

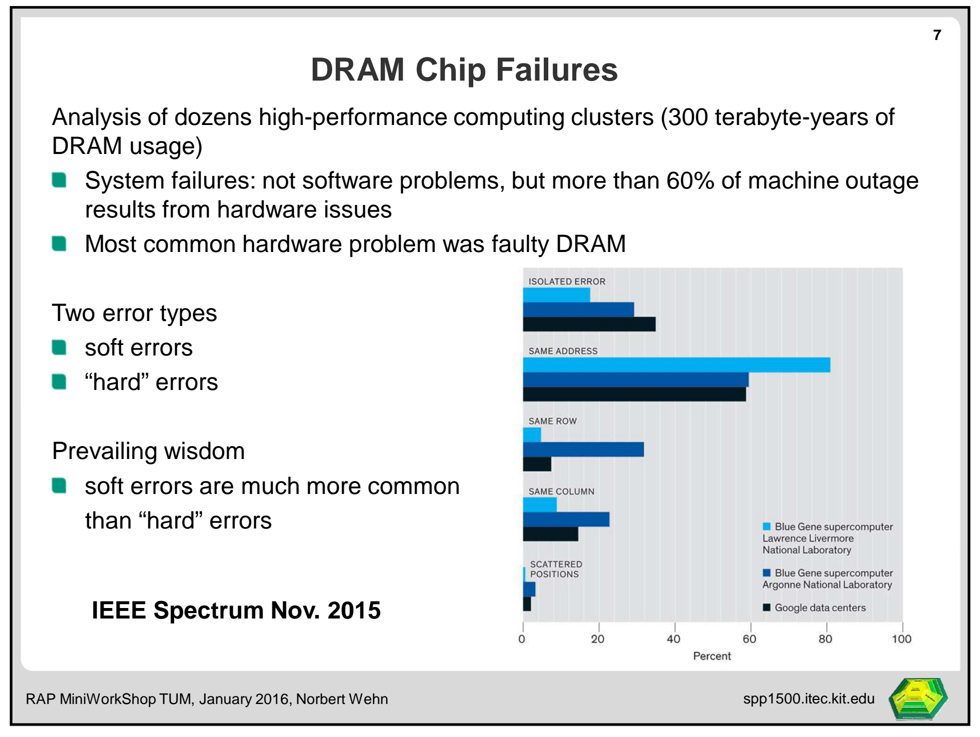

3
Static Voltage Noise Margin Behavior
SRAM Cell can flip if noise V_noise is larger than V_SVNM
$P_{noisefault}(V_{noise} > V_{SVNM}) = \int_{V_{SVNM}}^{\infty} PDF(V_{noise})dv$
Left inverter
Right inverter
SNM
6T SRAM Cell
8T SRAM Cell
SVNM [mV]
SVNM [mv]
3σ (% of Median Value)
Technology Node [nm]
RAP MiniWorkShop TUM, January 2016, Norbert Wehn
spp1500.itec.kit.edu

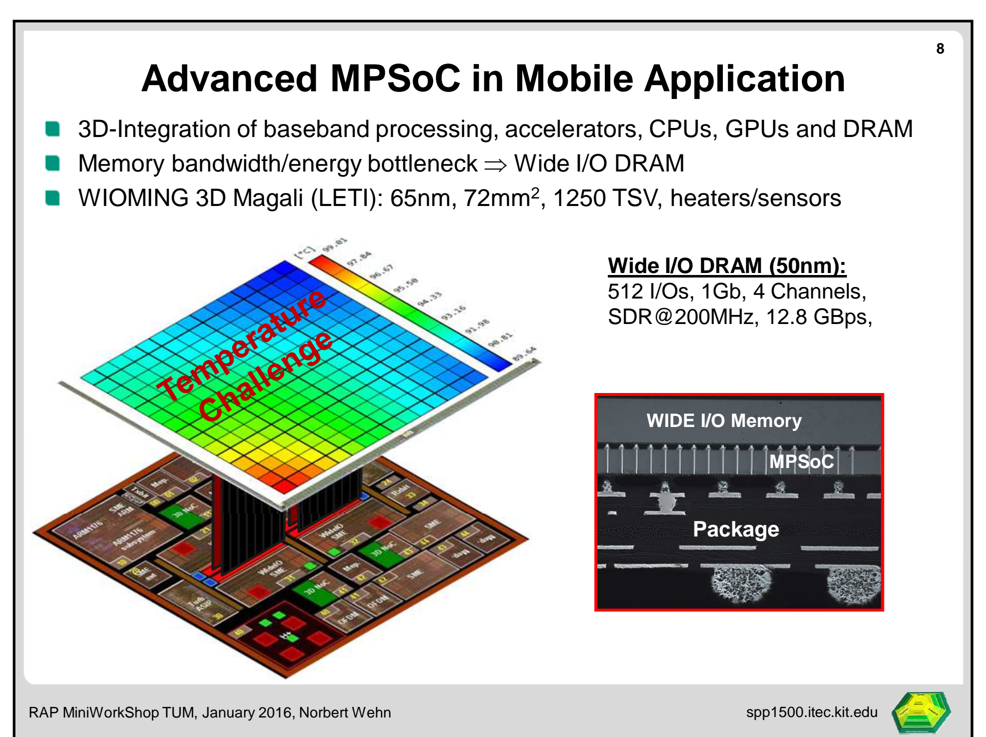

4
Q_crit Behavior
SRAM Cell can flip if injected charge Q by particle hit is larger than Q_crit
$P_{SEU}(Q > Q_{crit} \mid Node\,Q = 1) = \int_{Q_{crit}}^{\infty} f_Q(Q)dQ$
6T SRAM Cell
8T SRAM Cell
Qcrit [aC]
3σ (% of Median Value)
Technology Node [nm]
RAP MiniWorkShop TUM, January 2016, Norbert Wehn
spp1500.itec.kit.edu


