DDR Memory Errors Caused by Row Hammer

Barbara P. Aichinger
Vice President New Business Development

FuturePlus Systems Corporation
15 Constitution Drive
Bedford NH 03110 USA

FuturePlus Systems

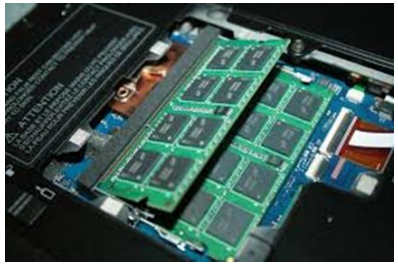
Power Tools for Bus Analysis

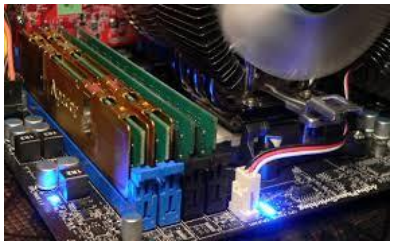
What is DDR3 Memory?

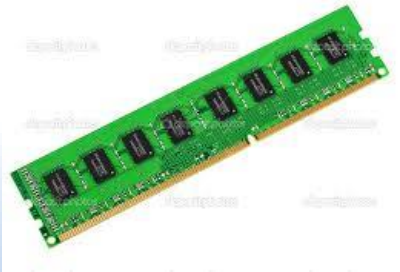
- The 3rd generation of the **D**ouble **D**ata **R**ate DRAM (Dynamic Random Access Memory)
- Most pervasive technology used in cloud computing and general computing design
- Billions of DDR3 DRAM parts have been shipped since ~ 2006.

FuturePlus Systems
Power Tools for Bus Analysis

Where is it used?



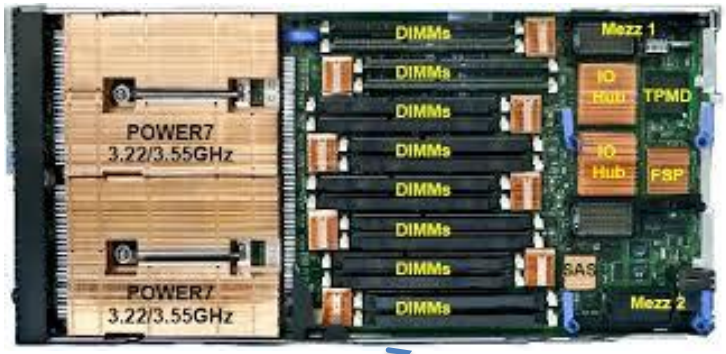




- Laptops
- Desktops
- Servers
- Embedded Applications
  - Defense
  - Medical
  - Automotive
  - Anywhere lots of memory is needed.

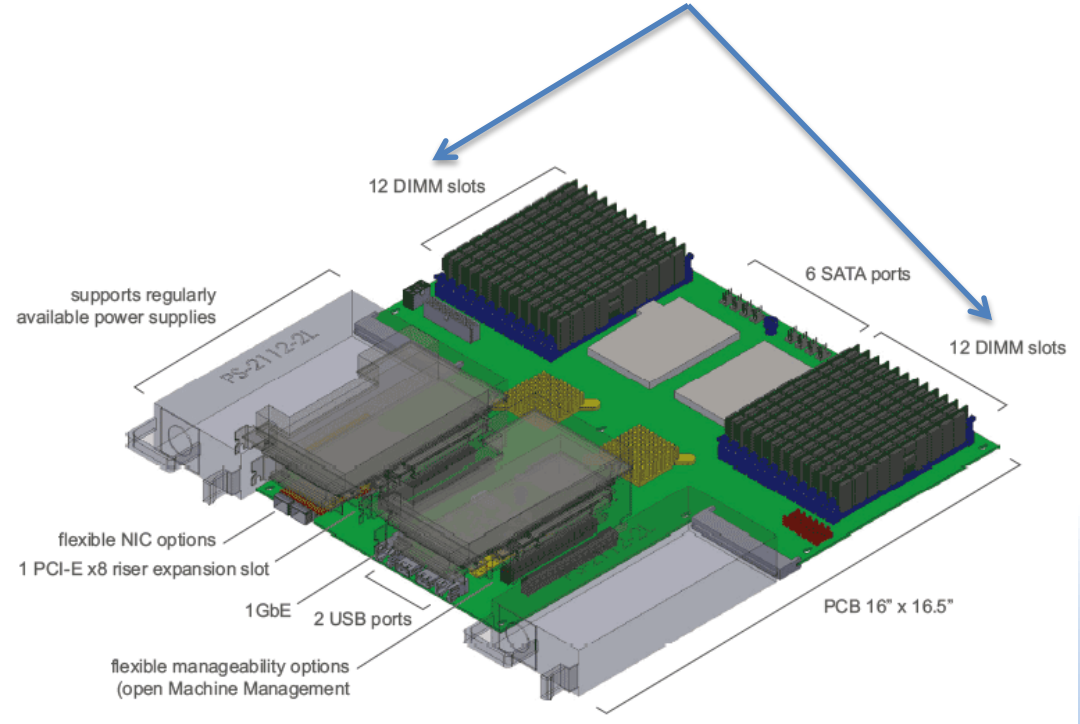
FuturePlus Systems
Power Tools for Bus Analysis

