

JEDEC PUBLICATION

SYSTEM LEVEL ROWHAMMER MITIGATION

JEP301-1

MARCH 2021

JEDEC SOLID STATE TECHNOLOGY ASSOCIATION



SPECIAL DISCLAIMER: This document is provided for general information only, without any express or implied warranties of any kind, including that the information is suitable for any general or particular use. The information is not intended to be and does not constitute technical, security, product design or any other form of advice. The information is not specific to any product or application. Users, including their employers or principals (collectively, "Users") should not make any decision or take any action based on the information without first undertaking an independent due diligence review, conducting patent searches, and securing competent advice with respect to suitability for any given product or application. Users agree that they are making use of the information at their own risk, and assume all liability resulting from such use.

NOTICE

JEDEC standards and publications contain material that has been prepared, reviewed, and approved through the JEDEC Board of Directors level and subsequently reviewed and approved by the JEDEC legal counsel.

JEDEC standards and publications are designed to serve the public interest through eliminating misunderstandings between manufacturers and purchasers, facilitating interchangeability and improvement of products, and assisting the purchaser in selecting and obtaining with minimum delay the proper product for use by those other than JEDEC members, whether the standard is to be used either domestically or internationally.

JEDEC standards and publications are adopted without regard to whether or not their adoption may involve patents or articles, materials, or processes. By such action JEDEC does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the JEDEC standards or publications.

The information included in JEDEC standards and publications represents a sound approach to product specification and application, principally from the solid state device manufacturer viewpoint. Within the JEDEC organization there are procedures whereby a JEDEC standard or publication may be further processed and ultimately become an ANSI standard.

No claims to be in conformance with this standard may be made unless all requirements stated in the standard are met.

Inquiries, comments, and suggestions relative to the content of this JEDEC standard or publication should be addressed to JEDEC at the address below, or refer to www.jedec.org under Standards and Documents for alternative contact information.

Published by
©JEDEC Solid State Technology Association 2021
3103 North 10th Street
Suite 240 South
Arlington, VA 22201-2108

JEDEC retains the copyright on this material. By downloading this file the individual agrees not to charge for or resell the resulting material.

PRICE: Contact JEDEC

Printed in the U.S.A.
All rights reserved

PLEASE!

DON'T VIOLATE
THE
LAW!

This document is copyrighted by JEDEC and may not be
reproduced without permission.

For information, contact:

JEDEC Solid State Technology Association
3103 North 10th Street
Suite 240 South
Arlington, VA 22201-2107

or refer to www.jedec.org under Standards-Documents/Copyright Information.

sobco

SYSTEM LEVEL ROWHAMMER MITIGATION

(From JEDEC Board Ballot JCB-21-06, formulated under the cognizance of the JC-42 Committee on Solid State Memories. Item 1866.02.)

1 Scope

A DRAM rowhammer security exploit is a serious threat to cloud service providers, data centers, laptops, smart phones, self-driving cars and IoT devices. Hardware research and development will take time. DRAM components, DRAM DIMMs, System-on-chip (SoC), chipsets and system products have their own design cycle time and overall life time.

- 1) Rowhammer vulnerability is a fundamental DRAM issue.
- 2) RFM is designed to alleviate rowhammer concerns, but cannot eliminate vulnerability to all possible forms of attacks.
- 3) System companies need the maximum amount of flexibility in monitoring rowhammer and deploying the appropriate mitigation measures (HW & SW):
 - a) MAC (Maximum Active Count) and blast radius. Also known as DRAM victim row vulnerability to aggressor row activation count.
 - b) Comprehensive ECC, BIST, BISR statistics
 - c) The ability for the OS to report an aggressor to DRAM and ask DRAM to take mitigation actions
 - d) The ability for DRAM to ask for pause (no new commands can be issued by SoC) if needed. It can be non-deterministic (Ready or Wait)

This publication recommends the following best practices to mitigate the security risks from rowhammer attacks.

- 1) At the product level (e.g., cloud, smart phones), each company has its reliability (bit error rate) and security (privilege escalation or denial of service) requirements. The following guidelines are recommended:
 - a) Companies share rowhammer test patterns (e.g., Github[1]) and tools (e.g., Github[2]) with each other. Security is a shared industry concern, not an arena for competitive advantage.
 - b) Companies invest in memory validation and a quality assurance process. The bit error rate metrics should be quantified clearly for the suppliers (e.g., DRAM package and DIMMs).