5
Read Failure Model
The read time t_read is smaller than te read delay t_read_delay
$P_{readfail}(t_{read} < t_{read_dealy}) = \int_0^{t_{read_dealy}} PDF(t_{read})dt$
6T SRAM Cell
8T SRAM Cell
Read delay [ps]
3σ (% of Median Value)
Technology Node [nm]
RAP MiniWorkShop TUM, January 2016, Norbert Wehn
spp1500.itec.kit.edu

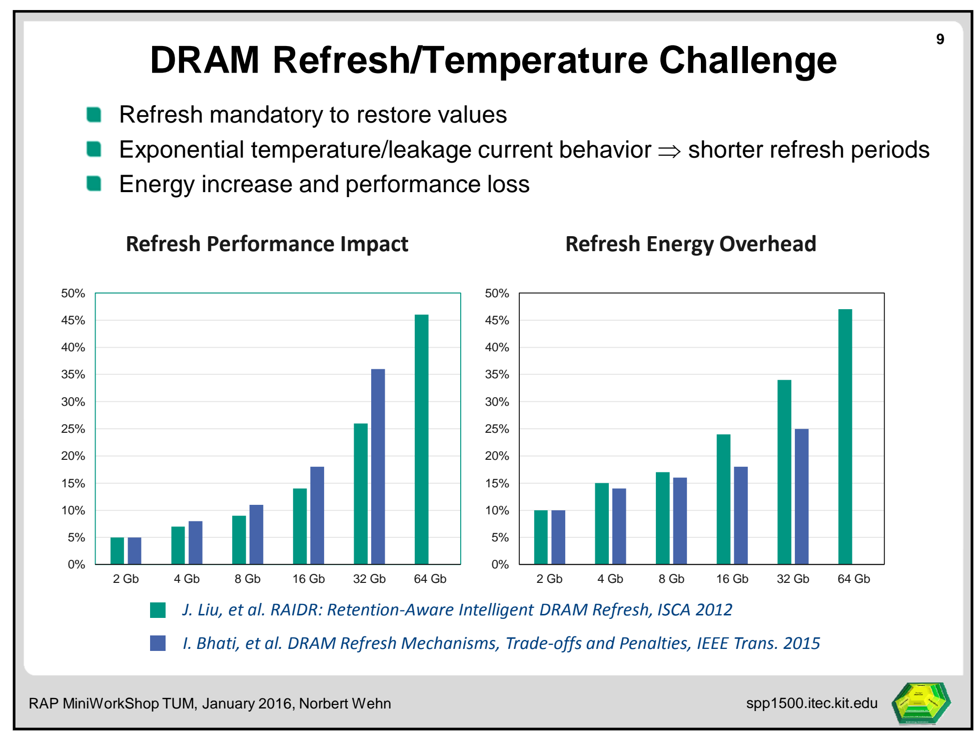

6
Write Voltage Failure Model
Voltage Swing V_s during a write cycle is not high enough, i.e. V_s < V_min_Swing
$P_{writefail}(V_S < V_{minS}) = \int_0^{V_{min_Swing}} PDF(V_s)dv$
6T SRAM Cell
8T SRAM Cell
WTV [mV]
WTV [mV]
3σ (% of Median Value)
Technology Node [nm]
RAP MiniWorkShop TUM, January 2016, Norbert Wehn
spp1500.itec.kit.edu