DDR3 is at the heart of Cloud Computing Servers



16 DIMMs

24 DIMMs



There are over 1 million servers on the planet. Each one have 16-24 DIMMs full of DDR3 memory.

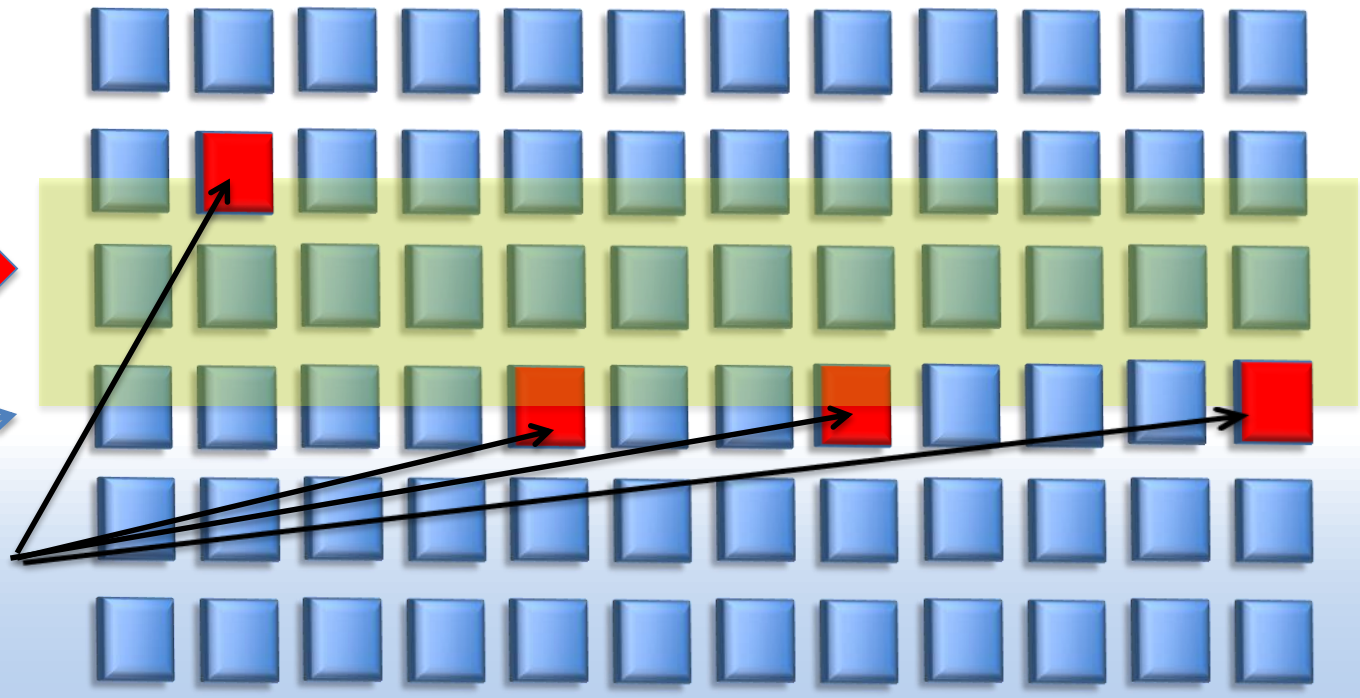
FuturePlus Systems
Power Tools for Bus Analysis

What is the problem?