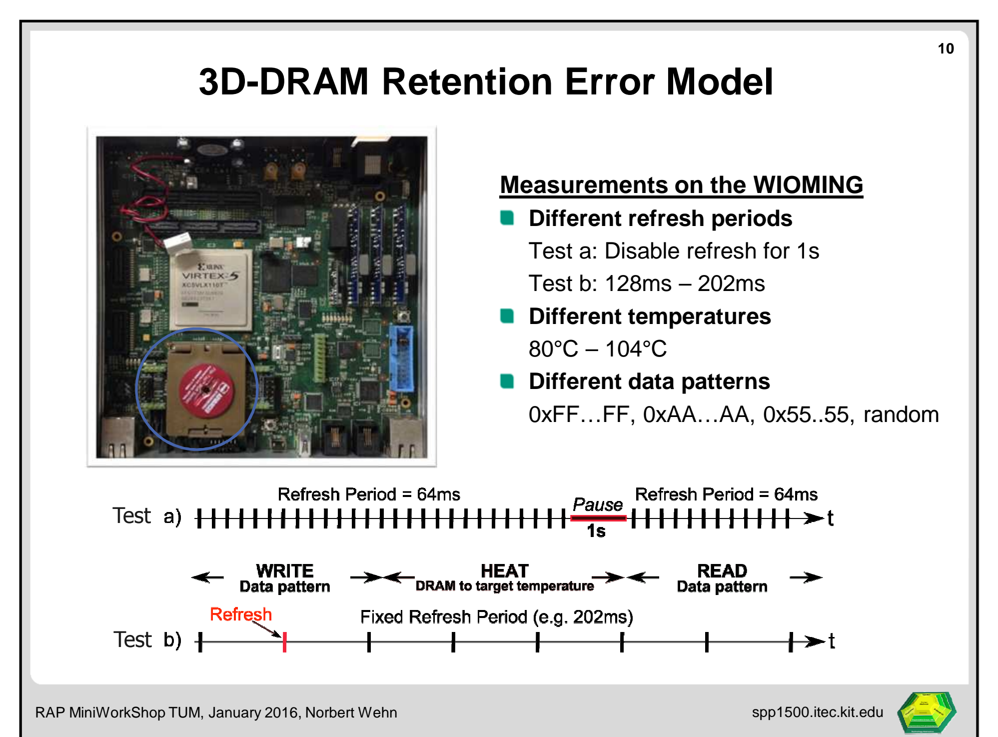
TECHNISCHE UNIVERSITÄT
KAISERSLAUTERN


7
DRAM Chip Failures
Analysis of dozens high-performance computing clusters (300 terabyte-years of DRAM usage)
System failures: not software problems, but more than 60% of machine outage results from hardware issues
Most common hardware problem was faulty DRAM
Two error types
soft errors
“hard” errors
Prevailing wisdom
soft errors are much more common than “hard” errors
IEEE Spectrum Nov. 2015
ISOLATED ERROR
SAME ADDRESS
SAME ROW
SAME COLUMN
SCATTERED POSITIONS
Blue Gene supercomputer Lawrence Livermore National Laboratory
Blue Gene supercomputer Argonne National Laboratory
Google data centers
0
20
40
60
80
100
Percent
RAP MiniWorkShop TUM, January 2016, Norbert Wehn
spp1500.itec.kit.edu

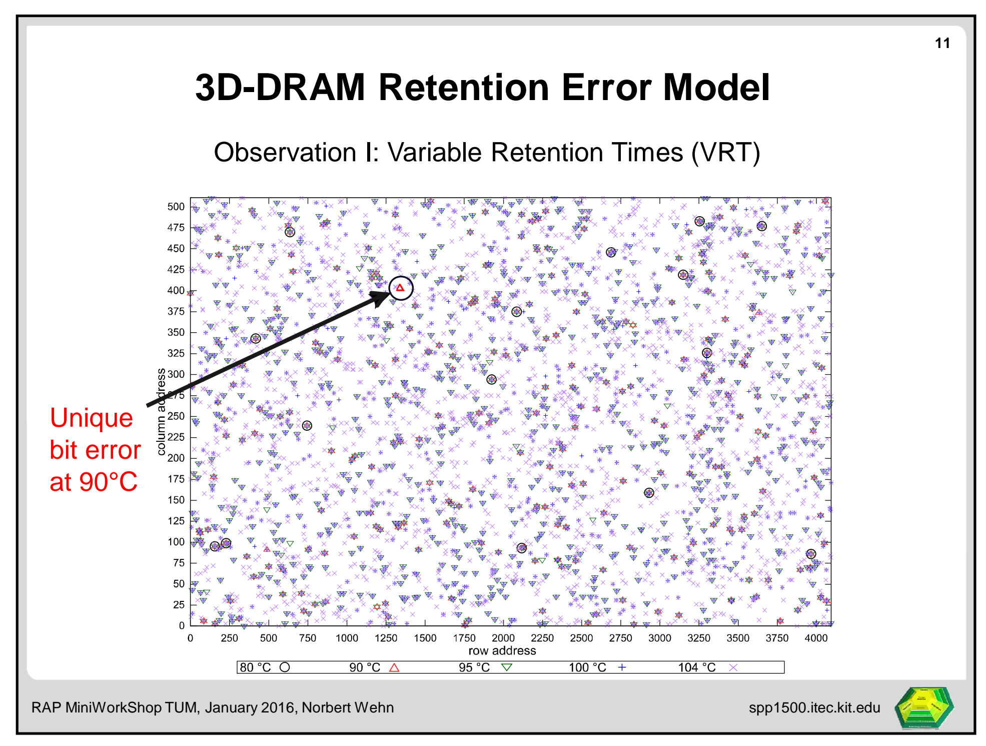

8
Advanced MPSoC in Mobile Application
3D-Integration of baseband processing, accelerators, CPUs, GPUs and DRAM
Memory bandwidth/energy bottleneck ⇒ Wide I/O DRAM
WIOMING 3D Magali (LETI): 65nm, 72mm², 1250 TSV, heaters/sensors
Temperature Challenge
Wide I/O DRAM (50nm):
512 I/Os, 1Gb, 4 Channels,
SDR@200MHz, 12.8 GBps,
WIDE I/O Memory
MPSoC
Package
RAP MiniWorkShop TUM, January 2016, Norbert Wehn
spp1500.itec.kit.edu