- Charge leakage from one row into another

Excessive ACTIVATE commands apply repeated charge to the memory cells

Electromagnetic field induced by applied voltage



Cells lose charge by repeated nearby electromagnetic field, causing a coupled bit

Source: http://www.eurosoft-uk.com/eurosoft-test-bulletin-testing-row-hammer/

FuturePlus Systems
Power Tools for Bus Analysis

What research has been done?

- July 2014
  - Carnegie Mellon

Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors

Yoongu Kim[1] Ross Daly* Jeremie Kim[1] Chris Fallin* Ji Hye Lee[1]
Donghyuk Lee[1] Chris Wilkerson[2] Konrad Lai Onur Mutlu[1]
[1]Carnegie Mellon University [2]Intel Labs

- March 2015
  - Google

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

- July 2015
  - University of Technology
  - Austria and France

Rowhammer.js: A Remote Software-Induced Fault Attack in JavaScript

Daniel Gruss
Graz University of Technology, Austria
daniel.gruss@iaik.tugraz.at

Clémentine Maurice
Technicolor, Rennes, France
Eurecom, Sophia-Antipolis, France
clementine.maurice@technicolor.com

Stefan Mangard
Graz University of Technology, Austria
stefan.mangard@tugraz.at

0100110010101010000011011000111010 1
Power Tools for Bus Analysis
FuturePlus Systems

Additional Press

SOFTPEDIA® DESKTOP MOBILE WEB NEWS

Softpedia > News > Security FLASH SALE

Row Hammer DRAM Bug Now Exploitable via JavaScript, Most DDR3 Memory Chips Vulnerable

ManageEngine ServiceDesk Plus FREE IT Help Desk Software

Row Hammer bug that affects memory chips can now be exploited via JavaScri...

In March, security researchers have published a report detailing a problem with some memory chips which can be exploited to give attackers access to any computer using the latest DDR3 DRAM chips.

The DDR3 Row Hammer Bug

by EvilDead
6 months ago

5 comments

Home » Forums » Tech and Help

EvilDead
It's a trick. Get an axe.

Mass

Posted: 6 months ago

I recently acquired a new PC and while running memtest86 v.6 it would fail during the "Rowhammer" test. However it would pass memtest86+ and Windows memory diagnostics with flying colors but they haven't been updated in a while. From what I'm reading it is very unlikely to ever occur in normal computing because it requires hammering rows of memory repeatedly to flip an adjacent bit.

Because I don't like the sound of "Very unlikely" I put some very old DD3 memory in and it passed (2 x 2GB sticks). So, as a next step, I purchased another set of 16 GB G.Skill Ripjaws (Newegg customer award winner) only to find out they also fail the row hammer test. I'm now reading that this is widespread in DDR3 memory especially in higher capacity sticks due to how tightly everything needs to be packed. I have read numbers as high as 85% of the RAM out there purchased from 2010 through 2014 (And likely a lot of the chips that are currently being manufactured)

amazon
Amazon.com
Search Go

Errata Security

Advanced persistent cybersecurity

Monday, March 09, 2015

Some notes on DRAM (#rowhammer)

By Robert Graham

My twitter feed is full of comments about the "rowhammer" exploit. I thought I'd write some quick notes about DRAM. The TL;DR version is this: *you* probably don't need to worry about this, but *we* (the designers of security and of computer hardware/software) do.