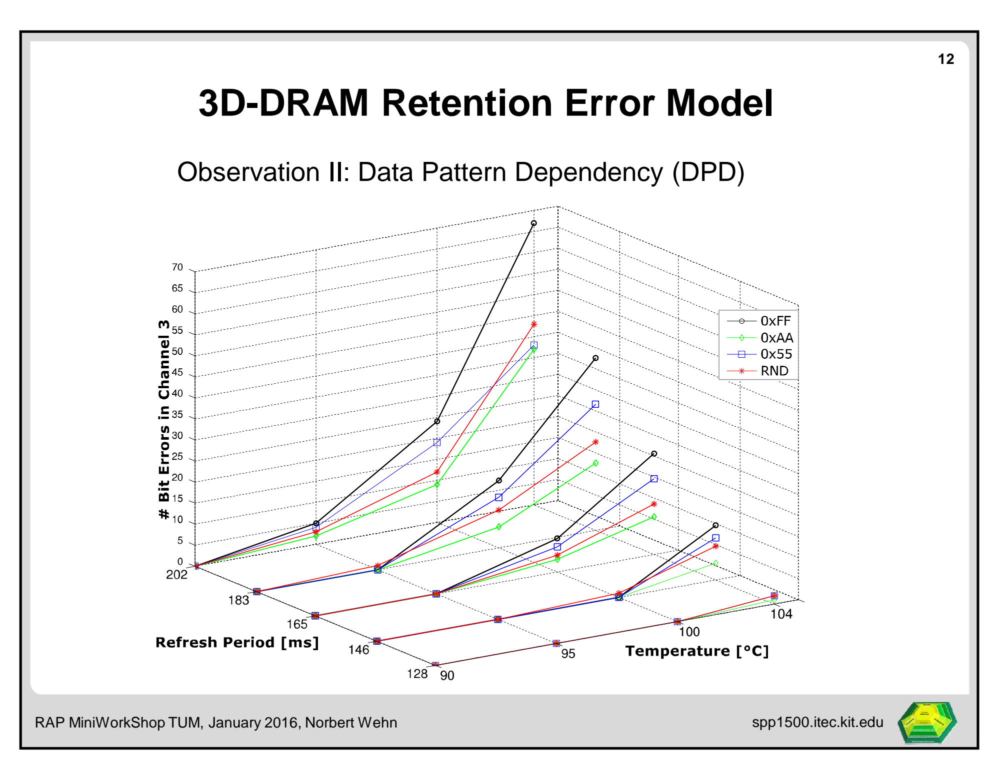
Technische Universität
Kaiserslautern

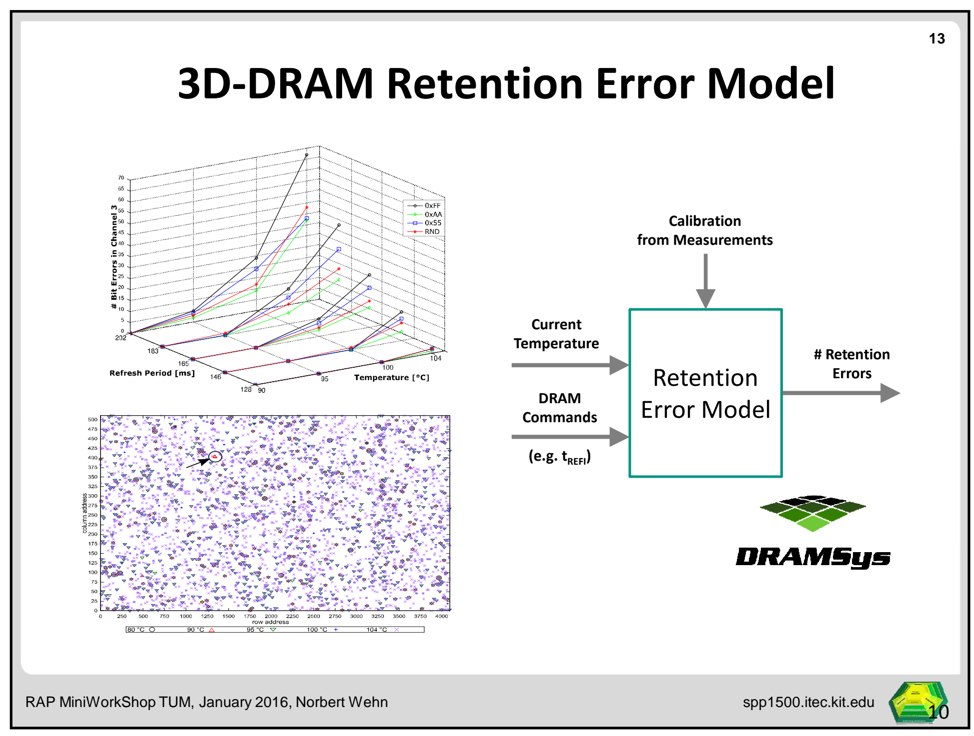

9
DRAM Refresh/Temperature Challenge
Refresh mandatory to restore values
Exponential temperature/leakage current behavior ⇒ shorter refresh periods
Energy increase and performance loss
Refresh Performance Impact
Refresh Energy Overhead
50%
45%
40%
35%
30%
25%
20%
15%
10%
5%
0%
2 Gb
4 Gb
8 Gb
16 Gb
32 Gb
64 Gb
J. Liu, et al. RAIDR: Retention-Aware Intelligent DRAM Refresh, ISCA 2012
I. Bhati, et al. DRAM Refresh Mechanisms, Trade-offs and Penalties, IEEE Trans. 2015
RAP MiniWorkShop TUM, January 2016, Norbert Wehn
spp1500.itec.kit.edu


10
3D-DRAM Retention Error Model
Measurements on the WIOMING
Different refresh periods
Test a: Disable refresh for 1s
Test b: 128ms – 202ms
Different temperatures
80°C – 104°C
Different data patterns
0xFF…FF, 0xAA…AA, 0x55..55, random
Refresh Period = 64ms
Pause
1s
Refresh Period = 64ms
Test a)
t
WRITE
Data pattern
HEAT
DRAM to target temperature
READ
Data pattern
Refresh
Fixed Refresh Period (e.g. 202ms)
Test b)
t
RAP MiniWorkShop TUM, January 2016, Norbert Wehn
spp1500.itec.kit.edu

TECHNISCHE UNIVERSITÄT
KAISERSLAUTERN


11
3D-DRAM Retention Error Model
Observation I: Variable Retention Times (VRT)
Unique bit error at 90°C
column address
row address
80 °C
90 °C
95 °C
100 °C
104 °C
RAP MiniWorkShop TUM, January 2016, Norbert Wehn
spp1500.itec.kit.edu


12
3D-DRAM Retention Error Model
Observation II: Data Pattern Dependency (DPD)
Bit Errors in Channel 3
Refresh Period [ms]
Temperature [°C]
0xFF
0xAA
0x55
RND
RAP MiniWorkShop TUM, January 2016, Norbert Wehn
spp1500.itec.kit.edu



3D-DRAM Retention Error Model

- Bit flips: only bit flips from 1 to 0 possible (No-Anticells)
- Modelling of Data Pattern Dependency (DPD)
- Modelling of Variable Retention Times (VRT)

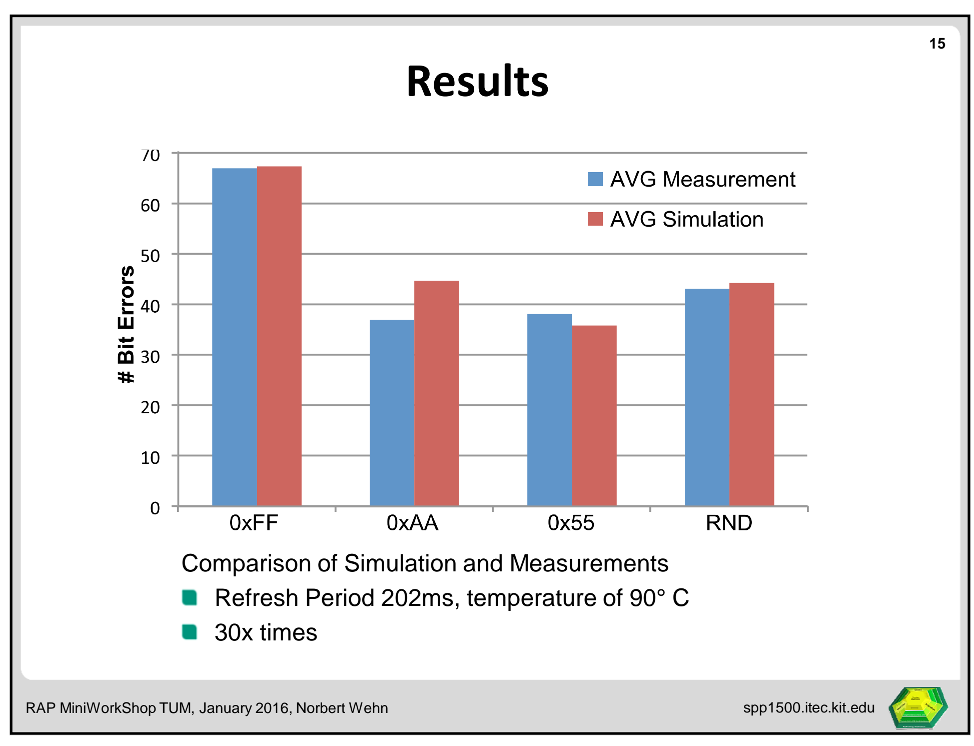
Assumptions for retention errors in a single DRAM bank