There are several technologies for computer memory. The densest, and hence cheapest-per-bit, is "DRAM". It consists of a small **capacitor** for each bit of memory. The thing about capacitors is that they lose their charge over time and must be **refreshed**. In the case of DRAM, every bit of memory must be read them re-written every 64-milliseconds or it becomes corrupt.

These tiny capacitors are prone to corruption from other sources. One common source of corruption is **cosmic rays**. Another source is small amounts of **radioactive** elements in the materials used to construct memory chips. So, chips must be built with

SYNOPSYS® TOOLS | IP | PROTOTYPING | SERVICES | SOLUTIONS | SUPPORT | COMMUNITY | COMPANY

HOME ▸ COMMUNITY ▸ BLOGS & FORUMS ▸ COMMITTED TO MEMORY

Committed to Memory

« Zero to Green Light in minutes: Prototype your DDR Designs faster with new DDR IP Prototyping Kit | Home | LPDDR4 is here! Samsung Galaxy S6 and LG Gflex 2 released »

Search

Subscribe

Follow Synopsys

Categories

DDR Controller
DDR PHY
DDR3

Row Hammering: What it is, and how hackers could use it to gain access to your system

Posted by Marc Greenberg on March 9th, 2015

I have written on the topic of Row Hammering in a White Paper I published last year (link here) but since it is in the spotlight recently I thought I'd dedicate a blog entry to it. I had never considered this to be a security hole until this morning.

This morning Google Project Zero – the same team that discovered the Heartbleed bug – published this blog entry, "Exploiting the DRAM rowhammer bug to gain kernel privileges"
The blog entry is very detailed so here's a short summary:
- Some DDR devices have a property called "row hammer" that can cause some bits in DRAM to flip under certain conditions
- The conditions that cause row hammering are so rare in normal operation that nobody even knew it

ars technica

MAIN MENU | MY STORIES: 25 | FORUMS | SUBSCRIBE | JOBS | ARS CONSORTIU

RISK ASSESSMENT / SECURITY & HACKTIVISM

Cutting-edge hack gives super user status by exploiting DRAM weakness

"Rowhammer" attack goes where few exploits have gone before, into silicon itself.

by Dan Goodin - Mar 9, 2015 11:01pm EDT

Share Tweet 146

FuturePlus Systems
Power Tools for Bus Analysis

Row Hammer failures on DDR4?

Rowhammer mitigation

My i7-5820K/GA-X99-UD4/2400MHz Crucial Ballistix DDR4 system was failing rowhammer (a few hundred errors per pass) until I reduced the refresh interval timing from the default of 7.8ms, in spite of the fact that DDR4 is supposed to include rowhammer mitigation (source: https://en.wikipedia.org/wiki/Row_hammer#Mitigation)

In my board's BIOS, the two settings were tREFI (default of 9360) and tREFIX9 (default of 82).

refresh interval (ms) = tREFI / (RAM clock (MHz) / 2)

tREFIX9 = 8.9 * tREFI / 1024

so...

9360/(2400/2)=7.8ms

(Source: page 123 of http://www.intel.com/content/dam/www...-datasheet.pdf)

The standard recommendation is to reduce the refresh interval to 3.9ms and thereby double the refresh rate (source: http://support.lenovo.com/us/en/prod...ity/row_hammer). Doing that gave me one error per pass at the same address both times, so I reduced the interval to 75% of 3.9ms (i.e. tREFI=3510, tREFIX9=31) and it's now error free over 8 passes overnight.

Passmark Blog

FuturePlus Systems
Power Tools for Bus Analysis

How big of a problem is it?