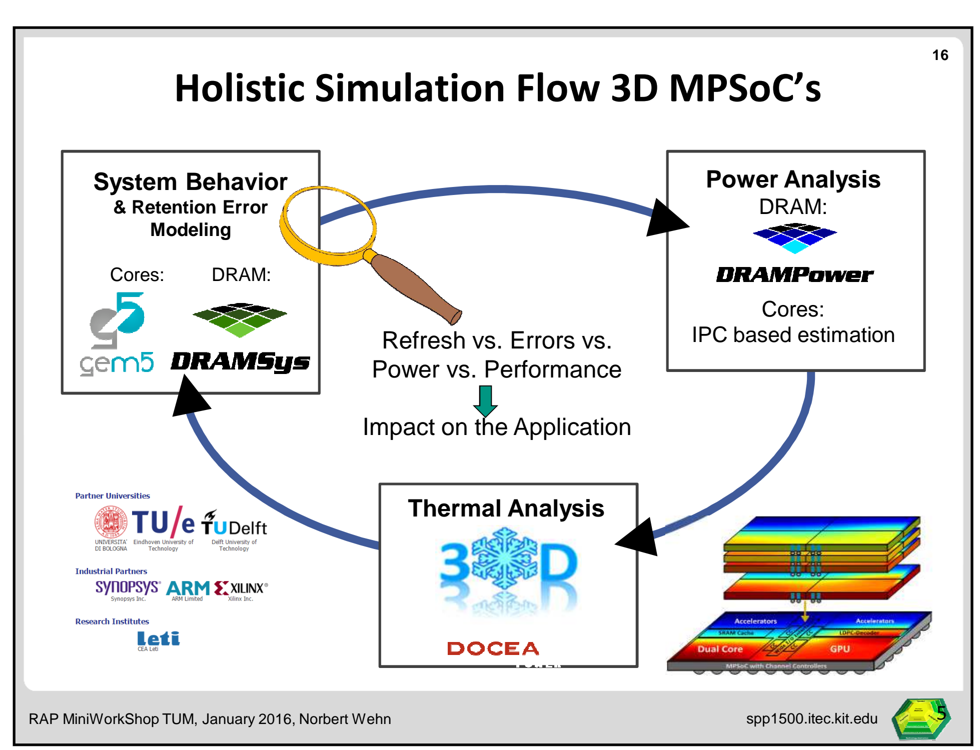
- Gaussian distributed (μ, σ) for each temperature value T and refresh time t_{REF}

Measurement Table			
Temp.	Time	μ	σ
90°C	202ms	5	0.2
...	...	..	...
100°C	202ms	25	3

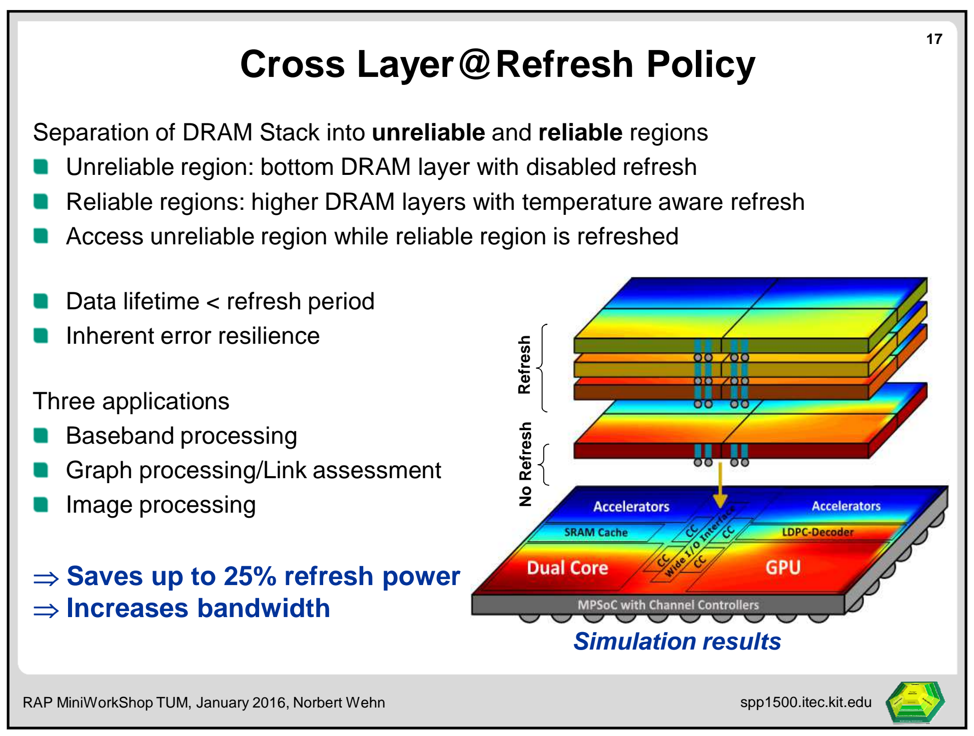
- Retention errors uniformly distributed in a DRAM bank
- DPD: x% (in our case ~10%) of errors assumed to be data dependent neighboring cells are considered ⇒ flip only if neighbor “1” ≤ 4