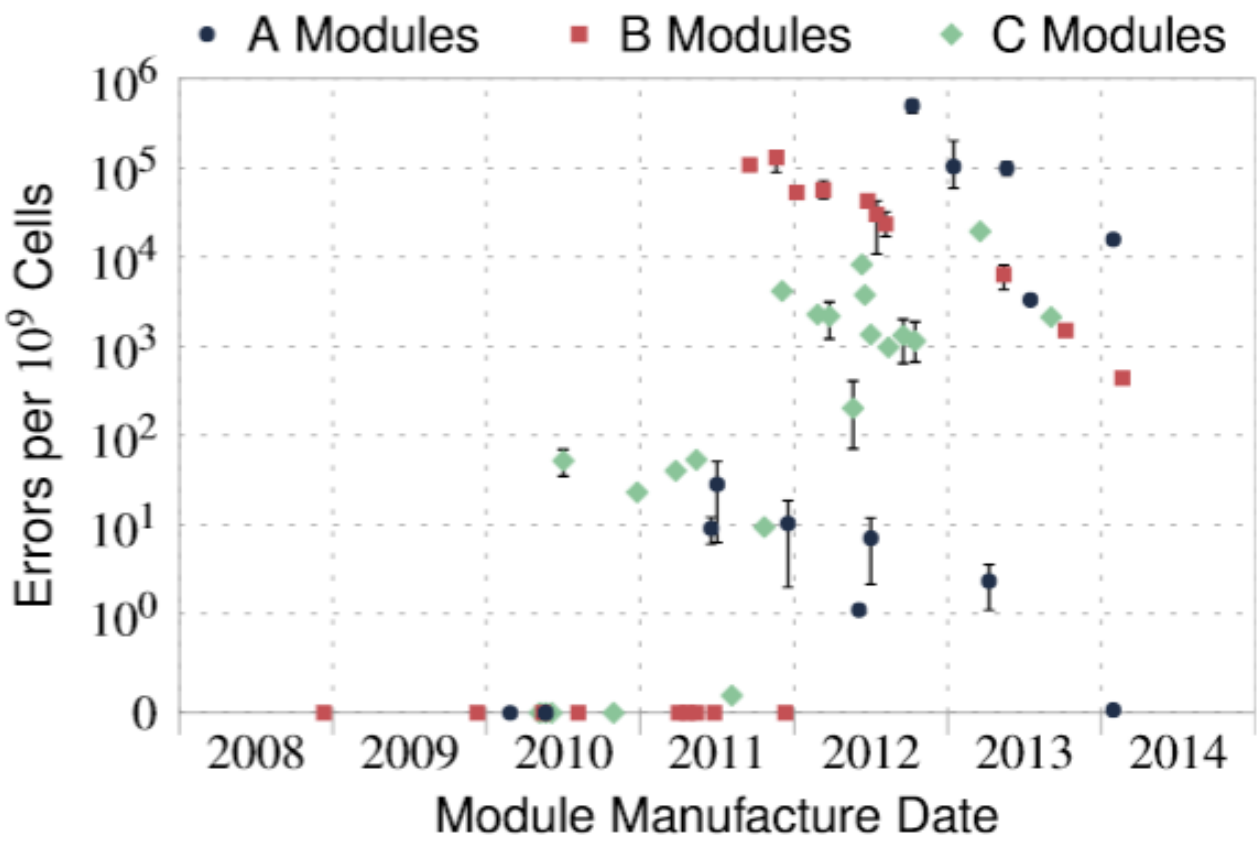


Figure 3. Normalized number of errors vs. manufacture date

Source: https://users.ece.cmu.edu/~omutlu/pub/dram-row-hammer_kim_talk_isca14.pdf

FuturePlus Systems
Power Tools for Bus Analysis

Results of the CMU Study

1. Most Modules Are at Risk

A company	B company	C company
86% (37/43)	83% (45/54)	88% (28/32)
Up to 1.0×10^{7} errors	Up to 2.7×10^{6} errors	Up to 3.3×10^{5} errors

Source: https://users.ece.cmu.edu/~omutlu/pub/dram-row-hammer_kim_talk_isca14.pdf

FuturePlus Systems
Power Tools for Bus Analysis

ECC helps but will not prevent undetected data corruption

- **E**rror **C**orrection **C**odes on DDR3 are Single Error Detection and Correction and Double Error Detection
- Research showed more than 2 bits on a single 64 bit access
  - However the rate of failures was much less
- Multibit errors will not be detected or erroneously flagged as SEDC

FuturePlus Systems
Power Tools for Bus Analysis

Mitigation Strategies

- Row Activate Counters: Counts Activates to ROWS and issues dummy ACT to neighboring rows
  - Requires significant changes the memory controller/DRAM
- Probabilistic Row Activation: Memory controller issues dummy ACT commands to neighboring rows
  - Requires changes to the memory controller and knowledge of the DRAM layout
- Double the Refresh Rate
  - Best Solution: Performance and power penalty
- Targeted Row Refresh
  - Requires special DRAM and changes to memory controller

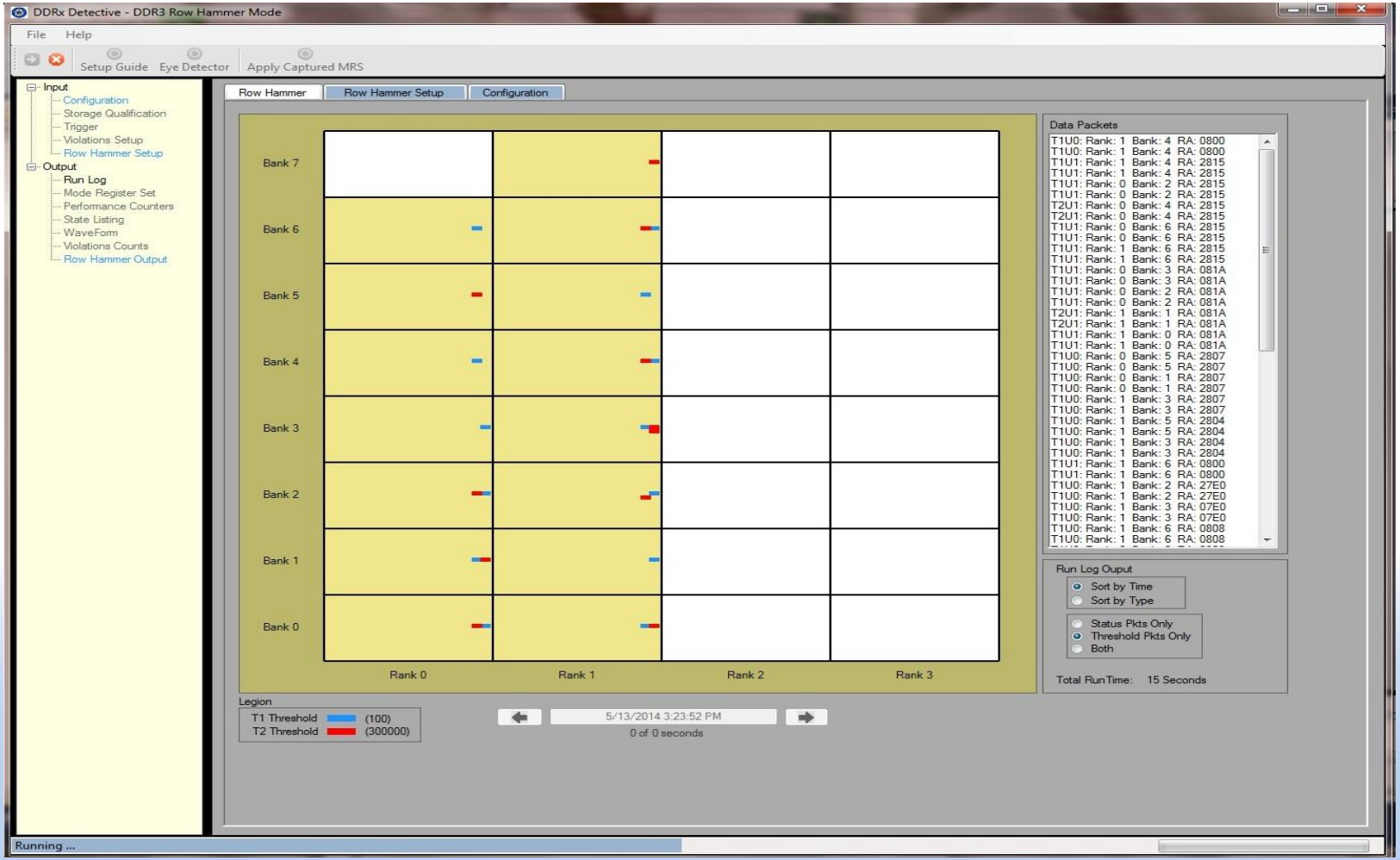
FuturePlus Systems
Power Tools for Bus Analysis