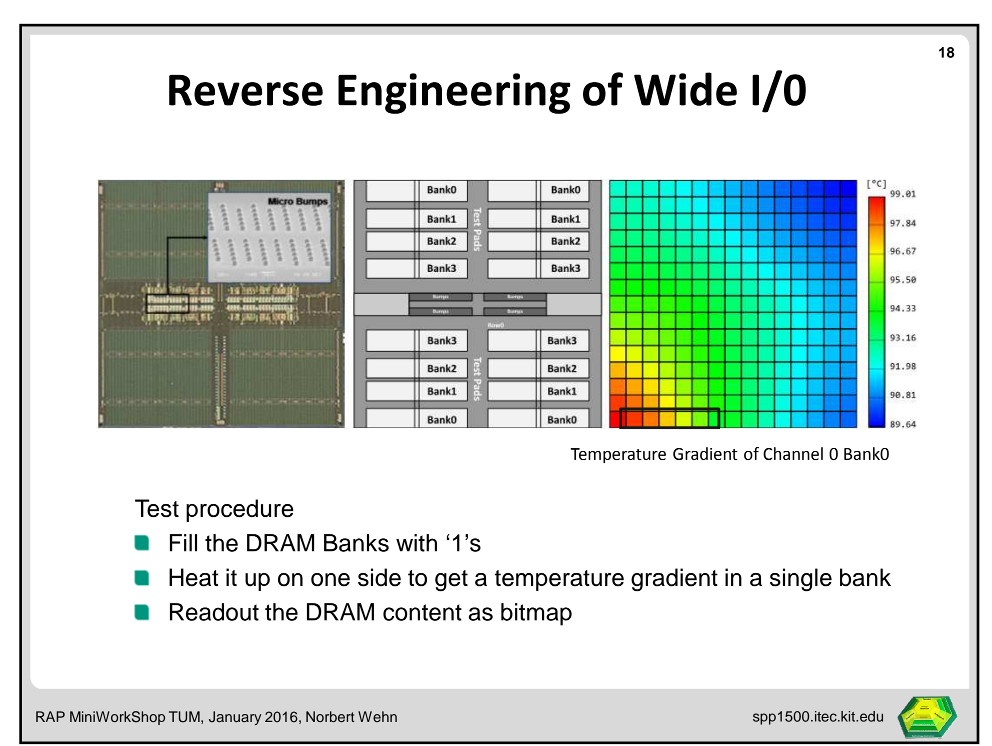
Technische Universität
Kaiserslautern


15
Results
70
60
50
40
30
20
10
0
Bit Errors
AVG Measurement
AVG Simulation
0xFF
0xAA
0x55
RND
Comparison of Simulation and Measurements
Refresh Period 202ms, temperature of 90° C
30x times
RAP MiniWorkShop TUM, January 2016, Norbert Wehn
spp1500.itec.kit.edu


16
Holistic Simulation Flow 3D MPSoC's
System Behavior
& Retention Error Modeling
Cores:
DRAM:
gem5
DRAMSys
Power Analysis
DRAM:
DRAMPower
Cores:
IPC based estimation
Refresh vs. Errors vs.
Power vs. Performance
Impact on the Application
Thermal Analysis
DOCEA
Partner Universities
TU/e
TUDelft
Industrial Partners
SYNOPSYS
ARM
XILINX
Research Institutes
leti
Accelerators
Dual Core
GPU
RAP MiniWorkShop TUM, January 2016, Norbert Wehn
spp1500.itec.kit.edu

Technische Universität
Kaiserslautern


17
Cross Layer@Refresh Policy
Separation of DRAM Stack into **unreliable** and **reliable** regions
Unreliable region: bottom DRAM layer with disabled refresh
Reliable regions: higher DRAM layers with temperature aware refresh
Access unreliable region while reliable region is refreshed
Data lifetime < refresh period
Inherent error resilience
Three applications
Baseband processing
Graph processing/Link assessment
Image processing
⇒ Saves up to 25% refresh power
⇒ Increases bandwidth
Refresh
No Refresh
Accelerators
SRAM Cache
LDPC-Decoder
Dual Core
GPU
Wide I/O Interface
CC
MPSoC with Channel Controllers
Simulation results
RAP MiniWorkShop TUM, January 2016, Norbert Wehn
spp1500.itec.kit.edu


18
Reverse Engineering of Wide I/0
Micro Bumps
Bank0
Bank1
Bank2
Bank3
Test Pads
[°C]
99.01
97.84
96.67
95.50
94.33
93.16
91.98
90.81
89.64
Temperature Gradient of Channel 0 Bank0
Test procedure
Fill the DRAM Banks with ‘1’s
Heat it up on one side to get a temperature gradient in a single bank
Readout the DRAM content as bitmap
RAP MiniWorkShop TUM, January 2016, Norbert Wehn
spp1500.itec.kit.edu

DRAM Reverse Engineering

- Precise heating capability
- Exploitation of retention errors

⇒ Reverse engineering of internal DRAM structures possible

Rowhammer attacks on DRAMs

- Continuously activate/precharge/activate/precharge on a specific row flips bits in neighbouring rows

Project Zero

News and updates from the Project Zero team at Google

Monday, March 9, 2015

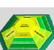
Exploiting the DRAM rowhammer bug to gain kernel privileges

Posted by Mark Seaborn, sandbox builder and breaker, with contributions by Thomas Dullien, reverse engineer

[This guest post continues Project Zero's practice of promoting excellence in security research on the Project Zero blog]

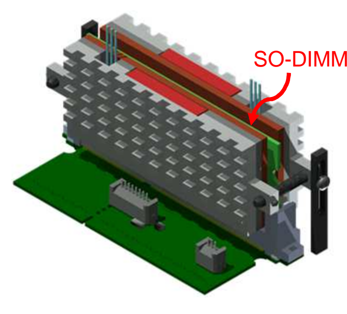
Overview

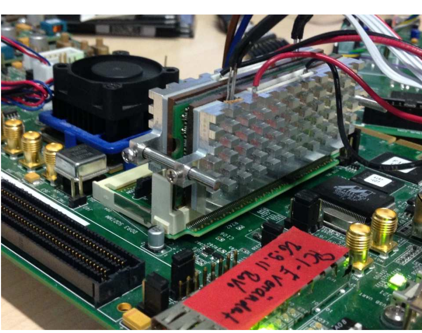
"Rowhammer" is a problem with some recent DRAM devices in which repeatedly accessing a row of memory can cause bit flips in adjacent rows. We tested a selection of laptops and found that a subset of them exhibited the problem. We built two working privilege escalation exploits that use this effect. One exploit uses rowhammer-induced bit flips to gain kernel privileges on x86-64 Linux when run as an unprivileged userland process. When run on a machine vulnerable to the rowhammer problem, the process was able to induce bit flips in page table entries (PTEs). It was able to use this to gain write access to its own page table, and hence gain read-write access to all of physical memory.

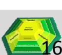


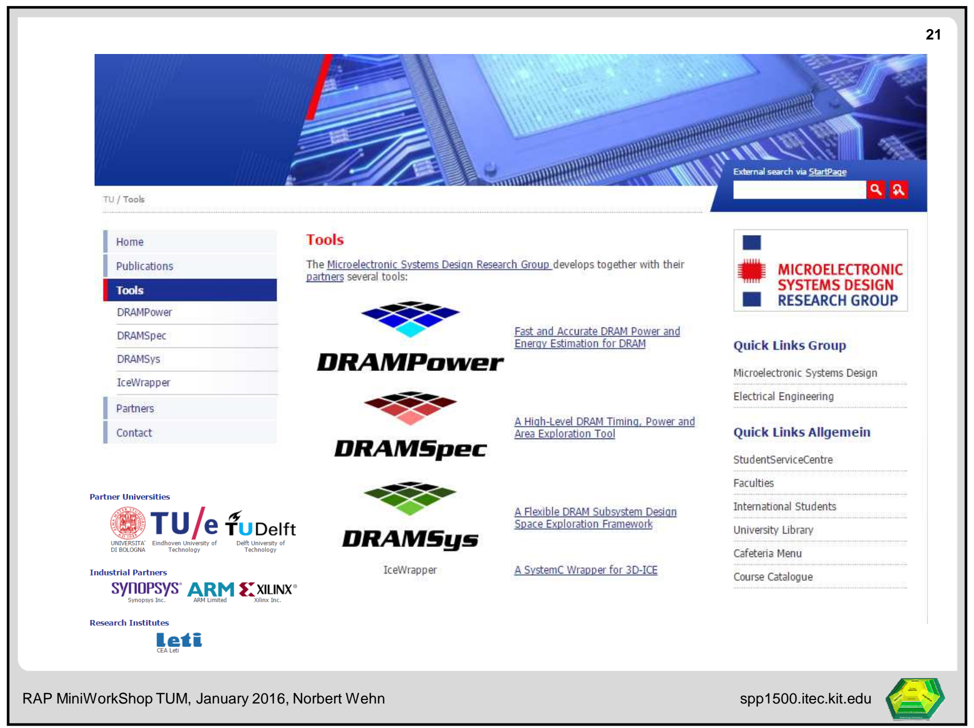
DRAMMeasure

- Precise control of temperature (heating and cooling) of DRAM SO-DIMMs
- Measuring currents / power of DRAM SO-DIMMs
- Can be applied to any DDR3/4 SO-DIMM based platform (FPGA, CPU …)
- Measuring retention errors









Literature

Circuit Resilience Roadmap
V. Kleeberger, C. Weis, U. Schlichtmann, N. Wehn *Chapter 7 in: Reis, Ricardo, Cao, Yu, Wirth, Gilson (Eds.): Circuit Design for Reliability, Springer*, January, 2015, p. 121-143

A Cross Layer Approach for Efficient Thermal Management in 3D Stacked SoCs
M. Jung, C. Weis, N. Wehn. *Accepted for publication, Journal of Microelectronics Reliability,* Elsevier 2016.

Efficient Reliability Management in SoCs - An Approximate DRAM Perspective
M. Jung, D. Mathew, C. Weis, N. Wehn. *Accepted for publication, 21st Asia and South Pacific Design Automation Conference (ASP-DAC)*, January, 2016, Macao, China.

Omitting Refresh - A Case Study for Commodity and Wide I/O DRAMs
M. Jung, Éder Zulian, M. Mathew, M. Herrmann, C. Brugger, C. Weis, N. Wehn. *1st International Symposium on Memory Systems* (MEMSYS 2015), October, 2015, Washington, DC, USA.

Retention Time Measurements and Modelling of Bit Error Rates of WIDE-I/O DRAM in MPSoCs
C. Weis, M. Jung, P. Ehses, C. Santos, P. Vivet, S. Goossens, M. Koedam, N. Wehn. *IEEE Conference Design, Automation and Test in Europe* (DATE), March, 2015, Grenoble, France.

DRAMSys: A flexible DRAM Subsystem Design Space Exploration Framework
M. Jung, C. Weis, N. Wehn. IPSJ Transactions on System LSI Design Methodology (T-SLDM), August, 2015.