FuturePlus Systems Response

- Re-purposed our DDR Detective® Protocol Analyzer to count ACT commands to unique row addresses

FuturePlus Systems
Power Tools for Bus Analysis

Testing the system for excessive ACTIVATE commands



FuturePlus Systems
Power Tools for Bus Analysis

The industries response

- Blog Posts
  - Several that list failing parts
- Websites with Row Hammer mitigation
- Software to recreate the problem
  - Github https://github.com/google/rowhammer-test
- FuturePlus Systems working to form an industry group to produce quality information

FuturePlus Systems
Power Tools for Bus Analysis

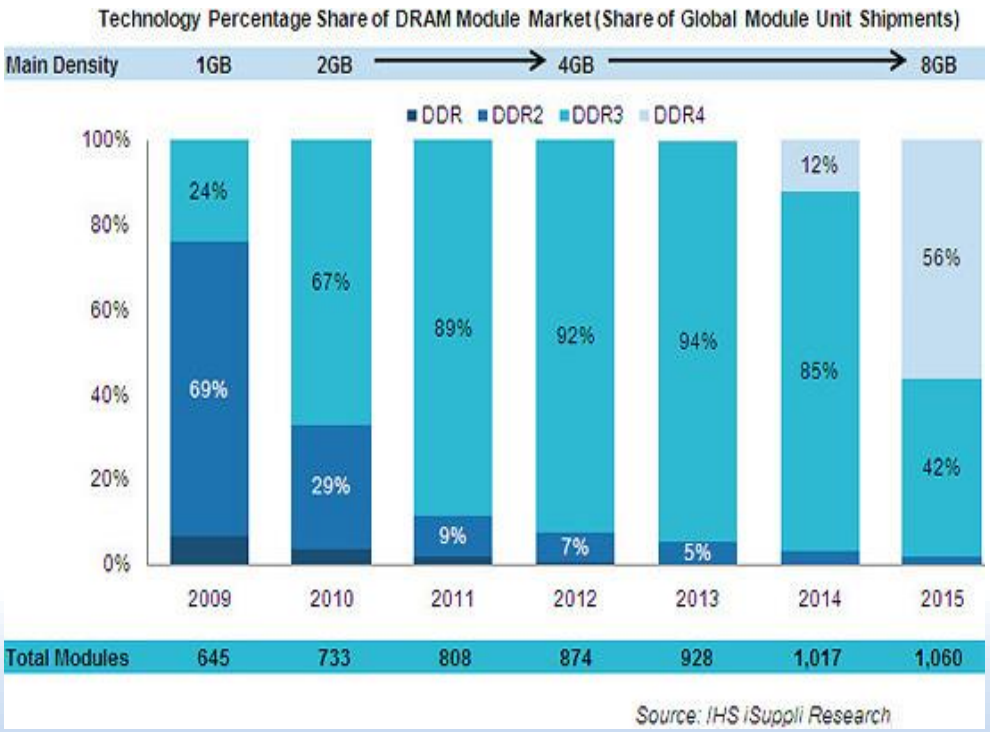
A call to action

- If you are using DDR memory in your designs be aware of this issue
- Promote standards that include compliance testing of DDR Memory
- If you are concerned about this problem contact me
  - Industry groups are forming

FuturePlus Systems
Power Tools for Bus Analysis

Summary

- DDR3 Memory is everywhere!
- Critical Applications need to be aware of this issue
  - Its both a reliability issue and a security issue
- ECC protected memory should be used but is not a fix for this problem



FuturePlus Systems
Power Tools for Bus Analysis

Contact Information

Barbara P. Aichinger

FuturePlus Systems

Barb.Aichinger@FuturePlus.com

603-472-5905

www.FuturePlus.com

www.DDRDetective.com